Cours 48 : Security Fundamentals

Dans ce cours nous verrons les fondamentaux de la sécurité informatique.
Nous verrons tout d'abord les concepts clés de la sécurité puis des types d'attaques communes qui visent les entreprises, nous verrons ensuite le concept des mot de passes et de l'authentification multifacteur ou Multifacteur Authentication (MFA) ensuite nous verrons le concept de Authentification, Authorization, Accounting (AAA). Nous verrons également les éléments de programme de sécurité.

Répondons tout d'abord à la question : Quelle est le but de la sécurité dans une entreprise ?
Le principe de la triade CIA forme les fondations de la sécurité :
- Confidentiality (Confidentialité): seulement les utilisateurs autorisés peuvent avoir accès à la donnée, certaines informations sont publiques et peuvent être accédés par n'importe qui, certaines sont secrètes et doivent uniquement être accessible par des personnes spécifiques.
- Intégrity (Intégrité) : Les données ne peuvent pas être altérés (modifiés) par des utilisateurs non autorisés.
Les données doivent rester correct et authentique.
- Availability (Disponibilité) : Le réseau/système doit être opérationnel et accessible aux utilisateurs autorisés.

Les attaquants peuvent menacer la confidentialité, l'intégrité et la disponibilité des informations du système d'une entreprise.

Il y a aussi certains concept fondamentaux qu'il faut comprendre :
- Vulnérabilité : il s'agit d'une faiblesse potentiel qui peut compromettre le CIA d'un système/info
Une faiblesse potentiel n'est pas un problème en tant que tel, les fenêtres d'une maison sont par exemple des faiblesses potentiel et peuvent être utilisés et exploités des voleurs.
- Exploit : il s'agit d'une chose qui peut potentiellement être utilisé pour exploiter une vulnérabilité.
Une chose qui peut potentiellement être utilisé comme exploit n'est pas un problème en tant que tel.
Par exemple une pierre peut exploiter la faiblesse d'une fenêtre et peut être utilisé pour entrer dans une maison, mais les pierres ne sont pas des problèmes en soit.
- Threat (Menace) : est le potentiel pour être vulnérabilité d'être exploité, par exemple le voleur est la menace qui pourrait utiliser la pierre pour casser la fenêtre et entrer dans la maison.
Un Hacker qui exploite une vulnérabilité du système est un Threat ou menace.
- Mitigation technique : est quelque chose qui peut protèger des menaces
Peut être implémenté de partout où une vulnérabilité peut être exploité : les appareils clients, les serveurs, les Switchs, Les routeurs,, Murs de feu, etc...
Un système n'est jamais parfaitement protégé, il existe toujours des menaces.

Voyons quelques menaces qui peuvent potentiellement exploiter des vulnérabilités pour compromettre la confidentialité, l'intégrité ou la disponibilité, CIA du système d'information d'une entreprise :
- Attaques DoS (Denial of Service)
- Attaques par Spoofing
- Attaque par Reflection/Amplification
- Attaque de Man in the middle
- Attaque de Reconnaissance
- Malware
- Attaque par Social Engineering
- Attaque de Mot de passe

Il existe bien plus d'attaques potentiels que celles ci mais les principales sont celles ci, voyons plus en détail chacune d'elles :

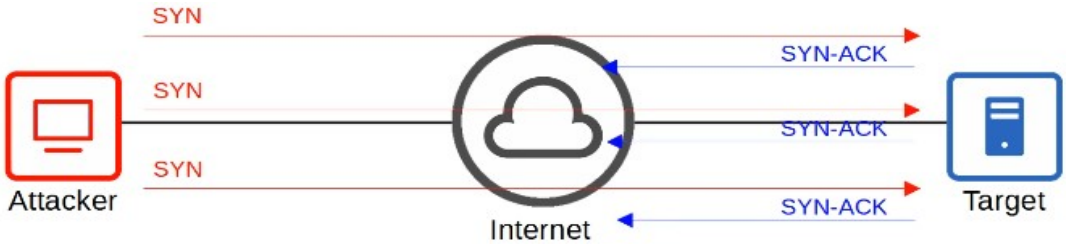
- Denial of Service (DoS) :

les attaque DoS menacent la disponibilité d'un système. Une attaque commune DoS est l'inondation TCP SYN flood qui exeploite le three way handshake : SYN | SYN-ACK | ACK

Dans une inondation SYN, l'attaquant envoie un certains nombre de messages TCP SYN vers la cibles. La cible envoie des messages SYN-ACK en réponse pour chacun des SYN qu'il reçoit. L'attaquant ne répond jamais avec le Ack final du TCP three way handshake.

La connexion incomplète remplie la table de connexion TCP de la cible, celle ci sera alors en timout et sera supprimé de la table après une certaine période de temps, mais l'attaquant continuera d'envoyer des messages SYN pour remplir la table. La cible ne sera plus capable de rendre la connexion TCP légitime.

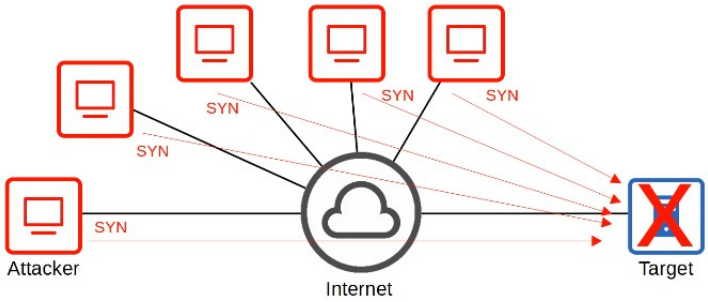
Le schéma suivant résume la situation :



Ce type d'attaque n'est généralement pas réalisé par un seule attaquant, un type d'attaque beaucoup plus puissant est l'attaque DDoS.

Dans une attaque DDoS (Distributed Denial Of Service) l'attaquant infecte plusieurs ordinateurs cibles avec des malware et les utilise pour initier des attaques par déni de service par exemple des attaques TCP SYN flood. Ce groupe d'ordinateurs infecté est appelé botnet.

Le schéma suivant résume la situation :



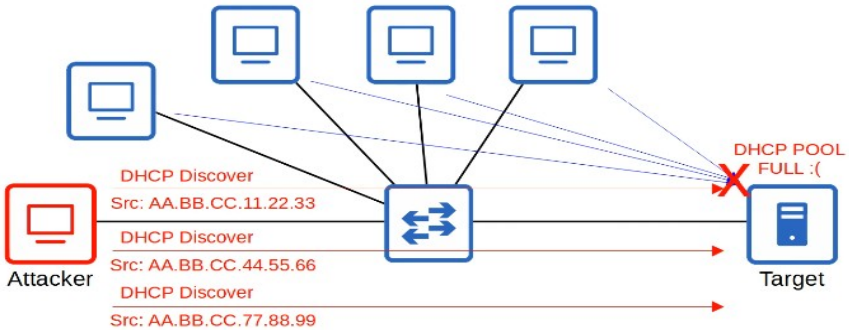
- Attaque Spoofing :

Le spoof d'une adresse est pour utilser une fausse adresse source (IP ou Adresse MAC)

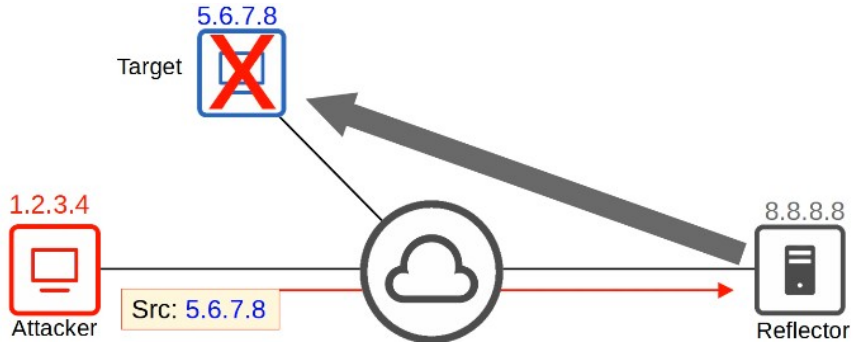
De nombreuses attaques implique le spoofing ça n'est pas un seul type d'attaque.

L'exemple d'un attaque Spoofing est le DHCP exhaustion. Un attaquant utilise l'usurpation d'adresse MAC pour inonder des messages DHCP Discover, le serveur cible qui est le POOL DHCP devient complet ce qui résulte en un DoS mais vers d'autres appareils.

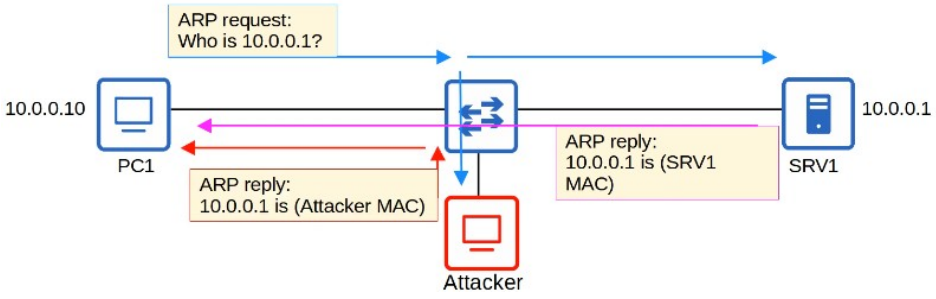
Ce schéma résume la situation :



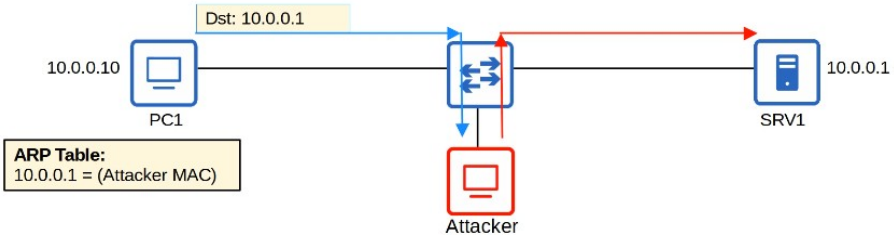
- Attaque Reflection/Amplification :
Dans une attaque par réflexion, l'attaquant envoie le trafique vers un réflecteur, et usurpe l'adresse source du paquet en utilisant l'adresse IP d'une cible.
Le réflecteur (Par exemple le serveur DNS) envoie la réponse à l'adresse IP cible.
Si le montant du trafique envoyé à la cible est suffisamment large, cela peut résulter en une attaque DoS. Il existe une forme d'attaque plus puissante appelé attaque par amplification.
Une attaque par réflexion devient une attaque par amplification lorsque le montant du trafique envoyé par l'attaquant est petit mais qu'il déclenche en un large montant de trafique pour être envoyé depuis le réflecteur vers la cible.
Le schéma suivant résume la situation :



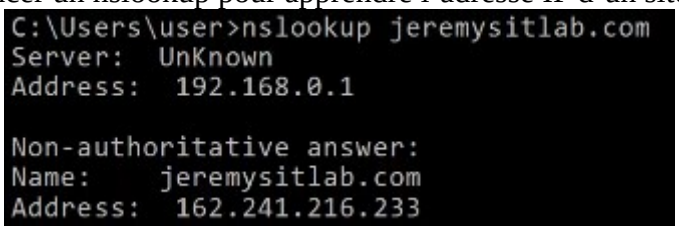
- Attaque Man in the Middle :
Dans une attaque Man in the Middle, l'attaquant se place entre la source et la destination pour espionner les communication, ou pour modifier le trafique avant qu'il n'atteigne la destination.
Un exemple commun est le ARP spoofing aussi connu comme ARP poisoning.
L'hôte envoie une requête ARP, pour demander une adresse MAC d'un autre appareil.
La cible de la requête envoie la réponse ARP pour informer la requête de sa propre adresse MAC.
L'attaquant attend et envoie une autre réponse ARP pour répondre après la réponse légitime.
Si l'attaquant la réponse ARP de l'attaquant arrive en dernier, il écrira par dessus l'entrée ARP dans la table ARP du PC1.
Le schéma suivant résume la situation :



Dans la table ARP du PC1 l'entrée pour 10.0.0.1 aura l'adresse MAC de l'attaquant.
Lorsque le PC1 essayera d'envoyer le trafique vers le SRV1, il le transmettre à l'attaquant, l'attaquant pourra inspecter les messages et les repartager au SRV1. L'attaquant peut aussi modifier les messages avant de les retransmettre au SRV1.
Cela compromet la confidentialité et l'intégrité des communication entre PC1 et SRV1



- Attaque par reconnaissance :
Les attaques par reconnaissance ne sont pas des attaques en elles même mais elles sont utilisé pour récupérer des informations à propose de la cible et peuvent être utilisé pour de future attaques.
C'est souvent des information publiquement disponibles.
Par exemple on peut lancer un nslookup pour apprendre l'adresse IP d'un site web :

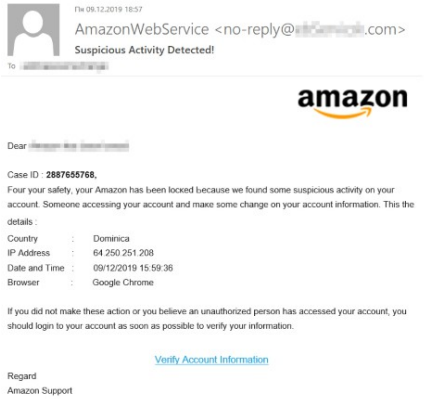


A partir de là il est possible de rechercher des ports ouverts qui peuvent être des vulnérabilités potentiels. Une requête whois permet d'apprendre l'adresse mail, le téléphone, l'adresse physique, etc...

- Malware : (Logiciel malicieux) se réfère à une variété de programmes qui peuvent infecter un ordinateur. Les virus infectent d'autre logiciel (ou programme). Le virus se propage puisque le logiciel est partagé par les utilisateurs. Cela corrompe ou modifie les fichier de l'ordinateur cible.
Les worms ne requière pas de programme hôte, ce sont des malware qui sont « standalone » et qui sont capables de se propager par eux même sans l'interaction d'un utilisateur. La propagation peut congestionner le réseau, mais le payload d'un vers peut causer des préjudices supplémentaires aux appareils de la cible.
Les cheval de Troie sont des logiciels nuisible qui se distinguent des logiciels légitime. Ils se propagent par l'interaction de l'utilisateur comme avec l'ouverture d'une pièce jointe, ou un téléchargement depuis Internet.
Les types de Malwares précédents peuvent exploiter des vulnérabilités variés pour menacer n'importe quelle CIA de l'appareil cible.

- Attaque par Social Engineering :
Les attaques par Social Engineering ciblent la partie la plus vulnérable d'un système qui est : les utilisateurs. Ils impliquent la manipulation psychologique pour faire que la cible révèle des informations confidentiel ou fasse certaines actions.
Phishing implique des mails frauduleux qui apparaissent comme étant d'un business légitime (Amazon, Banque, Compagnie de carte de crédit, etc...) et contient des liens vers des sites frauduleux qui semblent légitime. Les utilisateurs doivent se connecter au site frauduleux et donnent leurs identifiants à l'attaquant.
Spear phishing est une forme de phishing plus ciblé par exemple qui cible les employés de certaines compagnies.
Le Whaling est un phishing qui cible des individu avec un haut statut. Par exemple le président d'une compagnie.
Le Vishing (Voice Phishing) est un phishing qui se passe à travers le téléphone. Par exemple un individu vous appelle et se dis être l'ingénieur informatique de l'entreprise dans laquelle vous travaillez et vous demande de réinitialiser votre mot de passe.
Le Smishing (SMS phishing) est un phishing qui utilise les messages texte SMS.
Les attaques watering hole compromettent les sites que la victime visite fréquemment. Si un lien malicieux est placé sur un site web, la victime lui fais confiance et n'hésite pas à cliquer dessus.
Les attaques Tailgating impliquent une entrée restreint, une zone sécurisé en simplement marchant par derrière une personne autorisé lorsqu'elle entre.
Souvent la cible laisse la porte ouverte à l'attaquant pour rester polis et assume que l'attaquant est aussi une personne autorisé à entrer.

Voici un exemple de mail frauduleux qui permettent à l'attaquant de récupérer les identifiants d'un utilisateur :



Pie 09.12.2019 18:57

AmazonWebService <no-reply@[redacted].com>

Suspicious Activity Detected!

To [redacted]

amazon

Dear [redacted]

Case ID : **2887655768,**

Four your safety, your Amazon has been locked because we found some suspicious activity on your account. Someone accessing your account and make some change on your account information. This the details :

Country	:	Dominica
IP Address	:	64.250.251.208
Date and Time	:	09/12/2019 15:59:36
Browser	:	Google Chrome

If you did not make these action or you believe an unauthorized person has accessed your account, you should login to your account as soon as possible to verify your information.

Verify Account Information

Regard
Amazon Support

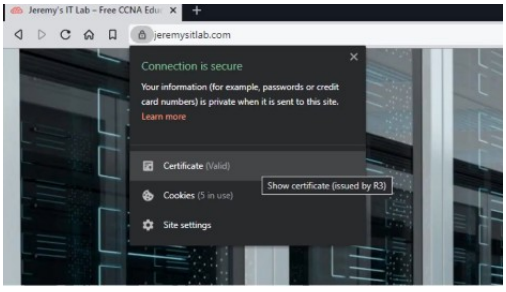
- Attaque de Mot de passe :

La plupart des systèmes utilisent un identifiant et mot de passe pour authentifier un utilisateur.
Le nom d'utilisateur est souvent simple et facile à deviner (par exemple le nom d'utilisateur d'une adresse mail) et la résistance et le secret d'un mot de passe est utilisé pour fournir assez de sécurité.
Les attaquants peuvent apprendre le mot de passe utilisateur par plusieurs méthodes :
En le devinant, avec une attaque par dictionnaire qui est un programme qui lance un dictionnaire ou liste des mot pour trouver le mot de passe de la cible.
L'attaque par Brute force est un programme qui essaye toutes les possibilité de combinaison de lettre, de nombres et de caractère spéciaux pour trouver le mot de passe de la cible.
Un mot de passe puissant doit contenir : au moins 8 caractères (De préférence plus) un mélange de lettres majuscules et minuscules, au moins un caractère spécial.
Il doit être changé régulièrement.

Voyons le concept de l'authentification multi-facteur, ou Multifactor Authentication (MFA) en Anglais. Le MFA implique plus que juste un nom d'utilisateur/mot de passe pour prouver son identité. Cela implique de fournir 2 des choses suivantes :
- Une chose que l'on sais : par exemple un nom utilisateur, un mot de passe, un PIN, etc...
- Une chose que l'on possède : par exemple en confirmant une notification qui apparaît sur téléphone, un badge devant être scanné, etc...
- Une chose que l'on est : un accès biométrique comme le scan du visage, le scan de la main, le scan de l'empreinte digitale, le scan de la rétine, etc...

Lorsque l'authentification multi-facteur est requise pour connexion la sécurité est grandement amélioré. Même si l'attaquant apprend le mot de passe (une chose que l'on sais) il ne pourra pas se connecter au compte.

Une autre forme d'authentification implique des certificats digitales qui sont utilisés pour prouver l'identité du porteur du certificat.
Ils sont utilisés pour les sites web pour vérifier que le site web est légitime. Les entités qui veulent un certificat pour prouver leurs identité envoient un CSR (Certificate Signing Request) au CA (Certificate Authority) qui va regénérer et signer le certificat.
On peut voir le certificat avec le symbole du cadenas qui indique que le site est sécurisé et légitime.



Le AAA (triple A) est l’acronyme de Authentication, Autorization et Accounting
C’est un cadre pour contrôler et gérer les utilisateurs de l’ordinateur du système (par exemple un réseau)
- Authentication (Authentification) est la procédure de v »rifier l’identité de l’utilisateur par le moyen de l’enregistrement.
- Authorization est la procédure qui accorde les permissions d’accès à un utilisateur.
Il accord l’accès utilisateur à certains fichiers/services, la restriction d’accès pour entrer dans un fichier/services est l’autorisation
- Accounting est la procédure d’enregistrement de l’activité de l’utilisateur dans le système.
Par exemple lorqu’un utilisateur fais le changement d’un fichier

Les entreprises utilisent des serveurs AAA pour fournir des services AAA
ISE (Identity Services Engine) est un serveur Cisco AAA
Les serveurs AAA supportent les protocoles AAA suivants :
- RADIUS : un protocole standard ouvert. Il utilise les ports UDP 1812 et 1813
- TACACS+ : un protocole Cisco propriétaire. Utilise le port TCP 49

Les éléments de sécurité d’un programme consistent à sensibiliser les employés à propos des des menaces de sécurité potentiel et des risques.
Par exemple une compagnie envoie de faux emails de phishing pour que les employés cliquent et un lien pour qu’ils signent avec leur identifiants.
Bien que les mails ne sont pas nuisibles les employés qui tombent dans le piège du faux mail seront informés par un programme qui leur avertit qu’ils doivent faire plus attention aus mails de phishing.

Les programmes d’entraînement des utilisateurs sont plus formateurs que les programmes de sensibilisation. Par exemple, un entraînement dédié qui éduque l’utilisateur sur la politique de sécurité et comment créer un mot de passe solide, er comment éviter les menaces potentiels.

Les contrôle d’accès physique protègent les équipement et les données d’attaques potentiels en autorisant seulement des utilisateurs permis dans une zone protégé comme un réseau privée ou le un data center.
Les verrous multi-facteurs peuvent protéger l’accès à des zones restreintes, par exemple une porte qui requière un badge et un contrôle de l’empreinte digitale pour entrer.
Les permissions d’un badge peuvent facilement être changés par exemple les permissions peuvent être supprimés lorsque l’employé quitte la compagnie.