easy Former
La formation à 360°

Support de cours

Initiation au Hacking

Auteur : Yann BENHAMRON
Version : 1.0
Date de création : 10/12/2022
Date de dernière modification : 17/12/2022

PROGRAMME DU COURS

I. Introduction au hacking et sécurité

II. Présentation des différent type vulnérabilité

III. TP sur les attaques les plus utilisées, mais aussi les plus efficaces et critique dans les infrastructure réseau :

- ✓ Sniffing réseau
- ✓ Spoofing réseau
- ✓ Man in the middle
- ✓ Déni de service
- ✓ Scanning
- ✓ Social Engineering

Sommaire

1.Introduction à la sécurité informatique

Objectif : Saisir les enjeux de la sécurité

Exigences fondamentales

- La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

- Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité :

1. **disponibilité :** demande que l'information sur le système soit *disponible* aux personnes autorisées.
2. **Confidentialité :** demande que l'information sur le système ne puisse être *lue* que par les personnes autorisées.
3. **Intégrité :** demande que l'information sur le système ne puisse être *modifiée* que par les personnes autorisées.

➢Du point de vue de la sécurité informatique, une menace est une violation potentielle de la sécurité.

➢Cette menace peut-être

1. Accidentelle
2. Intentionnelle (attaque)
   - **Active** : menace pour l'intégrité et la disponibilité des données
   - **Passive** : menace pour la confidentialité des données.

Étude des risques

- Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi.

- Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés.

- La sécurité certes ne fais pas gagner de l'agent, mais évite de faire perdre de l'argent à une Entreprise.

- Voici quelques éléments pouvant servir de base à une étude de risque:
  - Quelle est la valeur des équipements, des logiciels et surtout des informations ?
  - Quel est le coût et le délai de remplacement ?
  - Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs. De la société
  - Quel serait l'impact concernant des intrusions sur les ordinateurs de la société ?

Établissement d'une politique de sécurité

- Suite à l'étude des risques et avant de mettre en place des mécanismes de protection, il faut préparer une politique à l'égard de la sécurité.

- C'est elle qui fixe les principaux paramètres, notamment les niveaux de tolérance et les coûts acceptable.

- Voici quelques éléments pouvant aider à définir une politique :
  - Les coûts des incidents informatiques passés
  - Le degré de confiance envers les utilisateurs interne
  - Informations importantes sur des ordinateurs en réseaux accessible ou non de l'externe
  - La configuration du réseau et des services accessibles ou non de l'extérieur

Principaux défauts de sécurité

- Il ne faut pas perdre de vue que la sécurité est comme une chaîne, si l'un des maillons se brise la chaîne entière sera brisé.

- Les défauts de sécurité d'un système d'information les plus souvent constatés sont :
  - Défaut de configuration
  - Mises à jours non effectuées.
  - Mots de passe inexistants ou par défaut.
  - Procédures de sécurité obsolètes.
  - Authentification faible.
  - Failles de logicielles et systèmes

Éléments de droits

- La loi « Godfrain » du 5/1/88 est la première loi française réprimant les actes de criminalité informatique et de piratage :
  - **Art. 323-1 :** Le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système est puni d'un 1 ans d'emprisonnement et de 15 000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de 2 ans d'emprisonnement et de 30 000 € d'amende.
  - **Art. 323-2 :** Le fait d'entraver ou de fausser le fonctionnement d'un système est puni de 3 ans d'emprisonnement et de 45 000 € d'amende.
  - **Art. 323-3 :** Le fait d'introduire, de supprimer, de modifier frauduleusement des données dans un système est puni de 3 ans d'emprisonnement et de 45 000 € d'amende.

2.Introduction au hacking

Objectif : Saisir les enjeux sur le hacking et comprendre son fonctionnement

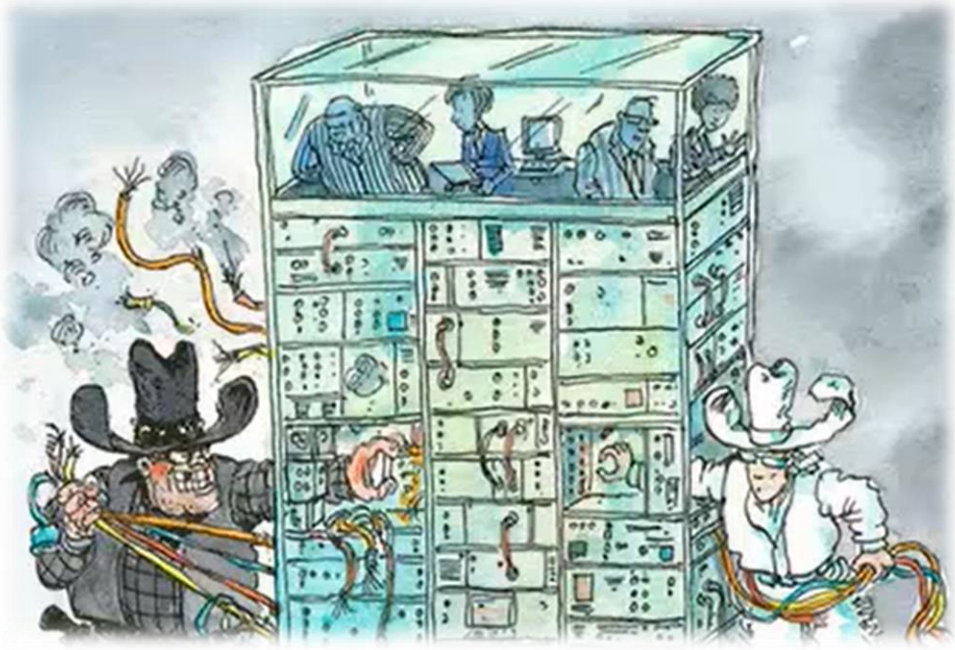
Hacker

- Le hacker est un spécialiste d'informatique, qui recherche les moyens de contourner les protections logicielles et matérielles :
  - Fin des années 50 ce terme désignait les programmeurs émérites.
  - Années 80, ce mot a été utilisé pour désigner les personnes impliqué dans le piratage des jeux.
  - Aujourd'hui = Pirate informatique

Types de Hacker

➢Il existe 3 type de Hackers :

- **White Hat hacker :** Hacker au sens nobles, dont le but est l'amélioration des systèmes et technologies informatique.
- **Black Hat hackers** : Plus couramment appelés pirates, c'est-à-dire des personnes s'introduisant dans les systèmes dans un but nuisible.
- **Hackivistes :** ce sont des hackers dont la motivation est principalement idéologique.

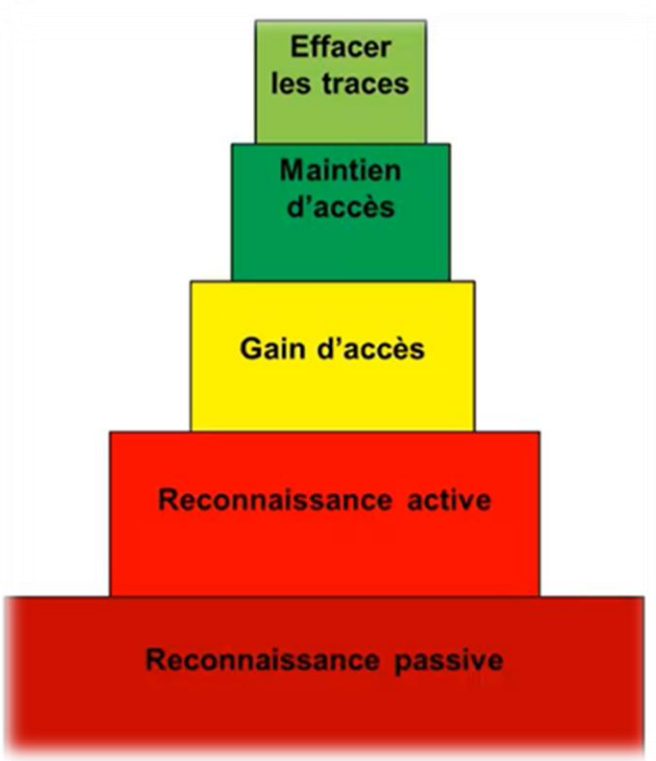


Motivations

- Les motivations des hackers sont nombreuses :
  - L'attrait de l'interdit
  - L'intérêt financier
  - L'intérêt politique
  - La renommée
  - La vengeance
  - L'envie de nuire

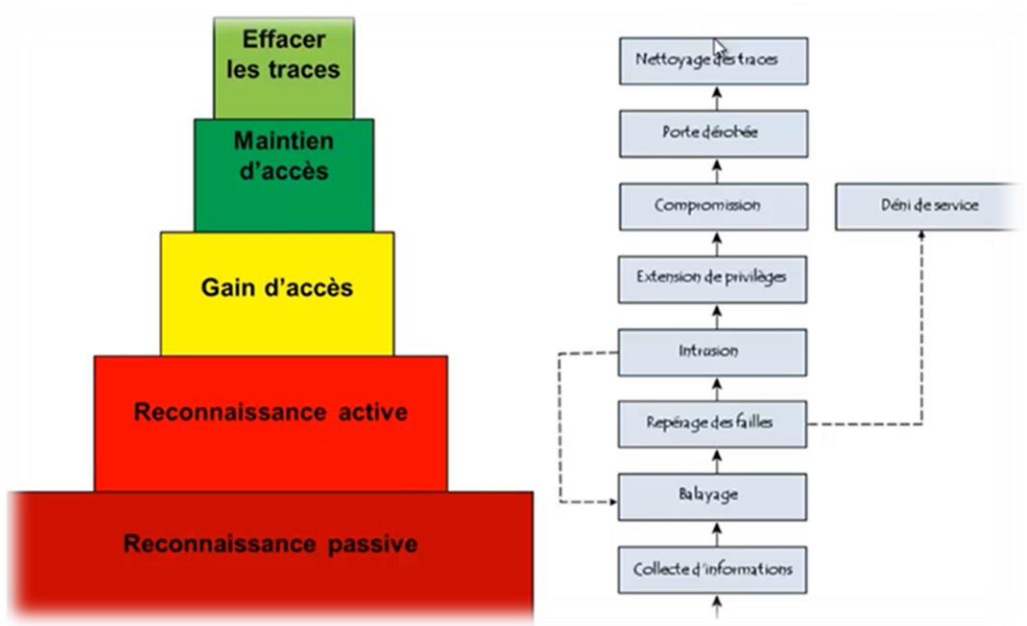
Etape du Hacking

- Le hacking est composé de 5 étapes :
  1. **Reconnaissance passive :** Avoir des informations sur le réseau, et sur l'entreprise, employés, sans interagir directement avec la cible.
  2. **Reconnaissance active :** ça concerne l'interaction du hacker avec la cible, ou il essayera d'interagir via des scans de ports, engineering sociale.
  3. **Gain d'accès :** L'hacker va essayer de gagner un accès, pas forcément avec des privilèges supérieurs, mais souvent avec des privilèges guest, ou il essayera d'élever ces privilèges vers un accès route.
  4. **Maintient d'accès :** Une fois l'accès établie, l'hacker va vouloir maintenir cette accès grâce à une porte dérobée (backdoor) pour pouvoir revenir au système quand il le voudra.
  5. **Effacer les traces :** il va essayer d'effacer ces traces.



Les étapes de façon plus détaillée

1. **Collecte d'information** :
   - La prise d'empreinte ou *foot Printing* est une étape préalable à toute attaque. Elle consiste à rassembler le maximum d'information sur la cible (adressage réseau, nom de domaine, protocole réseau, utilisateurs)
   - L'ingénierie social ou social ou *Social Engineering* est une méthode qui a pour but d'extirper des informations confidentielles à des personne selon plusieurs(téléphone, internet, lettre, contact direct)
2. **Le balayage du réseau** : Lorsque la topologie de réseau est connue, le pirates peut scanner les adresse IP, les ports, Les types des OS, les services)
3. **Repérages des failles :** Après avoir établi l'inventaire du parc logiciel, matériel, système, personnel, il reste au hacker de déterminer si des failles existent. Après avoir repéré les failles, deux possibilités s'offre au hacker
   a. Soit il fait un déni de service c'est-à-dire une attaque informatique ayant pour but de rendre indisponible le service, d'empêcher les utilisateurs d'un service de l'utiliser
   b. Soit il fait une intrusion
4. **Intrusion** : Lorsque le pirate a dressé une cartographie des ressources, il est en mesure de préparer son intrusion (Accéder à des comptes valides, Injection de codes, etc.)
5. **Extension de privilèges** : Lorsque le pirate a obtenu un ou plusieurs accès sur le réseau, celui-ci va chercher à augmenter ses privilèges en obtenant l'accès admin.
6. **Compromission** : Une fois l'accès obtenu, le pirate a pu dresser une cartographie de réseau, des machines, des failles, possède un accès admin, il lui est possible d'étendre son action en exploitant les relations d'approbation.
7. **Porte dérobée (Backdoor)** : Lorsqu'un pirate à infiltré un réseau d'entreprise, il peut arriver qu'il souhaite revenir. Il va installer une application afin de créer artificiellement une faille de sécurité ;
8. **Nettoyage des traces** : Le pirate lui rets à effacer les traces de son passage.

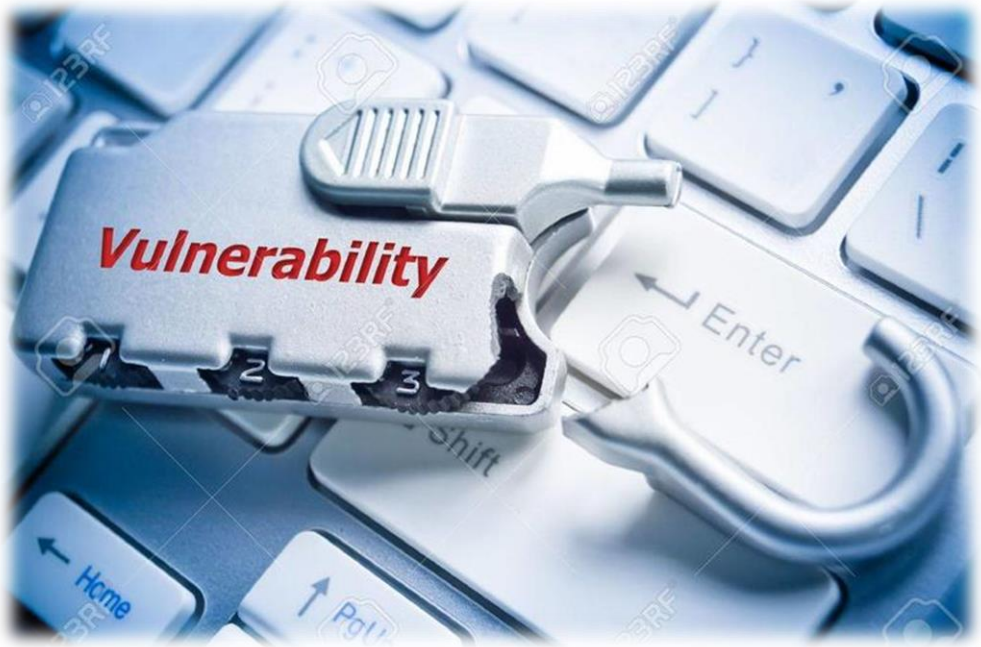


Les Vulnérabilité

Objectif: Comprendre le fonctionnement de plusieurs types d’attaque

Type de vulnérabilité

Dans le domaine de la sécurité informatique, une vulnérabilité ou faille est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.



Il existe 4 type de vulnérabilité :

1. **Vulnérabilités postes clients**
2. **Vulnérabilités réseau**
3. Vulnérabilités Web
4. Vulnérabilités applicatif

Vulnérabilité postes clients

- Les postes de travail des utilisateurs sont des composants critiques du système d'information et doivent être protégées en conséquence.
- La compromission d'un poste client peut donné accès au réseau interne d'un entreprise.
- La plus grande faille en informatique reste à ce jours la faille humaine.
- Il existe plusieurs type d'attaque pour s'introduire sur un poste de travaille, les plus connus sont :
  - **Le Brute force RDP**
  - **Le Backdoor**

Le Brute force RDP

- RDP est une fonctionnalité de Microsoft qui permet à un utilisateur de se connecter à distance sur un ordinateur en tapant un login et un mots de passe.
- L'attaque Brute force RDP consiste à réaliser une attaque par brute force sur le service RDP , grâce à des outils tel que Crowbar.

Le Backdoor

- Un backdoor (ou porte dérobée) est un programme informatique malveillant utilisé pour donner aux pirates un accès à distance non autorisé à un ordinateur infecté en exploitant les vulnérabilités du post client.
- Il permet de contourner les mécanismes de sécurité secrètement et de manière indétectable.
- Ce programme peut être un exécutable tell que Putty.exe, une fois que la victime ouvre ce programme malveillant sur son post de travaille, il donnera accès à distance au hacker à PC.

Vulnérabilités réseau

- La sécurité du réseau est un élément essentiel de toute organisation.
- Les vulnérabilités du réseau sont des failles ou des faiblesses présentes dans le réseau de l'organisation liées aux ports, aux hôtes, aux services, etc.
- Les vulnérabilité réseau sont assez nombreuses, parmi elles, les plus connus sont:

- **Sniffing réseau**
- **Spoofing réseau**
- **Man in the middle**
- **Déni de service**
- **Scanning**
- **Social Engineering**

Sniffing réseau

- Le Sniffing réseaux est une technique d'interception des données, il permet :
  - L'intercepter les données
  - Analyser les paquets
  - Décoder les paquets
  - Récupération d'infos

Fonctionnement

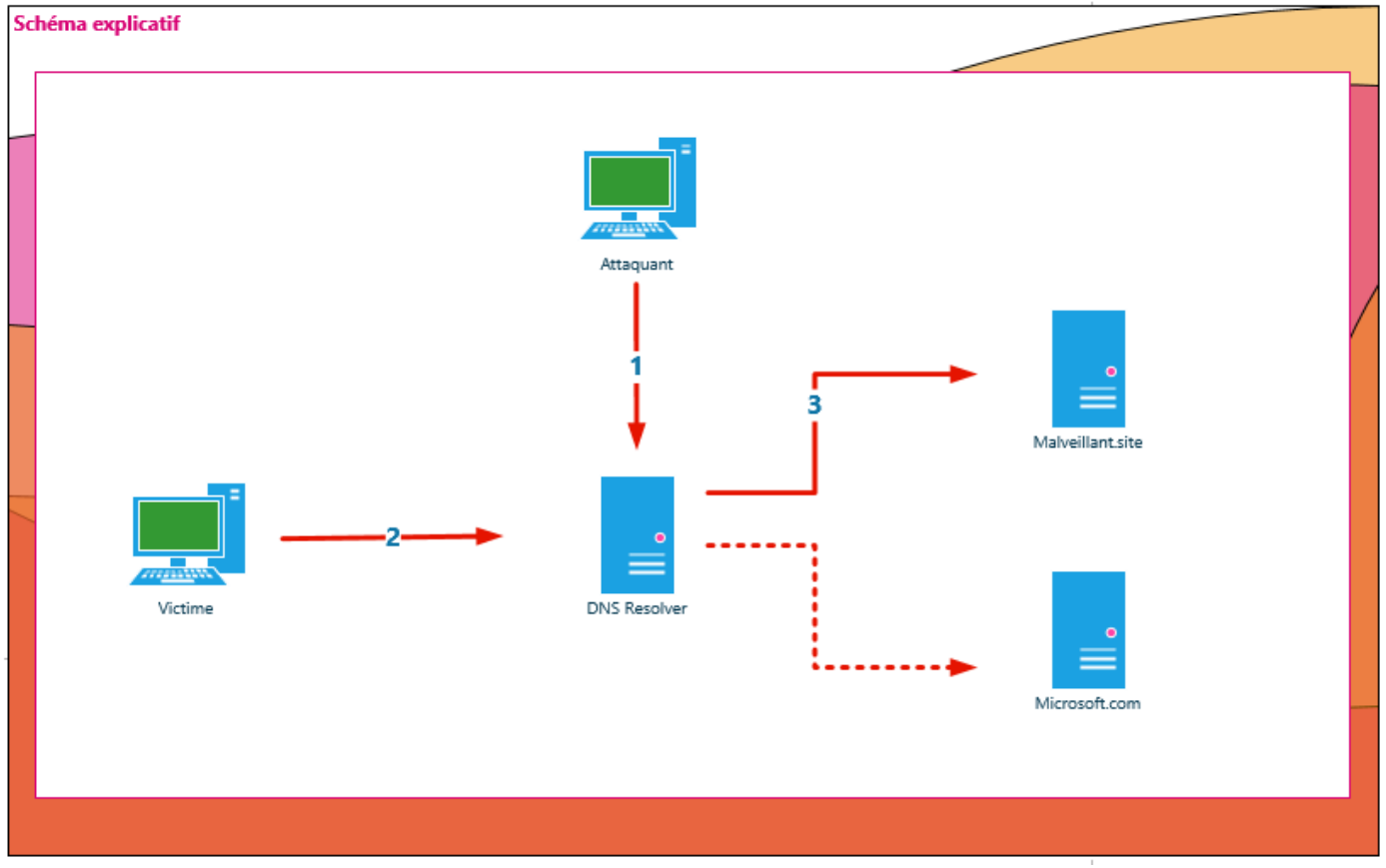
- Les renifleurs capturent le trafic réseau et analysent les flux de données afin de découvrir la nature, et parfois le contenu, des données qui transitent par un réseau. Son mode de fonctionnement est ainsi de suite :
  1. Vérifier l'utilisation du réseau de l'utilisateur
  2. Capturer tous les paquets réseau envoyés d'un endroit à un autre du réseau.
  3. Enregistrer les données des paquets capturés dans un fichier.
  4. Analyser les données enregistrées pour trouver des informations.

Le Spoofing

- Le Spoofing est un thermes anglais signifie l'usurpation d'identité
- Il consiste à déguiser une communication ou une identité afin qu'elle semble être associée à une source fiable et autorisée.
- Les attaques d'usurpation d'identité peuvent prendre de nombreuses formes:
  - **DNS Spoofing**
  - Email Spoofing
  - L'IP Spoofing

DNS Spoofing

1. Injecter une fausse entrée DNS
2. Emet une demande vers un site Web réel
3. La demande se résout à un faux site Web

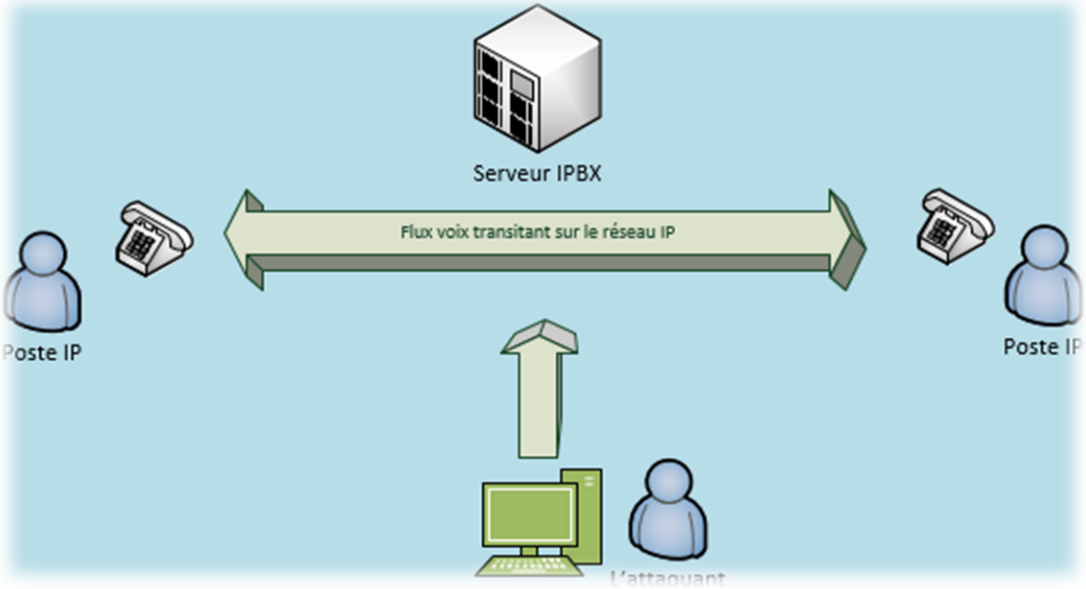


Man in the middle

- L'attaque de l'homme du milieu (HDM) ou man-in-the-middle attack (MITM), est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre puisse se douter que le canal de communication entre elles a été compromis.
- L'attaquant a non seulement la possibilité de lire, mais aussi de modifier les messages.
- Les attaques de l'homme du milieu peuvent prendre de nombreuses formes:
  - **ARP Poisoning**
  - DNS Poisoning

ARP Poisoning

- C'est probablement le cas le plus fréquent.
- Dans le scénario de réseau local, cette attaque peut être effectuée en empoisonnant le cache ARP avec une adresse MAC usurpée.

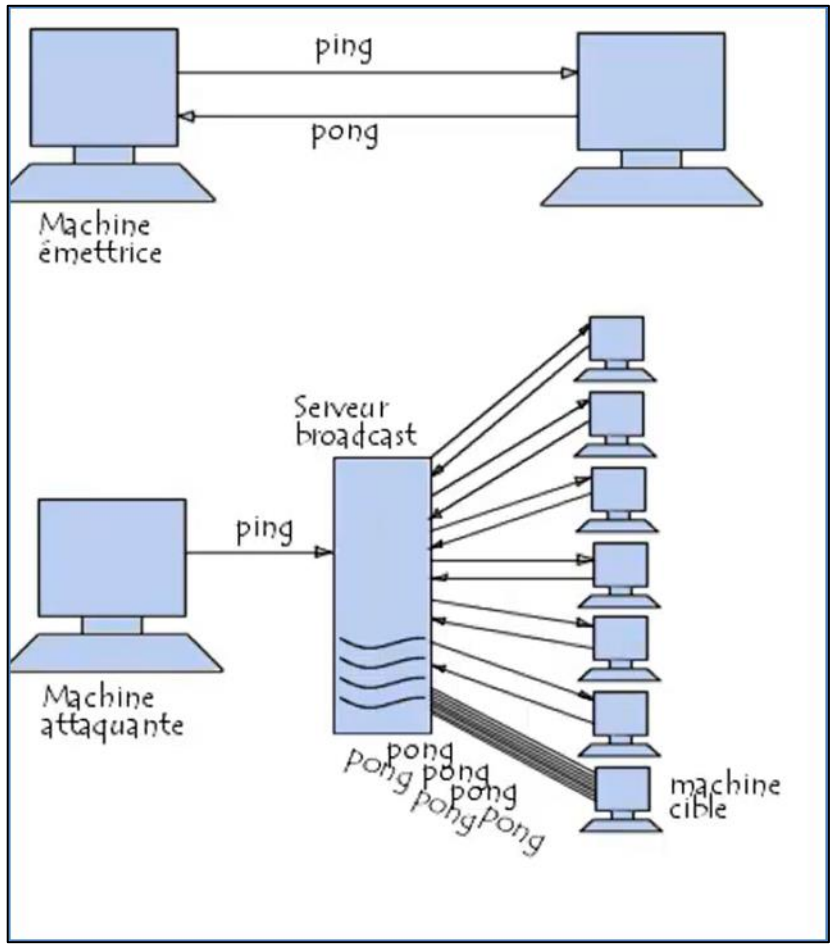


Déni de service

- Une attaque par déni de service(DOS) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.
- Il peut s'agir de :
  - L'inondation d'un réseau afin d'empêcher son fonctionnement
  - La perturbation des connexions entre deux machines, empêchant l'accès à un service particulier
- Il existe 2 type d'attaque pour le déni de service :
  - **Le Déni de service par Smurf**
  - **Le Déni de service par SYN flood**

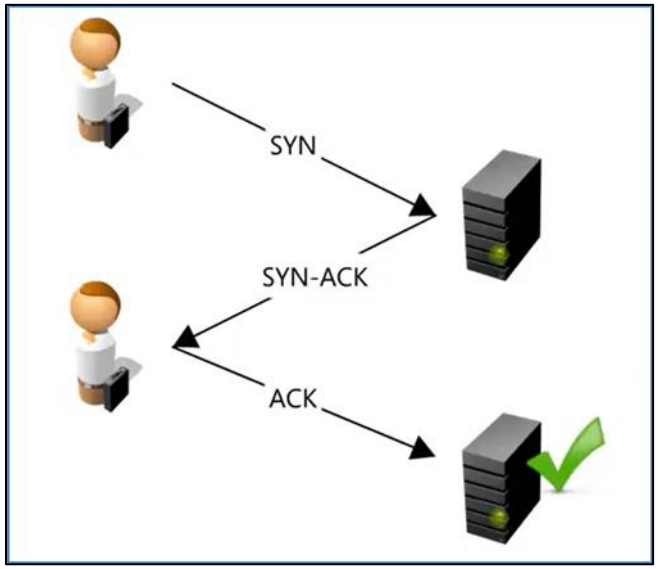
Le Déni de service par Smurf

- Une attaque Smurf est une attaque par déni de service distribué (DDoS) dans laquelle un pirate tente de saturer un serveur cible avec des paquets ICMP (Internet Control Message Protocol) :
  1. La machine attaquante envoie un ping à des serveurs broadcast
  2. Le serveur répercute la requête sur l'ensemble du réseau
  3. Toutes les machines répondent au serveur de broadcast
  4. Les serveurs redirigent les réponses vers la cible
-



Le déni de Service par SYN flood

- Le SYN flood est une attaque informatique visant à atteindre un déni de service. Elle s'applique dans le cadre du protocole TCP.
- Il consiste à envoyer une succession de requête SYN vers la cible



Le scanning

- Une analyse de port (scan) est une méthode permettant de déterminer quels ports d'un réseau sont ouverts.
- Les ports varient dans leurs services offerts. Ils sont numérotés de 0 à 65535.
- Une analyse de port envoie un paquet soigneusement préparé à chaque numéro de port de destination.
- Il existe plusieurs techniques de base que les logiciels d'analyse de port est capable d'inclure, et parmi ces techniques, le plus connue mais aussi la plus vieille est le **idle scan**.

idle scan

- L'idle scan est une technique qui permet de scanner une machine en nous faisant passer pour quelqu'un d'autre. Idle en anglais veut dire, à peu de choses près, inactif.
- Le principe est donc de scanner quelqu'un en faisant semblant d'être inactif (et faire porter le chapeau à Mme Michu, cette vieille bique !).

```
┌──(root㉿kali)-[~]
└─# nmap -P0 -sI 192.168.240.240:389 192.168.240.20
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-15 21:19 C
Idle scan using zombie 192.168.240.240 (192.168.240.240:389);
tal
Nmap scan report for 192.168.240.20
Host is up (0.039s latency).
Not shown: 998 closed|filtered tcp ports (no-ipid-change)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:0C:29:E1:58:56 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.77 seconds
```

Social Engineering

- Le social engineering (ingénierie sociale) est l'art de manipuler psychologiquement une personne afin de parvenir à une escroquerie.
- C'est une fraude psychologique qui pousse un individu à mener des actions contraires aux dispositifs de sécurité en vigueur.

Les méthodes

- Le social engineering a ainsi donné naissance à plusieurs méthodes de piratage ou d'escroquerie, tel que :
  - **L'hameçonnage :** Encore appelée phishing, est utilisée pour obtenir les données privées d'un individu. L'hacker entre en contact avec sa victime via une adresse électronique où il se fait passer pour un organisme de confiance.
  - **Le watering hole :** Le watering hole consiste à infecter à travers un site internet fréquenté par leurs victimes toutes les machines qui s'y connectent. Ce sont souvent des sites de divertissement comme les sites de jeux en ligne.
  - **La fraude au président** : Elle consiste à prendre l'identité du dirigeant d'une entreprise pour obtenir un virement bancaire. Dans ce cas, l'auteur de l'arnaque domine sa victime puisqu'il se présente comme étant son supérieur hiérarchique. Il peut ainsi aisément prendre comme prétexte une urgence, une confidence ou intimider et valoriser sa victime pour mieux l'atteindre.
  - **L'attaque par pièce jointe infectée :** Cette méthode classique est parfois facile à reconnaître. Son principe repose sur le piratage informatique à travers l'envoi d'un e-mail avec un fichier Word, Excel ou PowerPoint infecté.

Protection

Objectif: Comment se protéger contre ces type d’attack

Introduction

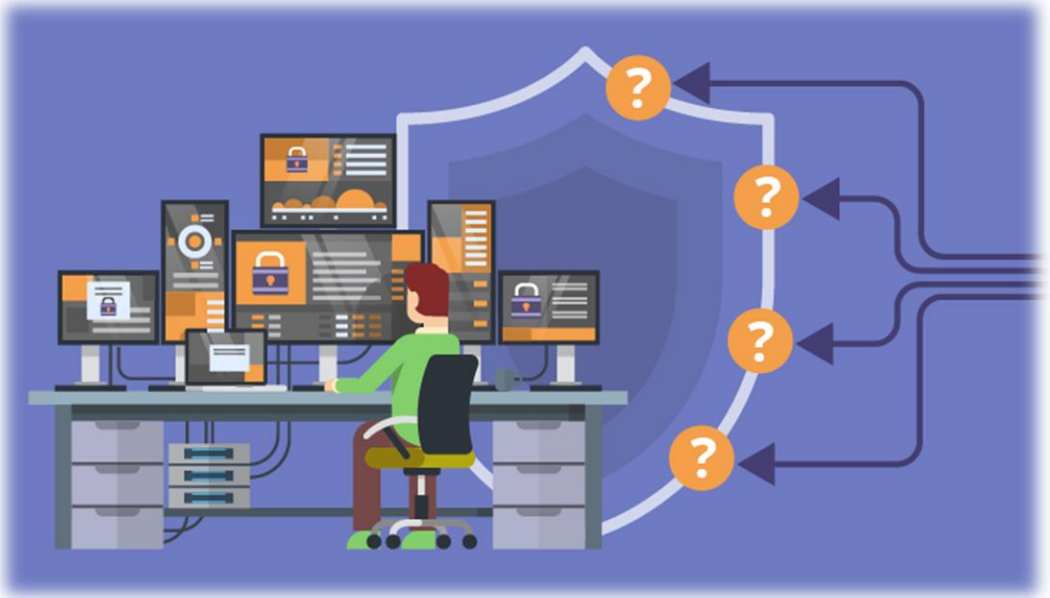
- Nous allons voir pour ce dernier chapitre les contre mesure général qui faut prendre pour éviter les vulnérabilité, les attaques de pirates.
- En règle général, une sécurité à 100% n'existe pas, mais nous pouvons ajouter des couches de difficulté aux hackers.
- Afin d'éviter le plus possible les attaques de pirates, il existe de nombreuses contre mesure, dont les principales sont:
  - La veille sécurité
  - Le Pen-testing
  - La séparation de droits
  - Firewall

La veille sécurité

- La veille en sécurité informatique est une activité indispensable, pour tous les professionnels. Elle vous permet de rester au fait des évolutions et tendances.
- Mais, plus important, la veille vous donne la capacité d'anticiper les attaques informatiques et mieux vous préparer et donc de limiter le risque d'un incident.
- Autant dire qu'il est indispensable :
  - de se tenir au courant des vulnérabilités et des patchs.
  - des tendances d'attaques des pirates.

Le Pen-Testing

- Un test d'intrusion , familièrement piratage éthique , est une cyberattaque simulée autorisée sur un système informatique, réalisée pour évaluer la sécurité du système.
- Pour une meilleur sécurité, il est important de planifier des test d’intrusion régulier
- Par la suite, réaliser un audit en recueillant les information lors du Pen-testing.

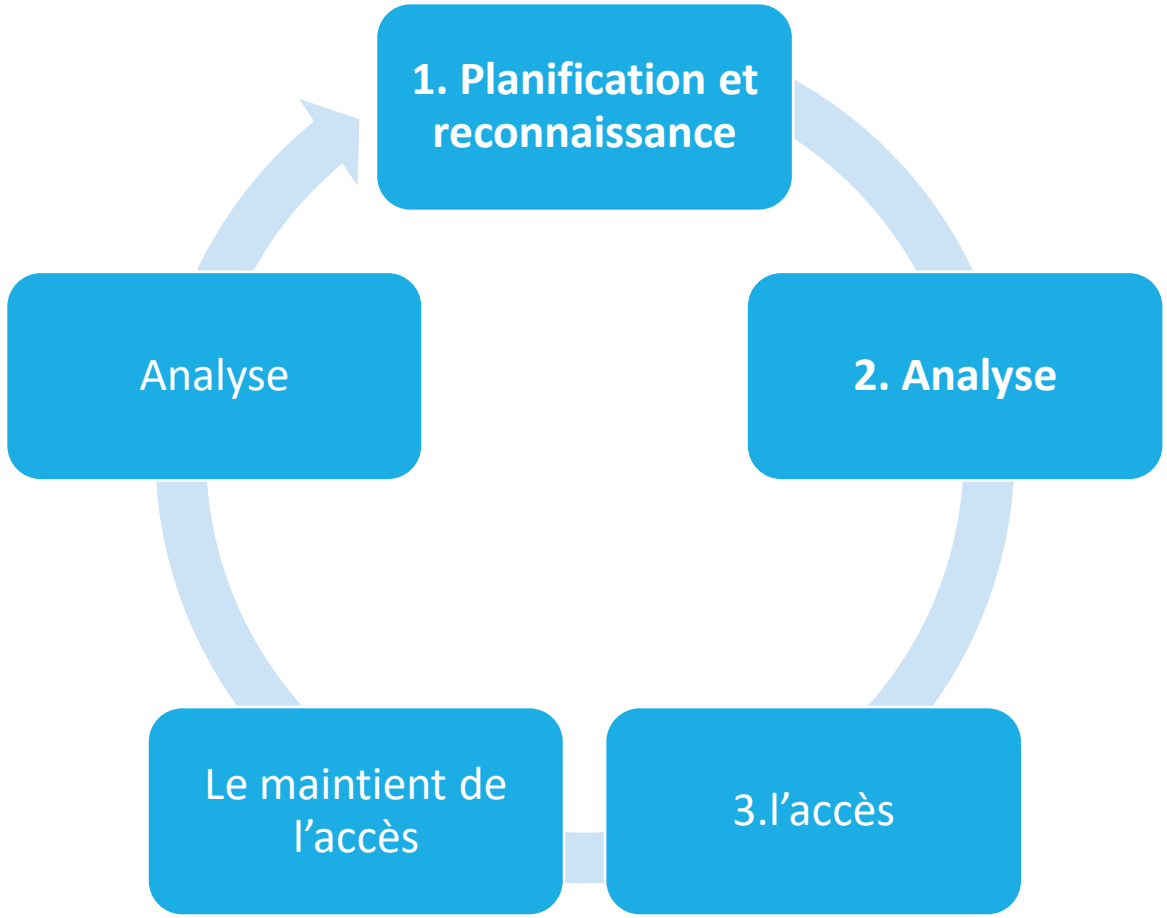


Type de contexte

- Nous définissons également le niveau d'informations dont nos pentesteurs bénéficient au commencement des tests :
  - boite noire (aucune information),
  - boite grise (accès à des comptes d'utilisateurs),
  - ou boite blanche (accès aux comptes d'administrateurs, voire plus)

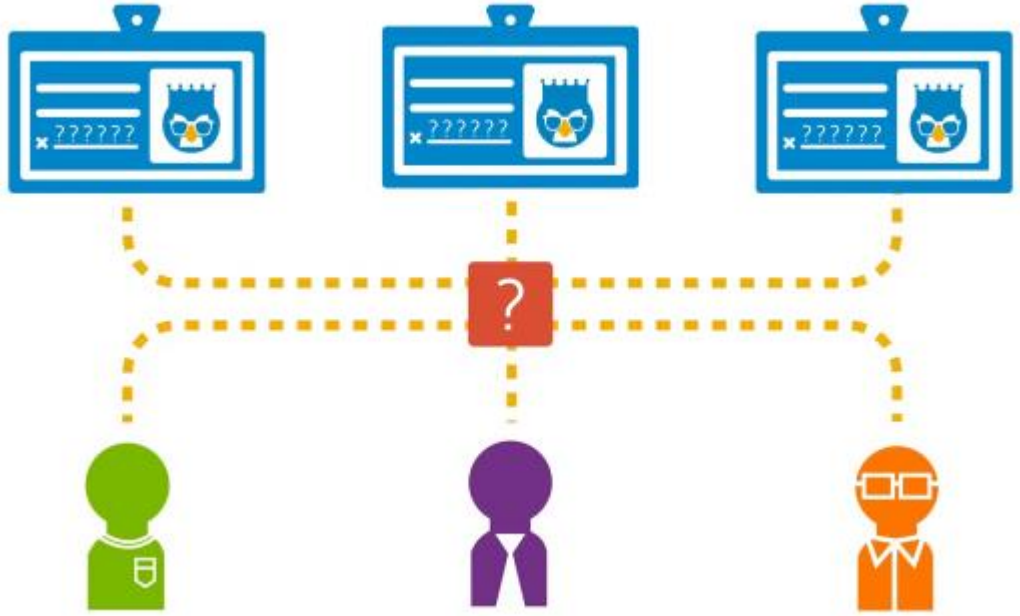
Étapes des tests d'intrusion

- Le processus de test de pénétration peut être décomposé en cinq étapes:
  1. **Planification et reconnaissance**: Définir la portée et les objectifs d'un test et recueillir des renseignement pour mieux comprendre la cible.
  2. **Analyse :** comprendre comment l'application cible répondra aux diverses tentatives d'intrusion
  3. **Obtenir l'accès :** Cette étape utilise des attaques d'applications (Backdoor), pour découvrir les vulnérabilités d'une cible. Les testeurs essaient ensuite d'exploiter ces vulnérabilités, généralement en augmentant les privilèges, en volant des données, en interceptant le trafic, etc., pour comprendre les dommages qu'elles peuvent causer.
  4. **Maintenir l'accès :** L'objectif de cette étape est de voir si la vulnérabilité peut être utilisée pour obtenir une présence persistante dans le système exploité
  5. **Analyse** : Les résultats du test d'intrusion sont ensuite compilés dans un rapport. Ces informations sont ensuite analysé afin de corriger les vulnérabilité et se protéger contre des attaques futur.



Gestion des Accès Privilèges

- La gestion des accès à privilèges fait référence à une stratégie de cyber sécurité complète, qui englobe les personnes à contrôler et à sécuriser toutes les identités et les activités à privilèges, humaines et non humaines, dans tout l'environnement informatique d'une entreprise. Car il faut pas oublier :
  - Une menace peut être aussi bien interne qu'externe
  - Une menace peut être aussi bien volontaire



Firewall

- C'est une machine dédiée au routage entre LAN et Internet.
- Le trafic est analysé au niveau des datagrammes IP (adresse, utilisateur, contenu...).
- Un datagramme non autorisé sera simplement détruit

TP

Objectif : réaliser des test d'intrusions sur une infrastructure réseau

Principaux mesures de sécurité

- Ces 10 mesures de sécurité comprennent les mesures prioritaires qu'une organisation devrait adopter comme base de référence pour renforcer son infrastructure de TI et protéger ses réseaux :
  1. Intégrer, surveiller et défendre les passerelles Internet
  2. Appliquer des correctifs aux applications et aux systèmes d'exploitation
  3. Mettre en vigueur la gestion des privilèges d'administrateur
  4. Renforcer les systèmes d'exploitation et les applications
  5. Segmenter et séparer l'information
  6. Miser sur une formation et une sensibilisation sur mesure
  7. Protéger l'information au niveau de l'organisation
  8. Assurer la protection au niveau de l'hôte
  9. Isoler les applications Web
  10. Mettre en place une liste d'applications autorisées