HACK-cès Sécurisé: Sécurités des Systèmes Informatiques

Mélanie Padaud **Rania Medjeldi** **Thomas Veitès**

Mercredi 20 Mars 2019

Master 1 CRYPTIS, Université de Limoges

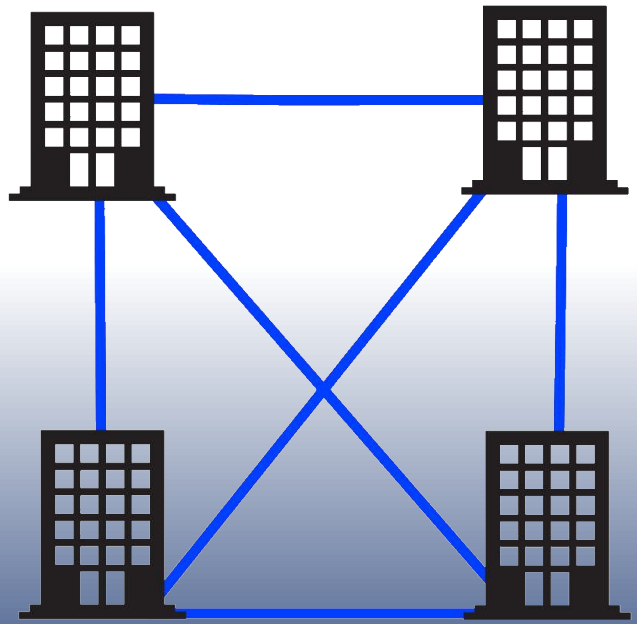
Sommaire

C'est Quoi ?

Réseau

Définition

Ensemble d'hôtes interconnectés entre eux pour échanger des informations.



Hôte

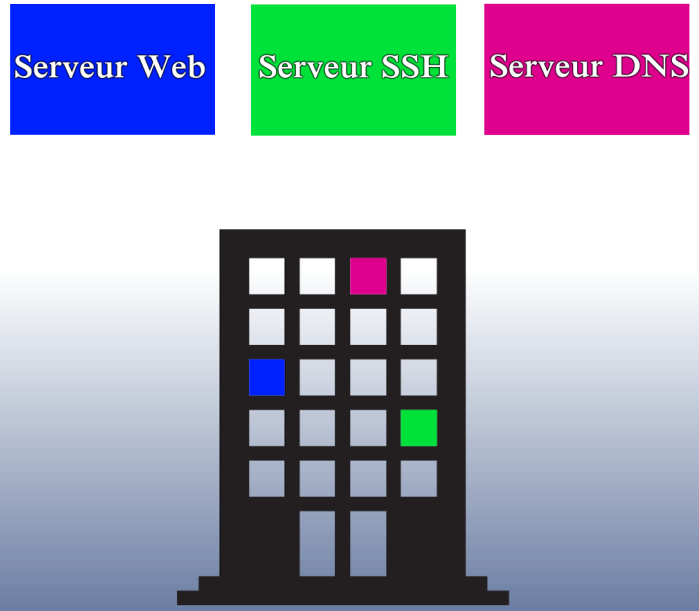
Définition

Un hôte est un terme général pour décrire toute machine reliée à un réseau informatique. Il peut fournir des services ou être un simple client. Un hôte est identifié par une adresse IP.

Notion de port

Définition

La notion de port est utilisée pour identifier les différents services tournant sur un hôte.



Faille de sécurité

Définition

Une faille ou une vulnérabilité est une faiblesse d'un système permettant à un attaquant de détourner son fonctionnement initial et de porter atteinte à la confidentialité ou à l'intégrité des données qu'il contient.

Quels sont les Intérêts ?

Illégaux

Intérêts illégaux

- Intérêt financier
- Pivot
- Modification de données
- Espionnage industriel
- Nuire à l'entreprise
- Intérêts personnels
- Hacktivisme

Légaux

Intérêts Légaux

- Bug Bounty
- Audit en entreprise
- Pentest

Comment ?

Première étape : Reconnaissance

Reconnaissance

Objectif

Récupérer le maximum d'informations sur le système cible dans le but d'identifier les potentielles failles présentes afin de les exploiter.

Il existe deux types de reconnaissance :

- Reconnaissance Passive
- Reconnaissance Active

Reconnaissance Passive

Objectif

Récupérer des informations sans interaction directe avec le système cible.

Exemples

- Recherche sur les réseaux sociaux
- Recherche dans des annuaires
- Créer une liste des employés qui pourra servir pour du social engineering

Reconnaissance Active

Objectif

Interagir avec le système cible afin de collecter des informations sur ses vulnérabilités.

Exemples

- Accéder au site internet
- Tester une connexion en SSH
- Analyser le réseau
- Rechercher les ports ouverts

Seconde étape : Scanner

Scan

Définition

Un scanner est un programme dont le but est d'aider à l'identification des vulnérabilités d'un système.

Exemples

- Scan Ping
- Scan Port
- Exploit DB
- Nessus

Scan Ping

Objectif

Envoyer des requêtes ICMP (Internet Control Message Protocol) à toutes les IP possibles du réseau dans le but de savoir quels hôtes existent ou non.

Attention

Si une machine ne répond pas au ping cela ne signifie pas qu'elle n'existe pas dans le réseau.

Exemples

- Fing (Android)
- Angryip

Nmap Scan

Objectif

Trouver des ports ouverts c'est à dire identifier les services hébergés sur la machine.

Attention

Grâce aux scans Nmap on peut obtenir des informations sur la version des services, voir même sur le système d'exploitation de la cible.

Exploit DB

Définition

Exploit DB est une base de données qui recense les failles connues sur des programmes et des systèmes.

Troisième étape : Exploitation

Force brute

Définition

Attaque consistant à deviner un mot de passe en essayant toutes les combinaisons possibles.

Exemples

- JohnTheRipper
- Hashcat

Payload (Charge Utile)

Définition

C'est le programme ou le script exploitant la faille, pour permettre d'accéder au système ou récupérer des informations parfois sensibles sur celui-ci.

Exemples

- Connexion en Bind
- Connexion en Reverse

Metasploit

Définition

Hack like in the Movies !
Il met en place les Payloads en utilisant la base de donnée de ExploitDB.
L'utilisateur doit simplement fournir les options de la Payload et Metasploit s'occupe de l'exploitation de la faille.

Élévation de privilège

Objectif

Exploiter la vulnérabilité d'une application en envoyant une requête spécifique, non prévue par son concepteur, afin d'avoir une application avec plus de privilèges et pouvoir effectuer des actions non autorisées.

Wireshark

Définition

Outil d'analyse de protocoles réseaux destinés aux administrateurs réseau. Il est notamment utilisé pour tester des protocoles réseaux mais aussi pour avoir un aperçu de ce qui se passe concrètement sur le réseau.

Social engineering

Objectif

Extirper des informations à des personnes sans qu'elles ne s'en rendent compte.
Le but étant de se faire passer pour quelqu'un d'autre afin d'obtenir la confiance de la victime et ainsi lui soutirer les informations souhaitées.

Exemple

- Social Engineering Toolkit

Web

Objectif

Abuser des fonctionnalités d'un service Web, afin d'exécuter du code ou avoir accès à des informations indisponible.

Exemples

- Injections SQL
- XSS
- Transversal Directory
- Attention aux Backups (extension nano, ...)

Quatrième étape : Post-Exploitation

Accès Shell

Définition

Possibilité de se connecter sur la machine infectée, avec un accès shell (ligne de commande).

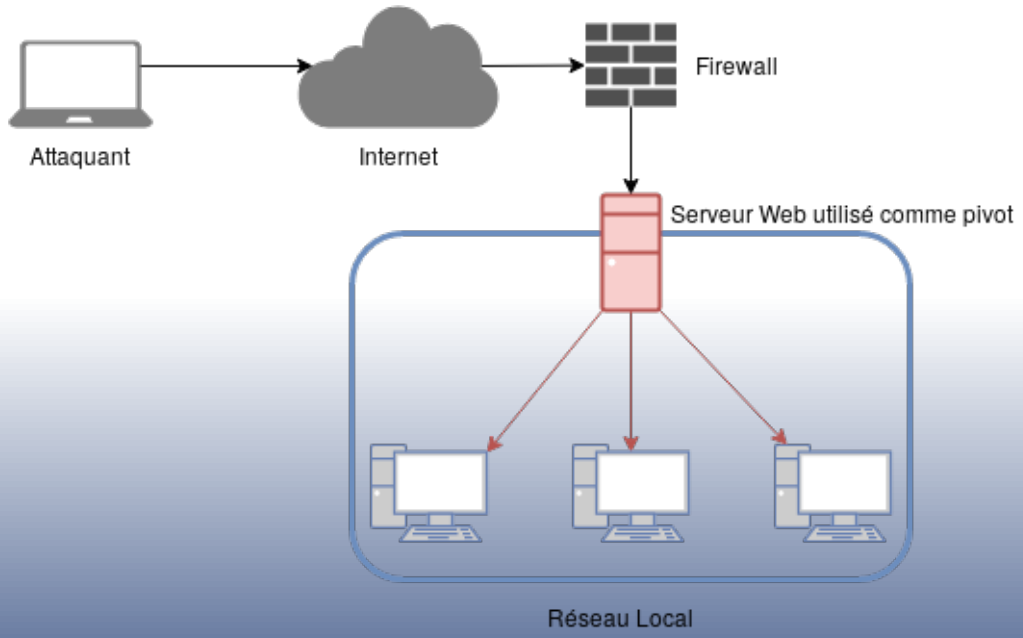
Exemples

- Netcat redirection vers Bash
- Meterpreter

Pivot

Définition

Accéder à des réseaux ou des machines avec lesquelles on n'est pas censé pouvoir communiquer par le biais d'un machine infectée.



Rootkit

Définition

Logiciels permettant de maintenir un accès sur une machine vérolée le plus furtivement possible. Il peut ainsi cacher des logiciels, des fichiers, des processus et s'exécuter dans un autre logiciel.

Exemples

- Hacker Defender
- XCP (Sony)

Comment se Protéger ?

Comment se protéger ?

- Mise à jour
- Pare-feu
- Configuration des droits
- Antivirus
- Utilisation d'un antirootkit (IceSword, Rkhunter)
- Système de détection d'intrusion

Comment se protéger ?

- Chiffrement du disque dur
- Sauvegardes de données
- Mots de passe solides

FIN

Quelques Questions ?