Formation
sécurité réseau et Internet

Réalisation pratique d'un test d'intrusion

Comprendre l'attaque pour mieux se défendre

Enoncés des exercices

Présentation du TP

Le PDG de l'entreprise « entreprise.net » vous a mandaté pour réaliser un test d'intrusion sur son réseau. Il souhaite obtenir un rapport exhaustif comportant les actions que vous avez réalisées, accompagnées des informations que vous avez récupérées (configurations, mots de passe, preuves de votre passage…)
Vous travaillerez à partir d'un filiale de « entreprise.net » et serez connectés sur le WAN de la société.

L'objectif à atteindre est simple : compromettre le réseau de entreprise.net.

Contrainte : ne rien casser ! L'entreprise doit pouvoir continuer à travailler normalement.

Conseils :

- Conserver une vision globale de votre avancée ;
- Organisez vos données dès le début ;
- Définissez des objectifs à atteindre.

1. Découverte réseau et qualification des cibles

1.1. Fuite d'informations via le DNS

Objectifs :

- Exploiter les fuites d'informations classiques des serveurs DNS

Enoncé :

Question 1 : Identifiez le serveur DNS du domaine entreprise.net

Question 2 : Identifiez le serveur ayant le type « MX ».

Question 3 : Identifiez les autres noms de machines qui se trouvent dans le plan d'adressage 35.35.35.0/24

Outils :

- `dig, dnsrecon`
- Attaque par dictionnaire :

```
dnsrecon -d entreprise.net -t brt -D /usr/share/dnsenum/dns.txt
```

- Résolution inverse des adresses du réseau cible :

```
for i in {0..254}; do host 35.35.35.$i; done
```

1.2. Topologie réseau : notion de TTL & TCP Timestamp

Objectif :

- Obtenir le détail de la topologie réseau entre votre machine et le réseau entreprise.net.
- Comprendre le mécanisme de routage des paquets IP.

Enoncé :

Découvrez les sauts réseaux entre votre machine et www.entreprise.net en utilisant les différents outils de « traceroute ».

Question 4 : Quelles sont les routes utilisées par les paquets de type ICMP, 80/TCP, 8080/TCP et 53/UDP à destination de la machine 35.35.35.1 ?

Question 5 : Quelles hypothèses pouvez-vous poser pour expliquer des différences ?

Question 6 : Depuis combien de temps la machine 35.35.35.1 est-elle allumée ?

Question 7 : Récupérez toutes les adresses IP des interfaces de chaque routeur (entrée et sortie)

Question 8 : Représentez l'architecture du réseau avec son plan d'adressage qui permet de rejoindre le réseau 35.35.35.0/24.

Outils :

- `traceroute, tcptraceroute, hping3, mtr`
- `wireshark`

1.3. Scan réseau

Objectifs :

- Se familiariser avec l'outil `nmap` et ses options
- Appréhender les limites d'un scan UDP

Enoncé :

Réalisez un scan TCP du réseau 35.35.35.0/24.

Question 9 : Dressez la liste des machines découvertes sur le réseau (`-sP`).

Question 10 : Identifiez les services réseaux disponibles (`-sS, -sT`) sur chacune des machines. Est-ce que ces deux techniques peuvent être utilisé en tant que simple utilisateur ? Pourquoi ?

Question 11 : Classez les machines selon leur type et tentez d'identifier leurs rôles supposés.

Réalisez un scan UDP de la machine 40.0.0.4 sur les ports UDP fréquents : `53, 67, 68, 111, 123, 161, 162, 500, 514, 1194, 1646, 1812, 1813 et 4500`) sans résolution de nom DNS.

Question 12 : Est-ce que le scan UDP vous parait fiable ? Quelle technique doit-on utiliser pour fiabiliser le scan UDP ?

Question 13 : Exploitez la fuite d'information triviale que vous avez trouvée pour compléter votre représentation du réseau.

Outil :

- `snmpwalk`

1.4. Identification des systèmes d'exploitation et services

Objectif :

Effectuez une prise d'empreinte des systèmes d'exploitation des machines identifiées lors de la phase précédente ainsi que de leurs services réseaux.

Enoncé :

Effectuez les prises d'empreinte de manière active et passive

Question 14 : précisez l'option à utiliser pour `nmap`

Question 15 : dans le cadre de `p0f`, précisez le signal TCP à prendre en considération pour « fingerprinter » un serveur.

Outils :

- prise d'empreinte active : `nmap`
- prise d'empreinte passive : `p0f, ettercap`

Question 16 : Complétez votre schéma en précisant :

- les équipements : routeurs, serveurs…
- les systèmes d'exploitation associés et leur version
- les services actifs et leurs versions
- les configurations IP, …