Cybersécurité - TP 2

GIBOZ Alexandre, MAURICE Romain, AINOUZ Nicolas

INFO1 2022-2025

Exercice 1 : Scan d’un réseau et les ports d’une station

1. **Scanner, par l’attaquant, les adresses IPs des machines connectées en utilisant les outils**

a) nmap avec l'option "-sP", Expliquer le role de l'option sP

On lance la commande la commande suivante pour obtenir l'adresse du réseau:

```
ip addr show
```

On obtient l'information suivante:

```
172.17.X.X/16
```

On peut a présent scanner le réseau avec la commande suivante:

```
nmap -sP 172.17.2.0/16
```

On obtient une liste des machines connectées au réseau, avec leur nom de domaine, leur adresse IP et leur adresse MAC.

Le paramètre -sP permet de scanner les machines connectées au réseau, sans scanner les ports de ces machines.

Il utilise le protocole ICMP pour obtenir les adresses IP, et ARP pour les adresses MAC.

SI ce paramètre n'est pas utilisé, nmap utilise TCP par défaut.

2. **Expliquer via wireshark par quel moyen nmap ou netdiscover arrivent à découvrir les adresses IP des machines connectés ?**

Nmap envoi des requêtes ARP en broadcast pour demander l'adresse MAC assignée à chaque adresse IP du réseau.

3. **Scanner par l’attaquant les ports ouverts sur la station S1.**

On lance la commande suivante pour scanner les ports ouverts sur la machine d'un voisin:

```
nmap -sS 172.17.2.11
```

Nmap envoi des paquets TCP avec un flag SYN sur chaque port, et, en fonction de la réponse retournée, en déduit les ports qui sont ouverts ou non. En général, un retour "RST, ACK" signifie que le port est fermé, et un retour "SYN, ACK" signifie que le port est ouvert.

4. **Ouvrir un port sur la station S1 par l'outil netcat, et re-scanner les ports ouverts. Est-ce que le nouveau port ouvert est détecté ?**

On se connecte en SSH sur la machine:

```
ssh tpreseau@172.17.2.11
```

On lance la commande suivante pour ouvrir un port sur la machine d'un voisin:

```
nc -lnp 1234
```

On relance la commande nmap TCP SYN afin de voir si le nouveau port est ouvert. Ce dernier est listé:

```
22/tcp open  ssh
25/tcp open  smtp
80/tcp open  http
1234/tcp open  hotline
```

Exercice 2 : Sniffing par ARP cache poisoning

1. **Vérifier via wireshark que le ping ente les deux stations S1 et S2 n'est pas intercepté par l'attaquant.**

On choisit deux machines:

- S1: `172.17.2.11`
- S2: `172.17.2.1`

On se connecte en SSH sur les deux machines et on lance la commande suivante sur la machine S1:

```
ping 172.17.2.1
```

On regarde si les paquets de ping sont interceptés par l'attaquant (par tcpdump mais wireshark marche de la meme façon):

```
sudo tcpdump -i eth0 -n icmp
```