Lab 1 — Attaque MITM avec Ettercap (ARP Spoofing)

Objectif

Réaliser une attaque Man-In-The-Middle entre :

- Machine attaquante : Kali Linux
- Victime 1 : Ubuntu
- Victime 2 : Machine physique Windows/Linux

Toutes les machines doivent être dans un réseau **Host-Only**.

---

1. Architecture réseau

Configuration VirtualBox / VMware

Créer un réseau Host-Only :

Exemple :

- Réseau : `192.168.56.0/24`

Machine	IP
Kali	192.168.56.10
Ubuntu	192.168.56.20
Machine physique	192.168.56.1

---

2. Configuration IP

Kali

```
sudo nano /etc/network/interfaces
```

Ou temporairement :

```
sudo ip addr add 192.168.56.10/24 dev eth0
sudo ip link set eth0 up
```

Ubuntu

```
sudo ip addr add 192.168.56.20/24 dev eth0
sudo ip link set eth0 up
```

Machine physique

Configurer manuellement :

- IP : `192.168.56.1`
- Masque : `255.255.255.0`

---

3. Vérification connectivité

Depuis Kali :

```
ping 192.168.56.20
ping 192.168.56.1
```

---

4. Activer le forwarding sur Kali

```
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
```

Vérification :

```
cat /proc/sys/net/ipv4/ip_forward
```

Doit retourner :

```
1
```

---

5. Installation Ettercap

Sur Kali :

```
sudo apt update
sudo apt install ettercap-graphical -y
```

---

6. Lancer Ettercap

Mode graphique

```
sudo ettercap -G
```

---

7. Configuration de l’attaque

Dans Ettercap :

Étape 1

- Sniff → Unified sniffing
- Choisir `eth0`

Étape 2

- Hosts → Scan for hosts

Étape 3

- Hosts → Hosts list

Ajouter :

- Ubuntu → Target 1
- Machine physique → Target 2

Étape 4

Lancer MITM :

- Mitm → ARP poisoning
- Cocher :
    - Sniff remote connections

Étape 5

Démarrer :

- Start → Start sniffing

---

8. Vérification ARP poisoning

Sur Ubuntu

```
arp -a
```

Vous verrez que l'adresse MAC de la gateway correspond à Kali.

Sur Windows

```
arp -a
```

---

9. Capture trafic

Sur Kali :

```
sudo tcpdump -i eth0
```

Ou :

```
sudo wireshark
```

Wireshark

---

10. Arrêter attaque

```
sudo pkill ettercap
```

Désactiver forwarding :

```
echo 0 | sudo tee /proc/sys/net/ipv4/ip_forward
```