# Lab 5 - Systèmes de filtrage de paquets (Pare-feu)

## I. *iptables*


**Netfilter**: pare-feu sous Linux que nous pourrons le configurer à travers plusieurs outils. Cependant, l'outil le plus connu et le plus facile à utiliser est **iptables**.

**iptables**: peut être défini comme une interface (langage) aidant à spécifier et de configurer les règles de filtrage sur le pare-feu **Netfilter**.

Dans ce lab, nous allons découvrir les tables et les chaines utilisées par le pare-feu et appliquer des règles de filtrage afin de protéger notre machine **Metasploitable** contre les scans et ainsi les attaques de la machine **Kali**.

### 1) Différentes tables utilisées par le pare-feu

- **filter**: correspond techniquement au pare-feu lui même et permet de filtrer les paquets.
- **mangle**: permet de modifier les paquets, exemple: modifier le champ TTL (Time To Live) d'un paquet afin d'augmenter sa durée de vie sur le réseau.
- **nat (Networt Address Translation)**: utilisé pour les règles NAT, l'objectif est de jouer sur les adresses IP source et destination pour changer le routage du trafic.
- **raw**: permet d'évaluer les paquets comme un ensemble (ou une session) et non pas paquet par paquet sans aucune liaison entre eux.

### 2) Différentes chaines

- **INPUT** (entrée): tous les paquets arrivant sur la machine concernée.
- **FORWARD** (relais): les paquets qui ne sont pas à destination de la machine mais ils la transitent pour atteindre la machine de destination.
- **OUTPUT** (sortie): tous les paquets sortant de la machine concernée (exemple: une demande de connexion).

**3)** Taper les commandes suivantes sur votre machine **Metasploitable** en tant que ***root*** et dire ce que vous avez comme information:

- `iptables -L`
- `iptable -L -t nat`
- `iptable -L -t mangle`

Quel est la différence entre les trois commandes ?

**4)** Nous allons maintenant voir comment appliquer des règles de sécurité sur les différentes chaînes **INPUT**, **FORWARD** et **OUTPUT**.

Nous avons vu lors du TP scanning réseau que la commande `nmap -sV <IP de la victime>` permet d'afficher les ports ouverts, le service associé à chaque port et la version du service.

a) Taper la commande `nmap -sV <IP de la victime>` sur la machine **Kali**. Quel est l'état des ports 21, 22 et 23 ?

b) Nous allons maintenant changer la politique de sécurité de notre pare-feu Netfilter sur la machine **Metasploitable**:

**i.** Taper la commande `iptables -P FORWARD DROP` sur votre machine **Metasploitable**, ensuite la commande `iptables -L`. Que remarquez-vous ?
Revenez sur la machine **Kali** et taper la commande `nmap -sV <IP de la victime>`. Que remarquez-vous ?

**ii.** Tapez maintenant la commande `iptables -P INPUT DROP` sur votre machine **Metasploitable**, ensuite la commande `nmap -sV <IP de la victime>` sur votre machine **Kali**. Que remarquez-vous ? Justifier votre réponse.

iii. Nous allons maintenant autoriser quelques ports (80, 53, 8180 et 445) avec la commande suivante:
`iptables -A INPUT -p tcp --dport <Destination PORT> -j ACCEPT`, en remplaçant le `<Destination PORT>` par les ports `80`, `53`, `8180` et `445`.
Taper la commande `iptables -L` et dire si les quatre règles de filtrage ont bien été ajoutées à la chaîne **INPUT**.
Revenir sur la machine **Kali** et taper la commande `nmap -sV <IP de la victime>`. Que remarquez-vous ? Pourquoi ?

iv. Entrer maintenant la commande : `iptables -P INPUT ACCEPT`
Ensuite filtrer quelques ports (21, 23 et 22) avec la commande suivante:
`iptables -A INPUT -p tcp --dport <Destination port> -j REJECT` en remplaçant le `<Destination PORT>` par les ports `21`, `22` et `23`.
Revenir sur la machine **Kali** et taper la commande `nmap -sV <IP de la victime>`. Que remarquez-vous ?

v. Taper les deux commandes suivantes:
```
iptables -A INPUT -p tcp -j REJECT
iptables -A INPUT -i eth0 -p udp -j REJECT
```
ensuite la commande `nmap -sV <IP de la victime>` sur votre machine **Kali**. Que remarquez-vous ?

## II. ***Résultats des attaques exécutées dans les TPs précédents***

**1)** Sur votre machine **Kali**, taper la commande: `telnet <IP de la victime>`. Quel est le résultat ?

**2)** Essayer d'exécuter la vulnérabilité sur le port 21 que nous avons vu sur la deuxième partie des Labs (Scanning Réseau et Gain d'accès). Quel est le résultat ?