TP-Iptables

Installation d'Iptables :

```
apt install iptables
```

Cette commande installe le paquet iptables, qui est un outil de configuration du pare-feu pour les systèmes Linux.

Lister les règles actuelles d'Iptables :

```
iptables -L -n -v
```

Cette commande liste toutes les règles actuellement configurées dans iptables. Les options -n et -v permettent d'afficher les adresses IP et les numéros de port au format numérique, et d'afficher des statistiques détaillées.

Exécuter le script.sh (Pour éxécutez un script) :

```
./script.sh
```

Cette commande exécute un script nommé script.sh situé dans le répertoire courant.

Exécuter le script.sh avec les privilèges sudo :

```
sudo ./script.sh
```

Cette commande exécute le script.sh en utilisant sudo, ce qui permet d'exécuter le script avec les privilèges administratifs.

```
Installation de sudo:
```

En essayant d'éxécuter avec la commande sudo je me suis rendu compte que je n'avais pas la commande installé donc du coup j'ai du le faire en faisant :

```
apt install sudo
```

Cette commande installe le paquet sudo, qui permet à un utilisateur d'exécuter des commandes avec les privilèges d'un autre utilisateur, généralement l'utilisateur root.

Changer les permissions du fichier script.sh :

```
chmod 700 script.sh
```

Cette commande définit les permissions du fichier script.sh de sorte que l'utilisateur propriétaire puisse lire, écrire et exécuter le fichier, tandis que les autres utilisateurs n'ont aucun droit sur le fichier, de toutes les façons on est pas nombreux sur cette machines .

Modification du fichier script.sh avec nano :

```
nano script.sh
```

Cette commande ouvre le fichier script.sh dans l'éditeur de texte nano, ce qui me permettra ainsi de modifier son contenu.

Ajout de règles iptables dans le script.sh :

```
Ce script iptables configure le pare-feu d'un routeur pour sécuriser le
réseau et autoriser uniquement les accès autorisés.

 1. Définir les politiques par défaut (DROP) :

   #!/bin/sh

   # On drop par défaut tous les paquets à destination du routeur
   iptables -t filter -P INPUT DROP

   # On drop par défaut tous les paquets émis par le routeur
   iptables -t filter -P OUTPUT DROP

   # On drop par défaut tous les paquets tranversants le routeur
   iptables -P FORWARD DROP
```

Ces lignes définissent la politique par défaut pour toutes les chaînes du pare-feu (INPUT, OUTPUT et FORWARD) pour DROPPER tous les paquets par défaut. Cela signifie que tous les paquets qui ne correspondent pas à une règle explicite seront bloqués.

Nettoyer les règles existantes :

```
 # Stateful mode ######################################################
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
#####################################################################
```

Ces lignes activent le mode Stateful pour les chaînes INPUT, OUTPUT et FORWARD. Le mode Stateful permet au pare-feu de suivre les connexions établies et d'autoriser les paquets de réponse qui font partie de ces connexions.

Autoriser les connexions SSH :

```
# Connexion SSH au routeur depuis le réseau de Beaup
iptables -A INPUT -p tcp -s 10.187.20.0/24 --dport 22 -j ACCEPT

# Connexion SSH au serveur depuis le réseau de Beaup
iptables -A FORWARD -p tcp -s 10.187.20.0/24 -d 10.31.16.1/32 --dport 22 -j
ACCEPT
```

Ces lignes autorisent les connexions SSH au routeur et au serveur depuis le réseau 10.187.20.0/24. Le port 22 est utilisé par défaut pour les connexions SSH.

Autoriser l'accès aux serveurs DNS :

```
#commande Andrea
#autoriser beaup à acceder au serveur dns 53-63
iptables -A FORWARD -p udp -s 10.187.20.0/24 -d 10.31.96.53/32 --dport 53 -j
ACCEPT
iptables -A FORWARD -p udp -s 10.187.20.0/24 -d 10.31.96.63/32 --dport 53 -j
ACCEPT
```

Ces lignes autorisent le réseau 10.187.20.0/24 à accéder aux serveurs DNS 10.31.96.53 et 10.31.96.63 sur le port 53 (UDP).

Autoriser l'accès aux serveurs DNS et aux services web :

```
 #autoriser les DNS 53-63 à acceder au port 80 et 443 de tous les services
qui écoutent sur ces ports
#autoriser les serveurs DNS 53-63 à avoir accès DNS de la machine 8.8.8.8
```

```
iptables -A FORWARD -p udp -s 10.31.96.53/32 -d 8.8.8.8 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -s 10.31.96.63/32 -d 8.8.8.8 --dport 53 -j ACCEPT

#autoriser Beaup à accéder au service munin sur les ports 80 et 443
```

Conclusion