**TP : Introduction à iptables sous Linux**

Objectifs pédagogiques

Comprendre les bases du pare-feu iptables

Apprendre à configurer des règles de filtrage simples

Sécuriser un serveur Linux basique

Prérequis

Une machine Linux (Ubuntu, Debian, etc.)

Droits administrateur (sudo)

Notions de base en réseau (IP, ports)

Partie 1 : Premiers pas avec iptables

1.1 Vérification de l'installation

*# Vérifier si iptables est installé*

sudo iptables -V

*# Si non installé, installer le package*

sudo apt-get update

sudo apt-get install iptables

1.2 Comprendre l'état actuel

*# Afficher toutes les règles actuelles*

Sudo iptables -L -v

1.3 Concepts de base

Iptables fonctionne avec trois chaînes principales :

INPUT : trafic entrant

OUTPUT : trafic sortant

FORWARD : trafic traversant

Partie 2 : Premières règles de filtrage

2.1 Politique par défaut

*# Configurer une politique restrictive*

Sudo iptables -P INPUT DROP

sudo iptables -P FORWARD DROP

Sudo iptables -P OUTPUT ACCEPT

2.2 Autoriser le trafic local

bash

Copy

*# Autoriser la boucle locale*

Sudo iptables -A INPUT -i lo -j ACCEPT

Sudo iptables -A OUTPUT -o lo -j ACCEPT

2.3 Autoriser les connexions établies

*# Permettre les connexions établies et relatives*

Sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Partie 3 : Exercices pratiques

3.1 Autoriser SSH

*# Autoriser les connexions SSH (port 22)*

Sudo iptables -A INPUT -p tcp --dport 22-j ACCEPT

3.2 Autoriser le Web

*# Autoriser HTTP et HTTPS*

Sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

3.3 Protection basique

*# Bloquer les pings (ICMP)*

Sudo iptables -A INPUT -p icmp -j DROP

*# Protéger contre le scan de ports*

Sudo iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP

Partie 4 : Gestion des règles

4.1 Sauvegarder les règles

*# Sauvegarder la configuration*

Sudo sh -c "iptables-save > /etc/iptables.rules"

4.2 Restaurer les règles

*# Restaurer la configuration*

Sudo sh -c "iptables-restore < /etc/iptables.rules"

4.3 Réinitialiser toutes les règles

*# Supprimer toutes les règles*

Sudo iptables -F

Sudo iptables -X

Exercices pratiques

1. **Exercice de base** :
   * Afficher les règles actuelles
   * Ajouter une règle pour autoriser le port 80
   * Vérifier que la règle est bien ajoutée
2. **Exercice intermédiaire** :
   * Créer une règle pour bloquer une IP spécifique
   * Ajouter une règle pour autoriser un intervalle de ports
   * Sauvegarder la configuration
3. **Exercice avancé** :
   * Mettre en place une protection contre les attaques DoS simples
   * Configurer le logging des paquets rejetés
   * Créer une règle avec limitation de connexions

Conseils de sécurité

Toujours faire une sauvegarde avant de modifier les règles

Tester les règles avant de les appliquer en production

Garder un accès SSH fonctionnel pour éviter de se bloquer

Documenter toutes les modifications apportées

Dépannage courant

**Problème** : Perte d'accès SSH **Solution** : Avoir une règle de secours :

Sudo iptables -I INPUT 1 -p tcp --dport 22 -j ACCEPT

**Problème** : Règles qui ne prennent pas effet **Solution** : Vérifier l'ordre des règles et les politiques par défaut

**Problème** : Services web inaccessibles **Solution** : Vérifier les règles pour les ports 80/443