**Installation d’un FireWall**

* **sudo nano /root/firewall.sh**

*Ajouter dans le fichier ->*

#!/bin/bash

#

# Interdire toute connexion entrante

iptables -t filter -P INPUT DROP

iptables -t filter -P FORWARD DROP

echo [OK] Interdire toute connexion entrante

# Interdire toute connexion sortante

iptables -t filter -P OUTPUT DROP

echo [OK] Interdire toute connexion sortante

# Vider les tables actuelles

iptables -t filter -F

iptables -t filter -X

# Ne pas casser les connexions etablies

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

iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Autoriser les requetes DNS, FTP, HTTP, NTP, GIT

iptables -t filter -A OUTPUT -p tcp --dport 21 -j ACCEPT

iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT

iptables -t filter -A OUTPUT -p tcp --dport 53 -j ACCEPT

iptables -t filter -A OUTPUT -p tcp --dport 9418 -j ACCEPT

iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT

iptables -t filter -A OUTPUT -p udp --dport 123 -j ACCEPT

iptables -t filter -A OUTPUT -p udp --dport 9418 -j ACCEPT

echo [OK] Autoriser les requetes DNS, FTP, HTTP, GIT

# Autoriser loopback

iptables -t filter -A INPUT -i lo -j ACCEPT

iptables -t filter -A OUTPUT -o lo -j ACCEPT

# Autoriser ping

iptables -t filter -A INPUT -p icmp -j ACCEPT

iptables -t filter -A OUTPUT -p icmp -j ACCEPT

# HTTP

iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT

iptables -t filter -A INPUT -p tcp --dport 443 -j ACCEPT

#FTP

modprobe ip\_conntrack\_ftp

iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT

iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

#DNS

iptables -t filter -A INPUT -p tcp --dport 53 -j ACCEPT

iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

#GIT

iptables -t filter -A INPUT -p tcp --dport 9418 -j ACCEPT

iptables -t filter -A INPUT -p udp --dport 9418 -j ACCEPT

# Autoriser SSH

iptables -t filter -A INPUT -p tcp --dport 3416 -m recent --rcheck --seconds 60 --hitcount 2 --name SSH -j LOG --log-prefix "SSH REJECT"

iptables -t filter -A INPUT -p tcp --dport 3416 -m recent --update --seconds 60 --hitcount 2 --name SSH -j DROP

iptables -t filter -A INPUT -p tcp --dport 3416 -m state --state NEW -m recent --set --name SSH -j ACCEPT

* **sudo chmod +x /root/firewall.sh**
* **sudo nano /etc/rc.local**

*Ajouter dans le fichier ->*

/root/firewall.sh