**#!/bin/bash**

## Script iptables

## Règles iptables.

## On efface les règles.

**iptables -F**

## On supprime toutes les chaînes utilisateurs.

**iptables -X**

## On refuse tout le trafic entrant.

**iptables -P INPUT DROP**

## On refuse tout le trafic sortant.

**iptables -P OUTPUT DROP**

## On refuse la redirection (forward).

**iptables -P FORWARD DROP**

## Refuser silencieusement tous les paquets broadcastés.

**iptables -A INPUT -m pkttype --pkt-type broadcast -j DROP**

## Permettre à une connexion ouverte de recevoir du trafic en entrée.

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

## Permettre à une connexion ouverte de recevoir du trafic en sortie.

**iptables -A OUTPUT -m state ! --state INVALID -j ACCEPT**

## Accepter tout le trafic web (www) à sortant et entrant.

**iptables -A OUTPUT -p tcp -i eth0 --dport 80 -j ACCEPT**

**iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT**

## On accepte la boucle locale en entrée.

**iptables -I INPUT -i lo -j ACCEPT**

## On journalise les paquets en entrée.

**iptables -A INPUT -j LOG**

## On journalise la redirection de paquets.

**iptables -A FORWARD -j LOG**

## On drop les scans XMAS et NULL.

**iptables -A INPUT -p tcp --tcp-flags FIN,URG,PSH -j DROP**

**iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP**

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

**iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j DROP**

exit 0