**Ejercicio 1: Análisis de la configuración de un cortafuegos**

*eth0: 192.168.1.2 (a Internet)*

*eth1: 192.168.10.1*

*eth2: 192.168.3.1*

#!/bin/sh

# ----------------------

# IPTABLES script

# ----------------------

**#1) FLUSH de reglas:**

**-F: Este parámetro indica "flush" o "eliminar". Cuando se utiliza con iptables, la opción -F se utiliza para eliminar todas las reglas existentes en las tablas de filtrado.**

**-X: se utiliza para eliminar las cadenas de usuario personalizadas creadas previamente con el comando iptables.**

**-Z: en iptables se utiliza para restablecer los contadores de paquetes y bytes de una regla específica, o de todas las reglas, en una cadena específica o en todas las cadenas.**

**-t nat -F: igual que -F, pero para todas las reglas relacionadas con una NAT.**

iptables −F

iptables −X

iptables −Z

iptables −t nat −F

**#2) Politicas por defecto: para cada cadena se definen políticas iniciales para “aceptar” o “rechazar” un tráfico especifico.**

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

iptables −t nat −P PREROUTING DROP

iptables −t nat −P POSTROUTING DROP

**#3) Los paquetes que acaban de llegar por la interfaz eth0 (internet) cambia la direccion de destino y envía los paquetes HTTP(80) y HTTPS(443) a 192.168.3.2**

iptables −t nat −A PREROUTING −i eth0 −p tcp −−dport 80 −j DNAT −−to 192.168.3.2:80

iptables −t nat −A PREROUTING −i eth0 −p tcp −−dport 443 −j DNAT −−to 192.168.3.2:443

**#4) Permite tráfico que venga de eth1 al firewall desde todas las IP de 192.168.10.0/24**

iptables −A INPUT −s 192.168.10.0/24 −i eth1 −j ACCEPT

**#5) Aplico NAT para las direcciones de los hosts de eth1 antes de sacarlas a Internet**

iptables −t nat −A POSTROUTING −s 192.168.10.0/24 −o eth0 −j MASQUERADE

iptables −t nat −A POSTROUTING −s 192.168.3.0/24 −o eth0 −j MASQUERADE

#6)

echo 1 > /proc/sys/net/ipv4/ip\_forward

**#7) Permite inicializar una comunicación con 2 redes locales, (por el RELATED puede ser una comunicación FTP).**

iptables -t filter -A FORWARD -i eth1 -o eth2 -m state –state NEW,ESTABLISHED,RELATED -j ACCEPT

iptables -t filter -A FORWARD -i eth2 -o eth1 -m state –state ESTABLISHED,RELATED -j ACCEPT

1. **¿Qué servicios pueden ser accedidos desde Internet?**

HTTP(80) y HTTPS(443)

1. **¿Existe una zona desmilitarizada (DMZ) en la red?**
2. **¿Los hosts de la red 192.168.10.0/24 pueden acceder a Internet?**

No, aunque haya un POSTROUTING en #5, no hay ninguna regla declarada FORWARD de eth1 a eth0. Por tanto, en este ejercicio por defecto se descartarían (iptables -P FORWARD DROP)

1. **¿Pueden los hosts de la red 192.168.10.0/24 recibir conexiones desde Internet?**

Tampoco.

1. **¿Pueden los hosts de la red 192.168.10.0/24 recibir conexiones desde la red 192.168.3.0/24?**

Si, por las reglas FORWARD recibe tráfico de Internet desde eth2.

**Ejercicio 3: Detección de intrusiones**

Se recomienda ejecutar los comandos como administrados (sudo -i)

Comando 1: snort -A console

Comando 2: snort -i **lo**



Comando 3: snort -c snort.conf