

Alumno: Ariadna Abigail Alanis Estrada Sistemas operativos

1-Muestre las reglas IPTABLES en su equipo

```
user@DESKTOP-HQFIPG5:~$ sudo iptables -L -v
Chain INPUT (policy DROP 22 packets, 1416 bytes)
  num  pkts bytes target     prot opt in     out     source               destination
  0     0      0 ACCEPT     all  --  eth1   any    anywhere            anywhere
  25    5568 ACCEPT     all  --  eth0   any    anywhere            anywhere
  0     0      0 ACCEPT     all  --  eth1   any    anywhere            anywhere
  10   992 ACCEPT     all  --  lo     any    anywhere            anywhere
  0     0      0 ACCEPT     tcp  --  any    any    anywhere            anywhere    tcp dpt:pop3 flags:FIN,SYN,RST,ACK/SYN
  0     0      0 ACCEPT     tcp  --  any    any    anywhere            anywhere    tcp dpt:pop3s flags:FIN,SYN,RST,ACK/SYN
  0     0      0 ACCEPT     tcp  --  any    any    anywhere            anywhere    tcp dpt:imap2 flags:FIN,SYN,RST,ACK/SYN
  0     0      0 ACCEPT     tcp  --  any    any    anywhere            anywhere    tcp dpt:imaps flags:FIN,SYN,RST,ACK/SYN
  0     0      0 ACCEPT     tcp  --  any    any    anywhere            anywhere    tcp dpt:pop3 flags:FIN,SYN,RST,ACK/SYN
  0     0      0 ACCEPT     tcp  --  any    any    anywhere            anywhere    tcp dpt:pop3s flags:FIN,SYN,RST,ACK/SYN
  0     0      0 ACCEPT     tcp  --  any    any    anywhere            anywhere    tcp dpt:imap2 flags:FIN,SYN,RST,ACK/SYN
  0     0      0 ACCEPT     tcp  --  any    any    anywhere            anywhere    tcp dpt:imaps flags:FIN,SYN,RST,ACK/SYN
  0     0      0 ACCEPT     tcp  --  eth1   any    anywhere            anywhere    tcp spt:68 dpt:67
  0     0      0 ACCEPT     udp  --  eth1   any    anywhere            anywhere    udp spt:bootps dpt:bootps
  0     0      0 DROP       tcp  --  any    any    anywhere            anywhere    tcp dpt:ssh
  0     0      0 DROP       tcp  --  any    any    nsasx4.uninet.net.mx anywhere    tcp dpt:telnet
  0     0      0 DROP       all  --  any    any    nsasx4.uninet.net.mx anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  num  pkts bytes target     prot opt in     out     source               destination
  0     0      0 ACCEPT     all  --  eth1   eth0   anywhere            anywhere
  0     0      0 ACCEPT     all  --  eth0   eth1   anywhere            anywhere

Chain OUTPUT (policy ACCEPT 64 packets, 8010 bytes)
  num  pkts bytes target     prot opt in     out     source               destination
  0     0      0 ACCEPT     all  --  any    any    anywhere            anywhere
  0     0      0 REJECT     all  --  any    any    192.168.0.0/24      nsasx4.uninet.net.mx reject-with icmp-port-unreachable

user@DESKTOP-HQFIPG5:~$ sudo iptables -nL
Chain INPUT (policy DROP)
target    prot opt source                destination
ACCEPT    0    --  0.0.0.0/0              0.0.0.0/0
ACCEPT    0    --  0.0.0.0/0              0.0.0.0/0
ACCEPT    0    --  0.0.0.0/0              0.0.0.0/0
ACCEPT    0    --  0.0.0.0/0              0.0.0.0/0
ACCEPT    6    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:110 flags:0x17/0x02
ACCEPT    6    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:995 flags:0x17/0x02
ACCEPT    6    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:143 flags:0x17/0x02
ACCEPT    6    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:993 flags:0x17/0x02
ACCEPT    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:110 flags:0x17/0x02
ACCEPT    6    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:995 flags:0x17/0x02
ACCEPT    6    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:143 flags:0x17/0x02
ACCEPT    6    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:993 flags:0x17/0x02
ACCEPT    6    --  0.0.0.0/0              0.0.0.0/0    tcp spt:68 dpt:67
ACCEPT    17   --  0.0.0.0/0              0.0.0.0/0    udp spt:68 dpt:67
DROP      6    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:22
DROP      6    --  0.0.0.0/0              0.0.0.0/0    tcp dpt:23
```

2-Cree dos reglas diferentes en IPTABLES, de las cuales

La primera permite las conexiones entrantes al puerto 22 esta permite el acceso remoto SSH al equipo.

```
user@DESKTOP-HQFIPG5:~$ sudo iptables -A INPUT -p tcp --sport 22 -j ACCEPT
user@DESKTOP-HQFIPG5:~$ sudo iptables -L -v
Chain INPUT (policy DROP 22 packets, 1416 bytes)
  num  pkts bytes target     prot opt in     out     source               destination
  1     0      0 ACCEPT     0    --  eth1   *      0.0.0.0/0            0.0.0.0/0
  2    39 6632 ACCEPT     0    --  eth0   *      0.0.0.0/0            0.0.0.0/0
  3     0      0 ACCEPT     0    --  eth1   *      0.0.0.0/0            0.0.0.0/0
  4    22 1992 ACCEPT     0    --  lo     *      0.0.0.0/0            0.0.0.0/0
  5     0      0 ACCEPT     6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:110 flags:0x17/0x02
  6     0      0 ACCEPT     6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:995 flags:0x17/0x02
  7     0      0 ACCEPT     6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:143 flags:0x17/0x02
  8     0      0 ACCEPT     6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:993 flags:0x17/0x02
  9     0      0 ACCEPT     6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:110 flags:0x17/0x02
  10    0      0 ACCEPT     6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:995 flags:0x17/0x02
  11    0      0 ACCEPT     6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:143 flags:0x17/0x02
  12    0      0 ACCEPT     6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:993 flags:0x17/0x02
  13    0      0 ACCEPT     6    --  eth1   *      0.0.0.0/0            0.0.0.0/0    tcp spt:68 dpt:67
  14    0      0 ACCEPT     17   --  eth1   *      0.0.0.0/0            0.0.0.0/0    udp spt:68 dpt:67
  15    0      0 DROP      6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:22
  16    0      0 DROP      6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:23
  17    0      0 DROP      0    --  *      *      200.33.146.217      0.0.0.0/0
  18    0      0 ACCEPT     6    --  *      *      0.0.0.0/0            0.0.0.0/0    tcp dpt:22

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  num  pkts bytes target     prot opt in     out     source               destination
  1     0      0 ACCEPT     0    --  eth1   eth0   0.0.0.0/0            0.0.0.0/0
  2     0      0 ACCEPT     0    --  eth0   eth1   0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 90 packets, 10074 bytes)
  num  pkts bytes target     prot opt in     out     source               destination
  1     0      0 ACCEPT     0    --  *      *      0.0.0.0/0            0.0.0.0/0
  2     0      0 REJECT     0    --  *      *      192.168.0.0/24      200.33.146.217 reject-with icmp-port-unreachable

user@DESKTOP-HQFIPG5:~$
```

La segunda bloquea todo el tráfico entrante al puerto 80, esta evita que el equipo reciba solicitudes HTTP.

```
uam@DESKTOP-HQFIPG5:~$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
uam@DESKTOP-HQFIPG5:~$ sudo iptables -L -v -n --line-numbers
Chain INPUT (policy DROP 22 packets, 1416 bytes)
num  pkts bytes target     prot opt in     out     source            destination
1    0      0 ACCEPT    0     --    eth1   *          0.0.0.0/0      0.0.0.0/0
2    44    7012 ACCEPT    0     --    eth0   *          0.0.0.0/0      0.0.0.0/0
3    0      0 ACCEPT    0     --    *      *          0.0.0.0/0      0.0.0.0/0
4    22    1992 ACCEPT    0     --    lo     *          0.0.0.0/0      0.0.0.0/0
5    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
6    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
7    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
8    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
9    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
10   0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
11   0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
12   0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
13   0      0 ACCEPT    6     --    eth1   *          0.0.0.0/0      0.0.0.0/0
14   0      0 ACCEPT    17    --    eth1   *          0.0.0.0/0      0.0.0.0/0
15   0      0 DROP      6     --    *      *          0.0.0.0/0      0.0.0.0/0
16   0      0 DROP      6     --    *      *          0.0.0.0/0      0.0.0.0/0
17   0      0 DROP      6     --    *      *          200.33.146.217  0.0.0.0/0
18   0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
19   0      0 DROP      6     --    *      *          0.0.0.0/0      0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out     source            destination
1    0      0 ACCEPT    0     --    eth1   eth0       0.0.0.0/0      0.0.0.0/0
2    0      0 ACCEPT    0     --    eth0   eth1       0.0.0.0/0      0.0.0.0/0

Chain OUTPUT (policy ACCEPT 95 packets, 10454 bytes)
num  pkts bytes target     prot opt in     out     source            destination
1    0      0 ACCEPT    0     --    *      *          0.0.0.0/0      0.0.0.0/0
2    0      0 REJECT    0     --    *      *          192.168.0.0/24  200.33.146.217  reject-with icmp-port-unreachable

uam@DESKTOP-HQFIPG5:~$
```

3-Muestre nuevamente las reglas en IPTABLES donde identifique las nuevas reglas creadas

```
uam@DESKTOP-HQFIPG5:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 22 packets, 1416 bytes)
num  pkts bytes target     prot opt in     out     source            destination
0    0      0 ACCEPT    0     --    eth1   *          0.0.0.0/0      0.0.0.0/0
50   0      0 ACCEPT    0     --    eth0   *          0.0.0.0/0      0.0.0.0/0
28   0      0 ACCEPT    0     --    lo     *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    17    --    eth1   *          0.0.0.0/0      0.0.0.0/0
0    0      0 DROP      6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 DROP      6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 DROP      6     --    *      *          200.33.146.217  0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 DROP      6     --    *      *          0.0.0.0/0      0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out     source            destination
0    0      0 ACCEPT    0     --    eth1   eth0       0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    0     --    eth0   eth1       0.0.0.0/0      0.0.0.0/0

Chain OUTPUT (policy ACCEPT 107 packets, 11410 bytes)
num  pkts bytes target     prot opt in     out     source            destination
0    0      0 ACCEPT    0     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 REJECT    0     --    *      *          192.168.0.0/24  200.33.146.217  reject-with icmp-port-unreachable

uam@DESKTOP-HQFIPG5:~$
```

4- Elimine una de las reglas creadas

```
uam@DESKTOP-HQFIPG5:~$ sudo iptables -D INPUT -p tcp --dport 80 -j DROP
```

5- Muestre las reglas en IPTABLES

```
uam@DESKTOP-HQFIPG5:~$ sudo iptables -D INPUT -p tcp --dport 80 -j DROP
uam@DESKTOP-HQFIPG5:~$ sudo iptables -L -v -n
Chain INPUT (policy DROP 22 packets, 1416 bytes)
num  pkts bytes target     prot opt in     out     source            destination
0    0      0 ACCEPT    0     --    eth1   *          0.0.0.0/0      0.0.0.0/0
56   0      0 ACCEPT    0     --    eth0   *          0.0.0.0/0      0.0.0.0/0
28   0      0 ACCEPT    0     --    lo     *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    17    --    eth1   *          0.0.0.0/0      0.0.0.0/0
0    0      0 DROP      6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 DROP      6     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 DROP      6     --    *      *          200.33.146.217  0.0.0.0/0
0    0      0 ACCEPT    6     --    *      *          0.0.0.0/0      0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target     prot opt in     out     source            destination
0    0      0 ACCEPT    0     --    eth1   eth0       0.0.0.0/0      0.0.0.0/0
0    0      0 ACCEPT    0     --    eth0   eth1       0.0.0.0/0      0.0.0.0/0

Chain OUTPUT (policy ACCEPT 113 packets, 11866 bytes)
num  pkts bytes target     prot opt in     out     source            destination
0    0      0 ACCEPT    0     --    *      *          0.0.0.0/0      0.0.0.0/0
0    0      0 REJECT    0     --    *      *          192.168.0.0/24  200.33.146.217  reject-with icmp-port-unreachable

uam@DESKTOP-HQFIPG5:~$
```

6-Describa que acciones realiza ACCEPT, DROP Y RETURN, en IPTABLES

El ACCEPT nos permite el paso del paquete, cuando una regla tiene el ACCEPT, el paquete es aceptado y se detiene el procesamiento de reglas en esa cadena.

El DROP nos permite descartar el paquete sin enviar ninguna respuesta al emisor, el paquete simplemente se elimina, como si nunca hubiera existido.

El RETURN nos permite detener el procesamiento en la cadena actual y devuelve el control a la cadena que la llamó. Cuando se usa en una cadena personalizada RETURN hace que iptables salga de esa cadena y continúe evaluando reglas en la cadena anterior.