Seguridad en Redes
Practica 3.3

David Antuña Rodríguez
Javier Carrión García

1 Filtrado de paquetes

1.1 Reglas para servidores externos

- Aceptar paquetes reenviados recibidos por la interfaz interno (eth1)

  sudo iptables -A FORWARD -i eth1 -j ACCEPT

- Aceptar paquetes reenviados recibidos por la interfaz externo (eth2) con el puerto destino HTTP o SSH y la dirección IP destino de interno.

  sudo iptables -A FORWARD -i eth2 -p tcp –dport 22 -d 192.168.1.2 -j ACCEPT
  sudo iptables -A FORWARD -i eth2 -p tcp –dport 80 -d 192.168.1.2 -j ACCEPT

- Aceptar paquetes reenviados recibidos por la interfaz externo pertenecientes a conexiones establecidas y relacionadas.

  sudo iptables -A FORWARD -i eth2 -m state –state ESTABLISHED,RELATED -j ACCEPT

- Registrar (LOG) el resto de paquetes reenviados (que serán descartados). Los paquetes descartados quedarán registrados en el fichero /var/log/syslog.

  sudo iptables -N LOGGING
  sudo iptables -A FORWARD -j LOGGING
  sudo iptables -A LOGGING -m limit –limit 2/min -j LOG –log-prefix "Dropped:" –log-level 4
  sudo iptables -A LOGGING -j DROP

¿Se puede hacer el ping desde las dos máquinas?
No, solo desde interno porque aceptamos nuevas conexiones de eth1 en el router y no de eth2. El ping sigue funcionando porque hay un funcionando porque hay una regla que permite conexiones si el estado es established o related.

¿Se pueden hacer las conexiones HTTP y SSH a las dos máquinas?
Tanto en HTTP como en SSH funcionan las conexiones en ambos sentidos.

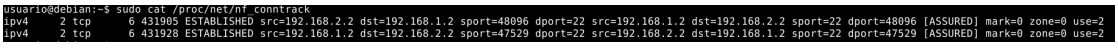

Figure 1.1.1 : Estado de las conexiones.

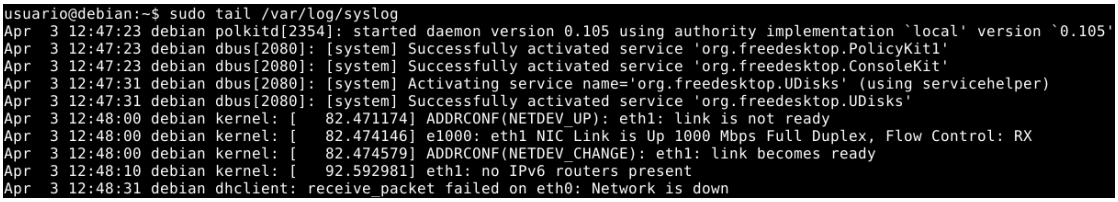

Figure 1.1.2 : Log de la máquina interna.

Figure 1.1.3 : IP tables.

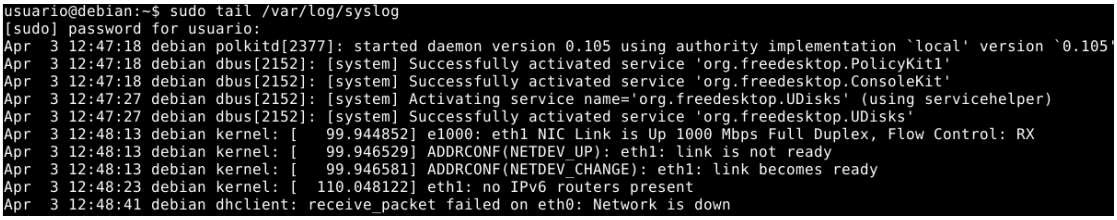

Figure 1.1.4 : Log de la maquina externa.

1.2 Prevención del ataque

Elimina la primera regla de la cadena FORWARD y añade otra regla que acepte paquetes reenviados recibidos por la interfaz interno, pero solo de direcciones origen pertenecientes a la red local (192.168.1.0/24). Insertar esta regla en la posición 1 de la cadena (usar opción –I).

sudo iptables -D FORWARD -i eth1 -j ACCEPT
sudo iptables -I FORWARD 1 -i eth1 -m iprange –src-range 192.168.1.0-192.168.1.255 -j ACCEPT

Figure 1.2.1 : IP tables.

Elimina las reglas de la cadena FORWARD que permiten el paso de paquetes HTTP y SSH por eth2 y añade otras que acepten paquetes reenviados recibidos por la interfaz

externo con puerto destino HTTP o SSH, dirección IP destino de interno y direcciones origen distintas a las de la red local (usa el operador negación !). Insertarlas en las posiciones 2 y 3 de la cadena (usar opción –I).

sudo iptables -D FORWARD -i eth2 -p tcp –dport 80 -d 192.168.1.2 -j ACCEPT
sudo iptables -D FORWARD -i eth2 -p tcp –dport 22 -d 192.168.1.2 -j ACCEPT
sudo iptables -I FORWARD 2 -i eth2 ! -s 192.168.1.0/24 -p tcp –dport http -d 192.168.1.2 -j ACCEPT
sudo iptables -I FORWARD 3 -i eth2 ! -s 192.168.1.0/24 -p tcp –dport ssh -d 192.168.1.2 -j ACCEPT

```
usuario@debian:~$ sudo iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  eth1   any     anywhere             anywhere             source IP range 192.168.1.0-192.168.1.255
    0     0 ACCEPT     tcp  --  eth2   any    !192.168.1.0/24       192.168.1.2          tcp dpt:http
    0     0 ACCEPT     tcp  --  eth2   any    !192.168.1.0/24       192.168.1.2          tcp dpt:ssh
  153 20296 ACCEPT     all  --  eth2   any     anywhere             anywhere             state RELATED,ESTABLISHED
    4   336 LOGGING    all  --  any    any     anywhere             anywhere

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    lo      anywhere             anywhere

Chain LOGGING (1 references)
 pkts bytes target     prot opt in     out     source               destination
    4   336 LOG        all  --  any    any     anywhere             anywhere             limit: avg 2/min burst 5 LOG level warning prefix "Dropped: "
    4   336 DROP       all  --  any    any     anywhere             anywhere
```

Figure 1.2.2 : IP tables.

2 ProxyHTTP

Aceptar paquetes entrantes recibidos por la interfaz interno con puerto destino 8888 (donde escucha el proxy).

sudo iptables -A INPUT -i eth1 -p tcp –dport 8888 -j ACCEPT

Aceptar paquetes salientes enviados por la interfaz externo con puerto destino HTTP.

sudo iptables -A OUTPUT -p tcp –dport http -j ACCEPT

Aceptar paquetes entrantes de conexiones establecidas.

sudo iptables -A INPUT -i eth1 -m state –state ESTABLISHED -j ACCEPT

Aceptar paquetes salientes de conexiones establecidas.

sudo iptables -A OUTPUT -m state –state ESTABLISHED -j ACCEPT

Descartar paquetes reenviados recibidos por la interfaz eth1 con puerto destino HTTP.

sudo iptables -I FORWARD 1 -i eth1 -p tcp –dport http -j DROP

```
usuario@debian:~$ sudo iptables -L -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
  422 33108 ACCEPT     tcp  --  eth1   any     anywhere             anywhere             tcp dpt:8888
    0     0 ACCEPT     tcp  --  eth1   any     anywhere             anywhere             tcp dpt:8888
    0     0 ACCEPT     all  --  eth2   any     anywhere             anywhere             state ESTABLISHED
    0     0 ACCEPT     all  --  eth1   any     anywhere             anywhere             state ESTABLISHED
    0     0 ACCEPT     tcp  --  eth1   any     anywhere             anywhere             tcp dpt:8888
    0     0 ACCEPT     all  --  eth2   any     anywhere             anywhere             state ESTABLISHED
    0     0 ACCEPT     all  --  eth1   any     anywhere             anywhere             state ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    3   180 DROP       tcp  --  eth1   any     anywhere             anywhere             tcp dpt:http
   68  7963 ACCEPT     all  --  eth1   any     anywhere             anywhere             source IP range 192.168.1.0-192.168.1.255
    7   483 ACCEPT     tcp  --  eth2   any    !192.168.1.0/24       192.168.1.2          tcp dpt:http
   71  5180 ACCEPT     tcp  --  eth2   any    !192.168.1.0/24       192.168.1.2          tcp dpt:ssh
  168 23128 ACCEPT     all  --  eth2   any     anywhere             anywhere             state RELATED,ESTABLISHED
    8   672 LOGGING    all  --  any    any     anywhere             anywhere

Chain OUTPUT (policy DROP 18 packets, 1260 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    lo      anywhere             anywhere
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
  333 43092 ACCEPT     all  --  any    any     anywhere             anywhere             state ESTABLISHED
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere             state ESTABLISHED
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere             state ESTABLISHED
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere             state ESTABLISHED

Chain LOGGING (1 references)
 pkts bytes target     prot opt in     out     source               destination
    8   672 LOG        all  --  any    any     anywhere             anywhere             limit: avg 2/min burst 5 LOG level warning prefix "Dropped: "
    8   672 DROP       all  --  any    any     anywhere             anywhere
```

Figure 2.1 : IP tables.

```
usuario@debian:~$ env http_proxy="http://192.168.1.1:8888" wget 192.168.2.2
--2018-04-03 13:47:15--  http://192.168.2.2/
Conectando con 192.168.1.1:8888... conectado.
Petición Proxy enviada, esperando respuesta... 403 Access denied
2018-04-03 13:47:15 ERROR 403: Access denied.

usuario@debian:~$ chromium --proxy-server="http://192.168.1.1:8888"
Gkr-Message: secret service operation failed: The name org.freedesktop.secrets was not provided by any .service files
OpenGL Warning: Failed to connect to host. Make sure 3D acceleration is enabled for this VM.
[2669:2669:0403/134718:ERROR:CONSOLE(0)] "Application Cache Error event: Manifest fetch failed (6) https://www.google.es/_/chrome/newtab/manifest?espv=2&ie=UTF-8", source: https://www.google
.es/_/chrome/newtab?espv=2&ie=UTF-8 (0)
```

Figure 2.2 : Conexión al servidor web.

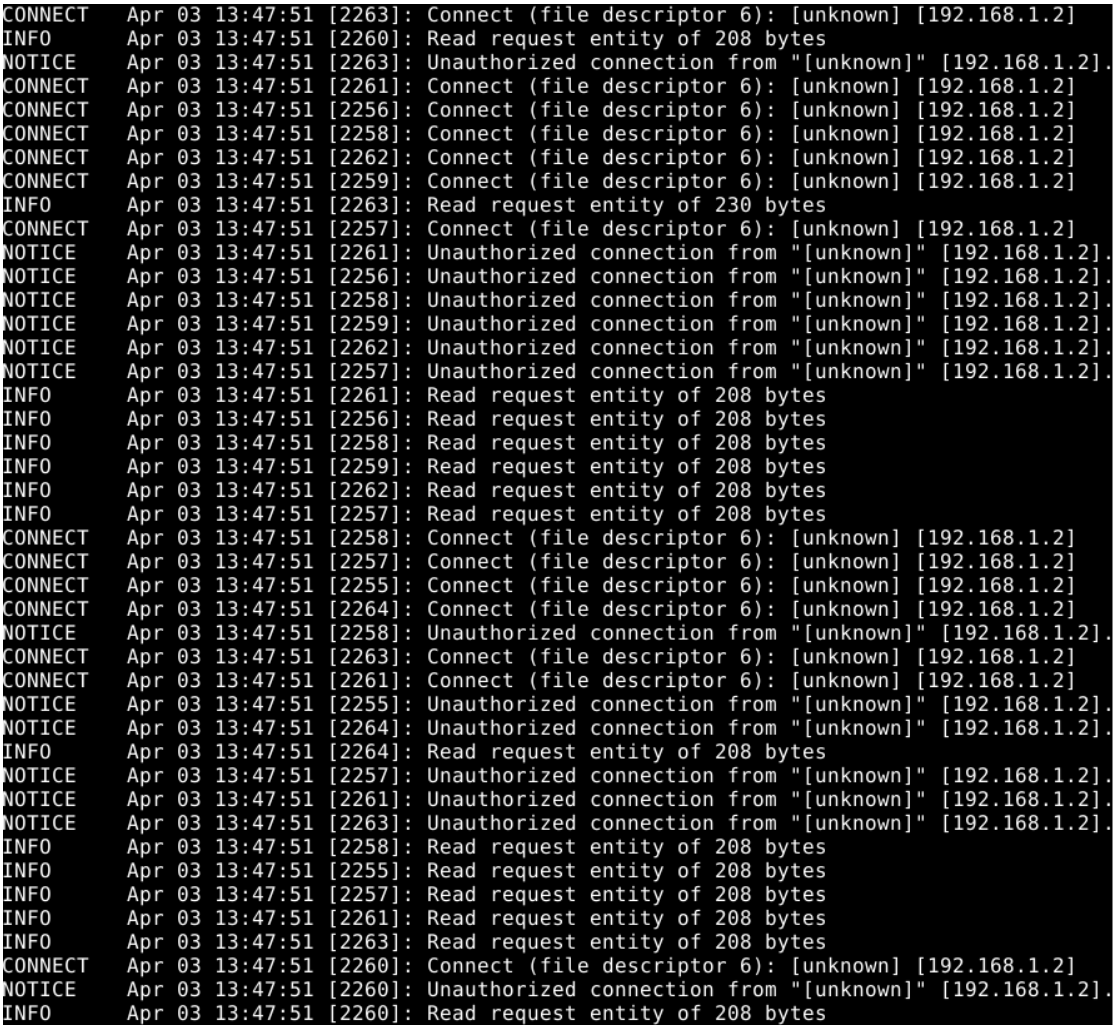

Figure 2.3 : Fichero de registro del router.

No hemos averiguado que regla tenemos mal pero sabemos que al menos una lo está porque la conexión al servidor se rechaza, lo cual está bien, pero la que se hace mediante el proxy también, y no debería.