Seguridad en Redes
Practica 3.2

David Antuña Rodríguez
Javier Carrión García

Las MACS de las máquinas son las siguientes:

- Gateway - 08:00:27:66:bf:ba
- Atacante - 08:00:27:7e:9a:1a
- Víctima - 08:00:27:bb:76:6b
- Externa - 08:00:27:ec:95:27

1 ARP Spoofing

1.1 Ataque 1

El atacante ha modificado la tabla arp de la víctima para que todo el tráfico que esta genere pase por él. El ping no funciona porque el atacante actua de router pero no tiene activada la retransmisión.

```
usuario@debian:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.2.2              ether   08:00:27:ec:95:27   C                     eth2
192.168.1.2              ether   08:00:27:bb:76:6b   C                     eth1
```

Figure 1.1.1 : Tabla ARP del router.

```
usuario@debian:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   08:00:27:7e:9a:1a   C                     eth1
```

Figure 1.1.2 : Tabla ARP de la víctima.

1.2 Ataque 2

El ping sí funciona porque ahora el atacante redirige el tráfico que intercepta, en el wireshark del atacante solo aparecen los echo request porque el ataque es sobre la tabla arp de la víctima y por tanto solo esta manda tráfico al atacante.

```
usuario@debian:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.2.2              ether   08:00:27:ec:95:27   C                     eth2
192.168.1.2              ether   08:00:27:bb:76:6b   C                     eth1
```

Figure 1.2.1 : Tabla ARP del router.

```
usuario@debian:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   08:00:27:7e:9a:1a   C                     eth1
```

Figure 1.2.2 : Tabla ARP de la víctima.

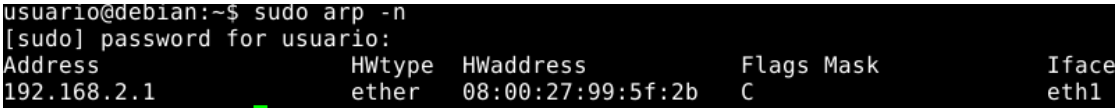

Figure 1.2.3 : Tabla ARP de la máquina externa.

1.3 Ataque 3

Ha cambiado la tabla del router, que ahora también reenvia los paquetes al atacante por lo cual en wireshark podemos ver los echo reply.

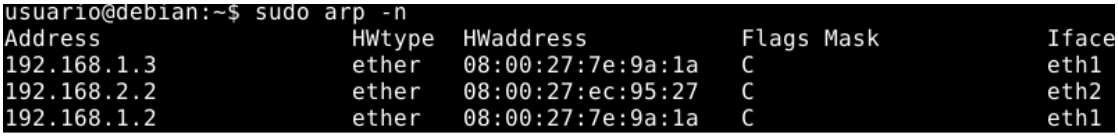

Figure 1.3.1 : Tabla ARP del router.

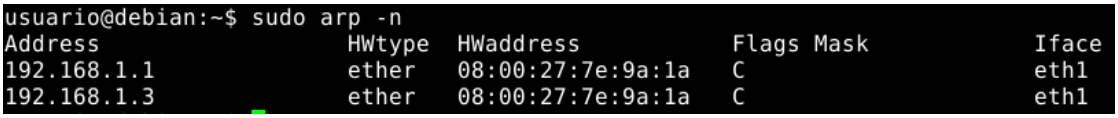

Figure 1.3.2 : Tabla ARP de la víctima.

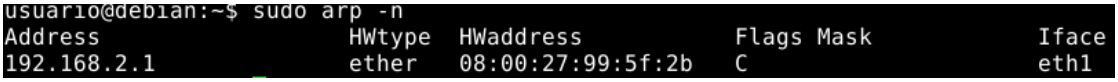

Figure 1.3.3 : Tabla ARP de la máquina externa.

2 Route cache poisoning con redirección ICMP

En las tablas de routa vemos que víctima envia a la red 2 mediante el atacante, en externo habla con víctima via el atacante. En wireshark podemos ver tanto los request como los reply.

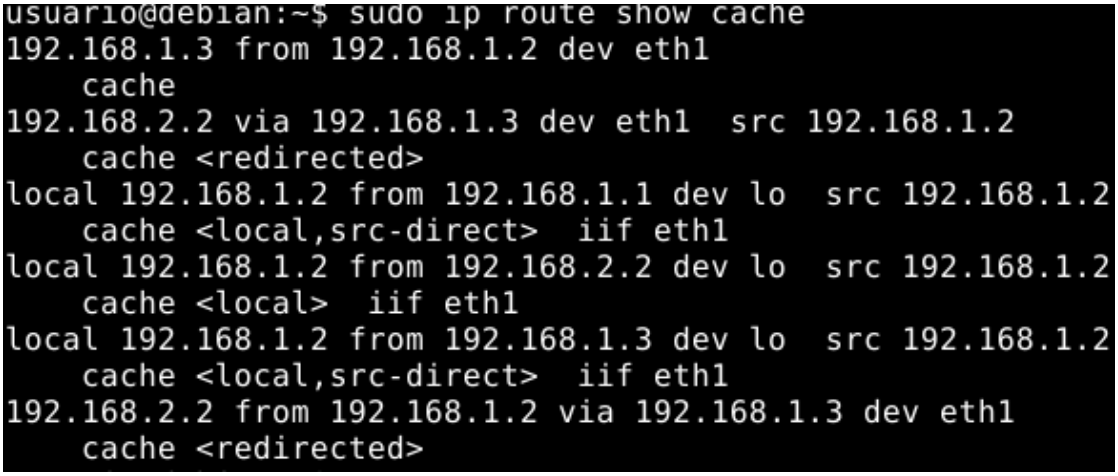

Figure 2.1 : Route cache de la víctima.

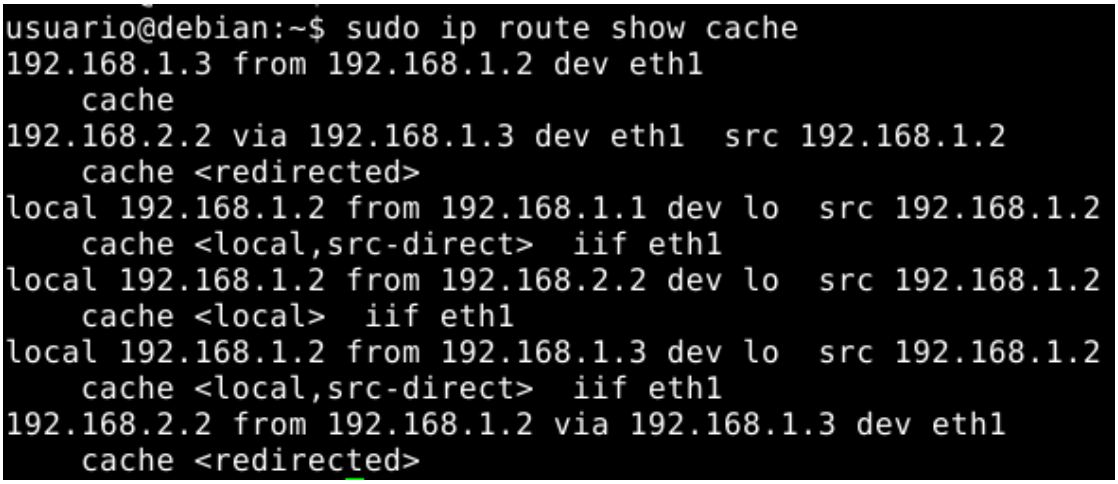

Figure 2.2 : Route cache de la máquina externa.

3 ICMP/Ping flooding

El atacante esta enviado request continuamente a la víctima, para que esta no pueda continuar atendiendo peticiones (ocupando su ancho de banda).

4 Smurf Attack

Ahora esta realizando un broadcast en la red y todas las máquinas le están contestando por lo que esta boqueando la red 1 completa y no solo la máquina víctima.

5 TCP SYN flooding

Este ataque consiste en el envio masivo de paquetes TCP SYN a la víctima con el fin de que la generacion de respuestas por parte de esta la deje fuera de servicio.

5.1 Ataque 1

La máquina víctima sigue funcionando y su cpu no parece sufrir consecuencias, esto se debe a que al no recibir confirmación de su respuesta elimina los paquetes de la cola.

5.2 Ataque 2

A pesar de que recibe mayor número de paquetes tampoco se queda colgada, similar a lo que pasaba en el ataque anterior la máquina elimina las entradas que no reciben confirmación.

5.3 Ataque 3

Este ataque no tiene ningún impacto en la víctima, las ip origen son aleatorias y por tanto la máquina víctima no puede contestar por lo que ignora dichos paquetes.

5.4 Ataque 4

A diferencia de los otros ataques este "cuelga" a la víctima en el estado ACK wait, esto hace que las conexiones no se cierren y por tanto la cpu se inunde, este ataque si consigue inutilizar la máquina.

6 UDP flooding

No pudimos realizar este ataque porque la máquina atacante se colgaba al iniciarlo, pero su funcionamiento es idéntico al de TCP flooding solo cambiando los puertos a los que ataca.