Taller ARP Spoofing

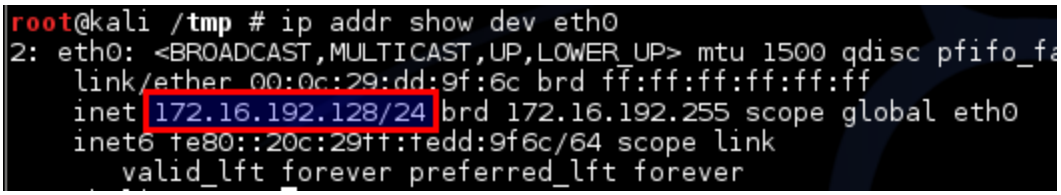
Ricardo Yepes

Objetivo: Envenenar tabla ARP de la víctima sin hacer uso de herramientas de alto nivel (ej: ettercap), sino fabricando paquetes ARP por usted mismo (ej: scapy).

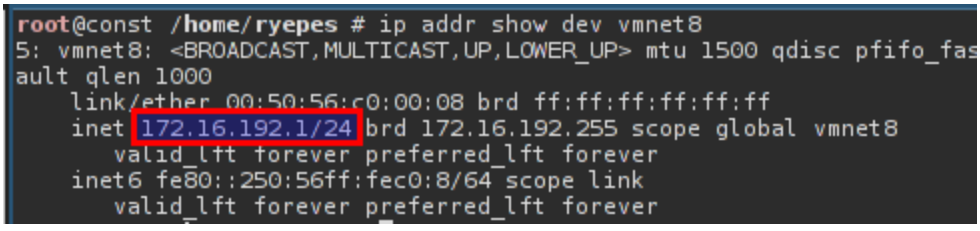
0. Escenario:

Para el ejercicio se requiere contar con dos equipos (En el documento se realizó usando VMware y con los equipos en NAT):

Atacante -Kali 172.16.192.128-: Linux con un sniffer (wireshark, tcpdump, scapy...) y un packet crafter (scapy).



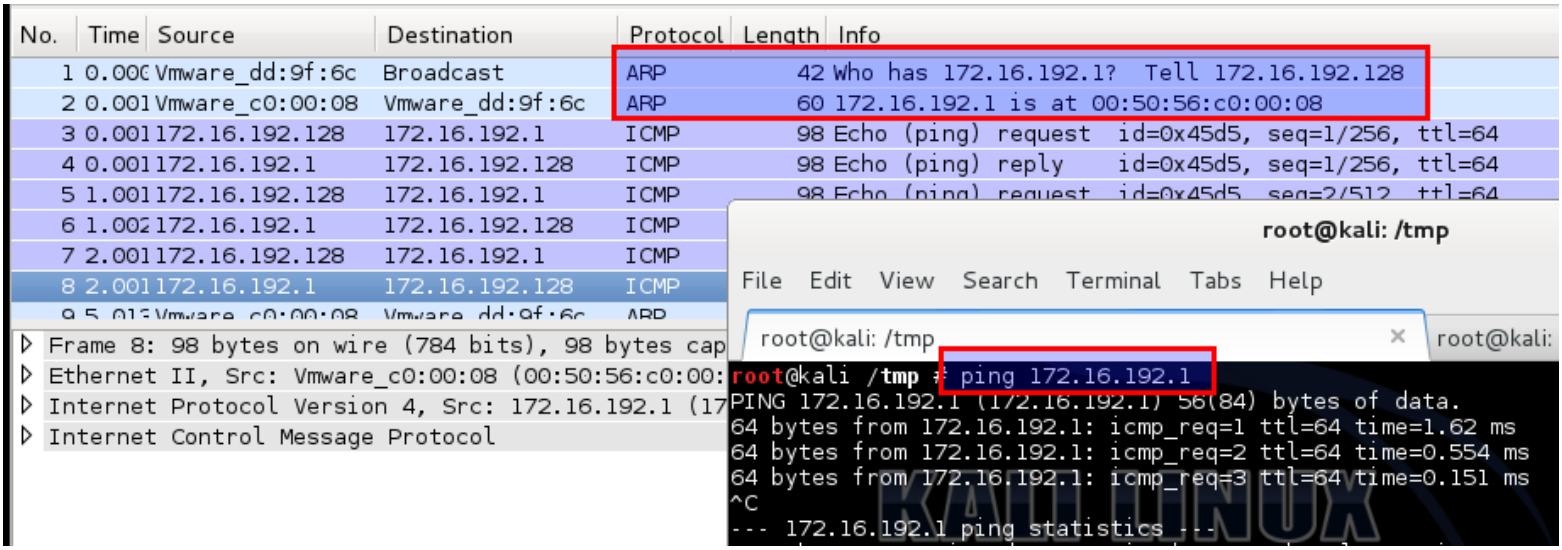
Víctima -Const 172.16.192.1-: Unix-like o Windows.



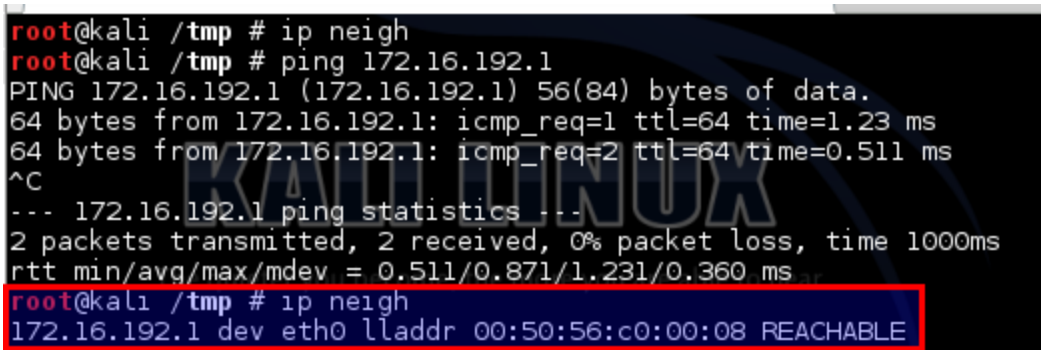
Verifique que no hayan entradas previas relacionadas en las tablas ARP de ambos equipos (**ip neigh**), y de ser necesario elimine las entradas correspondientes (**ip neigh del dev vmnet8 172.16.192.128**).

1. Entendiendo como funciona **ping**

El atacante utiliza el comando *ping* para hacer enviar paquetes ICMP a la víctima. Sin embargo puede comprobarse que previamente se hace un envío de paquete ARP (request) preguntando cuál es la dirección MAC asociada a dicha IP. Esto se debe a que las comunicaciones entre los equipos pertenecientes a una LAN, en realidad se realiza a nivel de capa 2 usando solo direcciones MAC.



El atacante puede verificar que en efecto se ha agregado una nueva entrada en su tabla ARP, gracias a la respuesta enviada por la víctima (ARP replay):



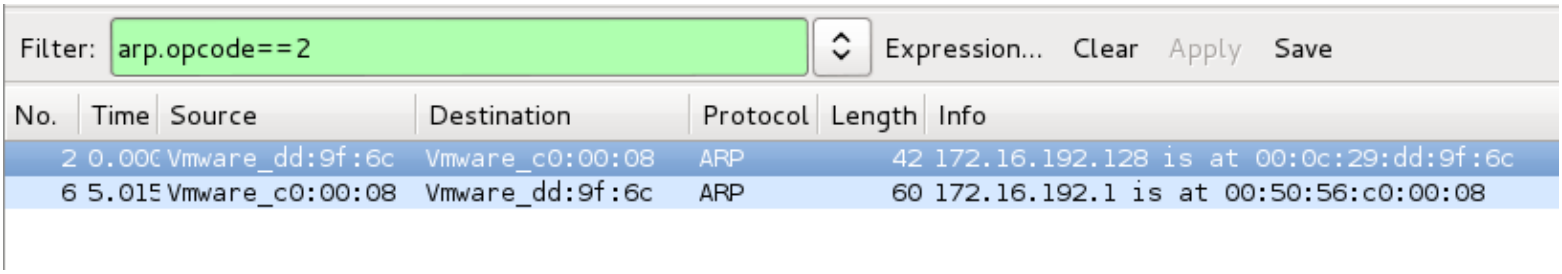
Al observar el listado de paquetes intercambiados, se nota que la víctima también pregunta por la dirección MAC del atacante (¿Por qué llega después de la respuesta ICMP?).

```
4 0.000 172.16.192.1      172.16.192.128    ICMP      98 Echo (ping) reply    id=0x4640, seq=1/256, ttl=64
5 5.010 Vmware_c0:00:08   Vmware_dd:9f:6c   ARP       60 Who has 172.16.192.128?  Tell 172.16.192.1
6 5.010 Vmware_dd:9f:6c   Vmware_c0:00:08   ARP       42 172.16.192.128 is at 00:0c:29:dd:9f:6c
```

Con la respuesta recibida por la víctima, se crea una entrada en su tabla ARP:

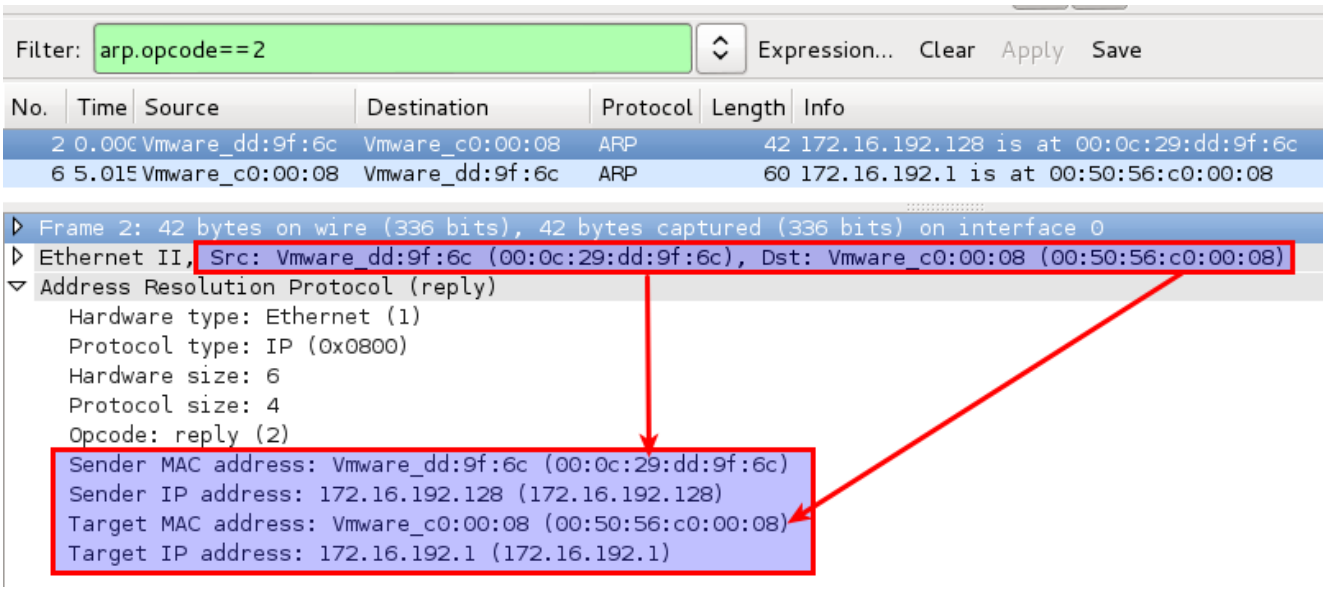
```
root@const /home/ryepes # ip neigh
172.16.192.128 dev vmnet8 lladdr 00:0c:29:dd:9f:6c STALE
192.168.30.51 dev wlan0 lladdr a2:4c:39:39:fa:65 REACHABLE
```

Es ese último paquete ARP de tipo ***is-at*** el que logró modificar la tabla ARP de la víctima. Esos paquetes se identifican por tener el valor 2 en el campo *opcode*, por tanto puede escribirse el siguiente filtro para encontrar solo ese tipo de paquetes: **arp.opcode==2**

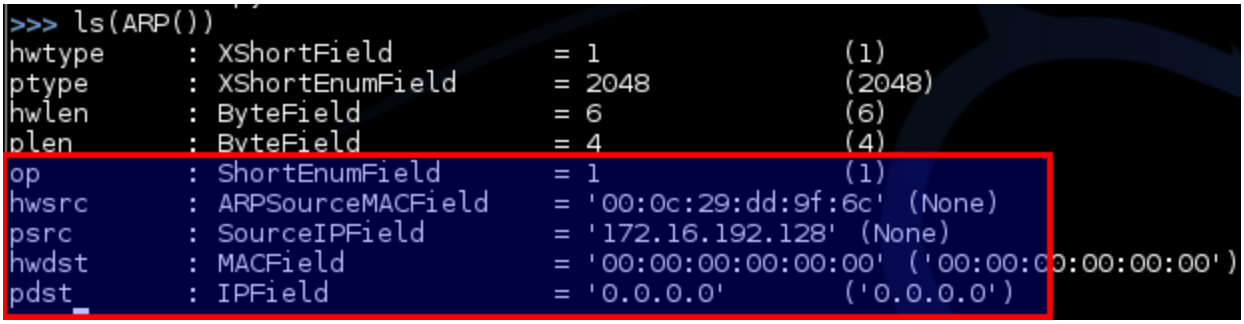


2. Envenenando tabla ARP

Quiere decir entonces que si logramos fabricar un paquete de ese estilo, la víctima creerá la información que estamos enviando. Analizando más de cerca la trama, vemos algunos campos de interés:



La información del *sender* corresponde a quién envía la información (atacante), y el *target* quien la recibe (víctima). En Scapy se asocian a ***src*** y ***dst*** respectivamente, y ***hw*** se refiere a la MAC y ***p*** a la IP.



Es así como el siguiente envío logra ingresar una MAC arbitraria como referencia a la IP del atacante en la tabla ARP de la víctima: