

Análisis de tráfico DHCP y ARP con Wireshark

1. Objetivo. – Analizar el tráfico de red generado por el protocolo DHCP y ARP usando Wireshark para comprender cómo funcionan en la asignación de IP y resolución de direcciones MAC.

2. Herramientas. - Para este laboratorio se utilizaron:

- Oracle VirtualBox.
- Cliente Ubuntu (máquina virtual)
- Wireshark

3. Metodología / Análisis realizado

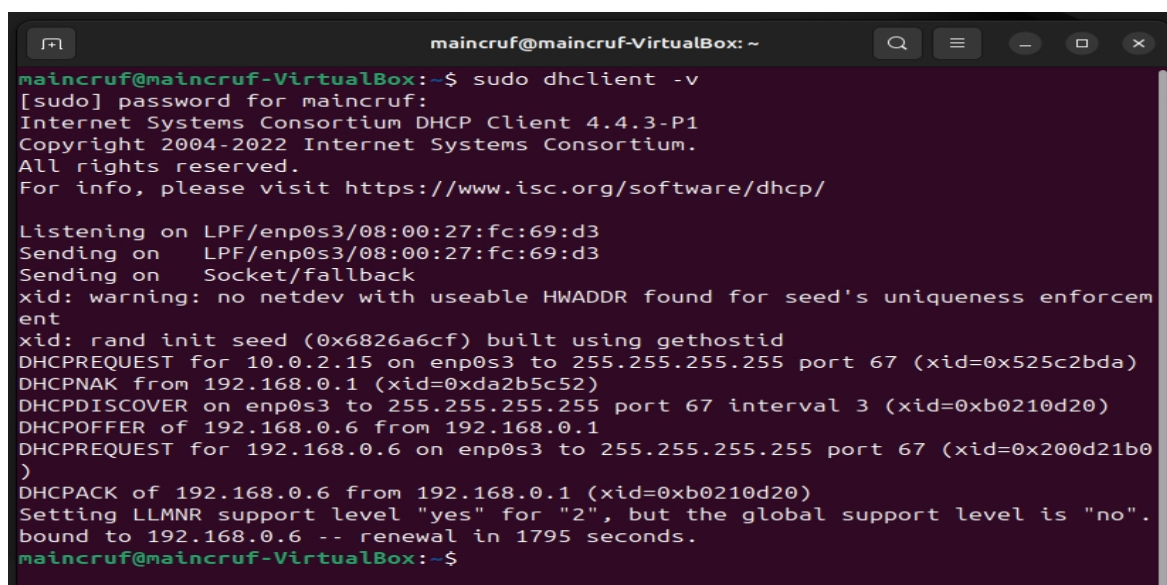
Esta sección describe la detección y análisis realizado sobre los paquetes ARP y DHCP. Todos los comandos utilizados se presentan en el Anexo A (página 4).

3.1 Configuración de red

Se configuró la red para que la máquina virtual Ubuntu se conecte a la red física. Posteriormente, se instaló y configuro Wireshark en la misma interfaz donde se tiene acceso a internet.

3.2 Captura de tráfico DHCP

Se ejecutó un comando para forzar una nueva solicitud DHCP. La salida de este comando muestra las etapas del proceso (DISCOVER, OFFER, PREQUEST, PACK), confirmando la negociación exitosa con el servidor DHCP. (ver Figura 1)



```
maincruf@maincruf-VirtualBox: ~  
maincruf@maincruf-VirtualBox:~$ sudo dhclient -v  
[sudo] password for maincruf:  
Internet Systems Consortium DHCP Client 4.4.3-P1  
Copyright 2004-2022 Internet Systems Consortium.  
All rights reserved.  
For info, please visit https://www.isc.org/software/dhcp/  
  
Listening on LPF/enp0s3/08:00:27:fc:69:d3  
Sending on LPF/enp0s3/08:00:27:fc:69:d3  
Sending on Socket/fallback  
xid: warning: no netdev with useable HWADDR found for seed's uniqueness enforcement  
xid: rand init seed (0x6826a6cf) built using gethostid  
DHCPREQUEST for 10.0.2.15 on enp0s3 to 255.255.255.255 port 67 (xid=0x525c2bda)  
DHCPNAK from 192.168.0.1 (xid=0xda2b5c52)  
DHCPDISCOVER on enp0s3 to 255.255.255.255 port 67 interval 3 (xid=0xb0210d20)  
DHCPPOFFER of 192.168.0.6 from 192.168.0.1  
DHCPREQUEST for 192.168.0.6 on enp0s3 to 255.255.255.255 port 67 (xid=0x200d21b0)  
DHCPACK of 192.168.0.6 from 192.168.0.1 (xid=0xb0210d20)  
Setting LLNMR support level "yes" for "2", but the global support level is "no".  
bound to 192.168.0.6 -- renewal in 1795 seconds.  
maincruf@maincruf-VirtualBox:~$
```

Figura 1. Solicitud DHCP.

Se capturaron los paquetes DHCP correspondiente a la asignación dinámica de IP. Todos los paquetes presentan el mismo Transaction ID (xid), lo que permite correlacionar los mensajes como parte de la misma operación DHCP. (ver Figura 2)

dhcp						
No.	Time	Source	Destination	Protocol	Length	Info
117	37.753115	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xda2b5c52
118	37.771255	192.168.0.1	255.255.255.255	DHCP	590	DHCP NAK - Transaction ID 0xda2b5c52
121	37.921087	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb0210d20
122	37.941091	192.168.0.1	192.168.0.6	DHCP	590	DHCP Offer - Transaction ID 0xb0210d20
123	37.944174	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xb0210d20
124	37.981129	192.168.0.1	192.168.0.6	DHCP	590	DHCP ACK - Transaction ID 0xb0210d20

Figura 2. Captura de paquetes DHCP en Wireshark

Mediante varios comandos, se verificó que la máquina virtual recibió correctamente una dirección IP válida y una ruta por defecto hacia el gateway, confirmando la correcta aplicación de la configuración DHCP. (ver Figura 3)

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:fc:69:d3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.6/24 brd 192.168.0.255 scope global dynamic enp0s3
        valid_lft 2877sec preferred_lft 2877sec
    inet6 ::3cb2:3bd:8971:7228/64 scope global temporary dynamic
        valid_lft 3600sec preferred_lft 3600sec
    inet6 ::a00:27ff:fefc:69d3/64 scope global dynamic mngtmpaddr
        valid_lft 3600sec preferred_lft 3600sec
    inet6 fe80::a00:27ff:fefc:69d3/64 scope link
        valid_lft forever preferred_lft forever
maincruf@maincruf-VirtualBox:~$ ip r
default via 192.168.0.1 dev enp0s3
default via 192.168.0.1 dev enp0s3 proto dhcp src 192.168.0.6 metric 100
192.168.0.0/24 dev enp0s3 proto kernel scope link src 192.168.0.6
192.168.0.0/24 dev enp0s3 proto kernel scope link src 192.168.0.6 metric 100
maincruf@maincruf-VirtualBox:~$
```

Figura 3. Verificación de configuración de red

3.3 Captura de tráfico ARP

Se generó tráfico ARP mediante el comando ping hacia un host de la red local. Antes de enviar los paquetes ICMP, el sistema realizó solicitudes ARP para resolver la dirección MAC correspondiente a la IP destino. Se observaron múltiples mensajes ARP del tipo Who has/is at, comportamiento normal debido a la expiración de caché y anuncios ARP. (Ver figura 4)

arp					
No.	Time	Source	Destination	Protocol	Length Info
3	1.119432	Commscope_e9:ff:cc	PCSSystemtec_fc:69:...	ARP	60 Who has 192.168.0.6? Tell 192.168.0.1
4	1.119992	PCSSystemtec_fc:69:...	Commscope_e9:ff:cc	ARP	60 192.168.0.6 is at 08:00:27:fc:69:d3
125	38.034774	PCSSystemtec_fc:69:...	Broadcast	ARP	60 ARP Announcement for 192.168.0.6
139	40.035446	PCSSystemtec_fc:69:...	Broadcast	ARP	60 ARP Announcement for 192.168.0.6
147	42.215767	PCSSystemtec_fc:69:...	Broadcast	ARP	60 ARP Announcement for 192.168.0.6
152	44.481105	Commscope_e9:ff:cc	ASUSTekCOMPU_6b:4f:...	ARP	60 Who has 192.168.0.5? Tell 192.168.0.1
153	44.481123	ASUSTekCOMPU_6b:4f:...	Commscope_e9:ff:cc	ARP	42 192.168.0.5 is at 4c:ed:fb:6b:4f:e0
164	50.562885	Commscope_e9:ff:cc	PCSSystemtec_fc:69:...	ARP	60 Who has 192.168.0.6? Tell 192.168.0.1
165	50.563516	PCSSystemtec_fc:69:...	Commscope_e9:ff:cc	ARP	60 192.168.0.6 is at 08:00:27:fc:69:d3
295	93.923220	Commscope_e9:ff:cc	ASUSTekCOMPU_6b:4f:...	ARP	60 Who has 192.168.0.5? Tell 192.168.0.1
296	93.923238	ASUSTekCOMPU_6b:4f:...	Commscope_e9:ff:cc	ARP	42 192.168.0.5 is at 4c:ed:fb:6b:4f:e0
339	100.004095	Commscope_e9:ff:cc	PCSSystemtec_fc:69:...	ARP	60 Who has 192.168.0.6? Tell 192.168.0.1
340	100.004688	PCSSystemtec_fc:69:...	Commscope_e9:ff:cc	ARP	60 192.168.0.6 is at 08:00:27:fc:69:d3
874	126.091743	PCSSystemtec_fc:69:...	Commscope_e9:ff:cc	ARP	60 Who has 192.168.0.1? Tell 192.168.0.6
875	126.093342	Commscope_e9:ff:cc	PCSSystemtec_fc:69:...	ARP	60 192.168.0.1 is at 50:75:f1:e9:ff:cc
1069	143.365356	Commscope_e9:ff:cc	ASUSTekCOMPU_6b:4f:...	ARP	60 Who has 192.168.0.5? Tell 192.168.0.1
1070	143.365394	ASUSTekCOMPU_6b:4f:...	Commscope_e9:ff:cc	ARP	42 192.168.0.5 is at 4c:ed:fb:6b:4f:e0
1080	149.446113	Commscope_e9:ff:cc	PCSSystemtec_fc:69:...	ARP	60 Who has 192.168.0.6? Tell 192.168.0.1
1081	149.446807	PCSSystemtec_fc:69:...	Commscope_e9:ff:cc	ARP	60 192.168.0.6 is at 08:00:27:fc:69:d3
1702	192.807478	Commscope_e9:ff:cc	ASUSTekCOMPU_6b:4f:...	ARP	60 Who has 192.168.0.5? Tell 192.168.0.1
1703	192.807496	ASUSTekCOMPU_6b:4f:...	Commscope_e9:ff:cc	ARP	42 192.168.0.5 is at 4c:ed:fb:6b:4f:e0
1963	198.890075	Commscope_e9:ff:cc	PCSSystemtec_fc:69:...	ARP	60 Who has 192.168.0.6? Tell 192.168.0.1
1964	198.890506	PCSSystemtec_fc:69:...	Commscope_e9:ff:cc	ARP	60 192.168.0.6 is at 08:00:27:fc:69:d3
2467	226.257301	PCSSystemtec_fc:69:...	Broadcast	ARP	60 Who has 192.168.0.5? Tell 192.168.0.6
2526	242.249589	Commscope_e9:ff:cc	ASUSTekCOMPU_6b:4f:...	ARP	60 Who has 192.168.0.5? Tell 192.168.0.1
2527	242.249622	ASUSTekCOMPU_6b:4f:...	Commscope_e9:ff:cc	ARP	42 192.168.0.5 is at 4c:ed:fb:6b:4f:e0
2536	248.329888	Commscope_e9:ff:cc	PCSSystemtec_fc:69:...	ARP	60 Who has 192.168.0.6? Tell 192.168.0.1
2537	248.330438	PCSSystemtec_fc:69:...	Commscope_e9:ff:cc	ARP	60 192.168.0.6 is at 08:00:27:fc:69:d3

Figura 4. Paquetes ARP en Wireshark.

4. Resultados obtenidos

En este laboratorio se utilizaron diversos comandos para generar tráfico de los protocolos DHCP y ARP, con el fin de comprender el comportamiento normal de los estos paquetes dentro del tráfico de red.

Como resultado, fue posible identificar los diferentes registros DHCP, observando y comparando el identificador de transacción (XID) de los paquetes, así confirmando la dirección IP que fue asignada dinámicamente a través de la terminal. Además, se identificaron los diferentes paquetes ARP, observando el proceso mediante el cual se resuelve entre direcciones IP y direcciones MAC en un entorno real.

Estas actividades contribuyeron a conocer con mayor profundidad el tráfico de red, y la importancia de estos protocolos en el ámbito de la ciberseguridad, ya que son muy utilizados para ataques como suplantación, envenenamiento ARP y dispositivos no autorizados.

5. Reflexión final

Este laboratorio permitió comprender el flujo real del tráfico en la red y la correcta interpretación de paquetes. El uso de la herramienta Wireshark facilitó la visualización y análisis detallado del tráfico, fortaleciendo las habilidades de monitoreo e investigación, las cuales son fundamentales para mejorar la seguridad en tarea de red.

Anexo A – Comandos Utilizados

`sudo dhclient -v`

`ip a`

`ip r`

`ping 192.168.0.5`