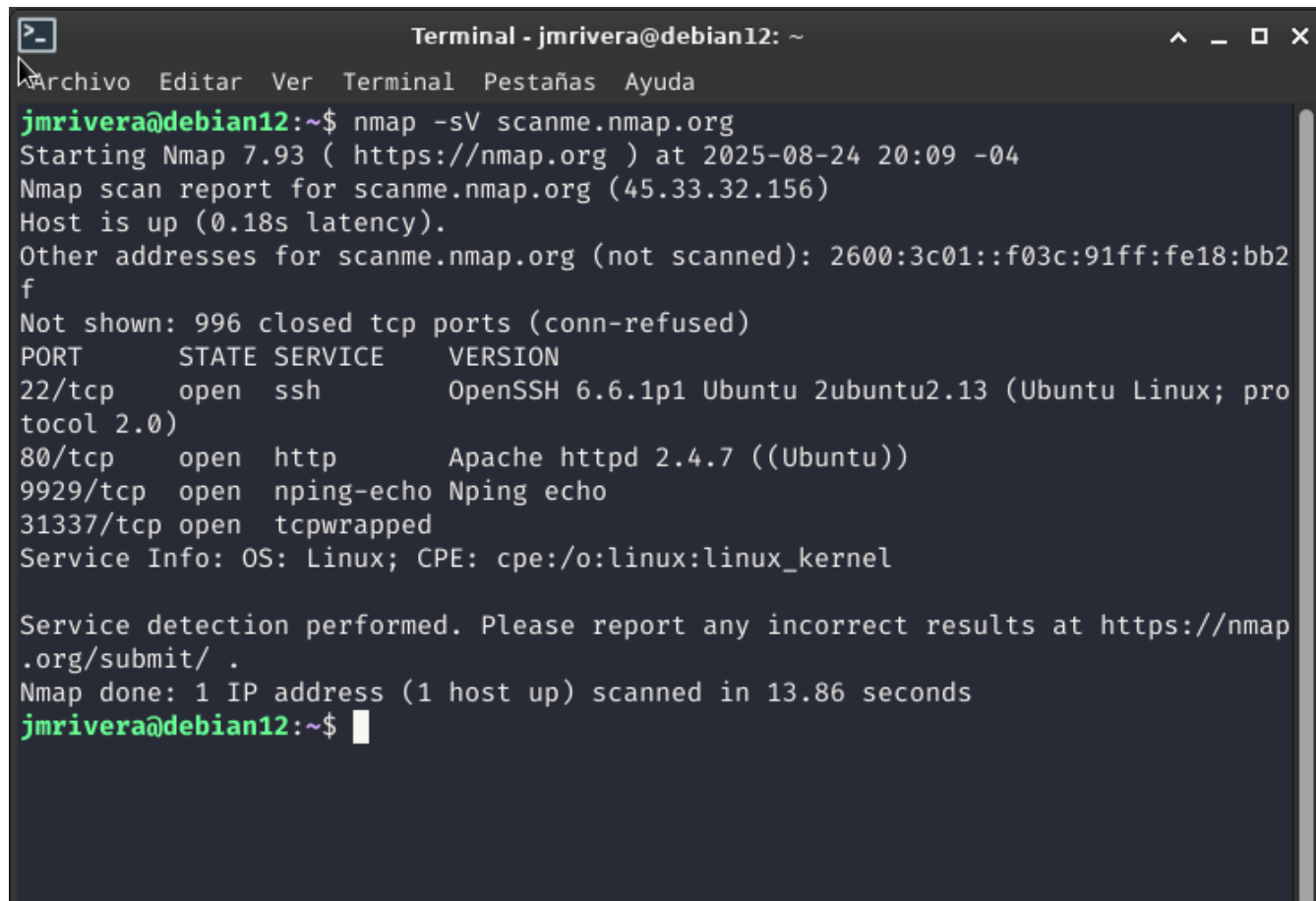


Desafío – análisis de tráfico en red

José Miguel Rivera

Requerimientos

1. Escaneo de Puertos con Nmap (3 Puntos) Ejecuta este comando y documenta los resultados:



```
Terminal - jmriviera@debian12: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
jmriviera@debian12:~$ nmap -sV scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2025-08-24 20:09 -04
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
9929/tcp   open  nping-echo    Nping echo
31337/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.86 seconds
jmriviera@debian12:~$
```

Objetivo: scanme.nmap.org

IP: 45.33.32.156

Puertos abiertos: 4

- 22 **servicio ssh**
- 80 **servicio http**
- 9929 **servicio nping-echo**
- 31337 **servicio tcpwrapped**

Escaneo tardó 0.18s

Se detectó sistema operativo Linux sin especificar que sistema, pero se observan servicios de Ubuntu.

El servidor web es Apache.

2. Análisis de Tráfico ARP (2 Puntos)

Se revisa y verifica el gateway para generar tráfico

```
Terminal - jmriviera@debian12: ~
Archivo Editar Ver Terminal Pestañas Ayuda

jmriviera@debian12:~$ ip route
default via 192.168.100.1 dev wlp2s0 proto dhcp src 192.168.100.17 metric 600
169.254.0.0/16 dev wlp2s0 scope link metric 1000
192.168.100.0/24 dev wlp2s0 proto kernel scope link src 192.168.100.17 metric 600
jmriviera@debian12:~$
```

Se verifica tráfico en wireshark (a través de kali linux)

The screenshot shows a Kali Linux terminal on the left and the Wireshark network protocol analyzer on the right. The terminal displays the output of the `ip route` command, showing the default gateway as `192.168.100.1` via `wlp2s0`. It also shows the output of `ping -c 4 192.168.100.1`, indicating successful connectivity. The `ip link show` command is also run, showing the state of the `eth0` interface. The Wireshark interface on the right shows a capture on the `eth0` interface. The packet list pane shows several ARP requests and announcements. The packet details pane for packet 74 shows an ARP request from `Intel_35:57:05` to `HuaweiTechno_ab:90:...`. The packet bytes pane shows the raw data of the ARP request.

This screenshot shows a closer view of the Wireshark interface. The packet list pane shows several ARP requests and announcements. The packet details pane for packet 74 shows an ARP request from `Intel_35:57:05` to `HuaweiTechno_ab:90:...`. The packet bytes pane shows the raw data of the ARP request.

dirección MAC: 5c:e0:c5:35:57:05

dirección IP: 192.168.100.17

Si hay muchos ARP request para la ip 192.168.100.17 se confirma que la MAC address indicada en el escaneo corresponde al dispositivo.

**** verificación:**

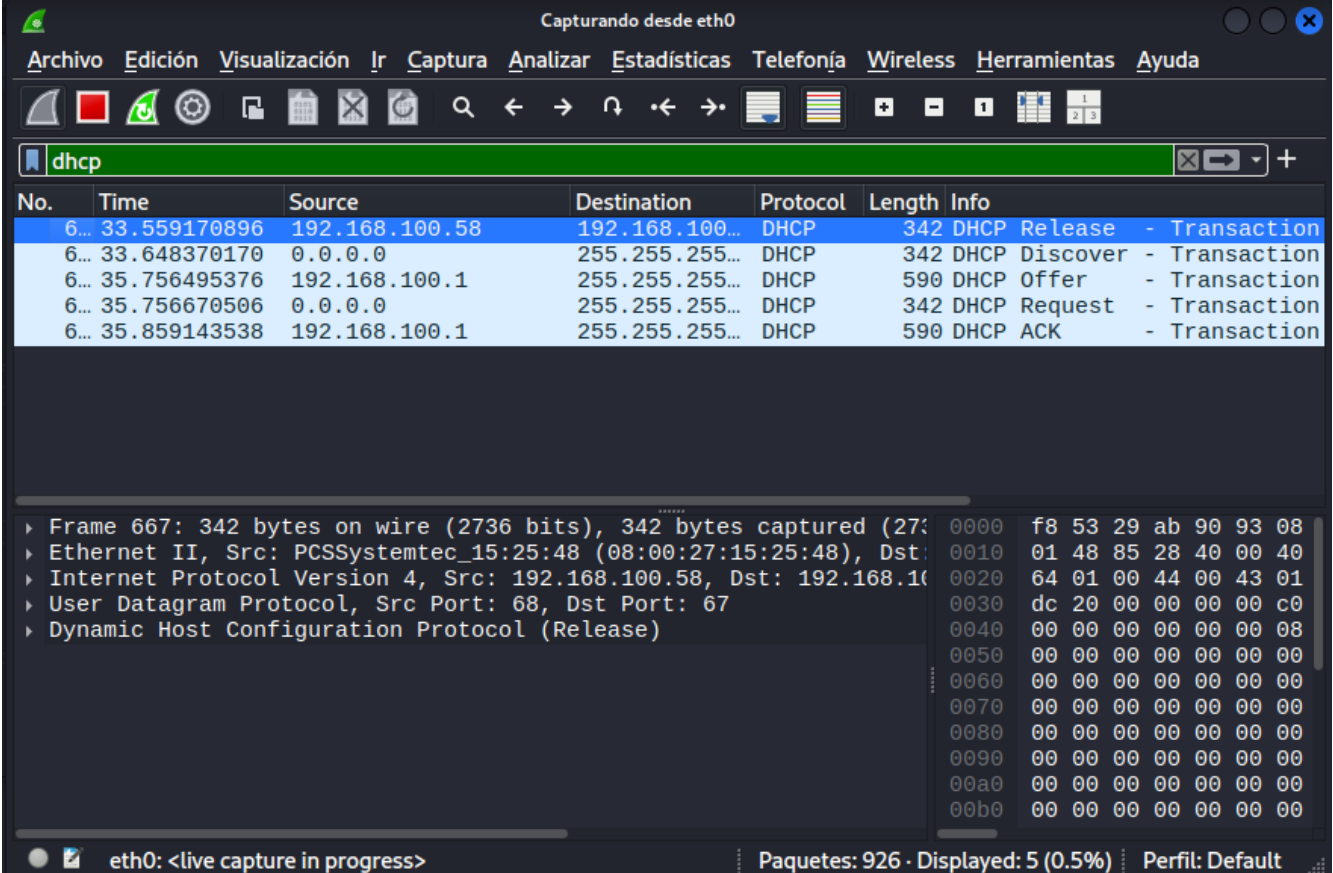
```
Terminal - jmriviera@debian12: ~
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
jmriviera@debian12:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT
   group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eno1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN
   mode DEFAULT group default qlen 1000
    link/ether 34:e6:d7:7e:ae:0e brd ff:ff:ff:ff:ff:ff
    altname enp0s25
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode
   DORMANT group default qlen 1000
    link/ether 5c:e0:c5:35:57:05 brd ff:ff:ff:ff:ff:ff
jmriviera@debian12:~$ ip route
default via 192.168.100.1 dev wlp2s0 proto dhcp src 192.168.100.17 metric 600
169.254.0.0/16 dev wlp2s0 scope link metric 1000
192.168.100.0/24 dev wlp2s0 proto kernel scope link src 192.168.100.17 metric 600
jmriviera@debian12:~$
```

3. Análisis de Tráfico DHCP (3 Puntos)

Se ejecuta comando en consola linux y se aplica filtro dhcp en wireshark

sudo dhclient -r eth0 && sudo dhclient eth0

nota: previamente se debió ejecutar “sudo apt install isc-dhcp-client”



Capturando desde eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
6...	33.559170896	192.168.100.58	192.168.100...	DHCP	342	DHCP Release - Transaction
6...	33.648370170	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction
6...	35.756495376	192.168.100.1	255.255.255...	DHCP	590	DHCP Offer - Transaction
6...	35.756670506	0.0.0.0	255.255.255...	DHCP	342	DHCP Request - Transaction
6...	35.859143538	192.168.100.1	255.255.255...	DHCP	590	DHCP ACK - Transaction

Frame 667: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on eth0

Ethernet II, Src: PCSSystemtec_15:25:48 (08:00:27:15:25:48), Dst: 01:00:5e:00:00:00

Internet Protocol Version 4, Src: 192.168.100.58, Dst: 192.168.100.1

User Datagram Protocol, Src Port: 68, Dst Port: 67

Dynamic Host Configuration Protocol (Release)

eth0: <live capture in progress> Paquetes: 926 · Displayed: 5 (0.5%) Perfil: Default

Se observa los tipos de mensaje DHCP:

Release: Para liberar la IP ocupada en el momento, 192.168.100.58

Discover: Para buscar una IP en el servidor

Offer: El servidor ofrecerá una IP de acuerdo a su solicitud

Request: Se acepta la dirección IP ofrecida

ACK: Se asignó la IP 60

4. Análisis de Tráfico HTTPS (2 Puntos)

Se ejecuta el comando `curl -v https://github.com`

Capturando desde eth0

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
341	12.197144070	20.201.28.151	192.168.100.60	TCP	66	443 →
342	12.197144115	20.201.28.151	192.168.100.60	TLSv1.3	90	Applic
343	12.197195147	192.168.100.60	20.201.28.151	TCP	54	34274
344	12.197445131	20.201.28.151	192.168.100.60	TCP	66	443 →
345	12.197457716	192.168.100.60	20.201.28.151	TCP	54	34274
346	12.197681836	20.201.28.151	192.168.100.60	TCP	66	443 →
347	12.197692152	192.168.100.60	20.201.28.151	TCP	54	34274
349	12.992257674	172.67.175.45	192.168.100.17	TLSv1.2	126	Applic
350	12.992258122	192.168.100.17	172.67.175.45	TCP	66	55808
356	15.988281131	172.67.175.45	192.168.100.17	TLSv1.2	126	Applic
357	15.988281536	192.168.100.17	172.67.175.45	TCP	66	55808

Frame 4: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface eth0

Ethernet II, Src: HuaweiTechno_ab:90:93 (f8:53:29:ab:90:93), Dst: 192.168.100.17

Internet Protocol Version 4, Src: 172.67.175.45, Dst: 192.168.100.17

Transmission Control Protocol, Src Port: 443, Dst Port: 55808, Seq: 34274, Win: 0, Len: 0

Transport Layer Security

eth0: <live capture in progress> Paquetes: 403 · Displayed: 353 (87.6%) Perfil: Default

** Se observa que el origen es la ip que dejó el dhcp del punto anterior.

La versión de TLS es la 1.3

Se negoció un paquete.