

Nmap for Pentester

HOST

DISCOVERY



Contenido

Introducción	3
Barrido de ping	3
Desactivar arp-ping	5
IP de envío.....	6
Banderas TCP	7
Tipos de exploraciones.....	8
Escaneo de ping TCP SYN	8
Escaneo de ping TCP ACK	10
Escaneo de ping de eco ICMP	11
Barrido de ping ICMP ECHO	12
Escaneo de máscara de dirección ICMP	13
Escaneo de marca de tiempo ICMP ECHO	13
Escaneo de ping UDP	13
Escaneo de ping del protocolo IP	15
Sin escaneo de ping	dieciséis
Escaneo de ping ARP	dieciséis
Ping de INIT SCTP	17
Trazado de ruta	18

Introducción

Nmap se ha convertido en una de las herramientas más populares en el escaneo de redes, dejando atrás a otros escáneres. Muchas veces, los hosts de algunas organizaciones están protegidos mediante firewalls o sistemas de prevención de intrusiones que provocan fallos en el escaneo debido al conjunto actual de reglas que se utilizan para bloquear el tráfico de la red. En Nmap, un pentester puede utilizar fácilmente técnicas alternativas de descubrimiento de host para evitar que esto suceda. Consta de ciertas características que hacen que el tráfico de la red sea un poco menos sospechoso. Por lo tanto, veamos varias técnicas de Host Discovery.

Barrido de ping

Comencemos escaneando toda la red usando el escaneo de barrido de Ping (-sP).

```
mapa n -sP 192.168.1.0/24
```

```
root@kali:~# nmap -sP 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:43 EST
Nmap scan report for dsldevice.lan (192.168.1.1)
Host is up (0.0012s latency).
MAC Address: 18:45:93:69:A5:10 (Taicang T&W Electronics)
Nmap scan report for 192.168.1.3
Host is up (0.00030s latency).
MAC Address: 8C:EC:4B:71:C5:DE (Dell)
Nmap scan report for 192.168.1.4
Host is up (0.024s latency).
MAC Address: 2A:84:98:9F:E5:5E (Unknown)
Nmap scan report for 192.168.1.5
Host is up (0.012s latency).
MAC Address: 30:24:32:1F:89:AC (Intel Corporate)
Nmap scan report for 192.168.1.8
Host is up (0.0058s latency).
MAC Address: 44:CB:8B:C2:20:DA (LG Innotek)
Nmap scan report for 192.168.1.12
Host is up (0.00027s latency).
MAC Address: 00:0C:29:78:20:90 (VMware)
Nmap scan report for 192.168.1.108
Host is up (0.00017s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap scan report for 192.168.1.9
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 23.67 seconds
root@kali:~#
```

Cuando observa de cerca los paquetes en Wireshark, verá que aquí solo se envían paquetes ARP mientras se escanea la red.

No.	Time	Source	Destination	Protocol	Length	Info
64	0.550463087	TaicangT_69:a5...	Dell_71:c5:de	ARP	60	Who has 192.168.1.3? Tell 192.168.1.1
65	0.550463118	Dell_71:c5:de	TaicangT_69:a5:10	ARP	60	192.168.1.3 is at 8c:ec:4b:71:c5:de
209	1.589157998	TaicangT_69:a5...	VMware_b2:bb:77	ARP	60	Who has 192.168.1.9? Tell 192.168.1.1
210	1.589181561	VMware_b2:bb:77	TaicangT_69:a5:10	ARP	42	192.168.1.9 is at 00:0c:29:b2:bb:77
228	1.974212283	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.9
229	1.974288490	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.9
230	1.974336247	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.3? Tell 192.168.1.9
231	1.974396043	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.4? Tell 192.168.1.9
232	1.974433312	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.5? Tell 192.168.1.9
233	1.974456184	Dell_71:c5:de	VMware_b2:bb:77	ARP	60	192.168.1.3 is at 8c:ec:4b:71:c5:de
234	1.974463392	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.6? Tell 192.168.1.9
235	1.974494541	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.7? Tell 192.168.1.9
236	1.974541930	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.8? Tell 192.168.1.9
237	1.974575204	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.10? Tell 192.168.1.9
238	1.974604008	VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.11? Tell 192.168.1.9

▶ Frame 64: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: TaicangT_69:a5:10 (18:45:93:69:a5:10), Dst: Dell_71:c5:de (8c:ec:4b:71:c5:de)
 ▶ Address Resolution Protocol (request)

```

0000  8c ec 4b 71 c5 de 18 45 93 69 a5 10 08 06 00 01  ..Kq...E .i.....
0010  08 00 06 04 00 01 18 45 93 69 a5 10 c0 a8 01 01  ....E .i.....
0020  00 00 00 00 00 00 c0 a8 01 03 00 00 00 00 00 00  ....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....

```

Nota: El funcionamiento de -sP y -sn es el mismo.

Intentemos lo mismo usando la opción sin escaneo de puertos (-sn) . En esta opción, también utilizamos la opción --packet-trace que le permitirá ver la transferencia de paquetes detallada sin utilizar Wireshark.

Aquí puede observar los paquetes ARP que se reciben.

```
nmap -sn 192.168.1.0/24 --rastreo de paquetes
```

```

root@kali:~# nmap -sn 192.168.1.0/24 --packet-trace
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:48 EST
SENT (0.0687s) ARP who-has 192.168.1.1 tell 192.168.1.9
SENT (0.0688s) ARP who-has 192.168.1.2 tell 192.168.1.9
SENT (0.0689s) ARP who-has 192.168.1.3 tell 192.168.1.9
SENT (0.0690s) ARP who-has 192.168.1.4 tell 192.168.1.9
SENT (0.0691s) ARP who-has 192.168.1.5 tell 192.168.1.9
SENT (0.0692s) ARP who-has 192.168.1.6 tell 192.168.1.9
SENT (0.0692s) ARP who-has 192.168.1.7 tell 192.168.1.9
SENT (0.0693s) ARP who-has 192.168.1.8 tell 192.168.1.9
SENT (0.0694s) ARP who-has 192.168.1.10 tell 192.168.1.9
SENT (0.0695s) ARP who-has 192.168.1.11 tell 192.168.1.9
RCVD (0.0690s) ARP reply 192.168.1.3 is-at 8C:EC:4B:71:C5:DE
RCVD (0.0699s) ARP reply 192.168.1.1 is-at 18:45:93:69:A5:10
SENT (0.0730s) ARP who-has 192.168.1.14 tell 192.168.1.9
SENT (0.0731s) ARP who-has 192.168.1.15 tell 192.168.1.9
SENT (0.0731s) ARP who-has 192.168.1.16 tell 192.168.1.9
SENT (0.0732s) ARP who-has 192.168.1.17 tell 192.168.1.9
RCVD (0.0791s) ARP reply 192.168.1.4 is-at 2A:84:98:9F:E5:5E
RCVD (0.0796s) ARP reply 192.168.1.5 is-at 30:24:32:1F:89:AC
SENT (0.0820s) ARP who-has 192.168.1.20 tell 192.168.1.9
SENT (0.0822s) ARP who-has 192.168.1.21 tell 192.168.1.9
SENT (0.0823s) ARP who-has 192.168.1.22 tell 192.168.1.9
SENT (0.0824s) ARP who-has 192.168.1.23 tell 192.168.1.9
SENT (0.1699s) ARP who-has 192.168.1.26 tell 192.168.1.9
SENT (0.1703s) ARP who-has 192.168.1.27 tell 192.168.1.9
SENT (0.1705s) ARP who-has 192.168.1.28 tell 192.168.1.9
SENT (0.1708s) ARP who-has 192.168.1.29 tell 192.168.1.9
SENT (0.1710s) ARP who-has 192.168.1.30 tell 192.168.1.9
SENT (0.1712s) ARP who-has 192.168.1.31 tell 192.168.1.9

```

Ahora que hemos determinado que los paquetes ARP están presentes en la red, usaremos el comando `-disable-arp-ping` opción, que muestra que se están enviando cuatro paquetes.

Desactivar-arp-ping

Para deshabilitar el descubrimiento de ARP, Nmap proporciona esta opción.

```
nmap -sn 192.168.1.108 --disable-arp-ping
```

```

root@kali:~# nmap -sn 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:58 EST
Nmap scan report for 192.168.1.108
Host is up (0.00027s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~#

```

Y verás que los paquetes ARP no son visibles.

Nota: Al escanear redes locales con Nmap se envía un paquete ARP con cada escaneo. Si se va a escanear una red externa; Nmap envía los siguientes paquetes de solicitud cuando se utiliza `-disable-arp-ping`:

ICMP echo request (Type 8)

ICMP timestamp request(Type 13)

TCP SYN to port 443

TCP ACK to port 80

Wireshark packet capture showing network traffic between 192.168.1.9 and 192.168.1.108. The capture includes an ICMP echo request, a TCP SYN packet, an ICMP timestamp request, a TCP ACK packet, and an ICMP echo reply. A red box highlights the ICMP echo request packet (No. 42).

No	Time	Source	Destination	Protocol	Length	Info
42	...	192.168.1.9	192.168.1.108	ICMP	42	Echo (ping) request id=0x3b18, seq=0/0, ttl=57 (req)
43	...	192.168.1.9	192.168.1.108	TCP	58	43181 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
44	...	192.168.1.9	192.168.1.108	TCP	54	43181 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
45	...	192.168.1.9	192.168.1.108	ICMP	54	Timestamp request id=0x4674, seq=0/0, ttl=44
46	...	192.168.1.108	192.168.1.9	ICMP	60	Echo (ping) reply id=0x3b18, seq=0/0, ttl=64 (req)
47	...	192.168.1.108	192.168.1.9	TCP	60	443 → 43181 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
48	...	192.168.1.108	192.168.1.9	TCP	60	80 → 43181 [RST] Seq=1 Win=0 Len=0
49	...	192.168.1.108	192.168.1.9	ICMP	60	Timestamp reply id=0x4674, seq=0/0, ttl=64

Frame 794: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0

- Ethernet II, Src: VMware_b2:bb:77 (00:0c:29:b2:bb:77), Dst: VMware_c8:9c:50 (00:0c:29:c8:9c:50)
- Internet Protocol Version 4, Src: 192.168.1.9, Dst: 192.168.1.108
- Internet Control Message Protocol

0000 00 0c 29 c8 9c 50 00 0c 29 b2 bb 77 08 00 45 00 ...P...)..w..E..

0010 00 1c 6c b8 00 00 39 01 91 63 c0 a8 01 09 c0 a8 ...1...9...c.....

0020 01 6c 08 00 bc e7 3b 18 00 00 ...1....:..

También puede utilizar la opción `-send-ip` para obtener los mismos resultados que en el paso anterior.

enviar-ip

```
nmap -sn 192.168.1.108 --packet-trace --send-ip
```



```

root@kali:~# nmap -sn 192.168.1.108 --packet-trace --send-ip
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 05:55 EST
SENT (0.0588s) ICMP [192.168.1.9 > 192.168.1.108 Echo request (type=8/code=0) id=297
SENT (0.0589s) TCP 192.168.1.9:43573 > 192.168.1.108:443 S ttl=58 id=30850 iplen=44
SENT (0.0589s) TCP 192.168.1.9:43573 > 192.168.1.108:80 A ttl=55 id=52947 iplen=40
SENT (0.0590s) ICMP [192.168.1.9 > 192.168.1.108 Timestamp request (type=13/code=0)
RCVD (0.0590s) ICMP [192.168.1.108 > 192.168.1.9 Echo reply (type=0/code=0) id=2974
NSOCK INFO [0.1030s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1030s] nsock_connect_udp(): UDP connection requested to 192.168.1.1:53
NSOCK INFO [0.1030s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeou
NSOCK INFO [0.1030s] nsock_write(): Write request for 44 bytes to IOD #1 EID 27 [192
NSOCK INFO [0.1030s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for E
NSOCK INFO [0.1030s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID
NSOCK INFO [0.1090s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID
NSOCK INFO [0.1090s] nsock_read(): Read request from IOD #1 [192.168.1.1:53] (timeou
NSOCK INFO [0.1090s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1090s] nevent_delete(): nevent_delete on event #34 (type READ)
Nmap scan report for 192.168.1.108
Host is up (0.00024s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

```

Host Discovery es el primer paso para recopilar información y proporciona resultados precisos sobre puertos activos y direcciones IP en una red.

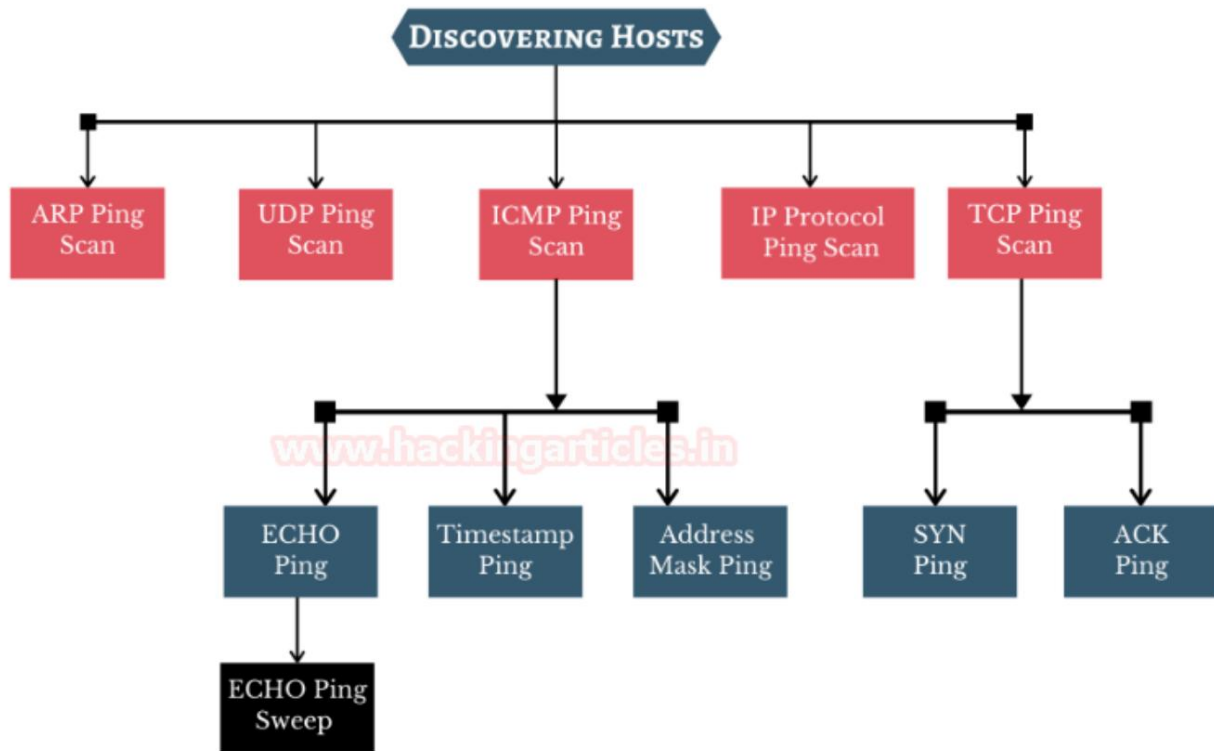
Banderas TCP

Primero, conozcamos los conceptos básicos de los indicadores de comunicación en TCP. El encabezado TCP consta principalmente de seis indicadores que gestionan la conexión entre los sistemas y les proporcionan instrucciones. Por lo tanto, cada indicador es de 1 bit y, por lo tanto, el tamaño de los indicadores TCP es de 6 bits. Ahora comprendamos brevemente cada bandera.

FLAG	DESCRIPTION
SYN	It stands for Synchronize. It assists in notifying when a new sequence number is transmitted. The SYN flag usually represents the Three-Way Handshake.
ACK	It stands for Acknowledgement. It notifies the status of transmission of packets and also assists in identifying the what sequence number to expect next.
RST	It stands for Reset. This flag shows when there is any error in that connection and sets the flag to 1 and the connection is broken.
URG	It stands for Urgent. This flag usually commands to process the packets as soon as possible.
FIN	It stands for Finish. This flag is set as 1 to indicate no further transmission of packets.
PSH	It stands for Push. It is used to start and end data transfer and prevent occurrence of buffer deadlocks.

Tipos de exploraciones

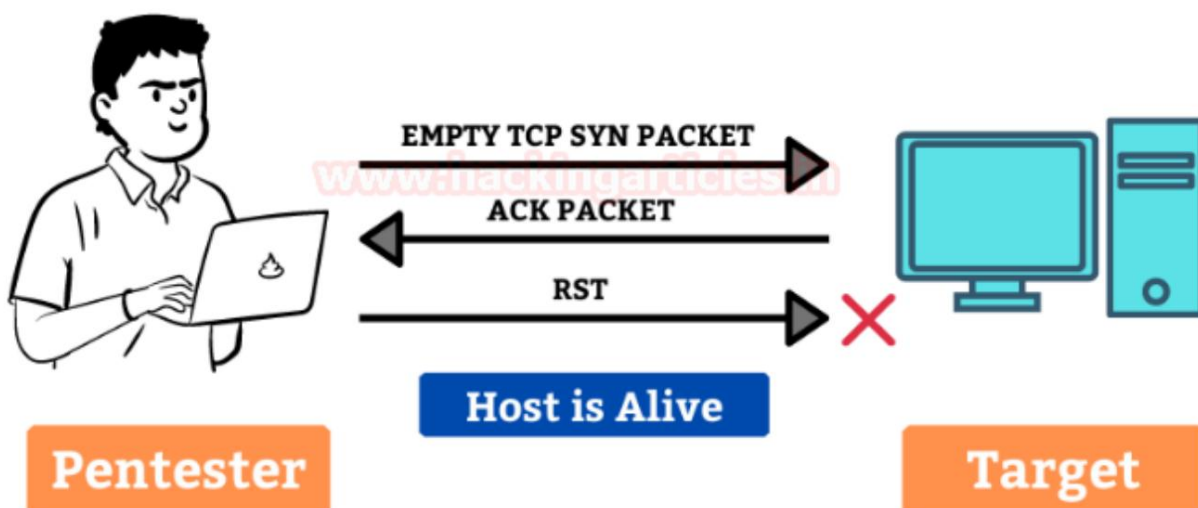
Para descubrir los hosts en la red, se pueden utilizar varios métodos de escaneo de ping.



Escaneo de ping TCP SYN

Es un método de descubrimiento de host que ayuda a descubrir si los puertos están abiertos y también a asegurarse de que coincidan con las reglas del firewall. Por lo tanto, el pentester puede enviar un indicador SYN vacío al objetivo para comprobar si está vivo. Se pueden definir varios puertos en este tipo de escaneo.

TCP SYN PING SCAN



El comando `-sP` en Nmap solo permite descubrir hosts en línea. Mientras que SYN Ping (`-PS`) envía un paquete TCP SYN a los puertos y, si están cerrados, el host responde con un paquete RST. Y si los puertos solicitados están abiertos, habrá una respuesta de TCP SYN/ACK y se enviará un paquete de reinicio para restablecer la conexión.

```
nmap -sn -PS 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PS 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 07:13 EST
Nmap scan report for 192.168.1.108
Host is up (0.00030s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

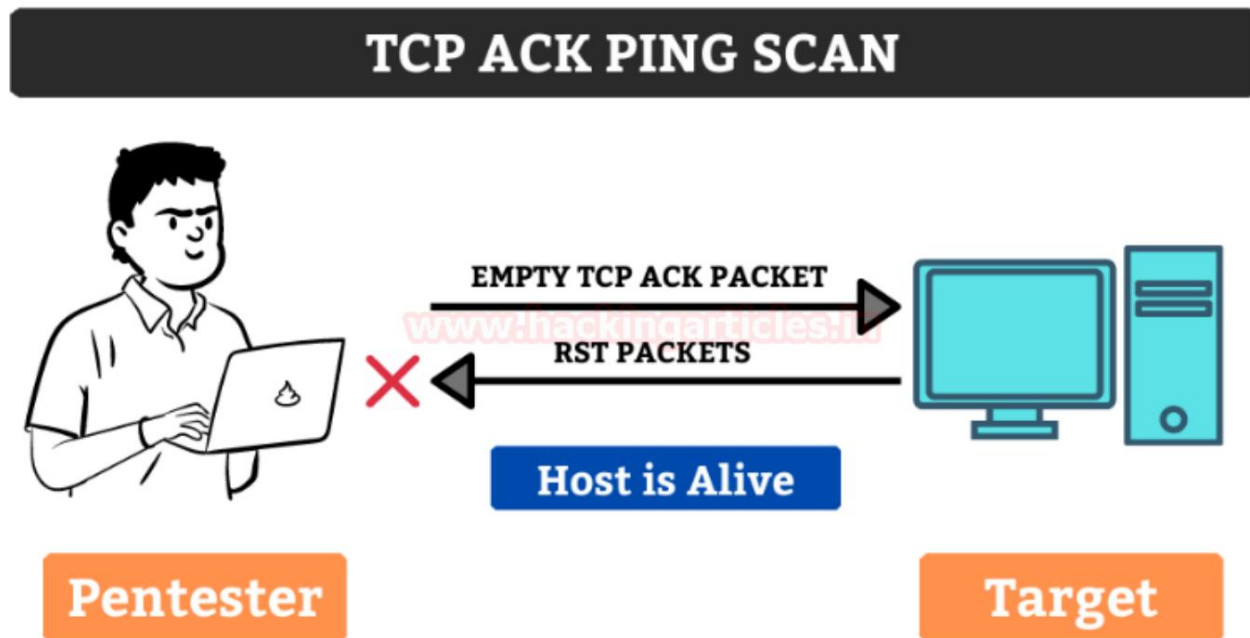
Los paquetes capturados con Wireshark pueden estar sobreservidos.

No	Tin	Source	Destination	Protocol	Length	Info
...	192.168.1.9	192.168.1.108	TCP	58	47752 → 80	[SYN] Seq=0 Win=1024 Len=0
...	192.168.1.108	192.168.1.9	TCP	60	80 → 47752	[SYN, ACK] Seq=0 Ack=1 Win=0
...	192.168.1.9	192.168.1.108	TCP	54	47752 → 80	[RST] Seq=1 Win=0 Len=0

La ventaja del escaneo TCP SYN Ping es que el pentester puede obtener el estado activo/inactivo del host sin siquiera crear una conexión, por lo tanto, ni siquiera crea un registro en el sistema o la red.

Escaneo de ping TCP ACK

Es un método de descubrimiento de host similar al escaneo TCP SYN Ping pero ligeramente diferente. Este escaneo también utiliza el puerto 80. El pentester envía un paquete TCP vacío al objetivo y, como no hay conexión entre ellos, recibirá un paquete de confirmación y luego restablecerá y finalizará la solicitud.

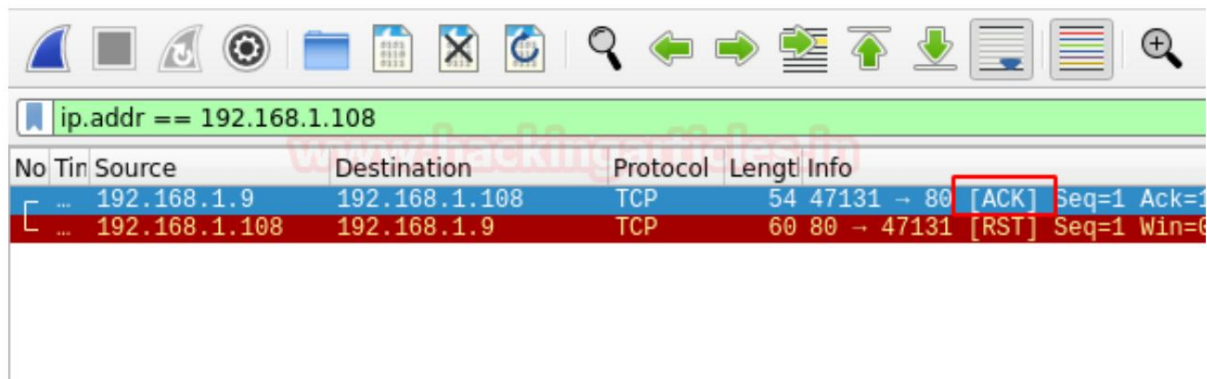


Este comando se utiliza para determinar la respuesta del objetivo y también verificar si los paquetes SYN o las solicitudes de eco ICMP están bloqueados en los firewalls más recientes.

```
nmap -sn -PA 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PA 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 07:14 EST
Nmap scan report for 192.168.1.108
Host is up (0.00023s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~#
```

Los paquetes capturados en Wireshark se pueden observar aquí.

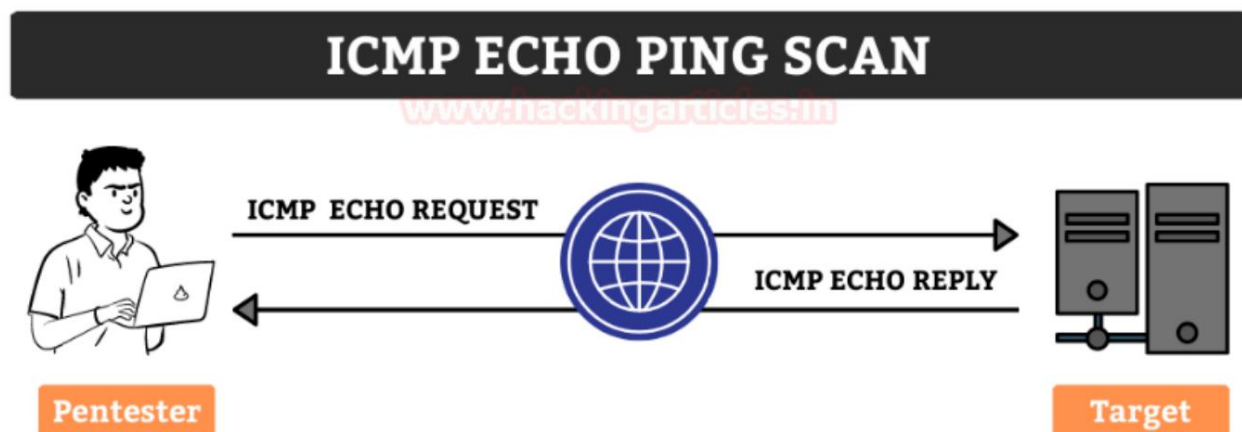


No	Time	Source	Destination	Protocol	Length	Info
...	...	192.168.1.9	192.168.1.108	TCP	54	47131 → 80 [ACK] Seq=1 Ack=1
...	...	192.168.1.108	192.168.1.9	TCP	60	80 → 47131 [RST] Seq=1 Win=0

Algunos firewalls están configurados para bloquear paquetes de ping SYN, por lo tanto, en este caso, este escaneo sería efectivo para evitar el firewall fácilmente.

Escaneo de ping de eco ICMP

El escaneo ICMP Ping se puede utilizar para recopilar información sobre los sistemas de destino, lo que lo diferencia del escaneo de puertos. El pentester puede enviar una solicitud ICMP ECHO al objetivo y obtener a cambio una respuesta ICMP Echo.



ICMP ahora no es efectivo en paquetes ICMP remotos que han sido bloqueados por los administradores. Todavía se puede utilizar para monitorear redes locales.

```
nmap -sn -PE 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PE 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 07:15 EST
Nmap scan report for 192.168.1.108
Host is up (0.00039s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
root@kali:~#
```

Se pueden observar los paquetes capturados en Wireshark.

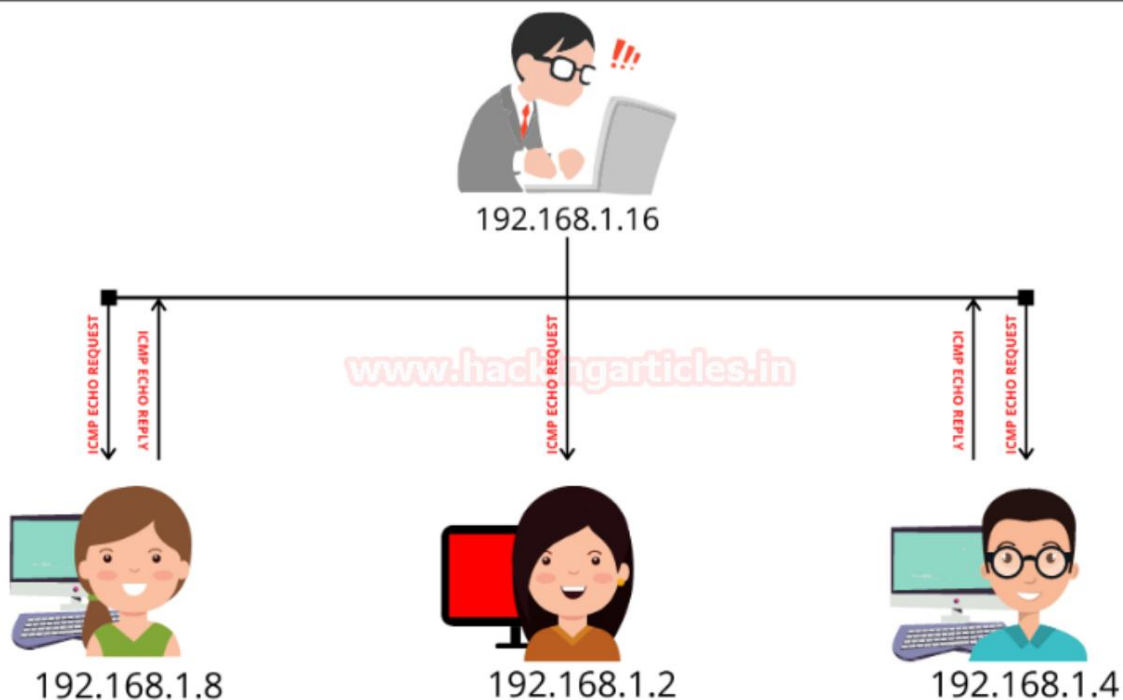
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.addr == 192.168.1.108						
No	Tin	Source	Destination	Protocol	Length	Info
...	...	192.168.1.9	192.168.1.108	ICMP	42	Echo (ping) request id=0xdb6
...	...	192.168.1.108	192.168.1.9	ICMP	60	Echo (ping) reply id=0xdb6

Barrido de ping ICMP ECHO

Es similar al Echo Ping Scan y se utiliza para escanear los hosts activos dentro de un rango determinado de direcciones IP. Envía solicitudes ICMP a una gran cantidad de objetivos y, si un objetivo en particular está vivo, devolverá una respuesta ICMP.

```
nmap-sn-PE 192.168.1-10
```

ICMP ECHO PING SWEEP



Escaneo de máscara de dirección ICMP

Es un método más antiguo de escaneo de ping ICMP ECHO. Proporciona información sobre el sistema y su máscara de subred.

```
nmap-sn-PM 192.168.1.108
```

```
root@kali:~# nmap -sn -PM 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:15 EST
Nmap scan report for 192.168.1.108
Host is up (0.00026s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~#
```

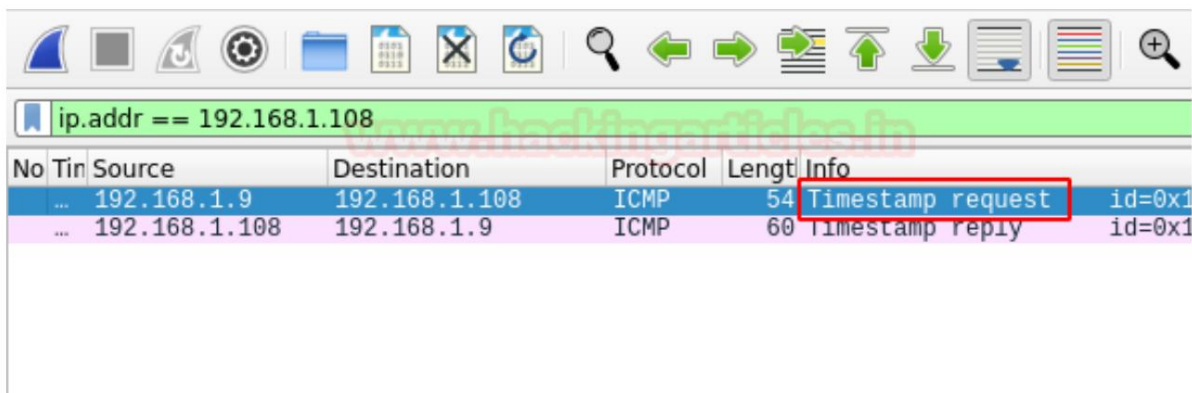
Escaneo de marca de tiempo ICMP ECHO

El pentester puede adoptar esta técnica en una condición particular cuando el administrador del sistema bloquea la marca de tiempo ICMP normal. Suele utilizarse para la sincronización del tiempo.

```
nmap -sn -PP 192.168.1.108 --disable-arp-ping
```

```
root@kali:~# nmap -sn -PP 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 07:17 EST
Nmap scan report for 192.168.1.108
Host is up (0.00059s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~#
```

Se pueden observar los paquetes capturados con Wireshark.



The image shows a Wireshark packet capture interface. The filter bar at the top is set to 'ip.addr == 192.168.1.108'. The packet list shows two packets: an ICMP timestamp request (ID 0x1) from 192.168.1.9 to 192.168.1.108, and an ICMP timestamp reply (ID 0x1) from 192.168.1.108 to 192.168.1.9. The packet details pane for the first packet shows 'Timestamp request' and 'id=0x1'.

No	Time	Source	Destination	Protocol	Length	Info
...	...	192.168.1.9	192.168.1.108	ICMP	54	Timestamp request id=0x1
...	...	192.168.1.108	192.168.1.9	ICMP	60	Timestamp reply id=0x1

Escaneo de ping UDP

Los escaneos de ping UDP utilizan un número de puerto predeterminado muy poco común, 40125, para enviar paquetes al destino. Es similar a un escaneo TCP Ping. El pentester enviará los paquetes UDP al objetivo y si hay una respuesta a cambio, significa que el host está vivo o está fuera de línea.

UDP PING SCAN WHEN TARGET IS ACTIVE



www.hackingarticles.in

UDP PING SCAN WHEN TARGET IS INACTIVE



La ventaja de un escaneo UDP es que puede detectar sistemas que tienen firewalls con reglas TCP estrictas, dejando las reglas UDP tranquilas.

```
nmap -sn -PU 192.168.1.108 --disable-arp-ping
```

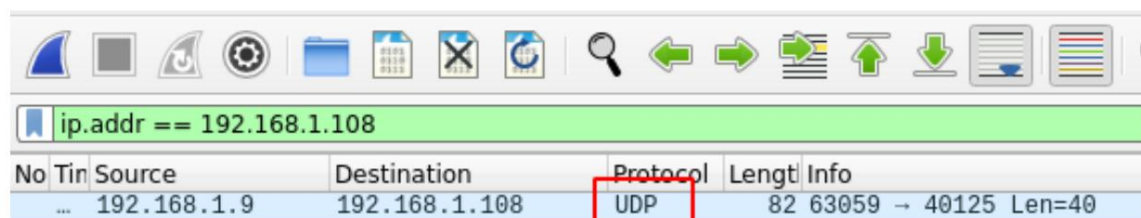


```

root@kali:~# nmap -sn -PU 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:06 EST
Nmap scan report for 192.168.1.108
Host is up (0.00032s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
root@kali:~#

```

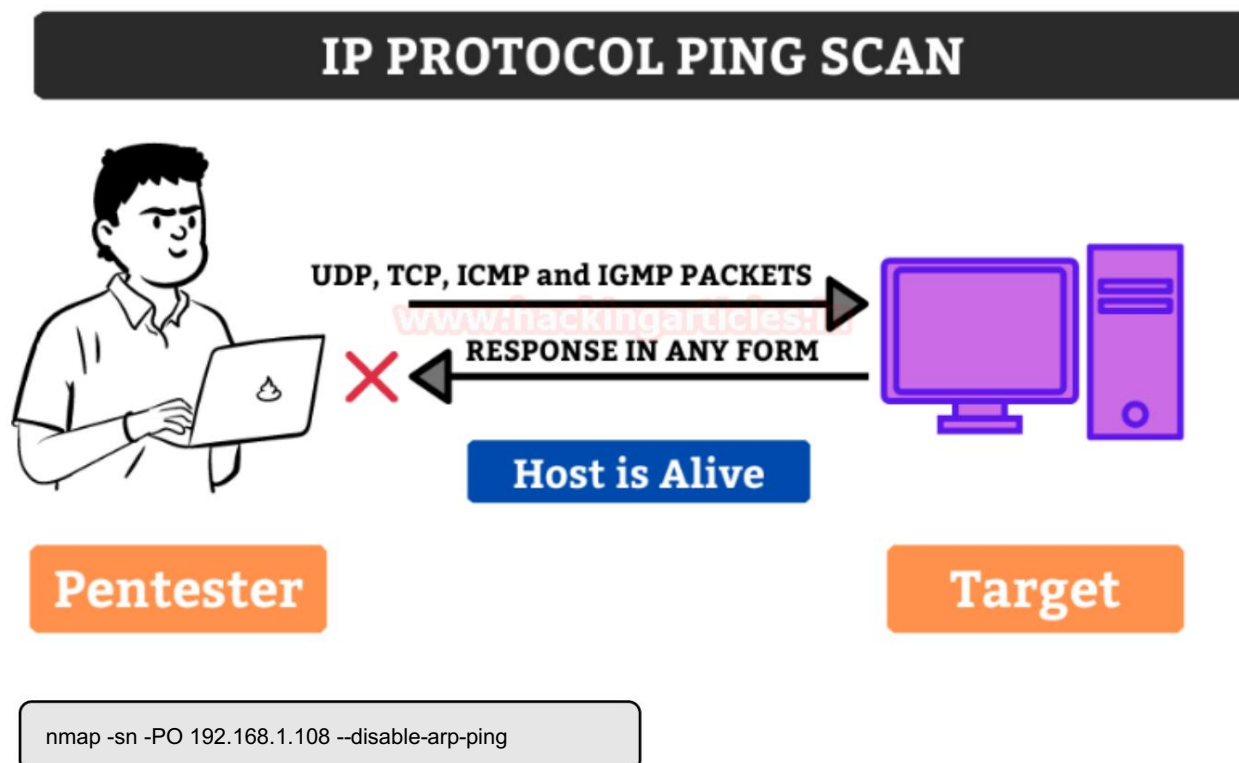
Puede observar los paquetes enviados utilizando Wireshark.



No	Tin	Source	Destination	Protocol	Length	Info
...	...	192.168.1.9	192.168.1.108	UDP	82	63059 → 40125 Len=40

Escaneo de ping del protocolo IP En

este método, el pentester envía varios paquetes usando diferentes protocolos IP y espera obtener una respuesta a cambio si el objetivo está vivo.

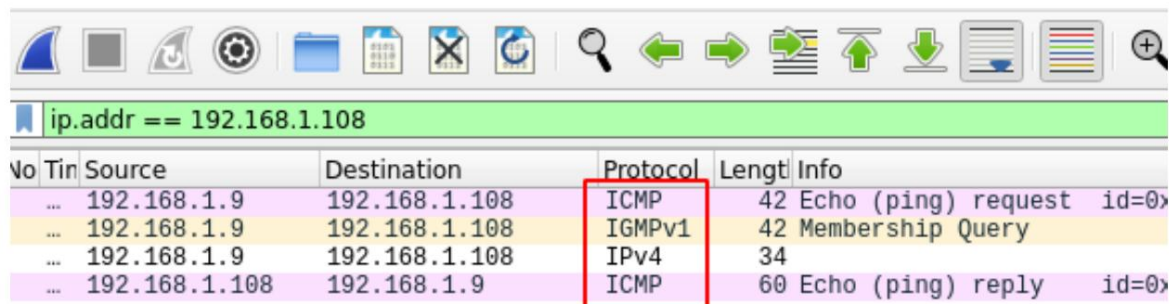


```

root@kali:~# nmap -sn -PO 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:07 EST
Nmap scan report for 192.168.1.108
Host is up (0.00040s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds

```

Los paquetes capturados se pueden observar utilizando Wireshark.



No	Tin	Source	Destination	Protocol	Length	Info
...	192.168.1.9	192.168.1.9	192.168.1.108	ICMP	42	Echo (ping) request id=0>
...	192.168.1.9	192.168.1.9	192.168.1.108	IGMPv1	42	Membership Query
...	192.168.1.9	192.168.1.9	192.168.1.108	IPv4	34	
...	192.168.1.108	192.168.1.108	192.168.1.9	ICMP	60	Echo (ping) reply id=0>

Sin escaneo de ping

En este método, el descubrimiento de host se omite por completo. El pentester puede usarlo para determinar máquinas activas para escaneos más intensos y aumentar la velocidad de la red.

```
nmap -sn -PN 192.168.1.108 --disable-arp-ping
```

```

root@kali:~# nmap -sn -PN 192.168.1.108 --disable-arp-ping
Host discovery disabled (-Pn). All addresses will be marked 'up' and s
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:10 EST
Nmap scan report for 192.168.1.108
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds

```

Escaneo de ping ARP

En este método, los paquetes ARP se envían a todos los dispositivos de la red, aunque son invisibles debido al firewall. Se considera extremadamente eficiente en comparación con otros descubrimientos de hosts. Se utiliza principalmente para el descubrimiento de sistemas. También menciona la latencia.

ARP PING SCAN



```
nmap-sn-PR 192.168.1.108
```

```
root@kali:~# nmap -sn -PR 192.168.1.108
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:12 EST
Nmap scan report for 192.168.1.108
Host is up (0.00029s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@kali:~#
```

Puede ver los paquetes capturados en Wirehark.

ip.addr == 192.168.1.108 || arp

No	Time	Source	Destination	Protocol	Length	Info
...		VMware_b2:bb:77	Broadcast	ARP	42	Who has 192.168.1.108
...		VMware_c8:9c:50	VMware_b2:bb:77	ARP	60	192.168.1.108 is at 00:0c:29:c8:9c:50
...		TaicangT_69:a5:10	VMware_b2:bb:77	ARP	60	Who has 192.168.1.97
...		VMware_b2:bb:77	TaicangT_69:a5:10	ARP	42	192.168.1.9 is at 00:0c:29:c8:9c:50
...		TaicangT_69:a5:10	VMware_c8:9c:50	ARP	60	Who has 192.168.1.108
...		VMware_c8:9c:50	TaicangT_69:a5:10	ARP	60	192.168.1.108 is at 00:0c:29:c8:9c:50

Ping de inicio de SCTP

Envía un paquete SCTP que contiene un fragmento INIT mínimo. Su puerto de destino predeterminado es 80. El fragmento INIT proporciona una sugerencia al sistema remoto de que el pentester está intentando establecer una asociación.

```
nmap -sn -PY 192.168.1.108 --disable-arp-ping
```

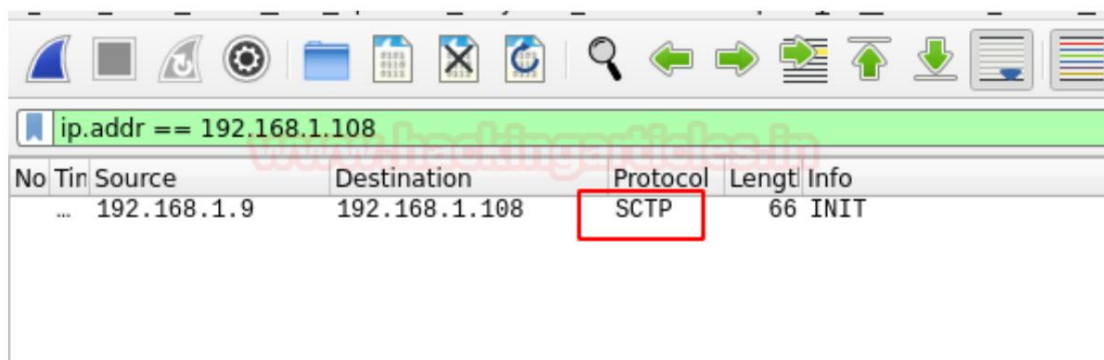


```

root@kali:~# nmap -sn -PY 192.168.1.108 --disable-arp-ping
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 12:13 EST
Nmap scan report for 192.168.1.108
Host is up (0.00030s latency).
MAC Address: 00:0C:29:C8:9C:50 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
root@kali:~#

```

Se pueden observar los paquetes que se capturan.



The image shows a Wireshark packet capture window. The filter bar at the top is set to 'ip.addr == 192.168.1.108'. The packet list below shows one packet with the following details:

No	Time	Source	Destination	Protocol	Length	Info
...		192.168.1.9	192.168.1.108	SCTP	66	INIT

ruta de seguimiento

Las rutas de seguimiento se utilizan después de finalizar el escaneo, utilizando la información de los resultados del escaneo para determinar el puerto y el protocolo que alcanzará el objetivo.

```
nmap -sn --traceroute 8.8.8.8
```

```

root@kali:~# nmap -sn --traceroute 8.8.8.8
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-20 11:38 EST
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.0014s latency).

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.85 ms dsldevice.lan (192.168.1.1)
2 1.57 ms dns.google (8.8.8.8)

```

Para obtener más información sobre Traceroute, puede consultar

Funcionamiento de Traceroute utilizando Wireshark

Referencia: <https://nmap.org/book/man-host-discovery.html>

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

