

Hacking ético e Test de intrusión

Máster Inter-Universitario en Ciberseguridad (MUNICS)

Universidade da Coruña (UDC) y Universidade de Vigo (UVigo)

Curso 2024-2025

Práctica 1 - Descubrimiento y enumeración

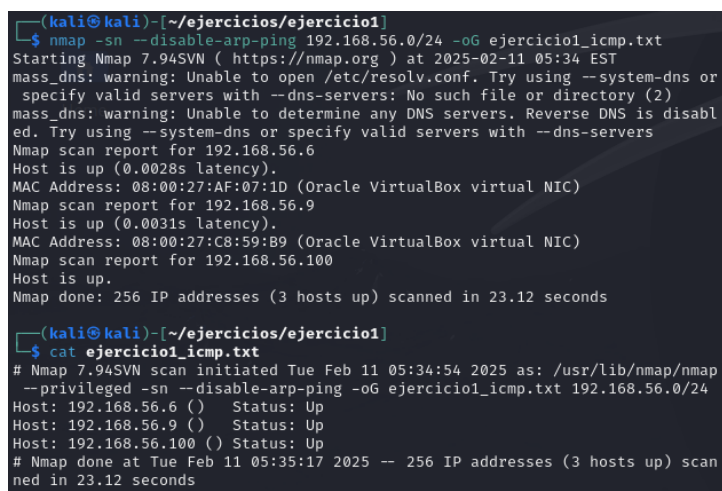
Nuria Codesido Iglesias

1 Realiza un barrido ping (ICMP) sobre las máquinas proporcionadas. Captura con wireshark e identifica los cuatro paquetes esenciales del barrido

El objetivo de este apartado es identificar qué máquinas están activas en la red mediante ICMP. Para ello, se utiliza la opción `-sn` para detectar únicamente los hosts que están activos en la red sin realizar un escaneo de puertos de manera menos intrusiva (sin generar más tráfico del necesario). Cabe destacar que se utiliza la opción `-disable-arp-ping` para forzar el uso de ICMP y cambiar el comportamiento del escaneo. Esto se debe a que cuando se realiza un escaneo en una red local (LAN), nmap suele priorizar ARP en vez de ICMP, ya que ARP es más confiable en estas redes. Finalmente, una vez que el escaneo se ha realizado, se guarda la salida en un fichero para poder procesar los resultados más tarde con herramientas como *grep*. El comando utilizado:

```
nmap -sn - -disable-arp-ping 192.168.56.0/24 -oG ejercicio1_icmp.txt
```

En esta primera imagen se visualiza la salida del comando anterior. El resultado nos indica que se escanearon 256 direcciones IP en la red 192.168.56.0/24 y encontraron 3 hosts activos: 192.168.56.6 (windows), 192.168.56.9 (linux) y 192.168.56.100 (máquina kali). Finalmente, se realiza un cat del fichero creado, para visualizar su contenido.



```
(kali@kali)~/ejercicios/ejercicio1
$ nmap -sn --disable-arp-ping 192.168.56.0/24 -oG ejercicio1_icmp.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 05:34 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.6
Host is up (0.0028s latency).
MAC Address: 08:00:27:AF:07:1D (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.9
Host is up (0.0031s latency).
MAC Address: 08:00:27:C8:59:B9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.100
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 23.12 seconds

(kali@kali)~/ejercicios/ejercicio1
$ cat ejercicio1_icmp.txt
# Nmap 7.94SVN scan initiated Tue Feb 11 05:34:54 2025 as: /usr/lib/nmap/nmap
--privileged -sn --disable-arp-ping -oG ejercicio1_icmp.txt 192.168.56.0/24
Host: 192.168.56.6 () Status: Up
Host: 192.168.56.9 () Status: Up
Host: 192.168.56.100 () Status: Up
# Nmap done at Tue Feb 11 05:35:17 2025 -- 256 IP addresses (3 hosts up) scan
ned in 23.12 seconds
```

Figure 1: Escaneo ping

Por otro lado, al mismo tiempo se captura el tráfico con la herramienta Wireshark. Se observan paquetes ICMP y ARP:

- **Solicitud ICMP Echo Request (Ping Request).** Se visualizan paquetes ICMP enviados desde 192.168.56.100 (origen) hacia otras IPs en la red, como 192.168.56.9 y 192.168.56.6. Para verificar que máquinas están activas. (descubrimiento de hosts) 2
- **Respuesta ICMP Echo Reply (Ping Reply).** Algunos hosts (192.168.56.9, 192.168.56.6) responden a la solicitud, confirmando que están activos en la red. 2
- **ARP Request (Broadcast.)** La máquina 192.168.56.100 (origen) está intentando descubrir las direcciones MAC asociadas a las IPs de la red. A pesar, de haber utilizado la opción *-disable-arp-ping*, es necesario para poder comunicarse con los hosts antes de enviar paquetes ICMP. 2
- **ICMP Timestamp Request.** Se usa para sincronizar la hora entre dispositivos de una red. 3

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::a00:27ff:fec8...	ff02::12	ICMPv6	70	Router Solicitation from 08:00:27:c8:59:b9
2	2.575504722	192.168.56.100	192.168.56.1	ICMP	42	Echo (ping) request id=0x810f, seq=0/0, ttl=50 (no response found!)
3	2.575673109	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.2? Tell 192.168.56.100
4	2.575721927	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.3? Tell 192.168.56.100
5	2.575751440	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.4? Tell 192.168.56.100
6	2.575784466	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.5? Tell 192.168.56.100
7	2.575814208	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.6? Tell 192.168.56.100
8	2.575846276	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.7? Tell 192.168.56.100
9	2.575916027	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.8? Tell 192.168.56.100
10	2.575948893	192.168.56.100	192.168.56.9	ICMP	42	Echo (ping) request id=0x77a7, seq=0/0, ttl=48 (reply in 14)
11	2.575975951	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.10? Tell 192.168.56.100
12	2.576888520	PCSSystemtec.af:07::	PCSSystemtec.6e:13::	ARP	60	192.168.56.6 is at 08:00:27:af:07:1d
13	2.576895068	192.168.56.100	192.168.56.6	ICMP	42	Echo (ping) request id=0x332f, seq=0/0, ttl=57 (reply in 15)
14	2.576888682	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0x77a7, seq=0/0, ttl=64 (request in 10)
15	2.578622977	192.168.56.6	192.168.56.100	ICMP	60	Echo (ping) reply id=0x332f, seq=0/0, ttl=128 (request in 13)
16	2.582105831	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.13? Tell 192.168.56.100
17	2.582219342	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.14? Tell 192.168.56.100
18	2.582347587	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.15? Tell 192.168.56.100
19	2.582418692	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.16? Tell 192.168.56.100
20	2.676618875	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.19? Tell 192.168.56.100
21	2.676833084	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.20? Tell 192.168.56.100
22	2.676980874	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.21? Tell 192.168.56.100
23	2.676978027	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.22? Tell 192.168.56.100
24	2.677048145	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.23? Tell 192.168.56.100
25	2.677127170	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.24? Tell 192.168.56.100
26	2.677193977	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.25? Tell 192.168.56.100
27	2.677255206	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.26? Tell 192.168.56.100
28	2.682553931	PCSSystemtec.6e:13::	Broadcast	ARP	42	Who has 192.168.56.29? Tell 192.168.56.100

Figure 2: Wireshark

Entre todos estos paquetes, los cuatro paquetes esenciales son los ICMP Echo Request y Reply de las máquinas: 192.168.56.9 (rojo) y la 192.168.56.6 (azul).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.56.100	192.168.56.1	ICMP	42	Echo (ping) request id=0x5925, seq=0/0, ttl=56 (no response found!)
9	0.000413229	192.168.56.100	192.168.56.9	ICMP	42	Echo (ping) request id=0x2097, seq=0/0, ttl=40 (reply in 11)
11	0.001477113	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0x2097, seq=0/0, ttl=64 (request in 9)
13	0.001511178	192.168.56.100	192.168.56.6	ICMP	42	Echo (ping) request id=0x703b, seq=0/0, ttl=51 (reply in 14)
14	0.002976732	192.168.56.6	192.168.56.100	ICMP	60	Echo (ping) reply id=0x703b, seq=0/0, ttl=128 (request in 13)
150	1.111220431	192.168.56.100	192.168.56.1	ICMP	42	Echo (ping) request id=0xc1ff, seq=0/0, ttl=41 (no response found!)
179	1.314339717	192.168.56.100	192.168.56.9	ICMP	42	Echo (ping) request id=0xf53b, seq=0/0, ttl=52 (reply in 180)
180	1.315332331	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0xf53b, seq=0/0, ttl=64 (request in 179)
230	1.330656278	192.168.56.100	192.168.56.255	ICMP	42	Echo (ping) request id=0xff05, seq=0/0, ttl=37 (no response found!)
564	3.581733663	192.168.56.100	192.168.56.9	ICMP	42	Echo (ping) request id=0xb945, seq=0/0, ttl=49 (reply in 567)
567	3.584092498	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0xb945, seq=0/0, ttl=64 (request in 564)
1024	6.783118795	192.168.56.100	192.168.56.9	ICMP	42	Echo (ping) request id=0xe8b3, seq=0/0, ttl=57 (reply in 1026)
1026	6.783676157	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0xe8b3, seq=0/0, ttl=64 (request in 1024)
1090	6.893629877	192.168.56.100	192.168.56.255	ICMP	42	Echo (ping) request id=0xa34a, seq=0/0, ttl=45 (no response found!)
1392	9.950334355	192.168.56.100	192.168.56.9	ICMP	42	Echo (ping) request id=0xa5d3, seq=0/0, ttl=49 (reply in 1414)
1414	9.951092244	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0xa5d3, seq=0/0, ttl=64 (request in 1392)
1725	13.022824524	192.168.56.100	192.168.56.1	ICMP	42	Echo (ping) request id=0xd755, seq=0/0, ttl=56 (reply in 1742)
1742	13.023751319	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0xd755, seq=0/0, ttl=64 (request in 1725)
1821	13.127013100	192.168.56.100	192.168.56.1	ICMP	54	Timestamp request id=0xebf6, seq=0/0, ttl=43
1825	13.228369303	192.168.56.100	192.168.56.1	ICMP	54	Timestamp request id=0xc6b7, seq=0/0, ttl=51
2143	16.194654875	192.168.56.100	192.168.56.9	ICMP	42	Echo (ping) request id=0x3c34, seq=0/0, ttl=50 (reply in 2160)
2160	16.195404730	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0x3c34, seq=0/0, ttl=64 (request in 2143)
2539	19.264167275	192.168.56.100	192.168.56.9	ICMP	42	Echo (ping) request id=0x7155, seq=0/0, ttl=48 (reply in 2548)
2548	19.265282276	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0x7155, seq=0/0, ttl=64 (request in 2539)
2571	19.366640938	192.168.56.100	192.168.56.255	ICMP	54	Timestamp request id=0x993e, seq=0/0, ttl=52
2633	19.469152230	192.168.56.100	192.168.56.255	ICMP	54	Timestamp request id=0x2ea2, seq=0/0, ttl=48
2968	22.432633391	192.168.56.100	192.168.56.9	ICMP	42	Echo (ping) request id=0x010c, seq=0/0, ttl=59 (reply in 2989)
2989	22.435548095	192.168.56.9	192.168.56.100	ICMP	60	Echo (ping) reply id=0x010c, seq=0/0, ttl=64 (request in 2968)

Figure 3: Wireshark

2 Llevar a cabo un escaneo sigiloso (Stealth) de toda la red virtualizada. Comprobar el tráfico producido con Wireshark.

El objetivo del escaneo sigiloso implica un enfoque más discreto para detectar los servicios disponibles en una red sin ser fácilmente identificado. Por lo que a la hora de elegir los puertos que se van a escanear, se seleccionan los que corresponden a servicios clave. Para ello, se utiliza la opción `-p` para especificar los puertos que se quieren escanear, ya que si no se usa, `Nmap` escanea los 1000 puertos más comunes, lo que puede ser ruidoso y detectable. Los puertos seleccionados son:

- 3389 (Windows) - Si este puerto está abierto, significa que se puede conectar a la máquina Windows usando Remote Desktop Protocol (RDP), lo que permite controlarla de manera remota.
- 135 (Windows) - Se usa para iniciar conexiones RPC (Remote Procedure Call) con el servicio RPC Endpoint Mapper en sistemas Windows. Este servicio ayuda a asignar dinámicamente puertos para otros servicios que usan RPC.
- 139 (Windows) - Se usa para compartir archivos e impresoras.
- 22, 23 - Permite acceso remoto.
- 21 - Protocolo de transferencia de archivos, sin cifrado por defecto.
- 512,513,514 (Linux) - Usados para servicios de acceso remoto y ejecución de comandos.
- 80 - Puerto estándar para tráfico web sin cifrado.
- 443 - Puerto estándar para tráfico web cifrado con SSL/TLS.
- 49154, 49156 (Windows) - Puertos efímeros usados por Windows para RPC, SMB o conexiones internas.
- 3306 (MySQL), 5432 (PostgreSQL) - Si estos puertos están abiertos, la máquina podría tener bases de datos activas.
- 5900 - Utilizado para control remoto de escritorio.
- 6000 (Linux) - Interfaz gráfica remota, si está abierto, se podrían espiar sesiones gráficas.

Por otro lado, también se utilizan más opciones de `Nmap` para hacerlo más discreto. La opción `-sS` realiza un escaneo "sigiloso" enviando paquetes sin establecer una conexión completa, lo que ayuda a evitar ser detectado. `-Pn` evita que `Nmap` envíe paquetes ICMP para verificar si los hosts están activos. Esto evita que el escaneo sea detectado por sistemas de monitoreo. Al usar esta opción se escanean todos los hosts, independientemente de si responden a los pings o no. Por último, `-n` evita que `Nmap` realice búsquedas DNS de las direcciones IP, lo que ayuda a prevenir que se genere tráfico visible en los registros de los servidores DNS. Cabe destacar que también se utiliza la opción `-oG` para guardar los resultados.

```

nmap -sS -n -Pn 192.168.56.0/24 -p
21,22,23,80,443,135,139,3389,49154,49156,3306,5432,5900,6000,512,513,514
-oG ejercicio2_sigiloso.txt

```

Una vez realizado el siguiente comando, se puede visualizar que puertos están activos en cada una de las máquinas. En las siguientes imágenes, se pueden observar que puertos están abiertos, filtrados o cerrados.

```

(kali@kali) ~/ejercicios/ejercicio2
$ nmap -sS -n -Pn 192.168.56.0/24 -p 21,22,23,80,443,135,139,3389,49154,49156,3306,5432,5900,6000,512,513,514 -oG ejercicio2_sigiloso.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-12 05:53 EST
Nmap scan report for 192.168.56.1
Host is up (0.00049s latency).

PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    filtered http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
443/tcp    filtered https
512/tcp    filtered exec
513/tcp    filtered login
514/tcp    filtered shell
3306/tcp   open      mysql
3389/tcp   filtered ms-wbt-server
5432/tcp   filtered postgresql
5900/tcp   filtered vnc
6000/tcp   filtered X11
49154/tcp  filtered unknown
49156/tcp  filtered unknown
MAC Address: 0A:00:27:00:00:4B (Unknown)

```

Figure 4: Escaneo silencioso - 192.168.56.1 (gateway)

```

Nmap scan report for 192.168.56.6
Host is up (0.0011s latency).

PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    filtered ssh
23/tcp    filtered telnet
80/tcp    open      http
135/tcp    open      msrpc
139/tcp    open      netbios-ssn
443/tcp    filtered https
512/tcp    filtered exec
513/tcp    filtered login
514/tcp    filtered shell
3306/tcp   filtered mysql
3389/tcp   filtered ms-wbt-server
5432/tcp   filtered postgresql
5900/tcp   filtered vnc
6000/tcp   filtered X11
49154/tcp  open      unknown
49156/tcp  open      unknown
MAC Address: 08:00:27:AF:07:1D (Oracle VirtualBox virtual NIC)

```

Figure 5: Escaneo silencioso - 192.168.56.6 (Windows)

```

Nmap scan report for 192.168.56.9
Host is up (0.0018s latency).

```

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
80/tcp	open	http
135/tcp	closed	msrpc
139/tcp	open	netbios-ssn
443/tcp	closed	https
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
3306/tcp	open	mysql
3389/tcp	closed	ms-wbt-server
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
49154/tcp	closed	unknown
49156/tcp	closed	unknown

```

MAC Address: 08:00:27:C8:59:B9 (Oracle VirtualBox virtual NIC)

```

Figure 6: Escaneo silencioso - 192.168.56.9 (Linux)

```

Nmap scan report for 192.168.56.100
Host is up (0.000012s latency).

```

PORT	STATE	SERVICE
21/tcp	closed	ftp
22/tcp	closed	ssh
23/tcp	closed	telnet
80/tcp	closed	http
135/tcp	closed	msrpc
139/tcp	closed	netbios-ssn
443/tcp	closed	https
512/tcp	closed	exec
513/tcp	closed	login
514/tcp	closed	shell
3306/tcp	closed	mysql
3389/tcp	closed	ms-wbt-server
5432/tcp	closed	postgresql
5900/tcp	closed	vnc
6000/tcp	closed	X11
49154/tcp	closed	unknown
49156/tcp	closed	unknown

```

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.51 seconds

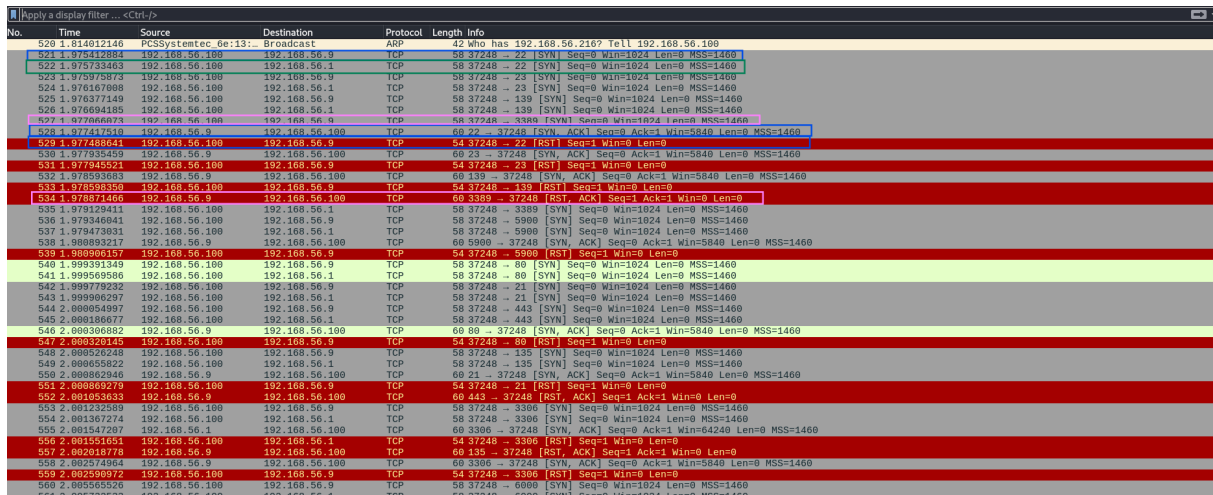
```

Figure 7: Escaneo silencioso - 192.168.56.100 (kali)

Al ejecutar el comando, Wireshark captura el tráfico. Primero, se capturan los paquetes ARP broadcast porque el tráfico TCP funciona a nivel de capa 2 y necesita la dirección MAC para enviar los paquetes correctamente. Luego, Nmap envía paquetes TCP con el flag SYN para intentar iniciar la conexión con los puertos especificados.

La respuesta puede variar dependiendo de si el puerto está abierto, cerrado o filtrado. Si un puerto está abierto, una vez establecida la conexión (SYN+ACK), en lugar de enviar un ACK para completar la conexión, Nmap envía un paquete RST para interrumpir la conexión. Esto no establece una conexión completa, simplemente permite verificar si el puerto está abierto sin completar el proceso de conexión. Con el fin de evitar la detección del escaneo por parte de firewalls o sistemas de intrusión. Un ejemplo (puerto 22 - máquina 192.168.56.9): en la imagen se visualiza en color azul, se verán 3 paquetes (SYN, SYN+ACK, RST).

Por otro lado, si el puerto está cerrado, la máquina de destino responderá con un paquete RST+ACK. Un ejemplo (puerto 3389 - máquina 192.169.56.9): en la imagen, se visualiza en color rosa, se verán 2 paquetes (SYN, RST+ACK). Y si el puerto está filtrado el dispositivo no responderá. Un ejemplo (puerto 22 - máquina 192.168.56.1): en la imagen, se visualiza en color verde, se verá solo un paquete (SYN).



No.	Time	Source	Destination	Protocol	Length	Info
520	1.814912146	PCSSysntec 6e:13:...	Broadcast	ARP	42	who has 192.168.56.210? Tell 192.168.56.100
521	1.975312854	192.168.56.100	192.168.56.9	TCP	58	37248 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
522	1.975733463	192.168.56.100	192.168.56.1	TCP	58	37248 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
523	1.975975873	192.168.56.100	192.168.56.9	TCP	58	37248 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
524	1.976167006	192.168.56.100	192.168.56.1	TCP	58	37248 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
525	1.976377149	192.168.56.100	192.168.56.9	TCP	58	37248 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
526	1.976694185	192.168.56.100	192.168.56.1	TCP	58	37248 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
527	1.977066073	192.168.56.100	192.168.56.9	TCP	58	37248 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
528	1.977417518	192.168.56.9	192.168.56.100	TCP	60	22 → 37248 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
529	1.977488641	192.168.56.100	192.168.56.9	TCP	54	37248 → 22 [RST] Seq=1 Win=0 Len=0
530	1.977733450	192.168.56.9	192.168.56.100	TCP	60	23 → 37248 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
531	1.977945521	192.168.56.100	192.168.56.9	TCP	54	37248 → 23 [RST] Seq=1 Win=0 Len=0
532	1.978593683	192.168.56.9	192.168.56.100	TCP	60	139 → 37248 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
533	1.978755952	192.168.56.100	192.168.56.9	TCP	54	37248 → 139 [RST] Seq=1 Win=0 Len=0
534	1.978971466	192.168.56.9	192.168.56.100	TCP	60	3389 → 37248 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
535	1.979129411	192.168.56.100	192.168.56.1	TCP	58	37248 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
536	1.979346841	192.168.56.100	192.168.56.9	TCP	58	37248 → 5980 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
537	1.979473031	192.168.56.100	192.168.56.1	TCP	58	37248 → 5980 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
538	1.980993217	192.168.56.9	192.168.56.100	TCP	60	5980 → 37248 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
539	1.980993157	192.168.56.100	192.168.56.9	TCP	54	37248 → 5980 [RST] Seq=1 Win=0 Len=0
540	1.980993140	192.168.56.100	192.168.56.9	TCP	58	37248 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
541	1.980995986	192.168.56.100	192.168.56.1	TCP	58	37248 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
542	1.980997922	192.168.56.100	192.168.56.9	TCP	58	37248 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
543	1.980998297	192.168.56.100	192.168.56.1	TCP	58	37248 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
544	2.000054987	192.168.56.100	192.168.56.9	TCP	58	37248 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
545	2.000188677	192.168.56.100	192.168.56.1	TCP	58	37248 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
546	2.000300882	192.168.56.9	192.168.56.100	TCP	60	80 → 37248 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
547	2.000320145	192.168.56.100	192.168.56.9	TCP	54	37248 → 80 [RST] Seq=1 Win=0 Len=0
548	2.000526248	192.168.56.100	192.168.56.9	TCP	58	37248 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
549	2.000658822	192.168.56.100	192.168.56.1	TCP	58	37248 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
550	2.000862946	192.168.56.9	192.168.56.100	TCP	60	21 → 37248 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
551	2.000869279	192.168.56.100	192.168.56.9	TCP	54	37248 → 21 [RST] Seq=1 Win=0 Len=0
552	2.001053033	192.168.56.9	192.168.56.100	TCP	60	443 → 37248 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
553	2.001323559	192.168.56.100	192.168.56.1	TCP	58	37248 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
554	2.001367274	192.168.56.100	192.168.56.1	TCP	58	37248 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
555	2.001547287	192.168.56.1	192.168.56.100	TCP	60	3389 → 37248 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
556	2.001551051	192.168.56.9	192.168.56.100	TCP	54	37248 → 3389 [RST] Seq=1 Win=0 Len=0
557	2.002018778	192.168.56.9	192.168.56.100	TCP	60	135 → 37248 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
558	2.002574964	192.168.56.9	192.168.56.100	TCP	60	3389 → 37248 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
559	2.002582076	192.168.56.100	192.168.56.9	TCP	54	37248 → 3389 [RST] Seq=1 Win=0 Len=0
560	2.005555526	192.168.56.100	192.168.56.9	TCP	58	37248 → 6000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
561	2.005712539	192.168.56.100	192.168.56.1	TCP	58	37248 → 6000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 8: Wireshark - escaneo silencioso

3 Realizar un escaneo agresivo sobre una máquina de internet (por ejemplo <http://scanme.nmap.org>) y sobre alguna de la red virtualizada. Ayudarse de otras herramientas como Wireshark o la opción *-packet-trace* de Nmap para comprobar similitudes y diferencias.

Para este apartado, se tiene como objetivo realizar un escaneo agresivo, que busca recopilar la mayor cantidad de información posible mediante técnicas avanzadas que pueden ser más ruidosas y detectables. Para este escaneo, se utiliza la opción *-T4* para realizar un escaneo más rápido y agresivo. La opción *-A* para obtener más información, ya que utiliza funciones avanzadas como: detección del sistema operativo, la identificación de versiones de servicios, el uso de scripts para obtener más información y el traceroute para mapear la ruta hacia el objetivo. Finalmente, la opción *- -packet-trace*, como indica el enunciado, se emplea para ver un registro detallado de los paquetes enviados y recibidos durante el escaneo.

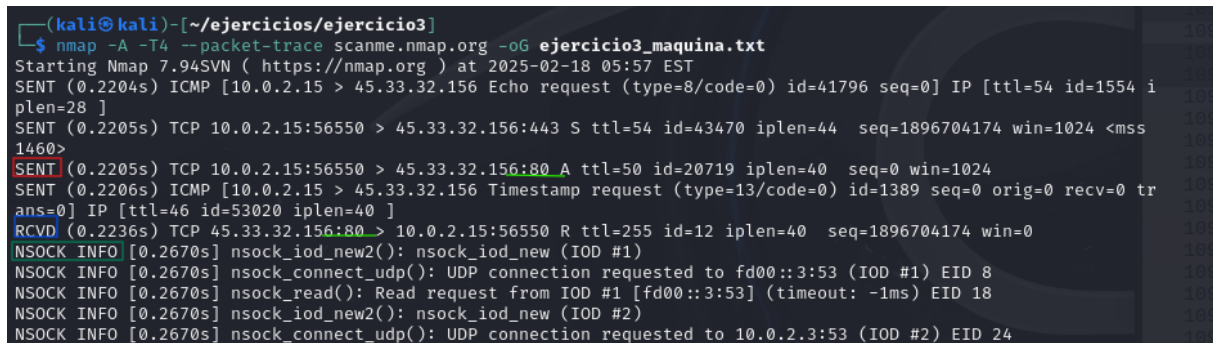
Escaneo agresivo - máquina de internet El primer comando utilizado es un escaneo agresivo a la máquina de internet (scanme.nmap.org - 45.33.32.156):

```
nmap -A -T4 - -packet-trace scanme.nmap.org -oG ejercicio3_maquina.txt
```

Una vez se ejecuta el comando, al principio se realiza una exploración de puertos. Se visualizan los paquetes enviados SENT, que incluyen solicitudes ICMP para comprobar si la máquina (scanme.nmap.org - 45.33.32.156) está activa, así como solicitudes TCP para investigar los puertos abiertos. Además, se muestran las respuestas recibidas a esos paquetes RCVD. Esto se debe a que, al inicio de este escaneo agresivo, Nmap envía múltiples paquetes al destino para investigar puertos, servicios y otros detalles relacionados con la máquina de destino. También aparecen mensajes de depuración (trace) NSOCK INFO, que

proporcionan información sobre el estado de los sockets que gestionan estas conexiones. Estos mensajes indican si las operaciones de escritura (SENT) y lectura (RCVD) en un socket fueron exitosas.

En la imagen 9 se visualizan estos paquetes enviados. Se muestra un ejemplo de un paquete SENT (color rojo) TCP al puerto 80 enviado a la máquina destino (`scanme.nmap.org` - 45.33.32.156) y su respuesta RCVD (color azul).



```
(kali@kali)-[~/ejercicios/ejercicio3]
$ nmap -A -T4 --packet-trace scanme.nmap.org -oG ejercicio3_maquina.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 05:57 EST
SENT (0.2204s) ICMP [10.0.2.15 > 45.33.32.156 Echo request (type=8/code=0) id=41796 seq=0] IP [ttl=54 id=1554 iplen=28 ]
SENT (0.2205s) TCP 10.0.2.15:56550 > 45.33.32.156:443 S ttl=54 id=43470 iplen=44 seq=1896704174 win=1024 <mss 1460>
SENT (0.2205s) TCP 10.0.2.15:56550 > 45.33.32.156:80 A ttl=50 id=20719 iplen=40 seq=0 win=1024
SENT (0.2206s) ICMP [10.0.2.15 > 45.33.32.156 Timestamp request (type=13/code=0) id=1389 seq=0 orig=0 recv=0 trans=0] IP [ttl=46 id=53020 iplen=40 ]
RCVD (0.2236s) TCP 45.33.32.156:80 > 10.0.2.15:56550 R ttl=255 id=12 iplen=40 seq=1896704174 win=0
NSOCK INFO [0.2670s] nssock_ioc_new2(): nssock_ioc_new (IOD #1)
NSOCK INFO [0.2670s] nssock_connect_udp(): UDP connection requested to fd00::3:53 (IOD #1) EID 8
NSOCK INFO [0.2670s] nssock_read(): Read request from IOD #1 [fd00::3:53] (timeout: -1ms) EID 18
NSOCK INFO [0.2670s] nssock_ioc_new2(): nssock_ioc_new (IOD #2)
NSOCK INFO [0.2670s] nssock_connect_udp(): UDP connection requested to 10.0.2.3:53 (IOD #2) EID 24
```

Figure 9: Escaneo agresivo - máquina (`scanme.nmap.org` - 45.33.32.156)

Una vez realizada la fase de exploración de puertos, se interactúa con los diferentes servicios que tienen los puertos activos. En esta parte, empiezan a aparecer mensajes NSE. Que indica que Nmap está utilizando scripts NSE para interactuar con el servicio, para obtener información adicional y realizar un análisis más profundo.

Estos scripts pueden realizar diversas acciones, como establecer conexiones con puertos abiertos (CONNECT), enviar solicitudes para recopilar información sobre los servicios en ejecución, verificar configuraciones específicas...

En la siguiente imagen 10 se visualiza que se están realizando muchas conexiones repetidas a los puertos 80 y 22.

```

NSOCK INFO [80.3010s] nsock_write(): Write request for 1 bytes to IOD #4 EID 147 [45.33.32.156:1434]
NSOCK INFO [80.3010s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 147 [45.33.32.156:1434]
NSE: UDP 10.0.2.15:45232 > 45.33.32.156:1434 | SEND
NSOCK INFO [80.3520s] nsock_read(): Read request from IOD #4 [45.33.32.156:1434] (timeout: 5000ms) EID 154
NSOCK INFO [80.4070s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 64 [45.33.32.156:31337]
NSE: TCP 10.0.2.15:52622 > 45.33.32.156:31337 | CONNECT
NSOCK INFO [80.4100s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 96 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48548 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4100s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 16 [45.33.32.156:22]
NSE: TCP 10.0.2.15:56824 > 45.33.32.156:22 | CONNECT
NSOCK INFO [80.4110s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 48 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48498 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4120s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 72 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48526 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4130s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48462 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4130s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48472 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4140s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 112 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48564 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4160s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 40 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48488 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4170s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 88 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48538 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4170s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 56 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48514 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4180s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 136 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48590 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4250s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 128 [45.33.32.156:22]
NSE: TCP 10.0.2.15:56834 > 45.33.32.156:22 | CONNECT
NSOCK INFO [80.4280s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 104 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48560 > 45.33.32.156:80 | CONNECT
NSOCK INFO [80.4300s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 120 [45.33.32.156:80]
NSE: TCP 10.0.2.15:48576 > 45.33.32.156:80 | CONNECT
NSE: TCP 10.0.2.15:48462 > 45.33.32.156:80 | 00000000: 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a GET / HT
TP/1.1

```

Figure 10: Escaneo agresivo - máquina (scanme.nmap.org - 45.33.32.156)

La siguiente imagen, es otro ejemplo de un mensaje, en el que se envía una petición HTTP al servidor `scanme.nmap.org` en el puerto 80. En este caso, se utiliza un script NSE para enviar una solicitud GET, que permite obtener detalles sobre la respuesta HTTP, como el código de estado (200 OK), los encabezados HTTP, el contenido de la página web, el servidor web utilizado (Apache), el sistema operativo que lo está ejecutando (Ubuntu) ...

```

NSE: TCP 10.0.2.15:48498 < 45.33.32.156:80 | HTTP/1.1 200 OK
Date: Tue, 18 Feb 2025 10:58:59 GMT
Server: Apache/2.4.7 (Ubuntu)
Accept-Ranges: bytes
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

4c
<!DOCTYPE html>
<html lang="en">
<head>
<title>Go ahead and ScanMe!</title>

```

Figure 11: Escaneo agresivo - máquina (scanme.nmap.org - 45.33.32.156)

Por último, aparecen los puertos abiertos y sus servicios. Se encontraron cinco puertos abiertos y otros 995 cerrados. A continuación, se proporciona información sobre la máquina 45.33.32.156:

- **Tipo de dispositivo detectado.** En la imagen se visualiza en color verde.
- **Posible sistema operativo y virtualización:** Sugiere que el host está corriendo sobre un entorno virtualizado. En la imagen se visualiza en color azul.
- **Identificadores CPE:** El primero indica que podría ser un S.O. basado en VirtualBox. El segundo un sistema que está corriendo sobre QEMU (otro software de virtualización) y el tercero a un posible switch de Bay Networks. En la imagen se visualiza en color naranja.

- **Predicción agresiva del sistema operativo:** La detección agresiva de S.O. confirma que la mejor suposición de Nmap es que se trata de una máquina virtual en VirtualBox o QEMU. En la imagen se visualiza en color rosa.
- **Distancia de red:** La máquina está a solo 1 salto de distancia. Lo que indica que podría estar directamente accesible en Internet (sin firewalls intermedios). En la imagen se visualiza en color amarillo.
- **Información del S.O detectado:** Se detecta que el sistema operativo base es Linux. En la imagen se visualiza en color morado.
- **Tiempo de escaneo:** 86.36 segundos.

```

Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
| 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
25/tcp    filtered smtp
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-favicon: Nmap Project
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (94%), Bay Networks embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack 450
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (94%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp) 45.33.32.156
HOP RTT ADDRESS
1 0.13 ms scanme.nmap.org (45.33.32.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 86.38 seconds

```

Figure 12: Escaneo agresivo - máquina (scanme.nmap.org - 45.33.32.156)

Al mismo tiempo que se está ejecutando el comando, la herramienta Wireshark captura el tráfico, mostrando cada paquete en detalle. En la siguiente imagen se visualiza los primeros paquetes capturados.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::983:e05c:606c...	ff02::c	UDP/XML	864	42972 → 3702 Len=802
2	0.001015424	fe80::c2	fe80::983:e05c:606c...	ICMPv6	912	Time Exceeded (hop limit exceeded in transit)
3	0.322699340	PCSSystemtec_6e:13:...	Broadcast	ARP	42	ARP Announcement for 10.0.2.15
4	3.553893267	PCSSystemtec_6e:13:...	Broadcast	ARP	42	who has 10.0.2.3? Tell 10.0.2.15
5	3.553886396	52:55:0a:00:02:03	PCSSystemtec_6e:13:...	ARP	64	10.0.2.3 is at 52:55:0a:00:02:03
6	3.553893911	10.0.2.15	10.0.2.3	DNS	75	Standard query 0x1f6c A scanme.nmap.org
7	3.553950469	10.0.2.15	10.0.2.3	DNS	75	Standard query 0x1603 AAAA scanme.nmap.org
8	3.582417156	10.0.2.3	10.0.2.15	DNS	91	Standard query response 0x1f6c A scanme.nmap.org A 45.33.32.156
9	3.598761713	10.0.2.3	10.0.2.15	DNS	103	Standard query response 0x1603 AAAA scanme.nmap.org AAAA 2600:3c01::f03c:91ff:fe18:bb2f
10	3.622091761	PCSSystemtec_6e:13:...	Broadcast	ARP	42	who has 10.0.2.2? Tell 10.0.2.15
11	3.623369709	52:55:0a:00:02:02	PCSSystemtec_6e:13:...	ARP	64	10.0.2.2 is at 52:55:0a:00:02:02
12	3.623381306	10.0.2.15	45.33.32.156	ICMP	42	Echo (ping) request id=0xa344, seq=0/0, ttl=54 (reply in 31)
13	3.623499988	10.0.2.15	45.33.32.156	TCP	58	56800 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	3.623592985	10.0.2.15	45.33.32.156	TCP	54	56550 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
15	3.623692721	10.0.2.15	45.33.32.156	ICMP	54	Timestamp request id=0x056d, seq=0/0, ttl=46
16	3.623692721	192.168.56.9	10.0.2.15	TCP	60	56550 → 80 [ACK] Seq=1 Ack=1 Win=0 Len=0
17	3.668111408	fd00::1b9c:ac22:717...	ff02::1:ff00:3	ICMPv6	86	Neighbor Solicitation for fd00::3 from 08:00:27:6e:13:6e
18	3.668581758	fd00::3	fd00::1b9c:ac22:717...	ICMPv6	86	Neighbor Advertisement fd00::3 (rtr, sol, ovr) is at 52:56:00:00:00:03
19	3.668634881	fd00::1b9c:ac22:717...	fd00::3	DNS	105	Standard query 0xed50 PTR 156.32.33.45.in-addr.arpa
20	3.719768897	fd00::3	fd00::1b9c:ac22:717...	DNS	134	Standard query response 0xed50 PTR 156.32.33.45.in-addr.arpa PTR scanme.nmap.org
21	3.737343252	10.0.2.15	45.33.32.156	TCP	58	56800 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	3.737718176	10.0.2.15	45.33.32.156	TCP	58	56800 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	3.737804696	10.0.2.15	45.33.32.156	TCP	58	56800 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	3.737838195	10.0.2.15	45.33.32.156	TCP	58	56800 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	3.737898809	10.0.2.15	45.33.32.156	TCP	58	56800 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	3.737902363	10.0.2.15	45.33.32.156	TCP	58	56800 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	3.737997324	10.0.2.15	45.33.32.156	TCP	58	56800 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	3.738054938	10.0.2.15	45.33.32.156	TCP	58	56800 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29	3.738116476	10.0.2.15	45.33.32.156	TCP	58	56800 → 507 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	3.738151672	10.0.2.15	45.33.32.156	TCP	58	56800 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
31	3.815627776	45.33.32.156	10.0.2.15	ICMP	60	Echo (ping) reply id=0xa344, seq=0/0, ttl=255 (request in 12)
32	3.926690554	45.33.32.156	192.168.56.9	TCP	60	56550 → 80 [ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460
33	3.926914505	10.0.2.15	45.33.32.156	TCP	54	56800 → 22 [RST] Seq=1 Win=0 Len=0
34	4.843197847	10.0.2.15	45.33.32.156	TCP	58	56800 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
35	4.843326030	10.0.2.15	45.33.32.156	TCP	58	56800 → 507 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
36	4.843415921	10.0.2.15	45.33.32.156	TCP	58	56800 → 1723 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
37	4.843478882	10.0.2.15	45.33.32.156	TCP	58	56800 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
38	4.843558951	10.0.2.15	45.33.32.156	TCP	58	56800 → 993 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
39	4.843615399	10.0.2.15	45.33.32.156	TCP	58	56800 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
40	4.843673760	10.0.2.15	45.33.32.156	TCP	58	56800 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 13: Wireshark - máquina (scanme.nmap.org - 45.33.32.156)

Escaneo agresivo - red virtualizada Para realizar este escaneo agresivo a una red virtualizada, se eligió la máquina 192.268.56.9 (Linux). Esta máquina se seleccionó porque tiene más puertos abiertos y menos puertos filtrados en comparación con la máquina de Windows.

```
nmap -A -T4 - -packet-trace 192.168.56.9 -oG ejercicio3_red.txt
```

Del mismo modo que en el escaneo a la máquina de internet, al ejecutar este comando, al principio se realiza una exploración de puertos. Se visualizan los paquetes enviados (SENT) y recibidos (RCVD), así como los mensajes de información NSOCK INFO.

En la imagen se representa en color rojo y azul, un paquete enviado (SENT) y su respuesta (RCVD) a un puerto abierto. Mientras que en color rosa y verde, un paquete enviado (SENT) a un puerto que no está abierto. La razón por la que se sabe que el puerto está cerrado es que, en este caso, el número de secuencia seq en la respuesta es igual a 0.

```

$ nmap -A -T4 --packet-trace 192.168.56.9 -oG ejercicio3_red.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 06:36 EST
SENT (0.1430s) ARP who-has 192.168.56.9 tell 192.168.56.100
RCVD (0.1440s) ARP reply 192.168.56.9 is-at 08:00:27:c8:59:b9
NSOCK INFO [0.2000s] nsock_ioc_new2(): nsock_ioc_new (IOD #1)
NSOCK INFO [0.2000s] nsock_connect_udp(): UDP connection requested to fd00::3:53 (IOD #1) EID 8
NSOCK INFO [0.2000s] nsock_trace_handler_callback(): Callback: CONNECT ERROR [Network is unreachable (101)] for
EID 8 [fd00::3:53]
NSOCK INFO [0.2000s] nsock_read(): Read request from IOD #1 [fd00::3:53] (timeout: -1ms) EID 18
NSOCK INFO [0.2000s] nsock_ioc_new2(): nsock_ioc_new (IOD #2)
NSOCK INFO [0.2000s] nsock_connect_udp(): UDP connection requested to 10.0.2.3:53 (IOD #2) EID 24
NSOCK INFO [0.2000s] nsock_read(): Read request from IOD #2 [10.0.2.3:53] (timeout: -1ms) EID 34
NSOCK INFO [0.2000s] nsock_write(): Write request for 43 bytes to IOD #1 EID 43 [fd00::3:53]
NSOCK INFO [0.2000s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [10.0.2.3:53]
NSOCK INFO [0.2000s] nsock_trace_handler_callback(): Callback: WRITE ERROR [Destination address required (89)]
for EID 43 [fd00::3:53]
NSOCK INFO [2.7330s] nsock_write(): Write request for 43 bytes to IOD #1 EID 51 [fd00::3:53]
NSOCK INFO [2.7330s] nsock_trace_handler_callback(): Callback: WRITE ERROR [Destination address required (89)]
for EID 51 [fd00::3:53]
NSOCK INFO [6.7580s] nsock_write(): Write request for 43 bytes to IOD #2 EID 59 [10.0.2.3:53]
NSOCK INFO [6.7580s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 59 [10.0.2.3:53]
NSOCK INFO [9.3810s] nsock_write(): Write request for 43 bytes to IOD #2 EID 67 [10.0.2.3:53]
NSOCK INFO [9.3810s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 67 [10.0.2.3:53]
NSOCK INFO [13.3810s] nsock_ioc_delete(): nsock_ioc_delete (IOD #1)
NSOCK INFO [13.3810s] nevent_delete(): nevent_delete on event #18 (type READ)
NSOCK INFO [13.3810s] nsock_ioc_delete(): nsock_ioc_delete (IOD #2)
NSOCK INFO [13.3810s] nevent_delete(): nevent_delete on event #34 (type READ)
SENT (13.3952s) TCP 192.168.56.100:64665 > 192.168.56.9:110 S ttl=44 id=45819 iplen=44 seq=50030929 win=1024 <
mss 1460>
SENT (13.3953s) TCP 192.168.56.100:64665 > 192.168.56.9:113 S ttl=43 id=65258 iplen=44 seq=50030929 win=1024 <
mss 1460>
SENT (13.3953s) TCP 192.168.56.100:64665 > 192.168.56.9:554 S ttl=49 id=21322 iplen=44 seq=50030929 win=1024 <
mss 1460>
SENT (13.3953s) TCP 192.168.56.100:64665 > 192.168.56.9:21 S ttl=50 id=30993 iplen=44 seq=50030929 win=1024 <m
ss 1460>
SENT (13.3953s) TCP 192.168.56.100:64665 > 192.168.56.9:1025 S ttl=46 id=42679 iplen=44 seq=50030929 win=1024
<mss 1460>
SENT (13.3953s) TCP 192.168.56.100:64665 > 192.168.56.9:1720 S ttl=47 id=10762 iplen=44 seq=50030929 win=1024
<mss 1460>
SENT (13.3953s) TCP 192.168.56.100:64665 > 192.168.56.9:3306 S ttl=43 id=26392 iplen=44 seq=50030929 win=1024
<mss 1460>
SENT (13.3953s) TCP 192.168.56.100:64665 > 192.168.56.9:53 S ttl=44 id=45496 iplen=44 seq=50030929 win=1024 <m
ss 1460>
SENT (13.3953s) TCP 192.168.56.100:64665 > 192.168.56.9:135 S ttl=57 id=21643 iplen=44 seq=50030929 win=1024 <
mss 1460>
SENT (13.3953s) TCP 192.168.56.100:64665 > 192.168.56.9:995 S ttl=52 id=54389 iplen=44 seq=50030929 win=1024 <
mss 1460>
RCVD (13.3980s) TCP 192.168.56.9:110 > 192.168.56.100:64665 RA ttl=64 id=0 iplen=40 seq=0 win=0
RCVD (13.3980s) TCP 192.168.56.9:113 > 192.168.56.100:64665 RA ttl=64 id=0 iplen=40 seq=0 win=0
RCVD (13.3980s) TCP 192.168.56.9:554 > 192.168.56.100:64665 RA ttl=64 id=0 iplen=40 seq=0 win=0
RCVD (13.3985s) TCP 192.168.56.9:21 > 192.168.56.100:64665 SA ttl=64 id=0 iplen=44 seq=2051115638 win=5840 <mss

```

Figure 14: Escaneo agresivo - máquina (192.168.56.9)

En este segundo escaneo, Nmap realiza un escaneo de servicios (**Service scan hard match**), enviando probes (sondeos) específicos para identificar el servicio que se está ejecutando en los puertos abiertos. En la siguiente imagen se visualiza un ejemplo (color azul).

Cabe destacar que en la imagen, dentro del primer rectángulo de color rojo, se observa un mensaje de (NSOCK INFO) el cual indica que el puerto 1524 está proporcionando acceso a un shell remoto, como se evidencia en la respuesta (**root@metasploitable:/**). Esto sugiere que dicho puerto está asociado a un servicio que permite la interacción directa con el sistema y que, en este caso, se ha obtenido acceso con privilegios de root.

Por otro lado, en el segundo rectángulo, se confirma que el puerto 1524 tiene un bind shell, lo que significa que ofrece acceso remoto a un shell en la máquina sin necesidad de autenticación.

```

NSOCK INFO [13.8270s] nsock_iod_delete(): nsock_iod_delete (IOD #12)
NSOCK INFO [13.8350s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 266 [192.168.56.9:512] (16
bytes): .Where are you?
Service scan hard match (Probe NULL matched with NULL line 585): 192.168.56.9:512 is exec. Version: |netkit-rs
h rexecd|||
NSOCK INFO [13.8350s] nsock_iod_delete(): nsock_iod_delete (IOD #10)
NSOCK INFO [13.8430s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 298 [192.168.56.9:1524] (2
3 bytes): root@metasploitable:/#
Service scan hard match (Probe NULL matched with NULL line 2994): 192.168.56.9:1524 is bindshell. Version: |Me
taspoitable root shell|||

```

Figure 15: Escaneo agresivo - máquina (192.168.56.9)

En la siguiente imagen se visualiza como se puede tener acceso a esta máquina objetivo.

```

(kali@kali)-[~/ejercicios/ejercicio3]
$ nc 192.168.56.9 1524

root@metasploitable:/#

```

Figure 16: Acceso remoto - máquina (192.168.56.9)

Del mismo modo, también aparecen mensajes NSE asociados con los diferentes scripts NSE ejecutados. En la siguiente imagen, se visualiza un ejemplo en el que se realizó una conexión HTTP y su respuesta, que indica que el puerto 80 está corriendo Apache y sirviendo una página web de Metasploitable2 (S.O.intencionalmente vulnerable).

```

NSE: TCP 192.168.56.100:45776 < 192.168.56.9:80 | HTTP/1.1 200 OK
Date: Tue, 18 Feb 2025 11:36:54 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html

<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
22 14.00345264 192.168.56.100 192.168.56.9 TCP
23 14.00367383 192.168.56.100 192.168.56.9 TCP
24 14.0037766 192.168.56.100 192.168.56.9 TCP
25 14.00387937 192.168.56.100 192.168.56.9 TCP
26 14.00398214 192.168.56.100 192.168.56.9 TCP
27 14.00408491 192.168.56.100 192.168.56.9 TCP
28 14.00418768 192.168.56.100 192.168.56.9 TCP
29 14.00429045 192.168.56.100 192.168.56.9 TCP
30 14.00439322 192.168.56.100 192.168.56.9 TCP
31 14.00449599 192.168.56.100 192.168.56.9 TCP
32 14.00460104 192.168.56.100 192.168.56.9 TCP
33 14.00470609 192.168.56.100 192.168.56.9 TCP
34 14.00481114 192.168.56.100 192.168.56.9 TCP
35 14.00491619 192.168.56.100 192.168.56.9 TCP
36 14.00502124 192.168.56.100 192.168.56.9 TCP
37 14.00512629 192.168.56.100 192.168.56.9 TCP
38 14.00523134 192.168.56.100 192.168.56.9 TCP
39 14.00533639 192.168.56.100 192.168.56.9 TCP
40 14.00544144 192.168.56.100 192.168.56.9 TCP
41 14.00554649 192.168.56.100 192.168.56.9 TCP
42 14.00565154 192.168.56.100 192.168.56.9 TCP
43 14.00575659 192.168.56.100 192.168.56.9 TCP
44 14.00586164 192.168.56.100 192.168.56.9 TCP
45 14.00596669 192.168.56.100 192.168.56.9 TCP
46 14.00607174 192.168.56.100 192.168.56.9 TCP
47 14.00617679 192.168.56.100 192.168.56.9 TCP
48 14.00628184 192.168.56.100 192.168.56.9 TCP
49 14.00638689 192.168.56.100 192.168.56.9 TCP
50 14.00649194 192.168.56.100 192.168.56.9 TCP
51 14.00659699 192.168.56.100 192.168.56.9 TCP
52 14.00670204 192.168.56.100 192.168.56.9 TCP
53 14.00680709 192.168.56.100 192.168.56.9 TCP
54 14.00691214 192.168.56.100 192.168.56.9 TCP
55 14.00701719 192.168.56.100 192.168.56.9 TCP
56 14.00712224 192.168.56.100 192.168.56.9 TCP
57 14.00722729 192.168.56.100 192.168.56.9 TCP
58 14.00733234 192.168.56.100 192.168.56.9 TCP
59 14.00743739 192.168.56.100 192.168.56.9 TCP
60 14.00754244 192.168.56.100 192.168.56.9 TCP
61 14.00764749 192.168.56.100 192.168.56.9 TCP
62 14.00775254 192.168.56.100 192.168.56.9 TCP
63 14.00785759 192.168.56.100 192.168.56.9 TCP
64 14.00796264 192.168.56.100 192.168.56.9 TCP
65 14.00806769 192.168.56.100 192.168.56.9 TCP
66 14.00817274 192.168.56.100 192.168.56.9 TCP
67 14.00827779 192.168.56.100 192.168.56.9 TCP
68 14.00838284 192.168.56.100 192.168.56.9 TCP
69 14.00848789 192.168.56.100 192.168.56.9 TCP
70 14.00859294 192.168.56.100 192.168.56.9 TCP
71 14.00869799 192.168.56.100 192.168.56.9 TCP
72 14.00880304 192.168.56.100 192.168.56.9 TCP
73 14.00890809 192.168.56.100 192.168.56.9 TCP
74 14.00901314 192.168.56.100 192.168.56.9 TCP
75 14.00911819 192.168.56.100 192.168.56.9 TCP
76 14.00922324 192.168.56.100 192.168.56.9 TCP
77 14.00932829 192.168.56.100 192.168.56.9 TCP
78 14.00943334 192.168.56.100 192.168.56.9 TCP
79 14.00953839 192.168.56.100 192.168.56.9 TCP
80 14.00964344 192.168.56.100 192.168.56.9 TCP
81 14.00974849 192.168.56.100 192.168.56.9 TCP
82 14.00985354 192.168.56.100 192.168.56.9 TCP
83 14.00995859 192.168.56.100 192.168.56.9 TCP
84 14.01006364 192.168.56.100 192.168.56.9 TCP
85 14.01016869 192.168.56.100 192.168.56.9 TCP
86 14.01027374 192.168.56.100 192.168.56.9 TCP
87 14.01037879 192.168.56.100 192.168.56.9 TCP
88 14.01048384 192.168.56.100 192.168.56.9 TCP
89 14.01058889 192.168.56.100 192.168.56.9 TCP
90 14.01069394 192.168.56.100 192.168.56.9 TCP
91 14.01079899 192.168.56.100 192.168.56.9 TCP
92 14.01090404 192.168.56.100 192.168.56.9 TCP
93 14.01100909 192.168.56.100 192.168.56.9 TCP
94 14.01111414 192.168.56.100 192.168.56.9 TCP
95 14.01121919 192.168.56.100 192.168.56.9 TCP
96 14.01132424 192.168.56.100 192.168.56.9 TCP
97 14.01142929 192.168.56.100 192.168.56.9 TCP
98 14.01153434 192.168.56.100 192.168.56.9 TCP
99 14.01163939 192.168.56.100 192.168.56.9 TCP
100 14.01174444 192.168.56.100 192.168.56.9 TCP
101 14.01184949 192.168.56.100 192.168.56.9 TCP
102 14.01195454 192.168.56.100 192.168.56.9 TCP
103 14.01205959 192.168.56.100 192.168.56.9 TCP
104 14.01216464 192.168.56.100 192.168.56.9 TCP
105 14.01226969 192.168.56.100 192.168.56.9 TCP
106 14.01237474 192.168.56.100 192.168.56.9 TCP
107 14.01247979 192.168.56.100 192.168.56.9 TCP
108 14.01258484 192.168.56.100 192.168.56.9 TCP
109 14.01268989 192.168.56.100 192.168.56.9 TCP
110 14.01279494 192.168.56.100 192.168.56.9 TCP
111 14.01289999 192.168.56.100 192.168.56.9 TCP
112 14.01300504 192.168.56.100 192.168.56.9 TCP
113 14.01311009 192.168.56.100 192.168.56.9 TCP
114 14.01321514 192.168.56.100 192.168.56.9 TCP
115 14.01332019 192.168.56.100 192.168.56.9 TCP
116 14.01342524 192.168.56.100 192.168.56.9 TCP
117 14.01353029 192.168.56.100 192.168.56.9 TCP
118 14.01363534 192.168.56.100 192.168.56.9 TCP
119 14.01374039 192.168.56.100 192.168.56.9 TCP
120 14.01384544 192.168.56.100 192.168.56.9 TCP
121 14.01395049 192.168.56.100 192.168.56.9 TCP
122 14.01405554 192.168.56.100 192.168.56.9 TCP
123 14.01416059 192.168.56.100 192.168.56.9 TCP
124 14.01426564 192.168.56.100 192.168.56.9 TCP
125 14.01437069 192.168.56.100 192.168.56.9 TCP
126 14.01447574 192.168.56.100 192.168.56.9 TCP
127 14.01458079 192.168.56.100 192.168.56.9 TCP
128 14.01468584 192.168.56.100 192.168.56.9 TCP
129 14.01479089 192.168.56.100 192.168.56.9 TCP
130 14.01489594 192.168.56.100 192.168.56.9 TCP
131 14.01500099 192.168.56.100 192.168.56.9 TCP
132 14.01510604 192.168.56.100 192.168.56.9 TCP
133 14.01521109 192.168.56.100 192.168.56.9 TCP
134 14.01531614 192.168.56.100 192.168.56.9 TCP
135 14.01542119 192.168.56.100 192.168.56.9 TCP
136 14.01552624 192.168.56.100 192.168.56.9 TCP
137 14.01563129 192.168.56.100 192.168.56.9 TCP
138 14.01573634 192.168.56.100 192.168.56.9 TCP
139 14.01584139 192.168.56.100 192.168.56.9 TCP
140 14.01594644 192.168.56.100 192.168.56.9 TCP
141 14.01605149 192.168.56.100 192.168.56.9 TCP
142 14.01615654 192.168.56.100 192.168.56.9 TCP
143 14.01626159 192.168.56.100 192.168.56.9 TCP
144 14.01636664 192.168.56.100 192.168.56.9 TCP
145 14.01647169 192.168.56.100 192.168.56.9 TCP
146 14.01657674 192.168.56.100 192.168.56.9 TCP
147 14.01668179 192.168.56.100 192.168.56.9 TCP
148 14.01678684 192.168.56.100 192.168.56.9 TCP
149 14.01689189 192.168.56.100 192.168.56.9 TCP
150 14.01699694 192.168.56.100 192.168.56.9 TCP
151 14.01710199 192.168.56.100 192.168.56.9 TCP
152 14.01720704 192.168.56.100 192.168.56.9 TCP
153 14.01731209 192.168.56.100 192.168.56.9 TCP
154 14.01741714 192.168.56.100 192.168.56.9 TCP
155 14.01752219 192.168.56.100 192.168.56.9 TCP
156 14.01762724 192.168.56.100 192.168.56.9 TCP
157 14.01773229 192.168.56.100 192.168.56.9 TCP
158 14.01783734 192.168.56.100 192.168.56.9 TCP
159 14.01794239 192.168.56.100 192.168.56.9 TCP
160 14.01804744 192.168.56.100 192.168.56.9 TCP
161 14.01815249 192.168.56.100 192.168.56.9 TCP
162 14.01825754 192.168.56.100 192.168.56.9 TCP
163 14.01836259 192.168.56.100 192.168.56.9 TCP
164 14.01846764 192.168.56.100 192.168.56.9 TCP
165 14.01857269 192.168.56.100 192.168.56.9 TCP
166 14.01867774 192.168.56.100 192.168.56.9 TCP
167 14.01878279 192.168.56.100 192.168.56.9 TCP
168 14.01888784 192.168.56.100 192.168.56.9 TCP
169 14.01899289 192.168.56.100 192.168.56.9 TCP
170 14.01909794 192.168.56.100 192.168.56.9 TCP
171 14.01920299 192.168.56.100 192.168.56.9 TCP
172 14.01930804 192.168.56.100 192.168.56.9 TCP
173 14.01941309 192.168.56.100 192.168.56.9 TCP
174 14.01951814 192.168.56.100 192.168.56.9 TCP
175 14.01962319 192.168.56.100 192.168.56.9 TCP
176 14.01972824 192.168.56.100 192.168.56.9 TCP
177 14.01983329 192.168.56.100 192.168.56.9 TCP
178 14.01993834 192.168.56.100 192.168.56.9 TCP
179 14.02004339 192.168.56.100 192.168.56.9 TCP
180 14.02014844 192.168.56.100 192.168.56.9 TCP
181 14.02025349 192.168.56.100 192.168.56.9 TCP
182 14.02035854 192.168.56.100 192.168.56.9 TCP
183 14.02046359 192.168.56.100 192.168.56.9 TCP
184 14.02056864 192.168.56.100 192.168.56.9 TCP
185 14.02067369 192.168.56.100 192.168.56.9 TCP
186 14.02077874 192.168.56.100 192.168.56.9 TCP
187 14.02088379 192.168.56.100 192.168.56.9 TCP
188 14.02098884 192.168.56.100 192.168.56.9 TCP
189 14.02109389 192.168.56.100 192.168.56.9 TCP
190 14.02119894 192.168.56.100 192.168.56.9 TCP
191 14.02130399 192.168.56.100 192.168.56.9 TCP
192 14.02140904 192.168.56.100 192.168.56.9 TCP
193 14.02151409 192.168.56.100 192.168.56.9 TCP
194 14.02161914 192.168.56.100 192.168.56.9 TCP
195 14.02172419 192.168.56.100 192.168.56.9 TCP
196 14.02182924 192.168.56.100 192.168.56.9 TCP
197 14.02193429 192.168.56.100 192.168.56.9 TCP
198 14.02203934 192.168.56.100 192.168.56.9 TCP
199 14.02214439 192.168.56.100 192.168.56.9 TCP
200 14.02224944 192.168.56.100 192.168.56.9 TCP
201 14.02235449 192.168.56.100 192.168.56.9 TCP
202 14.02245954 192.168.56.100 192.168.56.9 TCP
203 14.02256459 192.168.56.100 192.168.56.9 TCP
204 14.02266964 192.168.56.100 192.168.56.9 TCP
205 14.02277469 192.168.56.100 192.168.56.9 TCP
206 14.02287974 192.168.56.100 192.168.56.9 TCP
207 14.02298479 192.168.56.100 192.168.56.9 TCP
208 14.02308984 192.168.56.100 192.168.56.9 TCP
209 14.02319489 192.168.56.100 192.168.56.9 TCP
210 14.02329994 192.168.56.100 192.168.56.9 TCP
211 14.02340499 192.168.56.100 192.168.56.9 TCP
212 14.02351004 192.168.56.100 192.168.56.9 TCP
213 14.02361509 192.168.56.100 192.168.56.9 TCP
214 14.02372014 192.168.56.100 192.168.56.9 TCP
215 14.02382519 192.168.56.100 192.168.56.9 TCP
216 14.02393024 192.168.56.100 192.168.56.9 TCP
217 14.02403529 192.168.56.100 192.168.56.9 TCP
218 14.02414034 192.168.56.100 192.168.56.9 TCP
219 14.02424539 192.168.56.100 192.168.56.9 TCP
220 14.02435044 192.168.56.100 192.168.56.9 TCP
221 14.02445549 192.168.56.100 192.168.56.9 TCP
222 14.02456054 192.168.56.100 192.168.56.9 TCP
223 14.02466559 192.168.56.100 192.168.56.9 TCP
224 14.02477064 192.168.56.100 192.168.56.9 TCP
225 14.02487569 192.168.56.100 192.168.56.9 TCP
226 14.02498074 192.168.56.100 192.168.56.9 TCP
227 14.02508579 192.168.56.100 192.168.56.9 TCP
228 14.02519084 192.168.56.100 192.168.56.9 TCP
229 14.02529589 192.168.56.100 192.168.56.9 TCP
230 14.02540094 192.168.56.100 192.168.56.9 TCP
231 14.02550599 192.168.56.100 192.168.56.9 TCP
232 14.02561104 192.168.56.100 192.168.56.9 TCP
233 14.02571609 192.168.56.100 192.168.56.9 TCP
234 14.02582114 192.168.56.100 192.168.56.9 TCP
235 14.02592619 192.168.56.100 192.168.56.9 TCP
236 14.02603124 192.168.56.100 192.168.56.9 TCP
237 14.02613629 192.168.56.100 192.168.56.9 TCP
238 14.02624134 192.168.56.100 192.168.56.9 TCP
239 14.02634639 192.168.56.100 192.168.56.9 TCP
240 14.02645144 192.168.56.100 192.168.56.9 TCP
241 14.02655649 192.168.56.100 192.168.56.9 TCP
242 14.02666154 192.168.56.100 192.168.56.9 TCP
243 14.02676659 192.168.56.100 192.168.56.9 TCP
244 14.02687164 192.168.56.100 192.168.56.9 TCP
245 14.02697669 192.168.56.100 192.168.56.9 TCP
246 14.02708174 192.168.56.100 192.168.56.9 TCP
247 14.02718679 192.168.56.100 192.168.56.9 TCP
248 14.02729184 192.168.56.100 192.168.56.9 TCP
249 14.02739689 192.168.56.100 192.168.56.9 TCP
250 14.02750194 192.168.56.100 192.168.56.9 TCP
251 14.02760699 192.168.56.100 192.168.56.9 TCP
252 14.02771204 192.168.56.100 192.168.56.9 TCP
253 14.02781709 192.168.56.100 192.168.56.9 TCP
254 14.02792214 192.168.56.100 192.168.56.9 TCP
255 14.02802719 192.168.56.100 192.168.56.9 TCP
256 14.02813224 192.168.56.100 192.168.56.9 TCP
257 14.02823729 192.168.56.100 192.168.56.9 TCP
258 14.02834234 192.168.56.100 192.168.56.9 TCP
259 14.02844739 192.168.56.100 192.168.56.9 TCP
260 14.02855244 192.168.56.100 192.168.56.9 TCP
261 14.02865749 192.168.56.100 192.168.56.9 TCP
262 14.02876254 192.168.56.100 192.168.56.9 TCP
263 14.02886759 192.168.56.100 192.168.56.9 TCP
264 14.02897264 192.168.56.100 192.168.56.9 TCP
265 14.02907769 192.168.56.100 192.168.56.9 TCP
266 14.02918274 192.168.56.100 192.168.56.9 TCP
267 14.02928779 192.168.56.100 192.168.56.9 TCP
268 14.02939284 192.168.56.100 192.168.56.9 TCP
269 14.02949789 192.168.56.100 192.168.56.9 TCP
270 14.02960294 192.168.56.100 192.168.56.9 TCP
271 14.02970799 192.168.56.100 192.168.56.9 TCP
272 14.02981304 192.168.56.100 192.168.56.9 TCP
273 14.02991809 192.168.56.100 192.168.56.9 TCP
274 14.03002314 192.168.56.100 192.168.56.9 TCP
275 14.03012819 192.168.56.100 192.168.56.9 TCP
276 14.03023324 192.168.56.100 192.168.56.9 TCP
277 14.03033829 192.168.56.100 192.168.56.9 TCP
278 14.03044334 192.16
```

En la siguiente imagen 18 se visualiza que se están realizando muchas conexiones repetidas a los puertos 137, 80, 8180, 5900, 1434, entre otros. En comparación con la máquina de Internet, que solo la mayoría de conexiones repetidas pertenece a los puertos 80 y 22, esto sugiere que la máquina de Linux pertenece a una red interna con una mayor cantidad de servicios y puertos accesibles. Esto puede indicar que no está protegida por un firewall tan restrictivo como el de la máquina en Internet, permitiendo el escaneo y la interacción con una variedad más amplia de servicios.

```

NSE: TCP 192.168.56.100:44968 > 192.168.56.9:8180 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [192.168.56.9:137]
NSE: UDP 192.168.56.100:42851 > 192.168.56.9:137 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 16 [192.168.56.9:80]
NSE: TCP 192.168.56.100:45764 > 192.168.56.9:80 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 32 [192.168.56.9:8180]
NSE: TCP 192.168.56.100:44970 > 192.168.56.9:8180 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 40 [192.168.56.9:80]
NSE: TCP 192.168.56.100:45776 > 192.168.56.9:80 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 48 [192.168.56.9:5900]
NSE: TCP 192.168.56.100:51832 > 192.168.56.9:5900 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 56 [192.168.56.9:80]
NSE: TCP 192.168.56.100:45792 > 192.168.56.9:80 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT ERROR [Connection refused (111)] for EID
D 64 [192.168.56.9:25539]
NSE: TCP 192.168.56.100:59486 > 192.168.56.9:25539 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 80 [192.168.56.9:1434]
NSE: UDP 192.168.56.100:44382 > 192.168.56.9:1434 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 72 [192.168.56.9:8180]
NSE: TCP 192.168.56.100:44976 > 192.168.56.9:8180 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 88 [192.168.56.9:80]
NSE: TCP 192.168.56.100:45800 > 192.168.56.9:80 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 96 [192.168.56.9:80]
NSE: TCP 192.168.56.100:45814 > 192.168.56.9:80 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 104 [192.168.56.9:80]
NSE: TCP 192.168.56.100:45822 > 192.168.56.9:80 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 112 [192.168.56.9:8180]
NSE: TCP 192.168.56.100:44988 > 192.168.56.9:8180 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 120 [192.168.56.9:80]
NSE: TCP 192.168.56.100:45836 > 192.168.56.9:80 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 128 [192.168.56.9:80]
NSE: TCP 192.168.56.100:45852 > 192.168.56.9:80 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 136 [192.168.56.9:137]
NSE: UDP 192.168.56.100:54000 > 192.168.56.9:137 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 144 [192.168.56.9:8180]
NSE: TCP 192.168.56.100:44990 > 192.168.56.9:8180 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 152 [192.168.56.9:8180]
NSE: TCP 192.168.56.100:45002 > 192.168.56.9:8180 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 160 [192.168.56.9:8180]
NSE: TCP 192.168.56.100:45018 > 192.168.56.9:8180 | CONNECT
NSOCK INFO [26.3930s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 168 [192.168.56.9:8180]
NSE: TCP 192.168.56.100:45028 > 192.168.56.9:8180 | CONNECT
NSE: TCP 192.168.56.100:44968 > 192.168.56.9:8180 | 00000000: 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d 0a G
ET / HTTP/1.1

```

Figure 18: Acceso remoto - máquina (192.168.56.9)

Por último, aparecen los puertos abiertos (23) y sus servicios. A continuación, se proporciona información sobre la máquina 192.168.56.9:

- **Tipo de dispositivo detectado.** Se identifica como un dispositivo de propósito general, lo que significa que no es un dispositivo especializado, sino un sistema más general. En la imagen se visualiza en color verde.
- **Running:** Indica que la máquina está ejecutando Linux 2.6.X . En la imagen se visualiza en color verde oscuro.
- **Identificadores CPE:** Se refiere al kernel de Linux versión 2.6. En la imagen se visualiza en color naranja.
- **OS Details:** Se especifica que el sistema operativo es Linux 2.6.9 - 2.6.33. En la imagen se visualiza en color rosa.
- **Distancia:** La máquina está a solo 1 salto de distancia. Lo que indica que está directamente conectada a tu red sin intermediarios. En la imagen se visualiza en color amarillo.

- **Información del S.O detectado:** Los nombres de host asociados son `metasploitable.localdomain` y `irc.Metasploitable.LAN`. Esto indica que la máquina está identificada en la red como `metasploitable`. Por otro lado, el sistema operativo identificado es Unix (Linux). En la imagen se visualiza en color morado.
- **Tiempo de escaneo:** 41.34 segundos.

```

Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
| STAT:
| FTP server status:
|   Connected to 192.168.56.100
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPd 2.3.4 - secure, fast, stable
| End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is
no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ ssl-date: 2025-02-18T11:37:08+00:00; -1s from scanner time.
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCOD
ES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service

```

Figure 19: Acceso remoto - máquina (192.168.56.9)


```

111/tcp open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2             111/tcp    rpcbind
|   100000  2             111/udp    rpcbind
|   100003  2,3,4         2049/tcp   nfs
|   100003  2,3,4         2049/udp   nfs
|   100005  1,2,3         45954/udp  mountd
|   100005  1,2,3         52710/tcp  mountd
|   100021  1,3,4         33822/udp  nlockmgr
|   100021  1,3,4         53980/tcp  nlockmgr
|   100024  1             37762/tcp  status
|   100024  1             38609/udp  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login       OpenBSD or Solaris rlogind
514/tcp open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SwitchToSSLAfterHandshake, ConnectWithDatabase, LongColumnFlag, Speaks41P
|   rotocolNew, SupportsCompression, SupportsTransactions
|   Status: Autocommit
|   _Salt: g*8yysX=hs*q!I/Mt$PH
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| _ssl-date: 2025-02-18T11:37:08+00:00; -1s from scanner time.
| _ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is
no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|   VNC Authentication (2)
6000/tcp open  X11         (access denied)
5667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
| _ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1

```

Figure 20: Acceso remoto - máquina (192.168.56.9)

```

8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
| _http-favicon: Apache Tomcat
| _http-title: Apache Tomcat/5.5
| _http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:C8:59:B9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2025-02-18T06:36:54-05:00
|_ smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ cLock-skew: mean: 1h14m59s, deviation: 2h30m00s, median: -1s

TRACEROUTE
HOP RTT ADDRESS
1 1.07 ms 192.168.56.9

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 41.34 seconds

```

Figure 21: Acceso remoto - máquina (192.168.56.9)

Mientras se ejecuta el comando, Wireshark está capturando el tráfico de red y mostrando cada paquete en detalle. En la imagen siguiente se pueden ver los primeros paquetes capturados durante el proceso.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::983:e95c:606c...	ff02::c	UDP/XML	864	34271 → 3702 Len=802
2	0.246153873	192.168.56.100	239.255.255.250	UDP/XML	844	48505 → 3702 Len=802
3	0.560780517	fe80::983:e95c:606c...	ff02::c	UDP/XML	864	34271 → 3702 Len=802
4	1.195056398	192.168.56.100	239.255.255.250	UDP/XML	844	48505 → 3702 Len=802
5	1.196146615	fe80::983:e95c:606c...	ff02::c	UDP/XML	864	34271 → 3702 Len=802
6	1.358476438	PCSSystemtec_6e:13:...	Broadcast	ARP	42	Who has 192.168.56.9? Tell 192.168.56.100
7	1.351410330	PCSSystemtec_c8:59:...	PCSSystemtec_6e:13:...	ARP	60	192.168.56.9 is at 08:00:27:c8:59:b9
8	1.394336417	192.168.56.100	239.255.255.250	UDP/XML	844	48505 → 3702 Len=802
9	1.427151184	fe80::983:e95c:606c...	ff02::c	UDP/XML	864	34271 → 3702 Len=802
10	1.927982423	192.168.56.100	239.255.255.250	UDP/XML	844	48505 → 3702 Len=802
11	1.928716880	fe80::983:e95c:606c...	ff02::c	UDP/XML	864	34271 → 3702 Len=802
12	2.345205671	192.168.56.100	239.255.255.250	UDP/XML	844	48505 → 3702 Len=802
13	2.453387974	fe80::983:e95c:606c...	ff02::c	UDP/XML	864	34271 → 3702 Len=802
14	7.092151062	fe80::983:e95c:606c...	ff02::2	ICMPv6	62	Router Solicitation
15	7.965989994	PCSSystemtec_6e:13:...	Broadcast	ARP	42	Who has 192.168.56.1? Tell 192.168.56.100
16	9.088617677	PCSSystemtec_6e:13:...	Broadcast	ARP	42	Who has 192.168.56.1? Tell 192.168.56.100
17	10.152081536	PCSSystemtec_6e:13:...	Broadcast	ARP	42	Who has 192.168.56.1? Tell 192.168.56.100
18	14.602206170	PCSSystemtec_6e:13:...	Broadcast	ARP	42	Who has 192.168.56.9? Tell 192.168.56.100
19	14.603722825	PCSSystemtec_c8:59:...	PCSSystemtec_6e:13:...	ARP	60	192.168.56.9 is at 08:00:27:c8:59:b9
20	14.603722878	192.168.56.100	192.168.56.9	TCP	58	64605 → 110 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
21	14.603760473	192.168.56.100	192.168.56.9	TCP	58	64605 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	14.603845264	192.168.56.100	192.168.56.9	TCP	58	64605 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
23	14.603867383	192.168.56.100	192.168.56.9	TCP	58	64605 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	14.604107666	192.168.56.100	192.168.56.9	TCP	58	64605 → 1825 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
25	14.604164025	192.168.56.100	192.168.56.9	TCP	58	64605 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
26	14.604185398	192.168.56.100	192.168.56.9	TCP	58	64605 → 3308 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27	14.604282190	192.168.56.100	192.168.56.9	TCP	58	64605 → 53 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
28	14.604306568	192.168.56.100	192.168.56.9	TCP	58	64605 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
29	14.604328305	192.168.56.100	192.168.56.9	TCP	58	64605 → 95 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
30	14.605451876	192.168.56.9	192.168.56.100	TCP	60	110 → 64605 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
31	14.605451979	192.168.56.9	192.168.56.100	TCP	60	113 → 64605 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
32	14.605451999	192.168.56.9	192.168.56.100	TCP	60	554 → 64605 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	14.605507623	192.168.56.9	192.168.56.100	TCP	60	21 → 64605 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 MSS=1460
34	14.605597848	192.168.56.9	192.168.56.100	TCP	60	1825 → 64605 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
35	14.605597879	192.168.56.9	192.168.56.100	TCP	60	1720 → 64605 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
36	14.605577856	192.168.56.100	192.168.56.9	TCP	54	64605 → 21 [RST] Seq=1 Win=0 Len=0
37	14.606260848	192.168.56.9	192.168.56.100	TCP	60	3306 → 64605 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
38	14.606260874	192.168.56.9	192.168.56.100	TCP	60	53 → 64605 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
39	14.606261510	192.168.56.100	192.168.56.9	TCP	54	64605 → 3306 [RST] Seq=1 Win=0 Len=0
40	14.606366516	192.168.56.100	192.168.56.9	TCP	54	64605 → 53 [RST] Seq=1 Win=0 Len=0

Figure 22: Wireshark - máquina (192.168.56.9)

Diferencias.

- **Tiempo de escaneo:** La máquina de internet **scanme** tiene una menor velocidad (86.36 segundos), en relación a la máquina que se encuentra en la misma red (41.34 segundos). Esto se debe a factores como la mayor latencia de la red pública y la posible presencia de algún firewall que agregan retrasos en el proceso de escaneo.
- **Seguridad:** La máquina en Internet parece estar configurada con medidas de seguridad más estrictas, ya que solo tiene 5 puertos abiertos. En cambio, la máquina en la red local tiene 23 puertos abiertos, lo que indica una configuración de seguridad más débil y menos restricciones de acceso.
- **Wireshark:** En la máquina de Linux se observa una mayor cantidad de servicios disponibles y más tráfico debido a la mayor cantidad de puertos abiertos.
- **Paquete - Service scan hard match:** En la máquina Linux se registran paquetes de tipo **Service scan hard match**. Esto se debe a que Nmap tiene un acceso más directo a los servicios, debido a que la máquina tiene una configuración de red menos restrictiva en comparación con la máquina de Internet.

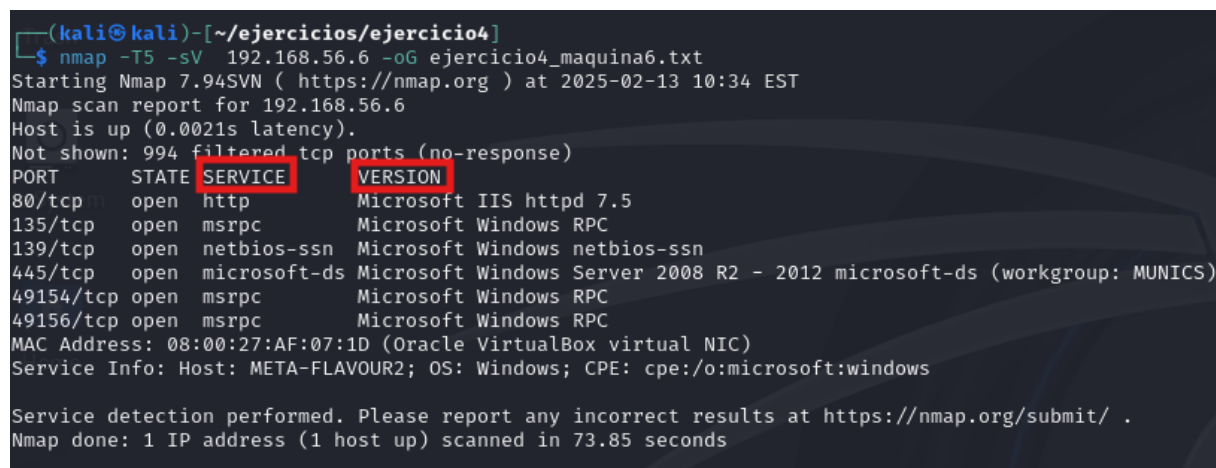
4 Realizar un escaneo lo más rápido posible (insane) sobre las máquinas disponibles. Comprobar además la versión de los servicios implementados. Buscar al menos una vulnerabilidad en <https://cve.mitre.org/> para cada uno de esos servicios.

Para este apartado, se tiene como objetivo realizar un escaneo lo más rápido posible (insane). Para ello, se utiliza la opción `-T5`, que permite establecer el escaneo en el modo más rápido. Además, se emplea la opción `-sV` para detectar las versiones de los servicios que están corriendo en los puertos abiertos.

Escaneo insane - máquina 192.168.56.6 La primera máquina en la que se realiza el escaneo insane es la de Windows (192.168.56.6). El comando utilizado es:

```
nmap -sV -T5 192.168.56.6 -oG ejercicio4_maquina6.txt
```

En la siguiente imagen se visualizan los puertos abiertos, los servicios detectados y sus respectivas versiones tras el escaneo.



```
(kali㉿kali)-[~/ejercicios/ejercicio4]
$ nmap -T5 -sV 192.168.56.6 -oG ejercicio4_maquina6.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-13 10:34 EST
Nmap scan report for 192.168.56.6
Host is up (0.0021s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 7.5
135/tcp    open  msrpc     Microsoft Windows RPC
139/tcp    open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: MUNICS)
49154/tcp  open  msrpc     Microsoft Windows RPC
49156/tcp  open  msrpc     Microsoft Windows RPC
MAC Address: 08:00:27:AF:07:1D (Oracle VirtualBox virtual NIC)
Service Info: Host: META-FLAVOUR2; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 73.85 seconds
```

Figure 23: Escaneo insane - máquina (192.168.56.6)

1. **Servicio - http:** En relación al servicio http con la versión Microsoft IIS httpd 7.5, se encontraron las vulnerabilidades CVE-2010-2730, CVE-2010-3972 y CVE-2010-1899.
 - **CVE-2010-2730:** [1] Esta vulnerabilidad es un desbordamiento de búfer que afecta a Microsoft IIS 7.5 cuando FastCGI está habilitado, permitiendo a un atacante remoto ejecutar código arbitrario mediante el envío de encabezados de solicitud especialmente diseñados.
 - **CVE-2010-3972:** [2] Esta vulnerabilidad es un desbordamiento de búfer que afecta a Microsoft IIS 7.5. Cuando un atacante envía solicitudes HTTP maliciosas al servidor IIS, se puede provocar una ejecución remota de código.
 - **CVE-2010-1899:** [3] Esta vulnerabilidad permite a un atacante realizar una elevación de privilegios en un sistema que ejecuta Microsoft IIS 7.5.

2. **Servicio - msrpc:** Se encontró la vulnerabilidad CVE-2020-1113 [4] en el servicio Microsoft Remote Procedure Call, la cual está relacionada con una falla en Windows RPC que permite la elevación de privilegios.
3. **Servicio - netbios-ssn:** En relación a este servicio se encontró la vulnerabilidad CVE-2018-7445 [5]. Esta vulnerabilidad está asociada con un desbordamiento de búfer en el servicio NETBIOS, que es utilizado en redes Windows para compartir recursos y realizar comunicación entre sistemas.
4. **Servicio - microsoft-ds:** Se detectó una vulnerabilidad en el servicio Microsoft SMBv1 a través del puerto 445/tcp, en el servicio *microsoft-ds*, que corresponde a la vulnerabilidad CVE-2017-0143 [6]. Esta vulnerabilidad afecta a varias versiones de Windows, incluida la versión utilizada en el servidor Windows Server 2008 R2. Este servicio contiene una debilidad crítica que permite a un atacante remoto ejecutar código arbitrario en el sistema afectado.

Escaneo insane - máquina 192.168.56.9 A continuación, se realiza el escaneo insane a la máquina de Linux (192.168.56.9). El comando utilizado es:

```
nmap -sV -T5 192.168.56.9 -oG ejercicio4_maquina9.txt
```

```
(kali@kali)~[~/ejercicios/ejercicio4]
$ nmap -sV -T5 192.168.56.9 -oG ejercicio4_maquina9.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-13 18:51 EST
Nmap scan report for 192.168.56.9
Host is up (0.00036s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind  2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rshd
513/tcp   open  login    Netkit rshd
514/tcp   open  shell    Netkit rshd
1099/tcp  open  java-rmi GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql    MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc      VNC (protocol 3.3)
6000/tcp  open  X11      (access denied)
6667/tcp  open  irc      UnrealIRCd
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:C8:59:B9 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, 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 24.53 seconds
```

Figure 24: Escaneo insane - máquina (192.168.56.9)

1. **Servicio - ftp:** Para este servicio, se encontró la vulnerabilidad CVE-2011-2523 [7], la cual afecta a *vsftpd* 2.3.4. Esta vulnerabilidad ocurre debido a la presencia de un backdoor en el código fuente comprometido del servidor FTP.

2. **Servicio - ssh:** Se encontró la vulnerabilidad CVE-2008-5161 [8], la cual afecta a la versión `OpenSSH 4.7p1 Debian 8ubuntu1`. Esta vulnerabilidad en los modos CBC permite a un atacante recuperar partes de texto sin cifrar analizando la longitud de los paquetes SSH.
3. **Servicio - telnet:** En relación a este servicio telnet, se encontró la vulnerabilidad CVE-2005-2040 [9], la cual es un desbordamiento de búfer en telnetd.
4. **Servicio - smtp:** Para este servicio, se encontró la vulnerabilidad CVE-2015-4000 [10]. Esta vulnerabilidad afecta a Postfix smtpd y permite un ataque de denegación de servicio (DoS).
5. **Servicio - domain:** Se encontró la vulnerabilidad CVE-2008-0122 [11], la cual está relacionada con un problema de desbordamiento de búfer en el servicio de DNS de BIND.
6. **Servicio - http:** Para este servicio, se encontró la vulnerabilidad CVE-2017-3167 [12]. Esta vulnerabilidad se relaciona con una falta de validación de las entradas de usuario en el módulo `mod_dav` de Apache HTTPD.
7. **Servicio - rpcbind:** Se encontró la vulnerabilidad CVE-2017-8779 [13], que permite causar una denegación de servicio (DoS) debido a una asignación incorrecta de memoria al enviar un paquete UDP malicioso al puerto 111.
8. **Servicio - netbios-ssn:** En relación con los servicios *Samba smbd 3.X - 4.X* en los puertos 139/tcp y 445/tcp, se encontró la vulnerabilidad CVE-2023-42670 [14].
9. **Servicio - exec:** Se encontró la vulnerabilidad CVE-1999-0651 [15], que afecta al servicio `netkit-rsh rshd`. Esta vulnerabilidad es una debilidad en la autenticación del servicio rshd, utilizado para ejecutar comandos de manera remota. De tal modo, que permite a un atacante ejecutar comandos arbitrarios.
10. **Servicio - login:** Se encontró la vulnerabilidad CVE-1999-0502 [16], la cual afecta al servicio `rexecd` en el puerto 513/tcp. Esta vulnerabilidad permite a los atacantes ejecutar comandos arbitrarios sin necesidad de autenticarse,
11. **Servicio - shell:** Se detectó la vulnerabilidad CVE-1999-1126 [17], que afecta al servicio `Netkit rshd` en el puerto 514/tcp. Esta vulnerabilidad se debe a un desbordamiento de búfer en el rshd, que permite la ejecución de código arbitrario.
12. **Servicio - java-rmi:** Se encontró la vulnerabilidad CVE-2011-3556 [18], que afecta al servicio `GNU Classpath grmiregistry` en el puerto 1099/tcp. Esta vulnerabilidad permite la ejecución remota de código al manipular objetos RMI.
13. **Servicio - bindshell:** No se encontró ninguna vulnerabilidad en CVE List.
14. **Servicio - nfs:** No se encontró ninguna vulnerabilidad en CVE List.
15. **Servicio - ftp:** El servicio FTP ProFTPD versión 1.3.1 está afectado por la vulnerabilidad CVE-2009-0543 [19]. Esta vulnerabilidad permite a los atacantes remotos ejecutar código SQL arbitrario en el sistema objetivo.

16. **Servicio - mysql:** Se encontró la vulnerabilidad CVE-2008-4097 [20] que afecta a MySQL 5.0.51a. Esta vulnerabilidad permite a usuarios locales eludir verificaciones de privilegios mediante el uso de `symlinks` en tablas MyISAM.
17. **Servicio - postgresql:** Se detectó la vulnerabilidad CVE-2010-1447 [21], que permite a atacantes eludir restricciones de acceso en el módulo `Safe.pm` de Perl, ejecutando código arbitrario.
18. **Servicio - vnc:** En relación a este servicio, se encontró la vulnerabilidad CVE-2002-1511 [22], que afecta a versiones anteriores a 3.3.3r2-21 debido al uso de `rand()` en lugar de `srand()`, lo que genera cookies débiles.
19. **Servicio - x11:** No se encontró ninguna vulnerabilidad en CVE List.
20. **Servicio - irc:** Se encontró la vulnerabilidad CVE-2010-2075 [23]. Esta vulnerabilidad afecta a UnrealIRCd 3.2.8.1 debido a una modificación externa (Trojan Horse) en el macro `DEBUG3_DOLOG_SYSTEM`, esto permite ejecutar comandos arbitrarios de manera remota.
21. **Servicio - ajp13:** Se encontró la vulnerabilidad CVE-2020-1938 [24] que afecta al puerto 8009/tcp y al servicio `ajp` versión 1.3. Esta vulnerabilidad, permite a los atacantes remotos leer archivos arbitrarios desde cualquier lugar de la aplicación web y procesar cualquier archivo como JSP (JavaServer Pages).
22. **Servicio - http:** Se detectó la vulnerabilidad CVE-2005-2090 [25], que afecta a la versión encontrada, Apache Tomcat 5.0.19 (Coyote/1.1), permitiendo ataques de HTTP Request Smuggling.

5 Describir las diferencias observadas en relación al descubrimiento de los equipos disponibles

A través de los escaneos realizados, se han identificado dos máquinas activas en la red virtualizada: máquina Windows (192.168.56.6) y máquina Linux (192.168.56.9). A continuación se describen las principales diferencias observadas entre ambas máquinas:

Sistema operativo. La diferencia más significativa entre ambas máquinas es el sistema operativo. En el caso de la máquina 192.168.56.9 el S.O. identificado, es Linux 2.6.9-2.6.33. Mientras que la 192-168.56.6 es Windows Server 2008 R2 Enterprise.

Además del sistema operativo, se observan diferencias en los nombres de host de las máquinas. El equipo 192.168.56.9 se identifica como `metasploitable` y el otro como `META-FLAVOUR2`.

Tiempo de respuesta. Otra diferencia es el tiempo de respuesta de cada máquina (latencia), se visualiza en la imagen 1. Windows tiene una latencia más baja (0.0028s) que Linux (0.0031s).

Puertos. En cuanto al escaneo de los puertos, se observan diferencias significativas en relación a sus estados. A la hora de realizar un escaneo stealth de los servicios clave, en la máquina de Windows, se obtuvieron algunos puertos abiertos y los restantes filtrados:

- **Puertos abiertos:** 80 (http), 135 (msrpc), 139 (netbios-ssn), 49154, 49156.
- **Puertos filtered:** 21 (ftp), 22 (ssh), 23 (telnet), 443 (https), 512 (exec), 513 (login), 514 (shell), 3306 (mysql), 3389 (ms-wbt-server), 5432 (postgresql), 5900 (vnc), 6000 (X11).

El hecho de que estos puertos estén en estado *filtered* sugiere que un firewall o un sistema de filtrado de tráfico está bloqueando las conexiones entrantes a esos puertos, lo que indica una configuración más restrictiva en la máquina de Windows.

Por otro lado, en el caso de linux, no hay ningún puerto filtrado. Los puertos abiertos y cerrados que se obtuvieron de la máquina 192.168.56.9 son:

- **Puertos abiertos:** 21 (ftp), 22 (ssh), 23 (telnet), 80 (http), 139 (netbios-ssn), 512 (exec), 513 (login), 514 (shell), 3306 (mysql), 5432 (postgresql), 5900 (vnc), 6000 (X11).
- **Puertos cerrados:** 135 (msrpc), 443 (https), 3389 (ms-wbt-server), 49154, 49156.

6 Usando la funcionalidad NSE buscar las vulnerabilidades SMB de los equipos disponibles

Para visualizar los script disponibles relacionados con SMB (Server Message Block), se utiliza el comando:

```
nmap -script-help all | grep smb
```

Estos scripts pueden ser utilizados para realizar diversas tareas de auditoría de seguridad en redes que utilicen SMB, como descubrir vulnerabilidades, obtener información de usuarios... En la siguiente imagen se visualiza la salida 25.

```

(kali㉿kali)-[~]
$ nmap --script-help all | grep smb
* smb-os-discovery
* smb-security-mode
* smb2-time
* smb2-vuln-uptime
NOTE: Communication with instances via named pipes depends on the <code>smb
</code>
documentation and arguments for the <code>smb</code> library for more infor
mation.
NOTE: Communication with instances via named pipes depends on the <code>smb
</code>
documentation and arguments for the <code>smb</code> library for more infor
mation.
NOTE: Communication with instances via named pipes depends on the <code>smb
</code>
documentation and arguments for the <code>smb</code> library for more infor
mation.
NOTE: Communication with instances via named pipes depends on the <code>smb
</code>
documentation and arguments for the <code>smb</code> library for more infor
mation.
NOTE: Communication with instances via named pipes depends on the <code>smb
</code>
documentation and arguments for the <code>smb</code> library for more infor
mation.

```

Figure 25: scripts SMB

Entre todos los scripts, se utiliza específicamente aquellos relacionados con vulnerabilidades. Se especifica el asterisco para abarcar todos los scripts de vulnerabilidades SMB (`smb-vuln*`). Estos scripts son: `smb-vuln-ms10-061` (Identifica una vulnerabilidad en el servicio de impresión de Windows), `smb-vuln-ms17-010` (Detecta la vulnerabilidad EternalBlue) y `smb-vuln-ms10-054` (Detecta fallas en SMB que pueden ser explotadas). Además, para evitar escanear todos los puertos y reducir el tráfico de red, es recomendable especificar únicamente los puertos abiertos en la máquina objetivo.

```

nmap - -script=smb-vuln* 192.168.56.6 -p 80,135,139,445,49154,49156 -oG
ejercicio6W.txt

```

Al ejecutar el comando, se obtuvo información sobre el estado de los diferentes puertos y los resultados de 3 scripts de detección de vulnerabilidades en SMB.

En el caso del primero, se denegó el acceso, lo que significa que no se pudo verificar si la vulnerabilidad está presente.

Por otro lado, el script `smb-vuln-ms17-010` confirmó que el sistema es *VULNERABLE* a MS17-010 (EternalBlue). Esta vulnerabilidad se identifica como CVE-2017-0143 y significa que tiene una falla crítica en el protocolo SMBv1, permitiendo la ejecución remota de código sin autenticación.

Por último, el script `smb-vuln-ms10-054` dió como resultado *False*, lo que indica que el sistema no es vulnerable a esa vulnerabilidad.

```
(kali@kali)-[~/ejercicios/ejercicio6]
$ nmap --script=smb-vuln* 192.168.56.6 -p 80,135,139,445,49154,49156 -oG ejercicio6W.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-17 13:28 EST
Nmap scan report for 192.168.56.6
Host is up (0.0014s latency).

```

PORT	STATE	SERVICE	Destination	Protocol	Length	Info
80/tcp	open	http	192.168.56.6	TCP	60	80 → 80 [SYN] Seq=0
135/tcp	open	msrpc	192.168.56.6	TCP	60	135 → 135 [SYN] Seq=0
139/tcp	open	netbios-ssn	192.168.56.6	TCP	60	139 → 139 [SYN] Seq=0
445/tcp	open	microsoft-ds	192.168.56.6	TCP	60	445 → 445 [SYN] Seq=0
49154/tcp	open	unknown	192.168.56.6	TCP	60	49154 → 49154 [SYN] Seq=0
49156/tcp	filtered	unknown	192.168.56.6	TCP	60	49156 → 49156 [SYN] Seq=0

```

MAC Address: 08:00:27:AF:07:1D (Oracle VirtualBox virtual NIC)

Host script results:
|_ smb-vuln-ms10-061: NT STATUS_ACCESS_DENIED
|_ smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|   State: VULNERABLE
|   IDs: CVE:CVE-2017-0143
|   Risk factor: HIGH
|   A critical remote code execution vulnerability exists in Microsoft SMBv1
|   servers (ms17-010).
|   Disclosure date: 2017-03-14
|   References:
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|   https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attack
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_ smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 19.79 seconds

```

Figure 26: scripts SMB - Máquina Windows

De la misma manera, se ejecuta el escaneo en una máquina Linux, especificando solo los puertos abiertos para optimizar el análisis y realizar el mínimo ruido posible.

```
nmap - -script=smb-vuln* 192.168.56.9 -p
21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,
5900,6000,6667,8009,8180 -oG ejercicio6L.txt
```

El resultado obtenido de los scripts, como se visualiza en la imagen 27, muestran que los scripts `smb-vuln-ms10-054` y `smb-vuln-ms10-061` son *False*, lo que indica que no son vulnerables a esa vulnerabilidad. Mientras que en el caso del script `smb-vuln-regsvc-dos`, da un error en la ejecución. Para el último script, se recomienda utilizar la opción `-d` para realizar un debug. Esta opción hace que Nmap muestre mucha más información durante la ejecución, lo que hace que sea mucho más ruidosa. Como se tiene como objetivo realizar el menor ruido posible, y por tanto, menos tráfico y registros, es mejor no usar `-d`.

```
(kali@kali)-[~/ejercicios/ejercicio6]
$ nmap --script=smb-vuln* 192.168.56.9 -p 21,22,23,25,53,80,111,139,445,512,513,514,1099,1524,2049,2121,3306,5432,5900,6000,6667,8009,8180 -oG ejercicio6L.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-17 13:47 EST
Nmap scan report for 192.168.56.9
Host is up (0.0057s latency).

|_ udp port == 80
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:C8:59:B9 (Oracle VirtualBox virtual NIC)

Host script results:
|_ smb-vuln-ms10-054: false
|_ smb-vuln-ms10-061: false
|_ smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 20.31 seconds
```

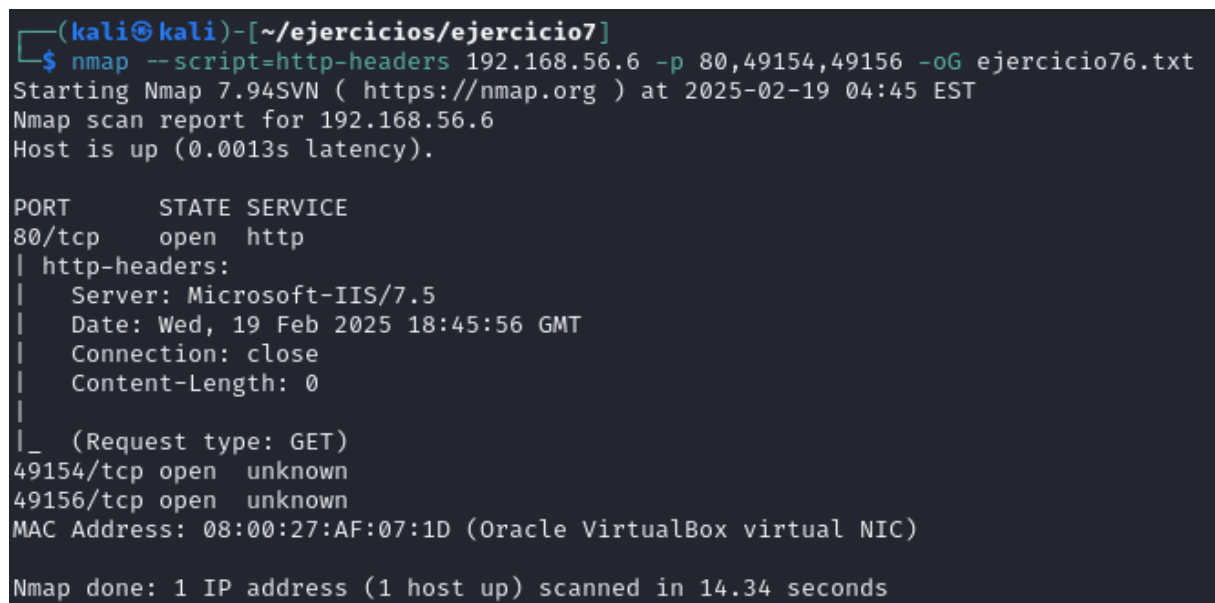
Figure 27: scripts SMB - Máquina Linux

7 Usando la funcionalidad NSE comprueba si el servicio http permite negociación de contenido.

En el caso de la máquina Windows, se especifican los puertos 80, 49154 y 49156. El puerto 80 ya que es el puerto estándar para HTTP. Mientras que los puertos 49154 y 49156, aparecen como **unknown** en los resultados anteriores, lo que sugiere que podría estar siendo utilizado por alguna aplicación o servidor HTTP personalizado.

Dado que en la máquina Windows no hay un servidor Apache, el uso del script `http-apache-negotiation` no es el más adecuado para comprobar la negociación de contenido. Por lo que no existe un script NSE que, de manera precisa indique que un servidor HTTP está realizando negociación de contenido. En este caso, se utiliza el script `http-headers` para intentar obtener información sobre la respuesta HTTP. Sin embargo, no devuelve información relevante (cabeceras específicas) de negociación de contenido para esos puertos. El comando utilizado es:

```
nmap - -script=http-headers 192.168.56.6 -p 80,49154,49156 -oG
ejercicio76.txt
```



```
(kali㉿kali)-[~/ejercicios/ejercicio7]
└─$ nmap --script=http-headers 192.168.56.6 -p 80,49154,49156 -oG ejercicio76.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-19 04:45 EST
Nmap scan report for 192.168.56.6
Host is up (0.0013s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-headers:
|   Server: Microsoft-IIS/7.5
|   Date: Wed, 19 Feb 2025 18:45:56 GMT
|   Connection: close
|   Content-Length: 0
|
|_ (Request type: GET)
49154/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 08:00:27:AF:07:1D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.34 seconds
```

Figure 28: script (http-headers) - Máquina Windows

Por otro lado, en la máquina de Linux si que hay servidor Apache, por lo que si que se utiliza el script `http-apache-negotiation`. Este script verifica si el servidor HTTP tiene habilitado el módulo `mod_negotiation` de Apache, que es responsable de la negociación de contenido. Además, se especifican los puertos 80 y 8180. El puerto 80 ya que es el puerto estándar para HTTP. Mientras, el puerto 8180 aparece como **unknown** en los resultados anteriores, lo que sugiere que podría estar siendo utilizado por alguna aplicación o servidor HTTP personalizado. El comando utilizado es:

```
nmap - -script=http-apache-negotiation 192.168.56.9 -p 80,8180 -oG
ejercicio79.txt
```

En este caso, el puerto 80/tcp está abierto y el script indica que el módulo *mod_negotiation* está habilitado, lo que significa que el servidor HTTP está configurado para permitir la negociación de contenido.

```
(kali@kali)-[~/ejercicios/ejercicio7]
$ nmap --script=http-apache-negotiation 192.168.56.9 -p 80,8180 -oG ejercicio79.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 11:51 EST
Nmap scan report for 192.168.56.9
Host is up (0.0014s latency).
PORT      STATE SERVICE
80/tcp    open  http
| http-apache-negotiation: mod negotiation enabled.
8180/tcp  open  unknown
MAC Address: 08:00:27:C8:59:B9 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.71 seconds
```

Figure 29: script (http-apache-negotiation) - Máquina Linux

8 Referencias

- [1] *Cve-2010-2730*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2730>.
- [2] *Cve-2010-3972*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3972>.
- [3] *Cve-2010-1899*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1899>.
- [4] *Cve-2020-1113*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1113>.
- [5] *Cve-2018-7445*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7445>.
- [6] *Cve-2017-0143*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>.
- [7] *Cve-2011-2523*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523>.
- [8] *Cve-2008-5161*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5161>.
- [9] *Cve-2005-2040*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2040>.
- [10] *Cve-2015-4000*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000>.
- [11] *Cve-2008-0122*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0122>.
- [12] *Cve-2017-3167*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3167>.

- [13] *Cve-2017-8779*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8779>.
- [14] *Cve-2023-42670*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-42670>.
- [15] *Cve-1999-0651*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0651>.
- [16] *Cve-1999-0502*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0502>.
- [17] *Cve-1999-1126*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1126>.
- [18] *Cve-1999-1126*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1126>.
- [19] *Cve-1999-1126*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1126>.
- [20] *Cve-1999-1126*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1126>.
- [21] *Cve-1999-1126*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1126>.
- [22] *Cve-2002-1511*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1511>.
- [23] *Cve-2010-2075*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2075>.
- [24] *Cve-2020-1938*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1938>.
- [25] *Cve-2005-2090*. [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2090>.