



7 DE JULIO DE 2025

OMAR ALEJANDRO PÉREZ ANOTA

PRÁCTICAS DEL EXAMEN

HACKING ÉTICO – IRIYC-91



Practica 1 : (PREGUNTA 1: Práctica – Interpretación de escaneo)

The screenshot shows a Kali Linux terminal running Nmap and Wireshark capturing the traffic. The terminal output is as follows:

```
kali@kali: ~  
$ sudo nmap -sS 10.10.53.223  
[sudo] password for kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 21:27 EDT
```

Wireshark is capturing on interface eth0. The packet list shows the following traffic:

No.	Time	Source	Destination	Protocol
52	0.000000	192.168.134.128	10.10.53.223	TCP
72	0.000000	192.168.134.128	10.10.53.223	TCP
99	0.000000	192.168.134.128	10.10.53.223	TCP
54	0.000000	192.168.134.128	10.10.53.223	TCP
91	0.000000	192.168.134.128	10.10.53.223	TCP
88	0.000000	192.168.134.128	10.10.53.223	TCP
78	0.000000	192.168.134.128	10.10.53.223	TCP
52	0.000000	192.168.134.128	10.10.53.223	TCP
93	0.000000	192.168.134.128	10.10.53.223	TCP
93	0.000000	192.168.134.128	10.10.53.223	TCP
91	0.000000	192.168.134.128	10.10.53.223	TCP
53	0.000000	192.168.134.128	10.10.53.223	TCP
11	0.000000	192.168.134.128	10.10.53.223	TCP
55	0.000000	192.168.134.128	10.10.53.223	TCP
53	0.000000	192.168.134.128	10.10.53.223	TCP

The packet details for the selected packet (No. 52) are as follows:

```
Frame 52: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0  
Ethernet II, Src: VMware_c0:00:08 (00:50:56:00:00:08), Dst: 02:00:00:00:00:00  
Protocol (request)
```

```
52 → 39151 [RST, ACK] Seq=1 Ack=1 Win=64240  
718 → 39151 [RST, ACK] Seq=1 Ack=1 Win=64240  
151 → 888 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  
88 → 39151 [RST, ACK] Seq=1 Ack=1 Win=64240  
151 → 8001 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  
151 → 2393 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  
8 → 39151 [RST, ACK] Seq=1 Ack=1 Win=64240  
91 → 39151 [RST, ACK] Seq=1 Ack=1 Win=64240  
151 → 7443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460  
93 → 39151 [RST, ACK] Seq=1 Ack=1 Win=64240  
151 → 1000 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
```

Packet details for the selected packet (No. 52):

```
480 bits), 60 b... 0000 ff ff ff ff ff ff 00  
0:00:08 (00:50:5... 0010 08 00 06 04 00 01 00  
1 (request) 0020 00 00 00 00 00 00 c0
```

Práctica 2: (PREGUNTA 3: Práctica – Verificación con Wireshark)

NTP	90	NTP Version 4, client
NTP	90	NTP Version 4, server
TCP	58 39151 → 2608	[SYN] Seq=0 Win=1024 Len=0
TCP	60 666 → 39151	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP	58 39151 → 32777	[SYN] Seq=0 Win=1024 Len=0
TCP	60 10621 → 39151	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP	60 2608 → 39151	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP	58 39151 → 2601	[SYN] Seq=0 Win=1024 Len=0
TCP	60 32777 → 39151	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP	58 39151 → 5226	[SYN] Seq=0 Win=1024 Len=0
TCP	58 39151 → 8654	[SYN] Seq=0 Win=1024 Len=0
TCP	60 2601 → 39151	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP	60 5226 → 39151	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0
TCP	58 39151 → 42510	[SYN] Seq=0 Win=1024 Len=0

```

(kali@kali)-[~]
└─$ sudo nmap -sS 10.10.53.223
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 21:38
Nmap scan report for 10.10.53.223
Host is up (0.0017s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realservice
3306/tcp   open  mysql
5432/tcp   open  postgresql

Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds

```

192.168.134.128	TCP	60 5432 → 39151	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 443 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 139 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 445 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 80 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 135 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 3306 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 139 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 5432 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 902 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 912 → 55411	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 912 → 55413	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=
192.168.134.128	TCP	60 139 → 55418	[SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=

Ethernet II, Src: VMware_e1:28:6e (00:50:00:00:00:00), Dst: 00:0c:29:15:20:f4 (08:00:27:00:00:00:00), Protocol: 0x0800
 Internet Protocol Version 4, Src: 10.10.53.223, Dst: 10.10.53.223
 Transmission Control Protocol, Src Port: 5432, Dst Port: 55411

60 0c 29 15 20 f4 00 50 56 e1 28 6e 00 10 00 2c 07 b3 00 00 80 06 ac 07 0a 0a 00 20 86 80 15 38 98 ef 30 15 09 fd 04 5b 00 30 fa f0 4f fa 00 00 02 04 05 b4 00 00

Frame (frame), 60 bytes
 Packets: 9345 · Displayed: 33 (0.4%) · Profile: Default

Practica 3 (PREGUNTA 5: Práctica – Descubrimiento real)

\$ sudo nmap -sS 10.10.53.223

```
(kali㉿kali)-[~]  
$ sudo nmap -sS 10.10.53.223  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 21:38  
Nmap scan report for 10.10.53.223  
Host is up (0.0017s latency).  
Not shown: 992 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
135/tcp   open  msrpc  
139/tcp   open  netbios-ssn  
443/tcp   open  https  
445/tcp   open  microsoft-ds  
902/tcp   open  iss-realsecure  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
  
Nmap done: 1 IP address (1 host up) scanned in 5.03 seconds  
  
(kali㉿kali)-[~]  
$
```

Practica 4 (PREGUNTA 7: Práctica – Uso del escaneo de versión)

nmap -sV -p 80 10.10.53.223 (Realizado a mi propio equipo con un servidor de XAMPP ejecutado)

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 21:53 EDT
Nmap scan report for 10.10.53.223
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.0.30)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.60 seconds

(kali㉿kali)-[~]
$
```

Práctica 5 (PREGUNTA 9: Práctica – Captura de tráfico)

nmap -sU -p 53,161 10.10.53.223

```
Service detection performed. Please report
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned

(kali@kali)-[~]
$ nmap -sU -p 53,161 10.10.53.223
Starting Nmap 7.95 ( https://nmap.org ) at
Nmap scan report for 10.10.53.223
Host is up (0.00098s latency).

PORT      STATE      SERVICE
53/udp    open|filtered domain
161/udp   open|filtered snmp

Nmap done: 1 IP address (1 host up) scanned

(kali@kali)-[~]
$
```

```
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
192.168.134.128 ICMP 70 Destination unreachable (Host unreachable)
224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "C
Frame 64: 101 bytes on wire (808 bits), 101
Ethernet II, Src: VMware_c0:00:08 (00:50:56
Internet Protocol Version 6, Src: fe80::3d7
User Datagram Protocol, Src Port: 5353, Dst
Frame (frame), 101 bytes
Packets: 13380 - Displayed: 3846 (28.7%) Profile: Defau
```