

PREGUNTA 1:

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.10.121
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 22:44 EDT
Nmap scan report for 192.168.10.121: 1 filtered (1 up), 1 undergoing SYN Stealth Scan
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.10.121 are in ignored states. remaining 1000
Not shown: 1000 closed tcp ports (reset)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
Not shown: 1000 filtered tcp ports (no-response)
└─$
└─$ done: 1 IP address (1 host up) scanned in 201.45 seconds
└─$
└─$
```

PREGUNTA 5: Práctica – Descubrimiento real

Realiza un escaneo SYN (-sS) en todos los puertos de un host que tengas en tu red.
¿Cuántos puertos abiertos detectas y cuáles son?

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 80 192.168.10.121
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 22:31 EDT
Nmap scan report for 192.168.10.121
Host is up (0.00013s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
└─$
└─$
```

```

(kali@kali)-[~]
$ sudo nmap -sS -p 999 192.168.10.121
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 22:34 EDT
Nmap scan report for 192.168.10.121
Host is up (0.000047s latency).

PORT      STATE SERVICE
999/tcp    closed garcon

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

(kali@kali)-[~]
$

```

```

(kali@kali)-[~]
$ sudo nmap -sS -p 135 192.168.10.121
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 22:35 EDT
Nmap scan report for 192.168.10.121
Host is up (0.00015s latency).

PORT      STATE SERVICE
135/tcp    closed msrpc

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

(kali@kali)-[~]
$

```

PREGUNTA 7: Práctica – Uso del escaneo de versión

Usa el escaneo de versión de Nmap (-sV) sobre un servidor activo. ¿Qué servicio corre el puerto 80?

R=El puerto 80 corre el servicio Apache httpd 2.4.38.

```

(kali@kali)-[~]
$ nmap -sV 192.168.10.121

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 21:47 EDT
Nmap scan report for 192.168.10.121
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.63 ((Debian))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.67 seconds

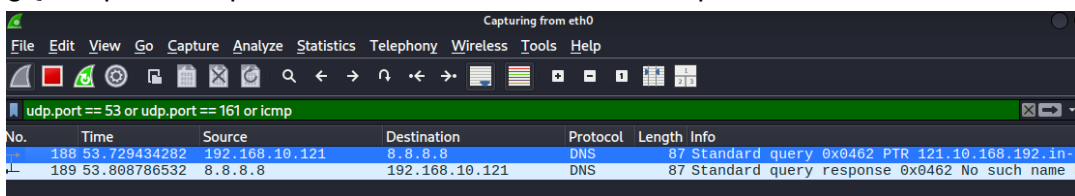
(kali@kali)-[~]
$

```

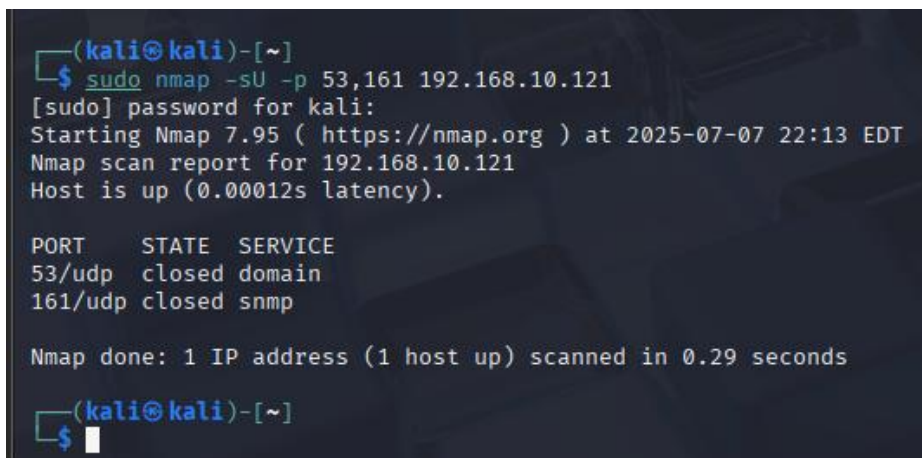
PREGUNTA 9: Práctica – Captura de tráfico

Captura el tráfico con Wireshark mientras haces un escaneo UDP a los puertos 53 y 161.

¿Qué tipo de respuestas observas del host si esos puertos están cerrados?



No.	Time	Source	Destination	Protocol	Length	Info
188	53.729434282	192.168.10.121	8.8.8.8	DNS	87	Standard query 0x0462 PTR 121.10.168.192.in-
189	53.808786532	8.8.8.8	192.168.10.121	DNS	87	Standard query response 0x0462 No such name f



```
(kali㉿kali)-[~]
└─$ sudo nmap -sU -p 53,161 192.168.10.121
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-07 22:13 EDT
Nmap scan report for 192.168.10.121
Host is up (0.00012s latency).

PORT      STATE SERVICE
53/udp    closed domain
161/udp    closed snmp

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
└─$
```