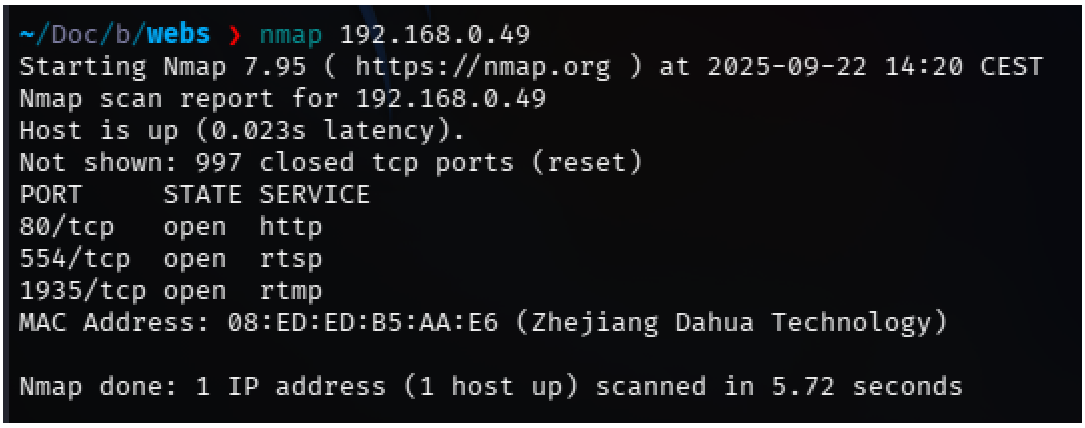
Ejercicios de Nmap (Redes y Seguridad Informática)

📘 1. Comprobar conectividad básica y escaneo simple

nmap 192.168.1.143

- Escanea el host con IP 192.168.1.143 para detectar puertos abiertos comunes.

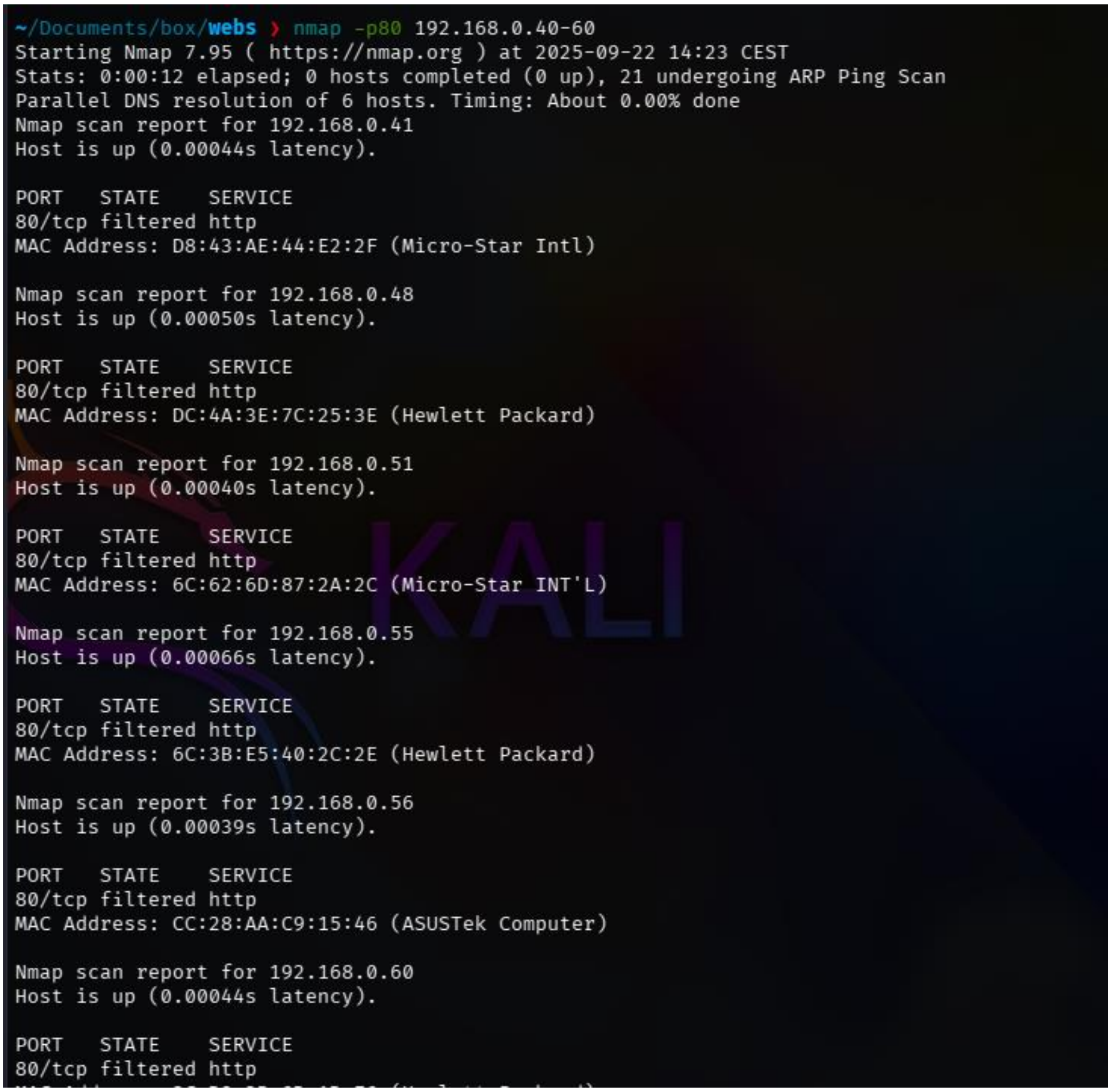


```
~/Doc/b/webs ❯ nmap 192.168.0.49
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:20 CEST
Nmap scan report for 192.168.0.49
Host is up (0.023s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
1935/tcp open  rtmp
MAC Address: 08:ED:ED:B5:AA:E6 (Zhejiang Dahua Technology)

Nmap done: 1 IP address (1 host up) scanned in 5.72 seconds
```

📘 2. Escaneo de un rango de IP

nmap 192.168.1.1-254

- Escanea todas las direcciones IP del rango 192.168.1.1 a 192.168.1.254.

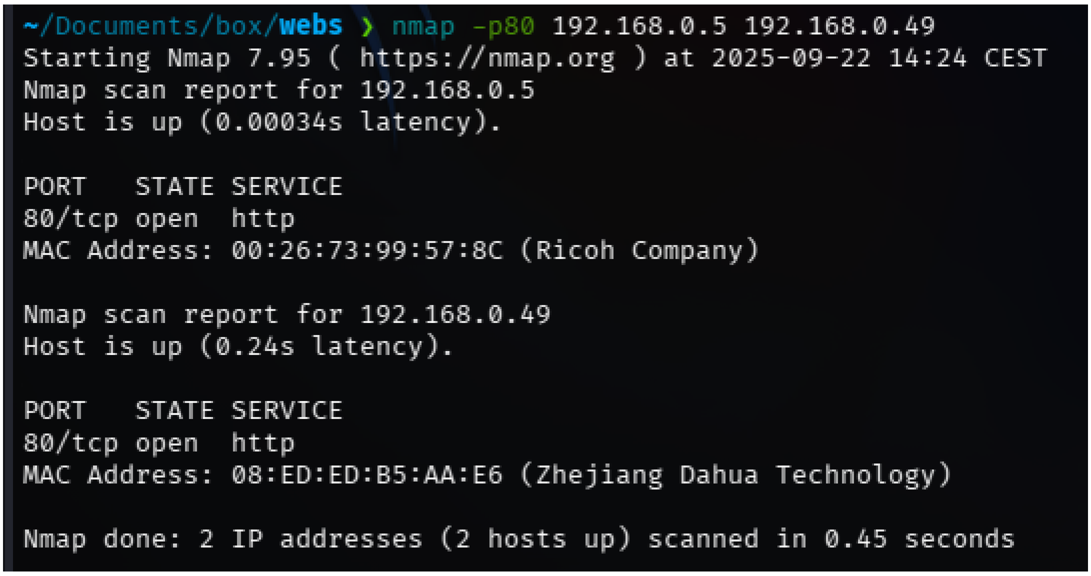


```
~/Documents/box/webs ❯ nmap -p80 192.168.0.40-60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:23 CEST
Stats: 0:00:12 elapsed; 0 hosts completed (0 up), 21 undergoing ARP Ping Scan
Parallel DNS resolution of 6 hosts. Timing: About 0.00% done
Nmap scan report for 192.168.0.41
Host is up (0.00044s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: D8:43:AE:44:E2:2F (Micro-Star Intl)

Nmap scan report for 192.168.0.48
Host is up (0.00050s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: DC:4A:3E:7C:25:3E (Hewlett Packard)

Nmap scan report for 192.168.0.51
Host is up (0.00040s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 6C:62:6D:87:2A:2C (Micro-Star INT'L)

Nmap scan report for 192.168.0.55
Host is up (0.00066s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 6C:3B:E5:40:2C:2E (Hewlett Packard)

Nmap scan report for 192.168.0.56
Host is up (0.00039s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: CC:28:AA:C9:15:46 (ASUSTek Computer)

Nmap scan report for 192.168.0.60
Host is up (0.00044s latency).

PORT   STATE    SERVICE
80/tcp filtered http
```

📘 3. Escaneo de varias direcciones IP específicas

nmap 192.168.1.1 192.168.1.4 192.168.1.43

- Escanea múltiples IP individuales especificadas manualmente.

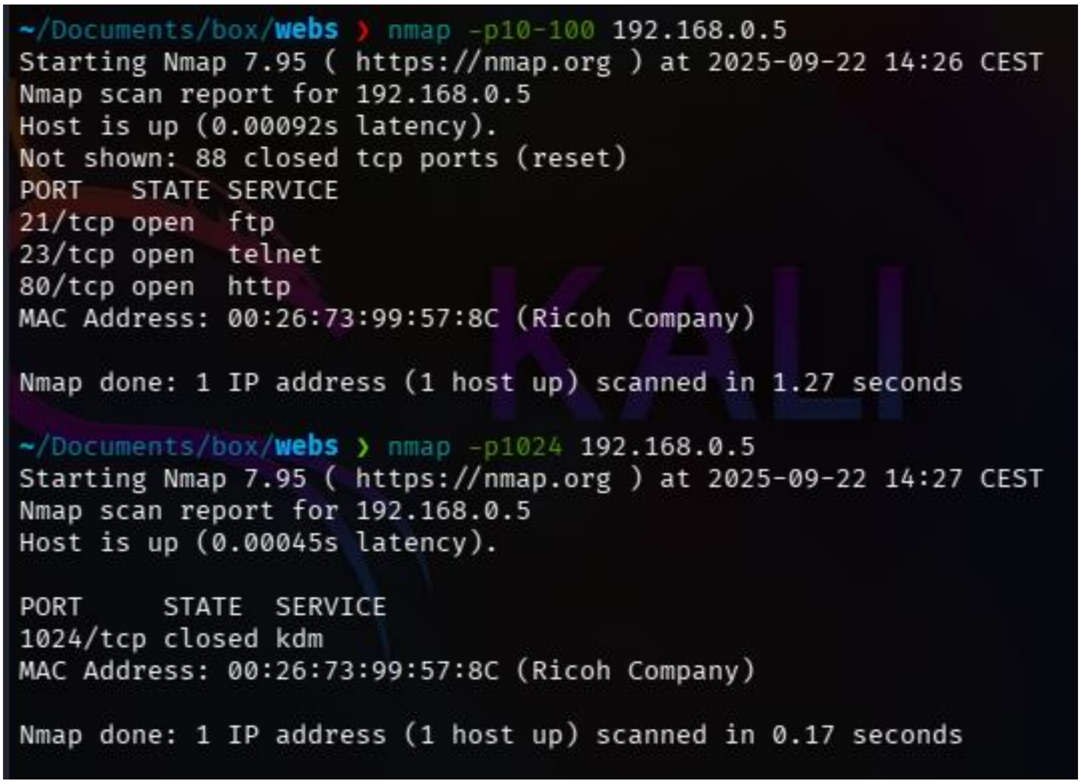


```
~/Documents/box/webs ❯ nmap -p80 192.168.0.5 192.168.0.49
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:24 CEST
Nmap scan report for 192.168.0.5
Host is up (0.00034s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:26:73:99:57:8C (Ricoh Company)

Nmap scan report for 192.168.0.49
Host is up (0.24s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:ED:ED:B5:AA:E6 (Zhejiang Dahua Technology)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.45 seconds
```

📘 4. Escaneo de puertos específicos

nmap -p 1042 192.168.1.143

- Escanea solo el puerto 1042 en la IP dada.

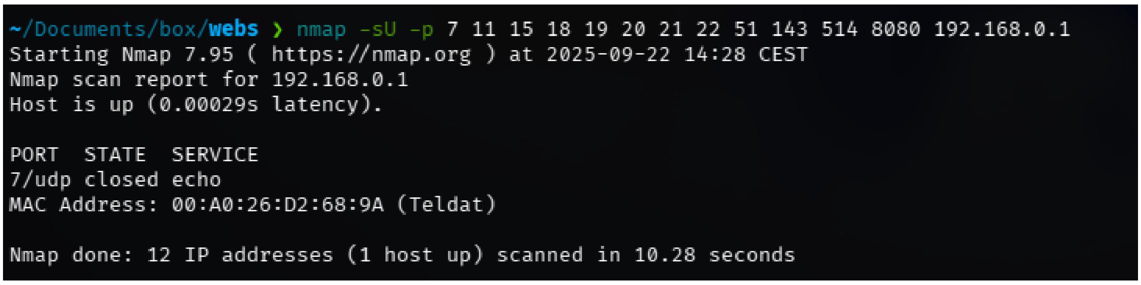


```
~/Documents/box/webs ❯ nmap -p10-100 192.168.0.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:26 CEST
Nmap scan report for 192.168.0.5
Host is up (0.00092s latency).
Not shown: 88 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
23/tcp open  telnet
80/tcp open  http
MAC Address: 00:26:73:99:57:8C (Ricoh Company)

Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds

~/Documents/box/webs ❯ nmap -p1024 192.168.0.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:27 CEST
Nmap scan report for 192.168.0.5
Host is up (0.00045s latency).

PORT     STATE  SERVICE
1024/tcp closed kdm
MAC Address: 00:26:73:99:57:8C (Ricoh Company)

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

📘 5. Escaneo de puertos UDP

nmap -sU -p 7 11 15 18 19 20 21 22 51 143 514 8080 192.168.1.143

- Escaneo en modo UDP de puertos específicos.
- El parámetro -sU indica que se trata de un escaneo de puertos UDP.

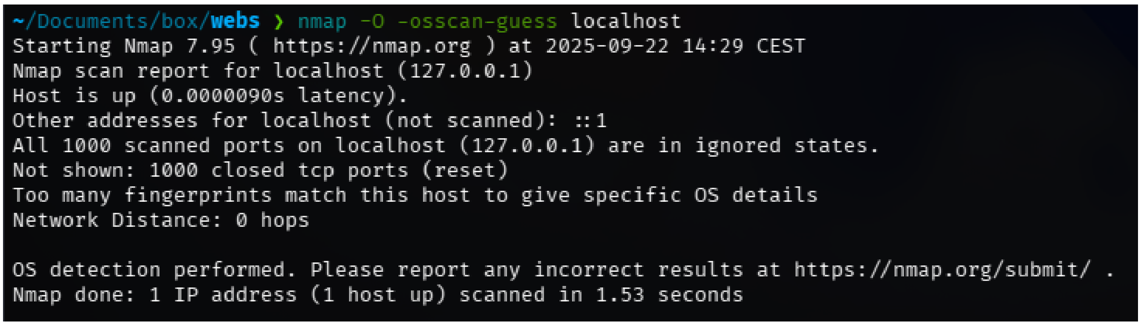


```
~/Documents/box/webs ❯ nmap -sU -p 7 11 15 18 19 20 21 22 51 143 514 8080 192.168.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:28 CEST
Nmap scan report for 192.168.0.1
Host is up (0.00029s latency).

PORT  STATE  SERVICE
7/udp closed echo
MAC Address: 00:A0:26:D2:68:9A (Teldat)

Nmap done: 12 IP addresses (1 host up) scanned in 10.28 seconds
```

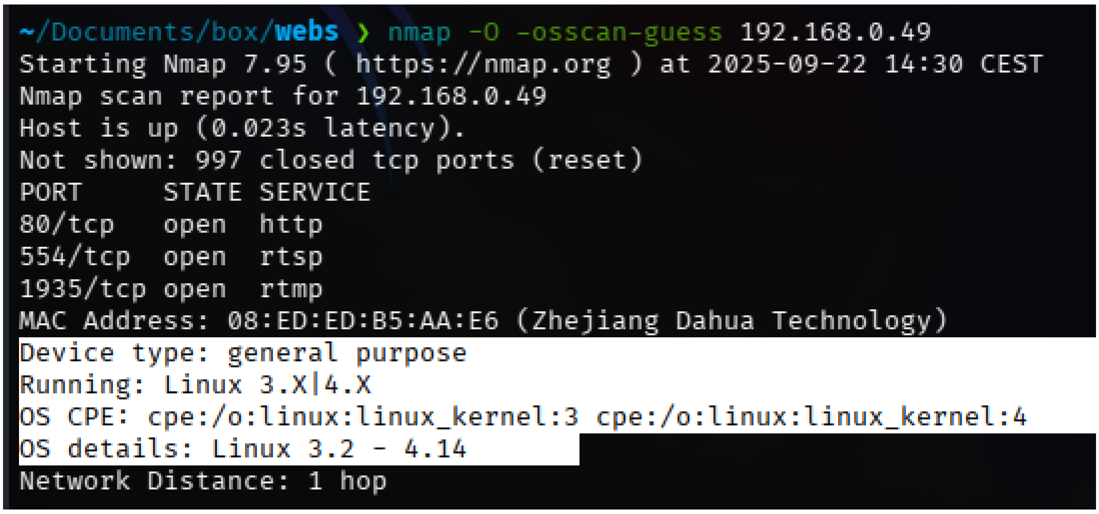
📘 6. Escaneo del sistema operativo

nmap -O -osscan-guess localhost

- Detecta el sistema operativo del host local.
- El parámetro --osscan-guess permite adivinar el sistema si no se reconoce con certeza.



```
~/Documents/box/webs ❯ nmap -O -osscan-guess localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:29 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000090s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds
```

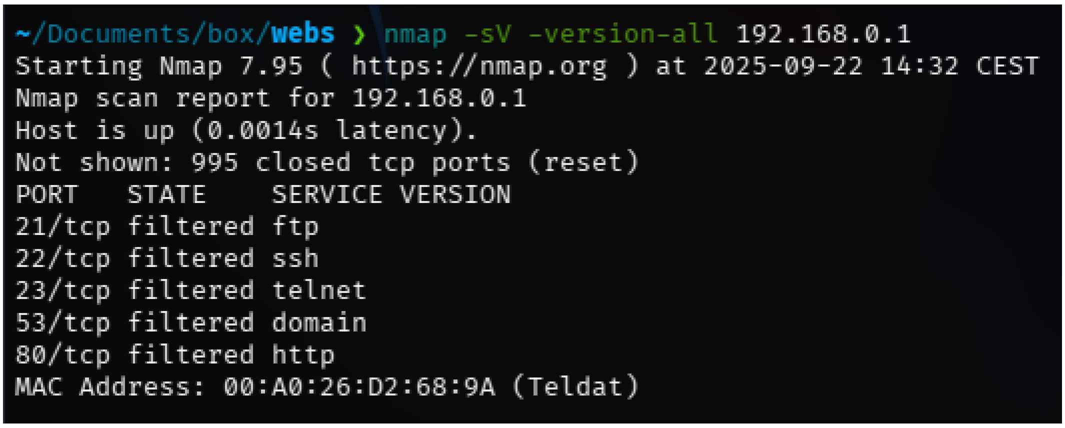


```
~/Documents/box/webs ❯ nmap -O -osscan-guess 192.168.0.49
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:30 CEST
Nmap scan report for 192.168.0.49
Host is up (0.023s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
554/tcp  open  rtsp
1935/tcp open  rtmp
MAC Address: 08:ED:ED:B5:AA:E6 (Zhejiang Dahua Technology)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14
Network Distance: 1 hop
```

📘 7. Mostrar versión de los servicios

nmap -sV -version-all localhost

- Muestra la versión de los servicios detectados en el host local.



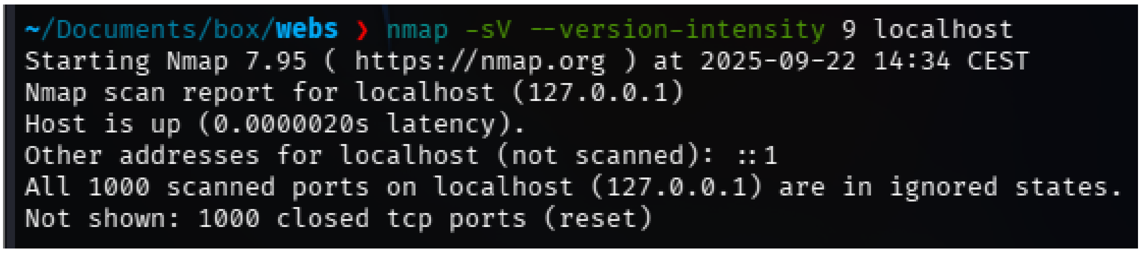
```
~/Documents/box/webs ❯ nmap -sV -version-all 192.168.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:32 CEST
Nmap scan report for 192.168.0.1
Host is up (0.0014s latency).
Not shown: 995 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
53/tcp filtered domain
80/tcp filtered http
MAC Address: 00:A0:26:D2:68:9A (Teldat)
```

📘 8. Mostrar información del sistema Nmap instalado

nmap -SV --version-1ll localhost

- Posible errata tipográfica, probablemente se refiere a:

nmap -sV --version-intensity 9 localhost

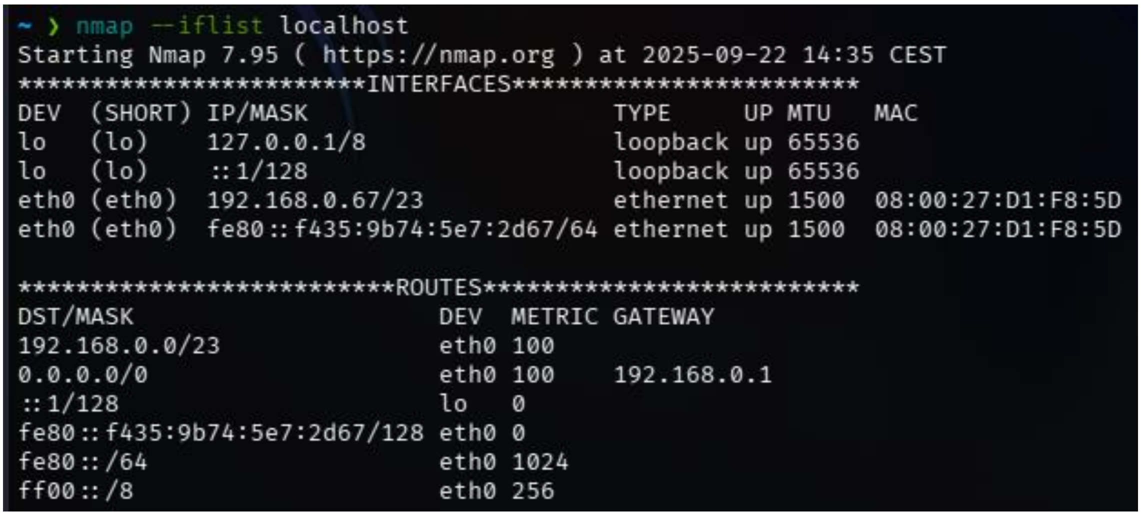


```
~/Documents/box/webs ❯ nmap -sV --version-intensity 9 localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:34 CEST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

📘 9. Ver interfaces de red

nmap --iflist localhost

- Muestra todas las interfaces de red y rutas de la máquina local.

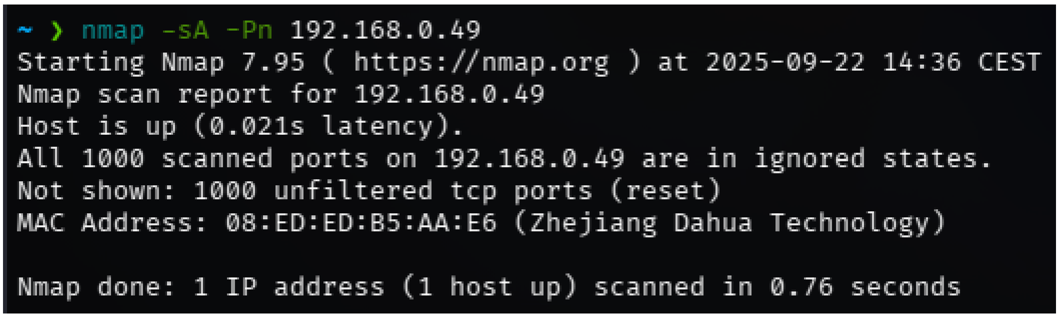


```
~ ❯ nmap --iflist localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:35 CEST
************************INTERFACES************************
DEV  (SHORT) IP/MASK                      TYPE     UP MTU   MAC
lo   (lo)    127.0.0.1/8                  loopback up 65536
lo   (lo)    ::1/128                      loopback up 65536
eth0 (eth0)  192.168.0.67/23              ethernet up 1500  08:00:27:D1:F8:5D
eth0 (eth0)  fe80::f435:9b74:5e7:2d67/64  ethernet up 1500  08:00:27:D1:F8:5D

**************************ROUTES**************************
DST/MASK                      DEV  METRIC GATEWAY
192.168.0.0/23                eth0 100
0.0.0.0/0                     eth0 100    192.168.0.1
::1/128                       lo   0
fe80::f435:9b74:5e7:2d67/128  eth0 0
fe80::/64                     eth0 1024
ff00::/8                      eth0 256
```

📘 10. Enviar paquetes TCP ACK

nmap -sA 192.168.1.143

- Escanea con paquetes TCP ACK para detectar hosts activos incluso tras firewall.



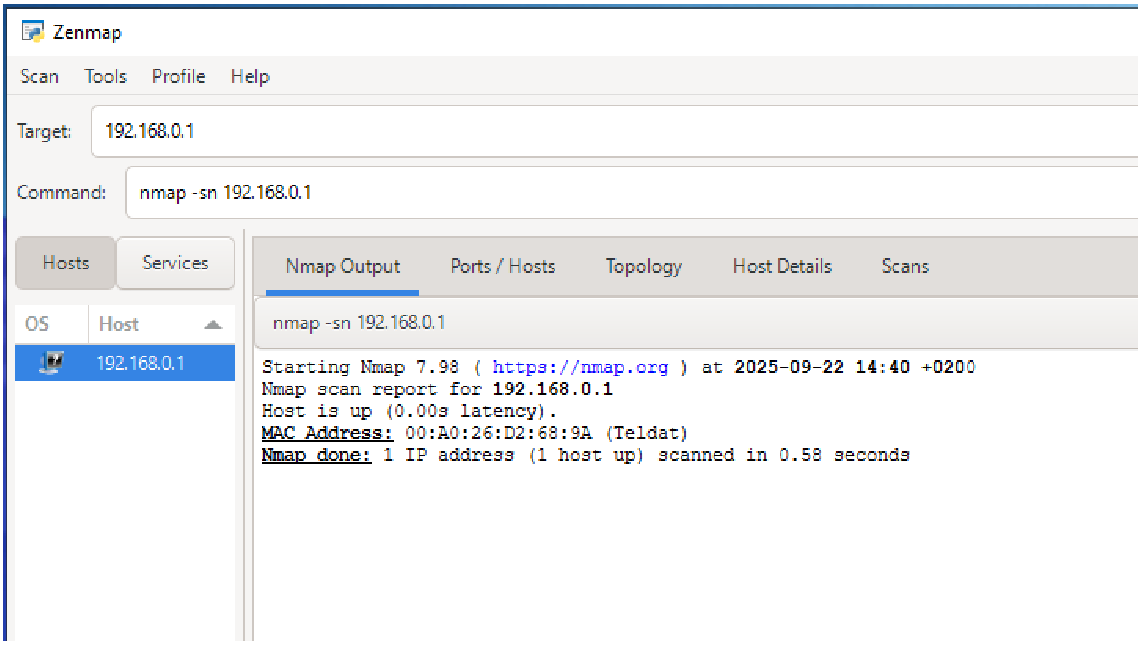
```
~ ❯ nmap -sA -Pn 192.168.0.49
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:36 CEST
Nmap scan report for 192.168.0.49
Host is up (0.021s latency).
All 1000 scanned ports on 192.168.0.49 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:ED:ED:B5:AA:E6 (Zhejiang Dahua Technology)

Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
```

📘 11. Actividad propuesta 1.9: Zenmap GUI para Nmap

🧩 Instrucciones del ejercicio:

Instala **Zenmap** (entorno gráfico para Nmap) en tu máquina Windows.

Investiga y explica **la utilidad de las diferentes pestañas** que ofrece la aplicación.



Target: 192.168.0.1

Command: nmap -sn 192.168.0.1

192.168.0.1

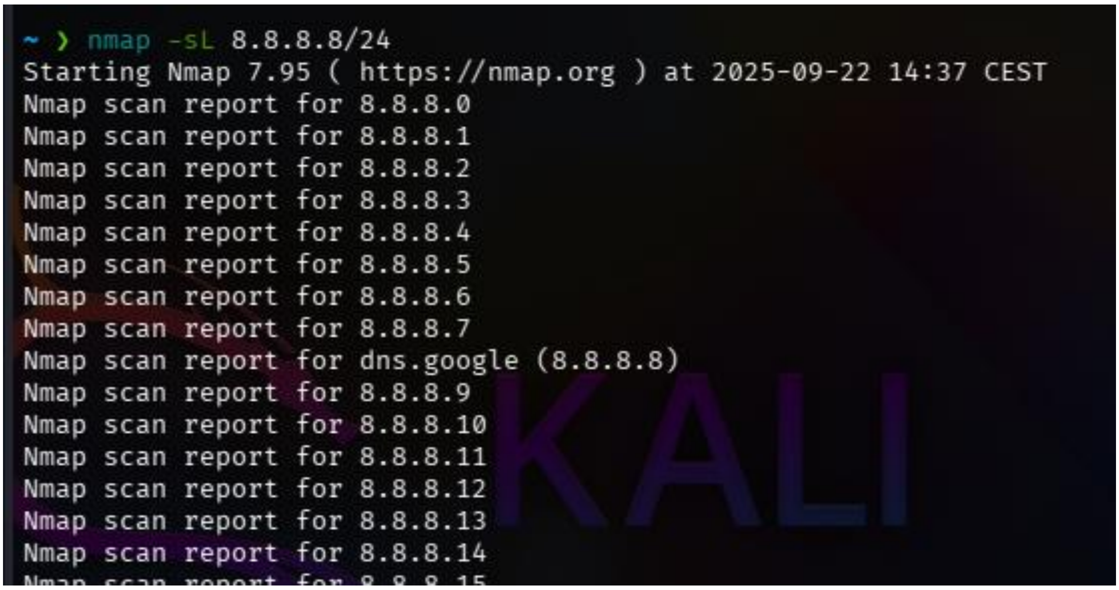
nmap -sn 192.168.0.1

```
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-22 14:40 +0200
Nmap scan report for 192.168.0.1
Host is up (0.00s latency).
MAC Address: 00:A0:26:D2:68:9A (Teldat)
Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

📘 12. Otros comandos avanzados (mencionados en la imagen):

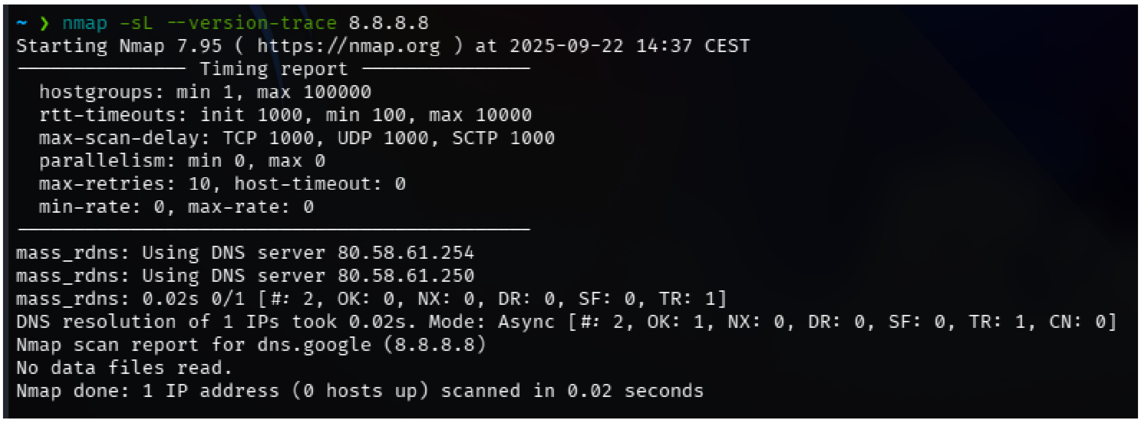
- Detección de DNS inverso:

nmap -sL 192.168.43.0/24



```
~ ❯ nmap -sL 8.8.8.8/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:37 CEST
Nmap scan report for 8.8.8.0
Nmap scan report for 8.8.8.1
Nmap scan report for 8.8.8.2
Nmap scan report for 8.8.8.3
Nmap scan report for 8.8.8.4
Nmap scan report for 8.8.8.5
Nmap scan report for 8.8.8.6
Nmap scan report for 8.8.8.7
Nmap scan report for dns.google (8.8.8.8)
Nmap scan report for 8.8.8.9
Nmap scan report for 8.8.8.10
Nmap scan report for 8.8.8.11
Nmap scan report for 8.8.8.12
Nmap scan report for 8.8.8.13
Nmap scan report for 8.8.8.14
Nmap scan report for 8.8.8.15
```

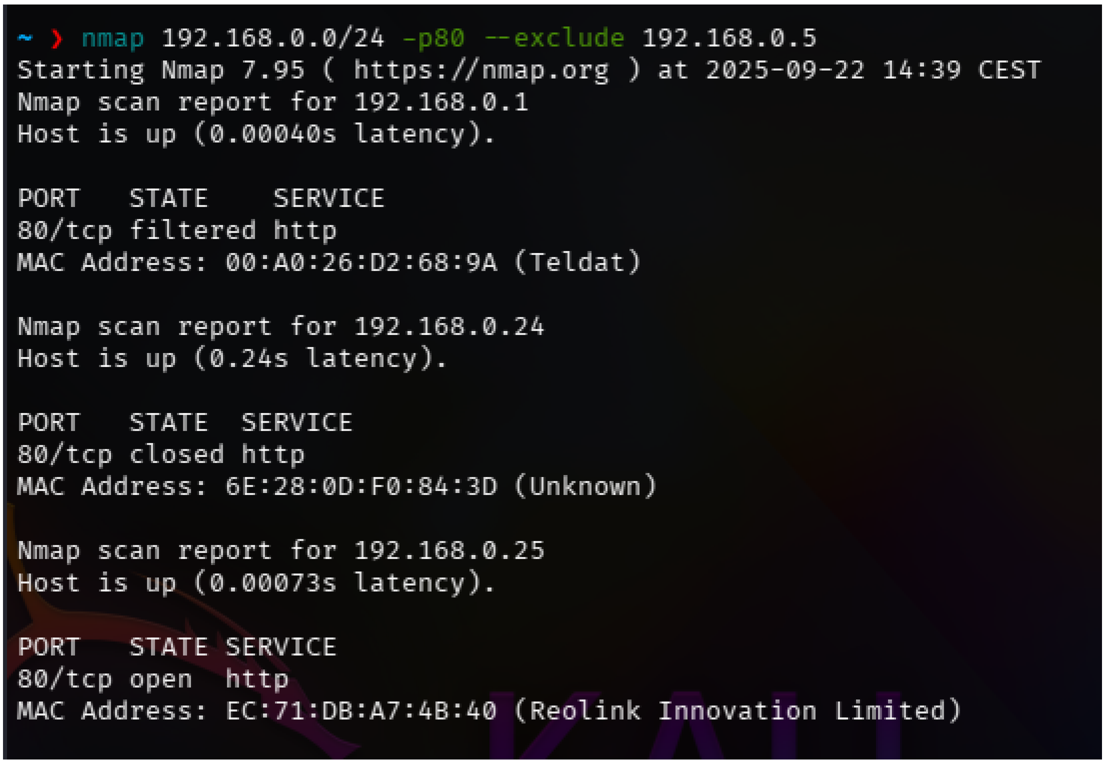
- Escaneo de versión con --version-trace



```
~ ❯ nmap -sL --version-trace 8.8.8.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:37 CEST
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
mass_rdns: Using DNS server 80.58.61.254
mass_rdns: Using DNS server 80.58.61.250
mass_rdns: 0.02s 0/1 [#: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Nmap scan report for dns.google (8.8.8.8)
No data files read.
Nmap done: 1 IP address (0 hosts up) scanned in 0.02 seconds
```

- Exclusión de host:

nmap 192.168.1.0/24 --exclude 192.168.1.1



```
~ ❯ nmap 192.168.0.0/24 -p80 --exclude 192.168.0.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 14:39 CEST
Nmap scan report for 192.168.0.1
Host is up (0.00040s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: 00:A0:26:D2:68:9A (Teldat)

Nmap scan report for 192.168.0.24
Host is up (0.24s latency).

PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 6E:28:0D:F0:84:3D (Unknown)

Nmap scan report for 192.168.0.25
Host is up (0.00073s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: EC:71:DB:A7:4B:40 (Reolink Innovation Limited)
```