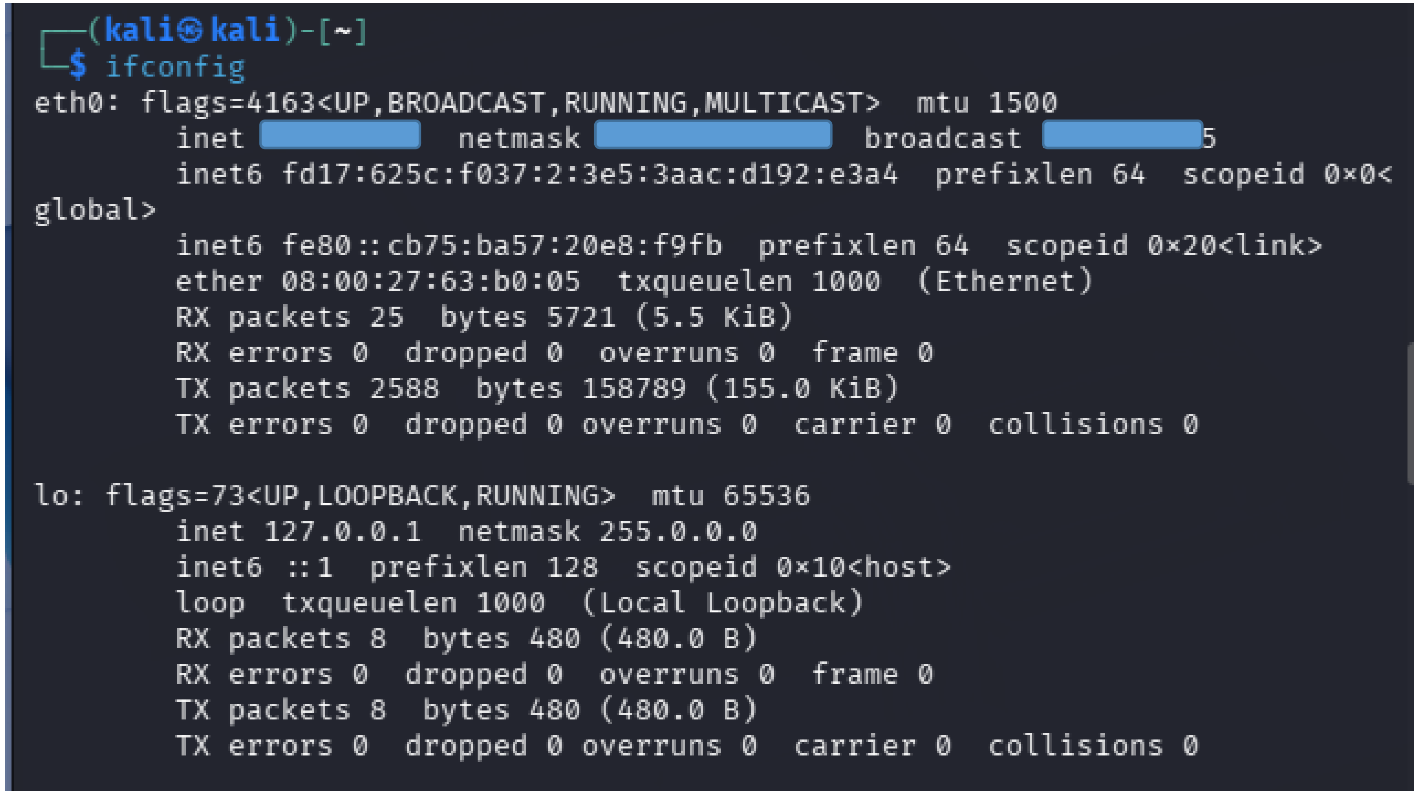
Auditoria de puertos vulnerables

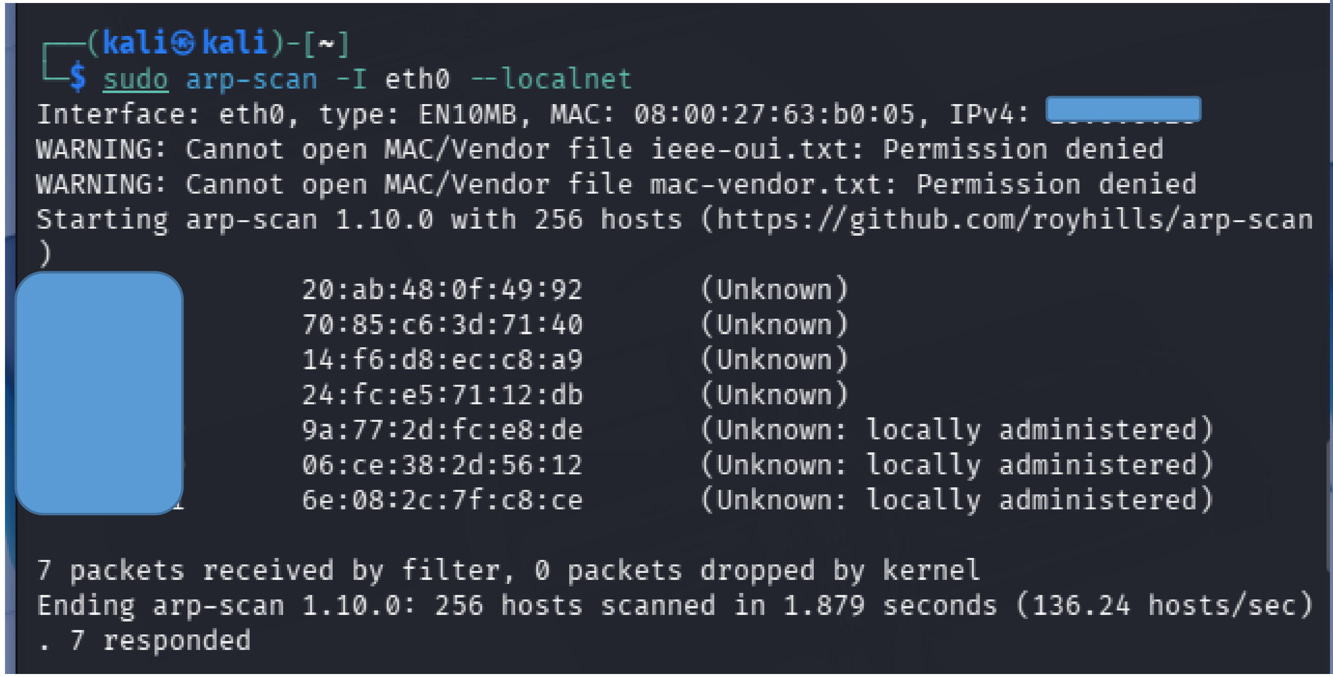
Luis Reyes Volquez

- En primer lugar buscamos la ip del auditor, la mascara de red y la ip de difusión para asi determinar la ip de id de la red y su prefijo.

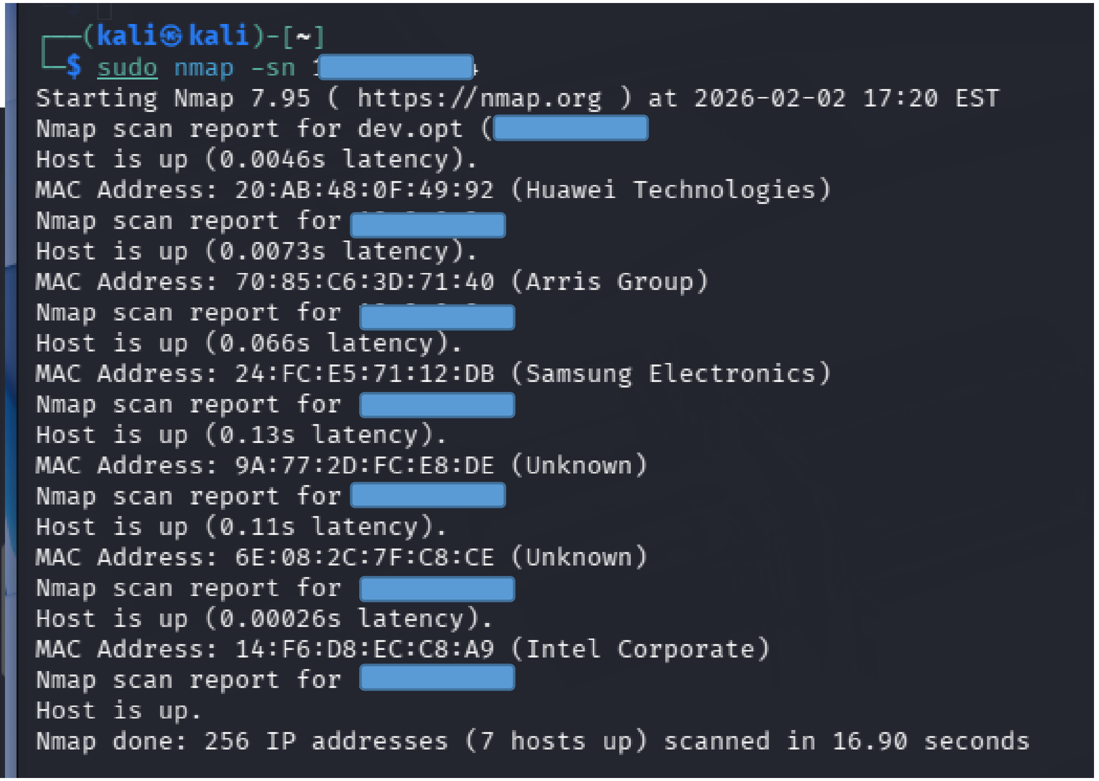


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask [redacted]  broadcast [redacted]
        inet6 fd17:625c:f037:2:3e5:3aac:d192:e3a4  prefixlen 64  scopeid 0x0<
global>
        inet6 fe80::cb75:ba57:20e8:f9fb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:63:b0:05  txqueuelen 1000  (Ethernet)
        RX packets 25  bytes 5721 (5.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2588  bytes 158789 (155.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Continuamos haciendo un escaneo de todos los dispositivos activos en la red.

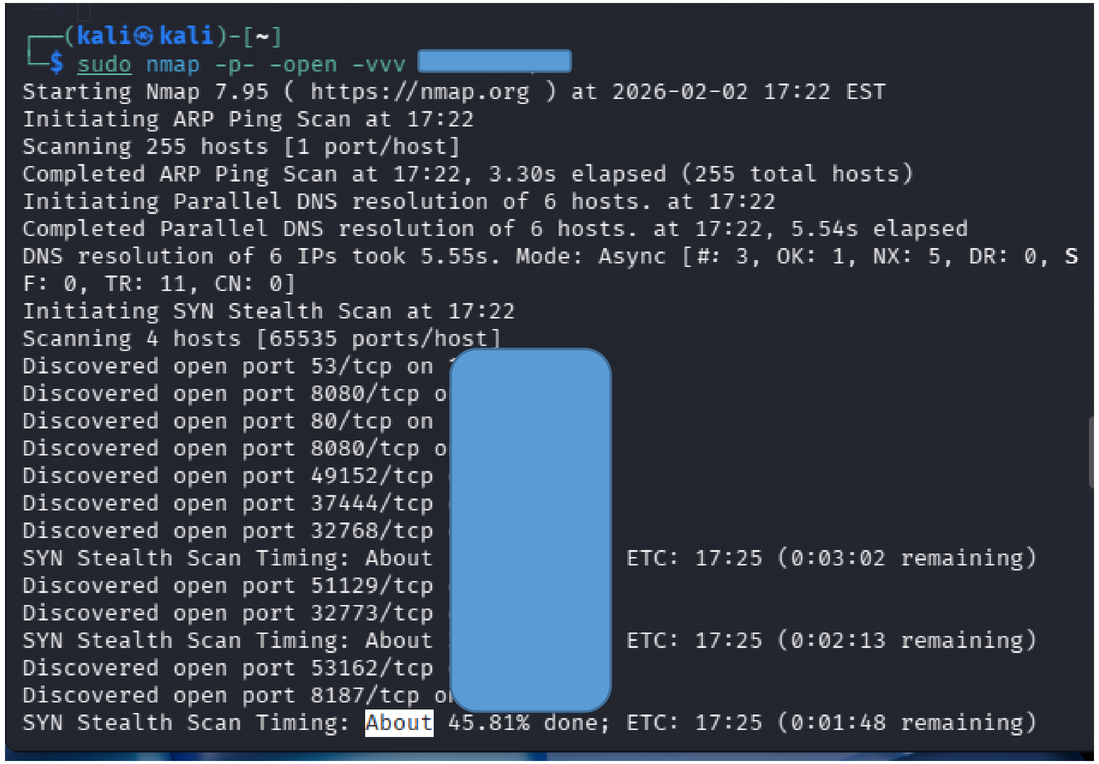


```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:63:b0:05, IPv4: [redacted]
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
[redacted]      20:ab:48:0f:49:92       (Unknown)
                70:85:c6:3d:71:40       (Unknown)
                14:f6:d8:ec:c8:a9       (Unknown)
                24:fc:e5:71:12:db       (Unknown)
                9a:77:2d:fc:e8:de       (Unknown: locally administered)
                06:ce:38:2d:56:12       (Unknown: locally administered)
                6e:08:2c:7f:c8:ce       (Unknown: locally administered)

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.879 seconds (136.24 hosts/sec)
. 7 responded
```

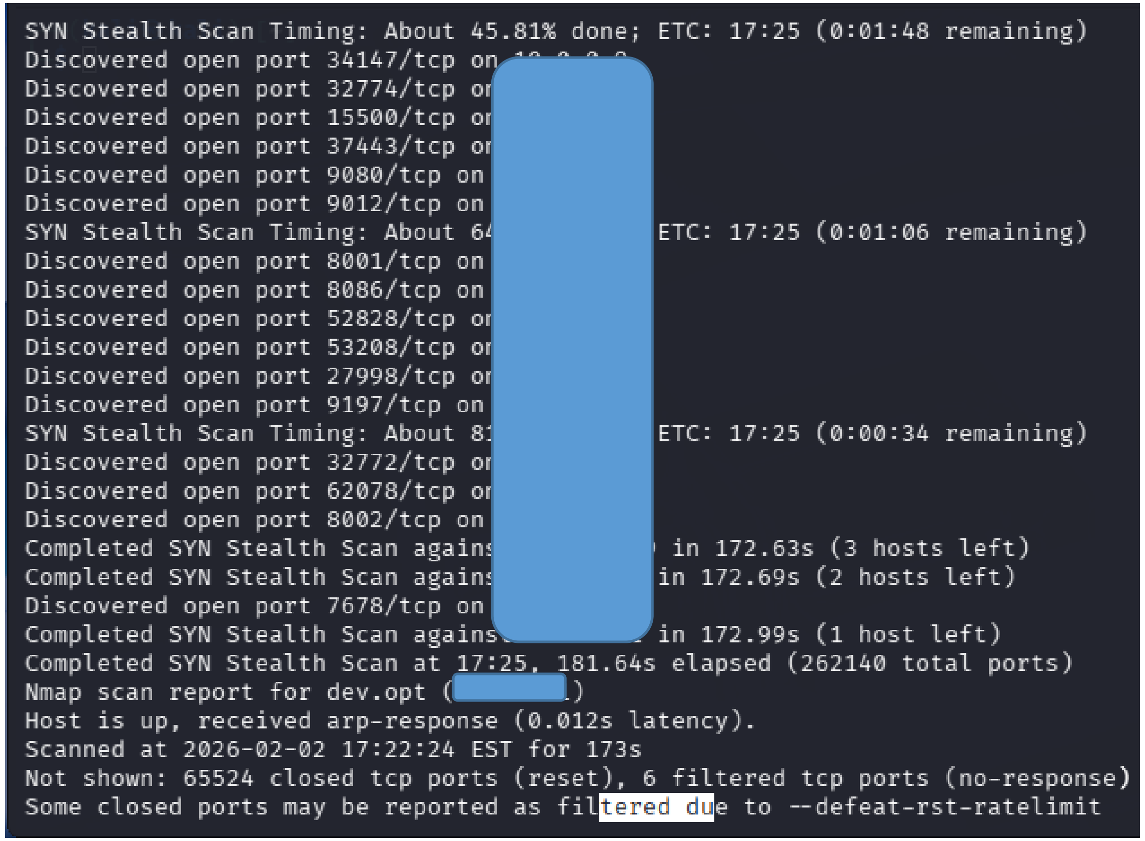


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 17:20 EST
Nmap scan report for dev.opt ([redacted]
Host is up (0.0046s latency).
MAC Address: 20:AB:48:0F:49:92 (Huawei Technologies)
Nmap scan report for [redacted]
Host is up (0.0073s latency).
MAC Address: 70:85:C6:3D:71:40 (Arris Group)
Nmap scan report for [redacted]
Host is up (0.066s latency).
MAC Address: 24:FC:E5:71:12:DB (Samsung Electronics)
Nmap scan report for [redacted]
Host is up (0.13s latency).
MAC Address: 9A:77:2D:FC:E8:DE (Unknown)
Nmap scan report for [redacted]
Host is up (0.11s latency).
MAC Address: 6E:08:2C:7F:C8:CE (Unknown)
Nmap scan report for [redacted]
Host is up (0.00026s latency).
MAC Address: 14:F6:D8:EC:C8:A9 (Intel Corporate)
Nmap scan report for [redacted]
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 16.90 seconds
```

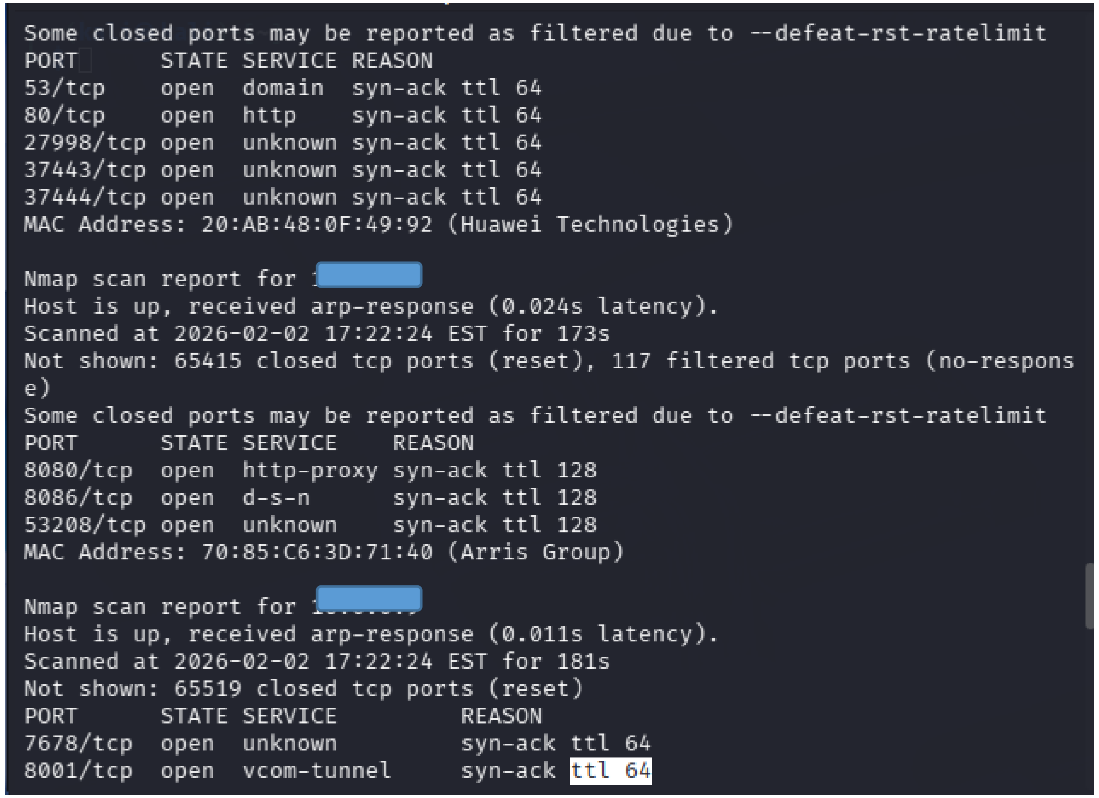
- Finalizamos consiguiendo todos los puertos abiertos de cada ip y también el servicio que se ejecuta por dicho puerto.



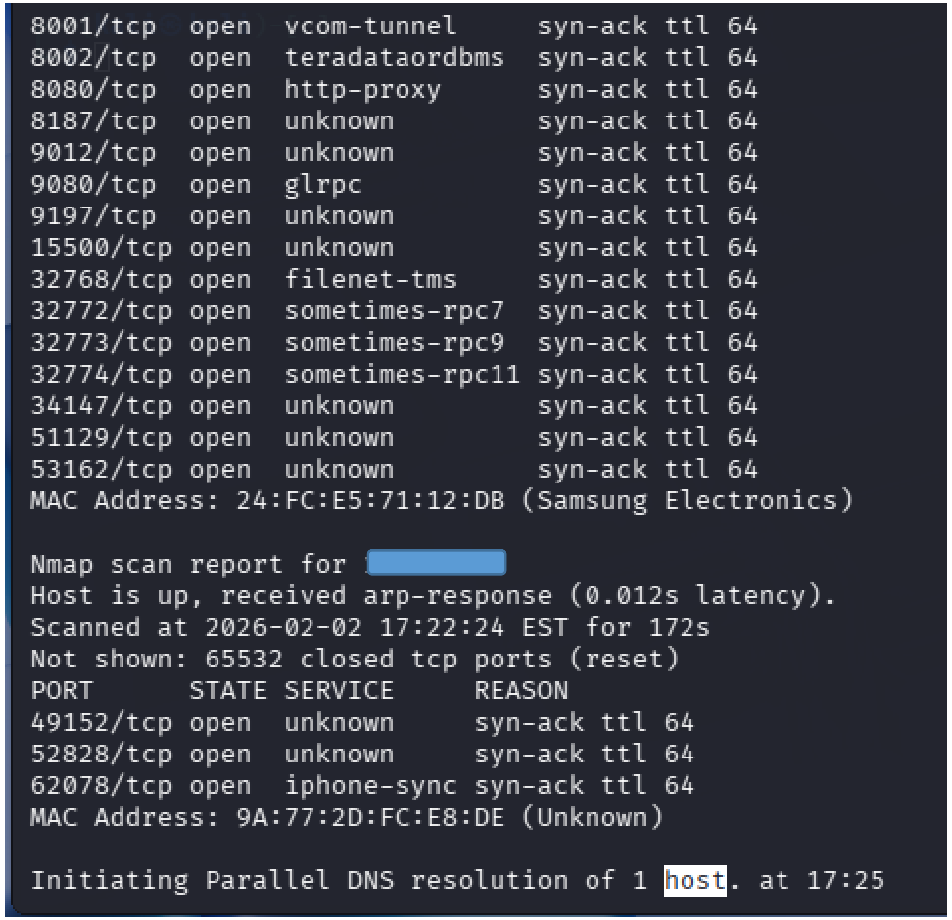
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -open -vvv [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 17:22 EST
Initiating ARP Ping Scan at 17:22
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 17:22, 3.30s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 6 hosts. at 17:22
Completed Parallel DNS resolution of 6 hosts. at 17:22, 5.54s elapsed
DNS resolution of 6 IPs took 5.55s. Mode: Async [#: 3, OK: 1, NX: 5, DR: 0, S
F: 0, TR: 11, CN: 0]
Initiating SYN Stealth Scan at 17:22
Scanning 4 hosts [65535 ports/host]
Discovered open port 53/tcp on [redacted]
Discovered open port 8080/tcp o
Discovered open port 80/tcp on
Discovered open port 8080/tcp o
Discovered open port 49152/tcp
Discovered open port 37444/tcp
Discovered open port 32768/tcp
SYN Stealth Scan Timing: About            ETC: 17:25 (0:03:02 remaining)
Discovered open port 51129/tcp
Discovered open port 32773/tcp
SYN Stealth Scan Timing: About            ETC: 17:25 (0:02:13 remaining)
Discovered open port 53162/tcp
Discovered open port 8187/tcp o
SYN Stealth Scan Timing: About 45.81% done; ETC: 17:25 (0:01:48 remaining)
```



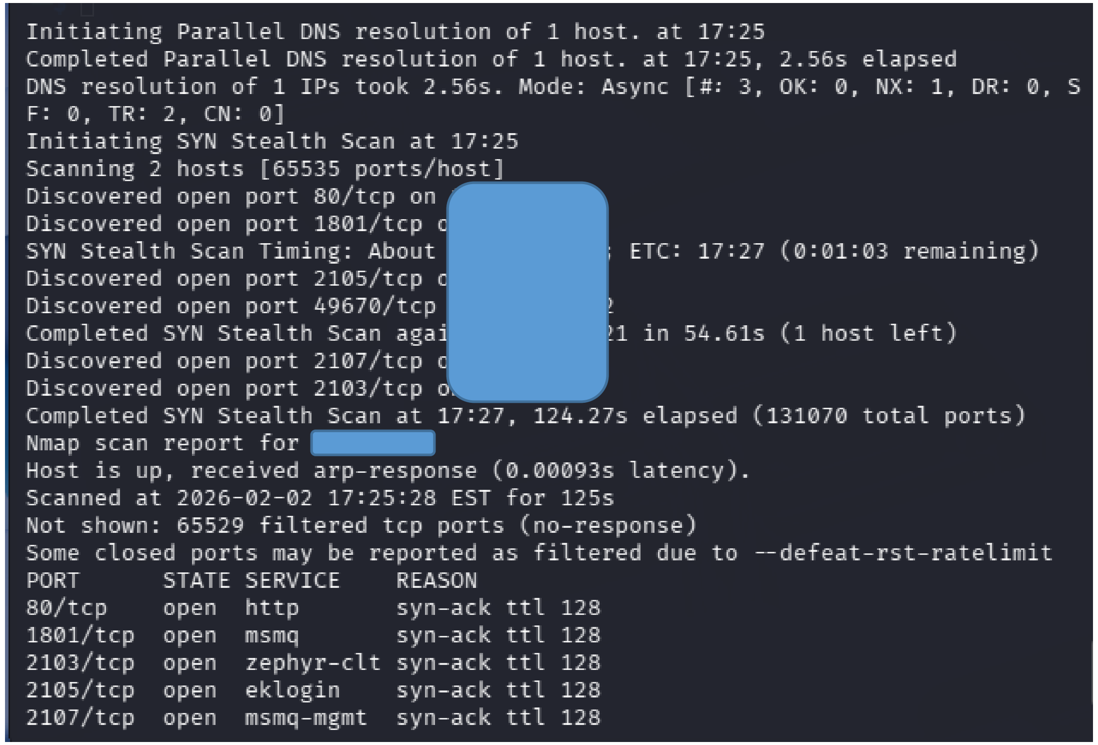
```
SYN Stealth Scan Timing: About 45.81% done; ETC: 17:25 (0:01:48 remaining)
Discovered open port 34147/tcp on [redacted]
Discovered open port 32774/tcp o
Discovered open port 15500/tcp o
Discovered open port 37443/tcp o
Discovered open port 9080/tcp on
Discovered open port 9012/tcp on
SYN Stealth Scan Timing: About 6        ETC: 17:25 (0:01:06 remaining)
Discovered open port 8001/tcp on
Discovered open port 8086/tcp on
Discovered open port 52828/tcp o
Discovered open port 53208/tcp o
Discovered open port 27998/tcp o
Discovered open port 9197/tcp on
SYN Stealth Scan Timing: About 8        ETC: 17:25 (0:00:34 remaining)
Discovered open port 32772/tcp o
Discovered open port 62078/tcp o
Discovered open port 8002/tcp on
Completed SYN Stealth Scan agains        in 172.63s (3 hosts left)
Completed SYN Stealth Scan agains        in 172.69s (2 hosts left)
Discovered open port 7678/tcp on
Completed SYN Stealth Scan agains        in 172.99s (1 host left)
Completed SYN Stealth Scan at 17:25, 181.64s elapsed (262140 total ports)
Nmap scan report for dev.opt ([redacted])
Host is up, received arp-response (0.012s latency).
Scanned at 2026-02-02 17:22:24 EST for 173s
Not shown: 65524 closed tcp ports (reset), 6 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
```



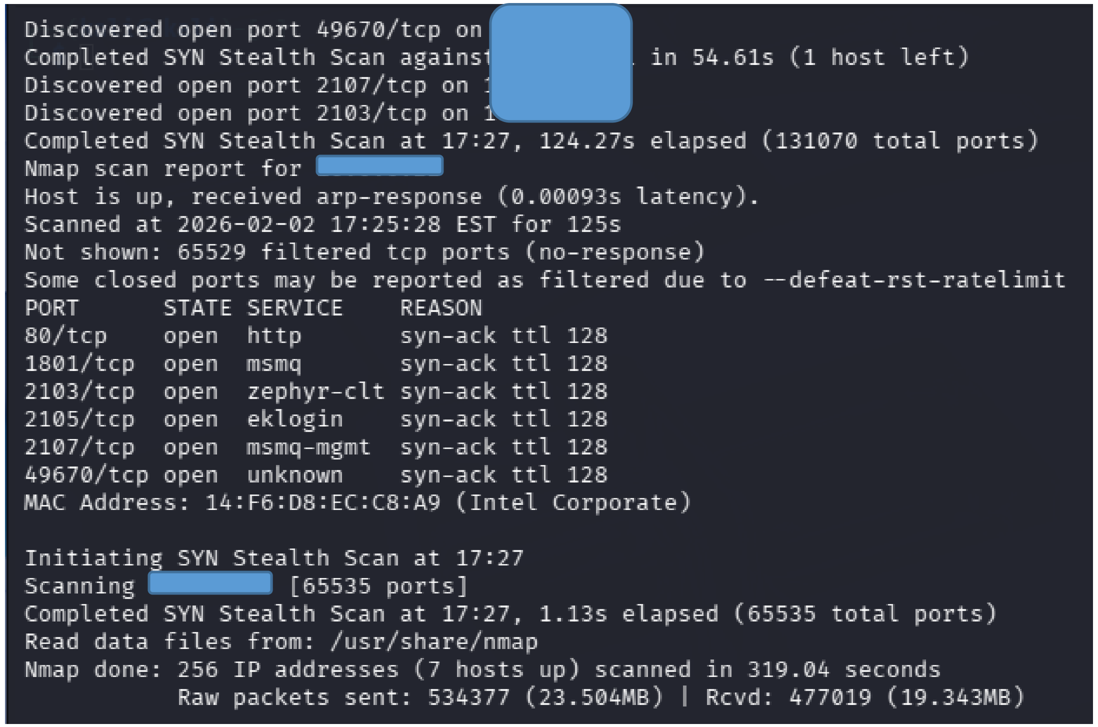
```
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
53/tcp    open  domain  syn-ack ttl 64
80/tcp    open  http    syn-ack ttl 64
27998/tcp open  unknown syn-ack ttl 64
37443/tcp open  unknown syn-ack ttl 64
37444/tcp open  unknown syn-ack ttl 64
MAC Address: 20:AB:48:0F:49:92 (Huawei Technologies)

Nmap scan report for [redacted]
Host is up, received arp-response (0.024s latency).
Scanned at 2026-02-02 17:22:24 EST for 173s
Not shown: 65415 closed tcp ports (reset), 117 filtered tcp ports (no-respons
e)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE    REASON
8080/tcp  open  http-proxy syn-ack ttl 128
8086/tcp  open  d-s-n      syn-ack ttl 128
53208/tcp open  unknown    syn-ack ttl 128
MAC Address: 70:85:C6:3D:71:40 (Arris Group)

Nmap scan report for [redacted]
Host is up, received arp-response (0.011s latency).
Scanned at 2026-02-02 17:22:24 EST for 181s
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE         REASON
7678/tcp  open  unknown         syn-ack ttl 64
8001/tcp  open  vcom-tunnel     syn-ack ttl 64
```



```
8001/tcp  open  vcom-tunnel     syn-ack ttl 64
8002/tcp  open  teradataordbms  syn-ack ttl 64
8080/tcp  open  http-proxy      syn-ack ttl 64
8187/tcp  open  unknown         syn-ack ttl 64
9012/tcp  open  unknown         syn-ack ttl 64
9080/tcp  open  glrpc           syn-ack ttl 64
9197/tcp  open  unknown         syn-ack ttl 64
15500/tcp open  unknown         syn-ack ttl 64
32768/tcp open  filenet-tms     syn-ack ttl 64
32772/tcp open  sometimes-rpc7  syn-ack ttl 64
32773/tcp open  sometimes-rpc9  syn-ack ttl 64
32774/tcp open  sometimes-rpc11 syn-ack ttl 64
34147/tcp open  unknown         syn-ack ttl 64
51129/tcp open  unknown         syn-ack ttl 64
53162/tcp open  unknown         syn-ack ttl 64
MAC Address: 24:FC:E5:71:12:DB (Samsung Electronics)

Nmap scan report for [redacted]
Host is up, received arp-response (0.012s latency).
Scanned at 2026-02-02 17:22:24 EST for 172s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE     REASON
49152/tcp open  unknown     syn-ack ttl 64
52828/tcp open  unknown     syn-ack ttl 64
62078/tcp open  iphone-sync syn-ack ttl 64
MAC Address: 9A:77:2D:FC:E8:DE (Unknown)

Initiating Parallel DNS resolution of 1 host. at 17:25
```



```
Initiating Parallel DNS resolution of 1 host. at 17:25
Completed Parallel DNS resolution of 1 host. at 17:25, 2.56s elapsed
DNS resolution of 1 IPs took 2.56s. Mode: Async [#: 3, OK: 0, NX: 1, DR: 0, S
F: 0, TR: 2, CN: 0]
Initiating SYN Stealth Scan at 17:25
Scanning 2 hosts [65535 ports/host]
Discovered open port 80/tcp on [redacted]
Discovered open port 1801/tcp o
SYN Stealth Scan Timing: About          ETC: 17:27 (0:01:03 remaining)
Discovered open port 2105/tcp o
Discovered open port 49670/tcp          2
Completed SYN Stealth Scan agai         21 in 54.61s (1 host left)
Discovered open port 2107/tcp o
Discovered open port 2103/tcp o
Completed SYN Stealth Scan at 17:27, 124.27s elapsed (131070 total ports)
Nmap scan report for [redacted]
Host is up, received arp-response (0.00093s latency).
Scanned at 2026-02-02 17:25:28 EST for 125s
Not shown: 65529 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE    REASON
80/tcp    open  http       syn-ack ttl 128
1801/tcp  open  msmq       syn-ack ttl 128
2103/tcp  open  zephyr-clt syn-ack ttl 128
2105/tcp  open  eklogin    syn-ack ttl 128
2107/tcp  open  msmq-mgmt  syn-ack ttl 128
```



```
Discovered open port 49670/tcp on [redacted]
Completed SYN Stealth Scan against           in 54.61s (1 host left)
Discovered open port 2107/tcp on 1
Discovered open port 2103/tcp on 1
Completed SYN Stealth Scan at 17:27, 124.27s elapsed (131070 total ports)
Nmap scan report for [redacted]
Host is up, received arp-response (0.00093s latency).
Scanned at 2026-02-02 17:25:28 EST for 125s
Not shown: 65529 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE    REASON
80/tcp    open  http       syn-ack ttl 128
1801/tcp  open  msmq       syn-ack ttl 128
2103/tcp  open  zephyr-clt syn-ack ttl 128
2105/tcp  open  eklogin    syn-ack ttl 128
2107/tcp  open  msmq-mgmt  syn-ack ttl 128
49670/tcp open  unknown    syn-ack ttl 128
MAC Address: 14:F6:D8:EC:C8:A9 (Intel Corporate)

Initiating SYN Stealth Scan at 17:27
Scanning [redacted] [65535 ports]
Completed SYN Stealth Scan at 17:27, 1.13s elapsed (65535 total ports)
Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (7 hosts up) scanned in 319.04 seconds
           Raw packets sent: 534377 (23.504MB) | Rcvd: 477019 (19.343MB)
```