

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.

```
SESSION ACTIONS Edit View Help
└─(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet [REDACTED] netmask 255.255.255.0 broadcast [REDACTED]
        inet6 fe80::5994:b23:2d92:bde3 prefixlen 64 scopeid 0x20<link>
        inet6 fd17:625c:f037:2:d6e4:1f9b:922d:9c6f prefixlen 64 scopeid 0x0
<global>
    ether 08:00:27:63:b0:05 txqueuelen 1000 (Ethernet)
    RX packets 2285359 bytes 2800460529 (2.6 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1071382 bytes 90496204 (86.3 MiB)
    TX errors 0 dropped 26 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 393317 bytes 16527700 (15.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 393317 bytes 16527700 (15.7 MiB)
    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
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:63:b0:05, IPv4: [REDACTED]
WARNING: Cannot open MAC/Vendor file ieeeoui.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] b8:3a:08:6c:de:00      (Unknown)
[REDACTED] 8c:55:2b:60:c4:84      (Unknown)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.845 seconds (138.75 hosts/sec)
. 2 responded
```

```
(kali㉿kali)-[~]
$ sudo nmap -sn [REDACTED]
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 23:00 EST
Nmap scan report for [REDACTED]
Host is up (0.0035s latency).
MAC Address: B8:3A:08:6C:DE:00 (Tenda Technology,Ltd.Dongguan branch)
Nmap scan report for [REDACTED]
Host is up (0.00094s latency).
MAC Address: 8C:55:2B:60:C4:84 (Unknown)
Nmap scan report for [REDACTED]
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 3.06 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]4
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-02 23:06 EST
Initiating ARP Ping Scan at 23:06
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 23:06, 1.83s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 23:06
Completed Parallel DNS resolution of 2 hosts. at 23:06, 0.04s elapsed
DNS resolution of 2 IPs took 0.04s. Mode: Async [#: 1, OK: 0, NX: 2, DR: 0, S
F: 0, TR: 2, CN: 0]
Initiating Parallel DNS resolution of 1 host. at 23:06
Completed Parallel DNS resolution of 1 host. at 23:06, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, S
F: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 23:06
Scanning 2 hosts [65535 ports/host]
Discovered open port 3306/tcp on [REDACTED]1
Discovered open port 80/tcp on [REDACTED]1
Discovered open port 135/tcp on [REDACTED]1
Discovered open port 9000/tcp on [REDACTED]1
Discovered open port 1980/tcp on [REDACTED]1
Completed SYN Stealth Scan again
Discovered open port 5357/tcp on [REDACTED]1
Discovered open port 5040/tcp on [REDACTED]1
Discovered open port 902/tcp on [REDACTED]1
Discovered open port 912/tcp on [REDACTED]1
Discovered open port 2179/tcp on [REDACTED]1
in 9.44s (1 host left)
```

```
Discovered open port 2179/tcp on [REDACTED]
Discovered open port 7680/tcp on [REDACTED]
Completed SYN Stealth Scan at 23:08, 103.71s elapsed (131070 total ports)
Nmap scan report for [REDACTED]
Host is up, received arp-response (0.0042s latency).
Scanned at 2026-02-02 23:06:40 EST for 9s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
80/tcp    open  http         syn-ack ttl 64
1980/tcp  open  pearldoc-xact syn-ack ttl 64
9000/tcp  open  cslistener   syn-ack ttl 64
MAC Address: B8:3A:08:6C:DE:00 (Tenda Technology,Ltd.Dongguan branch)

Nmap scan report for [REDACTED]1
Host is up, received arp-response (0.00043s latency).
Scanned at 2026-02-02 23:06:40 EST for 103s
Not shown: 65527 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 128
902/tcp   open  iss-realsecure syn-ack ttl 128
912/tcp   open  apex-mesh    syn-ack ttl 128
2179/tcp  open  vmrdp       syn-ack ttl 128
3306/tcp  open  mysql        syn-ack ttl 128
5040/tcp  open  unknown      syn-ack ttl 128
5357/tcp  open  wsdapi       syn-ack ttl 128
7680/tcp  open  pando-pub   syn-ack ttl 128
MAC Address: 8C:55:2B:60:C4:84 (Unknown)
```

```
Initiating SYN Stealth Scan at 23:08
Scanning [REDACTED] [65535 ports]
Completed SYN Stealth Scan at 23:08, 1.53s elapsed (65535 total ports)
Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (3 hosts up) scanned in 107.62 seconds
Raw packets sent: 262772 (11.554MB) | Rcvd: 196747 (8.132MB)
```