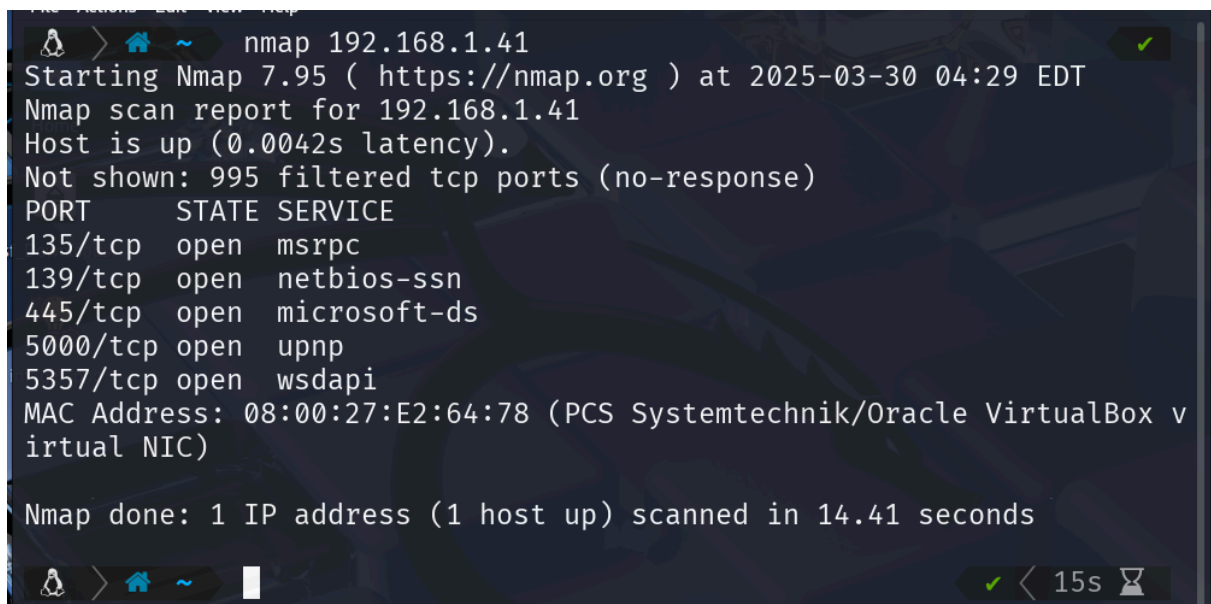


# Escaneos Básicos con Nmap



```
nmap 192.168.1.41
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 04:29 EDT
Nmap scan report for 192.168.1.41
Host is up (0.0042s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5000/tcp  open  upnp
5357/tcp  open  wsapi
MAC Address: 08:00:27:E2:64:78 (PCS Systemtechnik/Oracle VirtualBox v
irtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
```

## Escaneos de puertos

Partiendo de un reconocimiento de equipos que componen una red por ejemplo con arp-scan (**NOTA:** es aconsejable utilizar varias herramientas para hacer un reconocimiento de la red para evitar que algún equipo de la red se quede sin detectar). Escogemos un equipo objetivo. En nuestro caso el equipo señalado en la captura que como vemos es una maquina virtual.

```
sudo arp-scan -l eth0 --localnet
```

```
File Actions Edit View Help
~ sudo arp-scan -I eth0 --localnet
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:6e:13:6e, IPv4: 192.168.1.40
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)
192.168.1.1      08:33:ed:6d:55:d0      (Unknown)
192.168.1.33    f8:77:b8:a0:38:74      (Unknown)
192.168.1.39    e4:c7:67:0f:1f:40      (Unknown)
192.168.1.38    68:ed:a4:33:e9:46      (Unknown)
192.168.1.36    00:1d:94:0d:d5:99      (Unknown)
192.168.1.41    08:00:27:e2:64:78      (Unknown)

18 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.987 seconds (128.84 hosts/sec). 6 responded
```

Hacemos un Ping al equipo victima con una sola traza para intentar averiguar que clase de equipo es.

```
ping -c 1 192.168.1.41
```

```
~ ping -c 1 192.168.1.41
PING 192.168.1.41 (192.168.1.41) 56(84) bytes of data.
64 bytes from 192.168.1.41: icmp_seq=1 ttl=128 time=6.35 ms

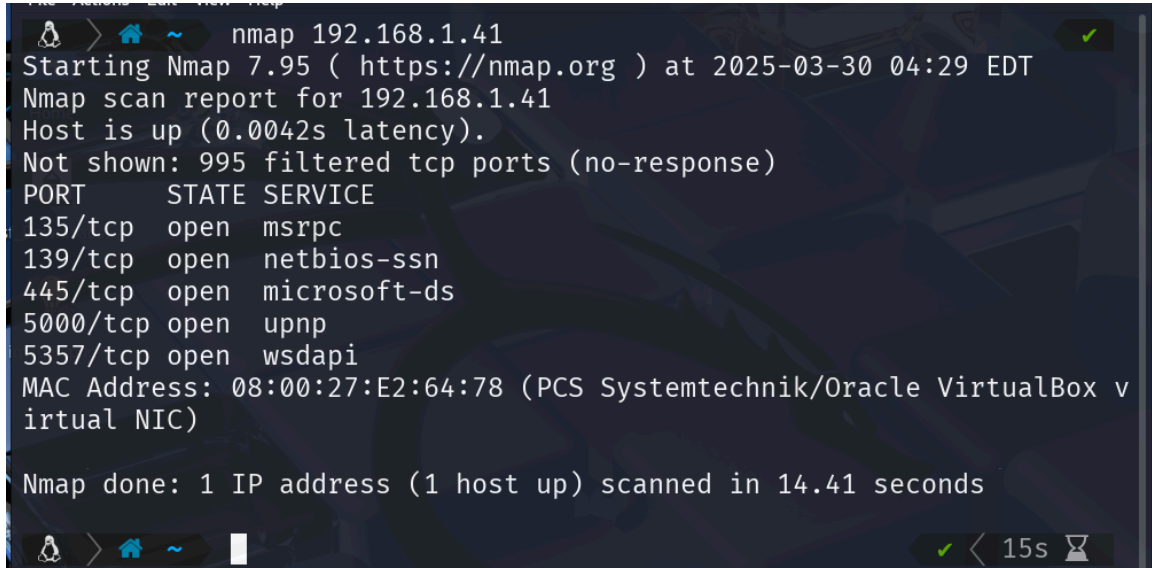
— 192.168.1.41 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 6.354/6.354/6.354/0.000 ms
```

Como vemos nos devuelve un **ttl de 128**. Esto nos da un gran porcentaje de seguridad que es una maquina **Windows**.

Queremos ver información mas concreta sobre la maquina , que puertos tiene abiertos, que corre en ellos y su versión, etec... . Para ello utilizaremos **nmap**.

- En su uso mas **básico de nmap** seria de esta manera:

```
nmap 192.168.1.41
```



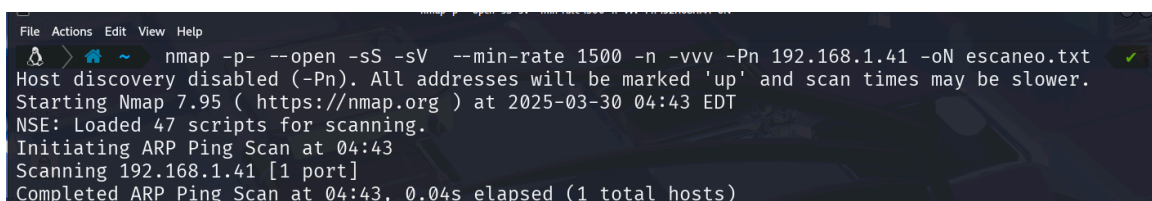
```
nmap 192.168.1.41
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 04:29 EDT
Nmap scan report for 192.168.1.41
Host is up (0.0042s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
5000/tcp   open  upnp
5357/tcp   open  wsddapi
MAC Address: 08:00:27:E2:64:78 (PCS Systemtechnik/Oracle VirtualBox v irtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.41 seconds
```

Como se ve no muestra mucha información excepto los puertos abiertos.

- Vamos a hacer que **nmap** nos muestre los puertos abiertos y los que este corriendo tras ellos.

```
nmap -p- --open -sS -sV --min-rate 1500 -n -vvv -Pn 192.168.1.41 -oN escaneo.txt
```



```
nmap -p- --open -sS -sV --min-rate 1500 -n -vvv -Pn 192.168.1.41 -oN escaneo.txt
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 04:43 EDT
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 04:43
Scanning 192.168.1.41 [1 port]
Completed ARP Ping Scan at 04:43, 0.04s elapsed (1 total hosts)
```

## Explicación de los parámetros:



**-p-:** Indica que se deben **escanear todos los puertos, desde el 1 hasta el 65535**. De manera predeterminada, Nmap solo analiza los 1000 puertos más comunes, pero con este parámetro amplías el alcance.

**- -open:** Solo **muestra los puertos** que están **abiertos**, omitiendo los que estén cerrados o filtrados.

**-sS:** Realiza un **escaneo SYN** (half-open), el cual es rápido y menos detectable por sistemas de seguridad, ya que no establece conexiones completas.

**-sV:** Permite **identificar las versiones de los servicios que se ejecutan en los puertos** abiertos, brindando más detalles sobre el software en uso.

**- -min-rate 1500:** **Asegura una velocidad mínima de 1500 paquetes** enviados **por segundo**, acelerando el escaneo.

**-n:** **Desactiva la resolución de nombres DNS**, lo que hace que el análisis sea más rápido al no buscar los nombres de host asociados a las direcciones IP.

**-vvv:** Incrementa la verbosidad del comando, **mostrando más información en tiempo real** sobre el progreso del escaneo.

**-Pn:** **Prescinde del ping previo** para verificar si el host está activo, asumiendo que el objetivo está accesible aunque no responda a solicitudes ICMP.

**192.168.1.41:** Es la **dirección IP del objetivo** que se desea analizar. En este caso, es un dispositivo específico dentro de la red local.

**-oN escaneo.txt:** **Guarda los resultados** del escaneo **en un archivo** llamado escaneo.txt en un formato fácil de leer.

```
File Actions Edit View Help
kali@kali~
Scanning 192.168.1.41 [65535 ports]
Discovered open port 135/tcp on 192.168.1.41
Discovered open port 139/tcp on 192.168.1.41
Discovered open port 445/tcp on 192.168.1.41
SYN Stealth Scan Timing: About 23.25% done; ETC: 04:46 (0:01:42 remaining)
SYN Stealth Scan Timing: About 46.14% done; ETC: 04:46 (0:01:11 remaining)
SYN Stealth Scan Timing: About 70.61% done; ETC: 04:46 (0:00:38 remaining)
Discovered open port 5357/tcp on 192.168.1.41
Discovered open port 5000/tcp on 192.168.1.41
Completed SYN Stealth Scan at 04:46, 123.30s elapsed (65535 total ports)
Initiating Service scan at 04:46
Scanning 5 services on 192.168.1.41
Completed Service scan at 04:48, 162.19s elapsed (5 services on 1 host)
NSE: Script scanning 192.168.1.41.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 04:48
Completed NSE at 04:48, 0.03s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 04:48
Completed NSE at 04:48, 1.01s elapsed
Nmap scan report for 192.168.1.41
Host is up, received arp-response (0.0028s latency).
Scanned at 2025-03-30 04:43:57 EDT for 287s
Not shown: 65530 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON      VERSION
135/tcp    open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp    open  netbios-ssn syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGR
OUP)
5000/tcp   open  upnp?        syn-ack ttl 128
5357/tcp   open  http         syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:E2:64:78 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: MARIO-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 286.79 seconds
Raw packets sent: 196690 (8.654MB) | Rcvd: 100 (4.384KB)
```