

[protegermipc.net](https://protegermipc.net)

# Tutorial y listado de comandos más útiles para Nmap

10-13 minutos

---

Cuando se trata de escoger las [mejores herramientas de hacking](#) o ciberseguridad, en el apartado de escaneo / inventariado de redes siempre hay una que destaca por encima del resto: *nmap*.

[Nmap](#) responde a la abreviatura de *Network Mapper* (mapeador de redes) y es una herramienta open source gratuita para realizar auditorias de seguridad y descubrimientos de red. Algunos administradores la utilizan también para realizar inventariado y monitorización de estado básica de los dispositivos.

Nmap admite como valores para escaneo diferentes elementos: nombres de host (hostnames), direcciones IP o redes completas, entre otros. Si el caso que te interesa es el último sigue leyendo más abajo.

Esta navaja suiza de las redes y seguridad ofrece una variedad de tipos de análisis y opciones (incluida la de usar *scripts*) que la convierte en preferible para muchos y cuyo alcance, por ser inmenso, no podría cubrirse en un único artículo como este.

## **Antes de empezar...**

No te pongas a lanzar escaneos con esta herramienta -ni con

ninguna otra similar- si pensar y a cualquier sitio. Especialmente, no lo hagas desde el trabajo (o recibirás una incómoda visita).

Si quieres practicar comandos de Nmap puedes usar tu propio equipo “localhost” como valor para los comandos más básicos.

Además, los desarrolladores ponen a nuestra disposición varios servidores que permiten ser escaneados.

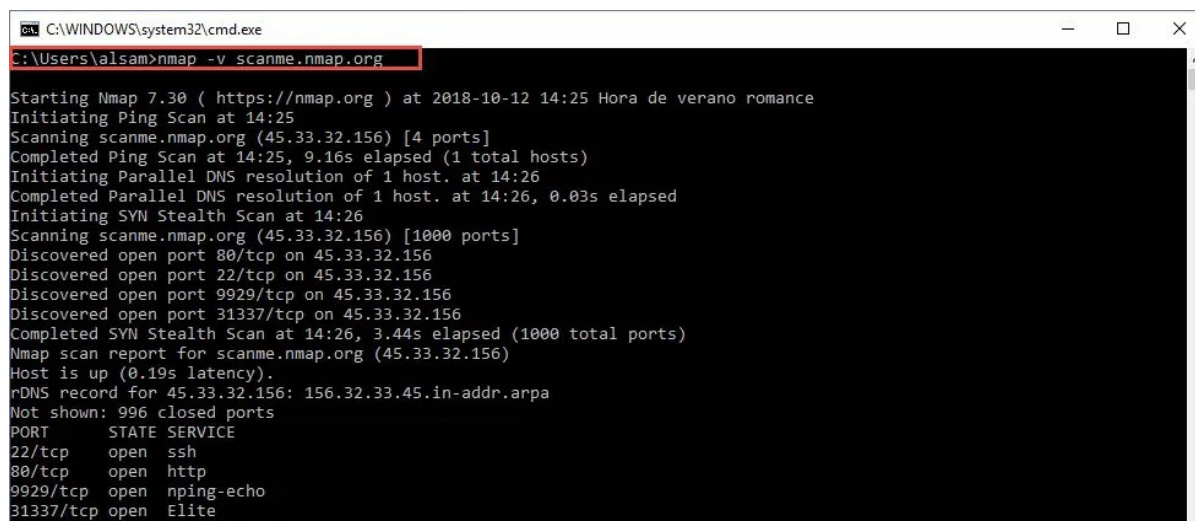
- [scanme.nmap.org](https://scanme.nmap.org)
- [analizame2.nmap.org](https://analizame2.nmap.org)

## Listado de comandos de NMAP comunes

A continuación una muestra de los comandos que considero más útiles o quizá más demandados por los usuarios y administradores de seguridad o sistemas. Evidentemente no es una lista completa, echarás en falta muchos si conoces la herramienta. No olvidemos que esto es un tutorial que busca servir de referencia rápida.

### Escaneo de puertos TCP básico

Esta opción analiza y muestra todos los puertos *TCP* (Transmission Control Protocol) reservados actualmente en la máquina destino.



```
C:\WINDOWS\system32\cmd.exe
C:\Users\alsam>nmap -v scanme.nmap.org

Starting Nmap 7.30 ( https://nmap.org ) at 2018-10-12 14:25 Hora de verano romance
Initiating Ping Scan at 14:25
Scanning scanme.nmap.org (45.33.32.156) [4 ports]
Completed Ping Scan at 14:25, 9.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:26
Completed Parallel DNS resolution of 1 host. at 14:26, 0.03s elapsed
Initiating SYN Stealth Scan at 14:26
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed SYN Stealth Scan at 14:26, 3.44s elapsed (1000 total ports)
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.19s latency).
rDNS record for 45.33.32.156: 156.32.33.45.in-addr.arpa
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
```

```
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 57.23 seconds
Raw packets sent: 1004 (44.152KB) | Rcvd: 1007 (40.308KB)
C:\Users\alsam>
```

## Detalles:

- La opción **-v** significa “verbose”, por lo que se nos indica lo que está haciendo el análisis al detalle

Se nos muestra además del número de puerto y su estado, el servicio al que corresponde -teóricamente- dicho puerto. Por ejemplo, el puerto *22/tcp* corresponde a *ssh* (secure shell)

## Escanear un rango de IPs con Nmap

Escanear un rango de IPs nos resultaría útil en casos de un posible ataque de red. si queremos intentar averiguar donde tiene lugar. También ahorraría tiempo al rastrear este tipo de ataques. Se usa simplemente delimitando el último campo.

```
nmap <IP>--<IP2>
```

Por ejemplo:

```
nmap 192.168.1.1-115
```

## Escanear puertos concretos o rangos de puertos con Nmap

Este método de escaneo se centra en un puerto concreto. De esta forma, conseguiremos que la salida sea más corta si no estamos interesados en otros:

```
nmap -p <número_puerto>
```

Ejemplo:

```
nmap -p 80 192.168.1.200
```

```
C:\Users\alsam>nmap -p 80 192.168.1.200
```

```
c:\users\alisan\cmd>nmap -p 80 192.168.1.200

Starting Nmap 7.30 ( https://nmap.org ) at 2018-10-12 16:38 Hora de verano romance
Nmap scan report for rufnas (192.168.1.200)
Host is up (0.0020s latency).
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 24:5E:BE: (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 39.39 seconds
```

De manera similar, delimitaremos el primer y último puerto para escanear rangos de puertos:

```
nmap -p 80-995 192.168.1.200
```

## Escanear todos los puertos con Nmap

Con este tipo de comando analizaremos los 65536 puertos disponibles en cada dispositivo. Este tipo de escaneo puede interesar a un administrador, pero desde luego no a un atacante. Primero, porque hace mucho ruido y segundo, porque normalmente ellos utilizan los conocidos como “half-opening” (canal a medio abrir).

```
nmap -p- localhost
```

Con el comando anterior verás todos los puertos actualmente detectados en tu equipo (abiertos o filtrados).

## Elegir el tipo de escáner usado por Network Mapper

A la hora de realizar escaneos con Nmap es importante saber que existen diferentes tipos de escaneo de puertos. Dependiendo del objetivo a escanear nos podrá interesar más uno u otro.

Por ejemplo, si queremos determinar si ciertos puertos TCP están activos en un sistema remoto, escogeremos un escaneo TCP. Los hackers suelen utilizar diferentes escaneos para intentar localizar

un puerto abierto vulnerable a cierto vector de ataque.

## Lanzar un escaneo TCP SYN (opción por defecto)

Este comando determina si el puerto objetivo está escuchando. Mediante este comando se puede llevar a cabo una técnica conocida como escaneo *half-opening*. Se le conoce así porque comienza como una conexión normal, pero no llega a establecerse un handshake por ambas partes, sino que enviamos un único paquete *SYN* y esperamos la respuesta.

Si el intérprete reciba una respuesta *SYN/ACK* o *RST* (reset) sabrá marcar que el puerto está escuchando.

```
nmap -sS <IP>
```

**Ejemplo:** `nmap -sS 192.168.1.200`

```
C:\Users\alsam>nmap -sS 192.168.1.200

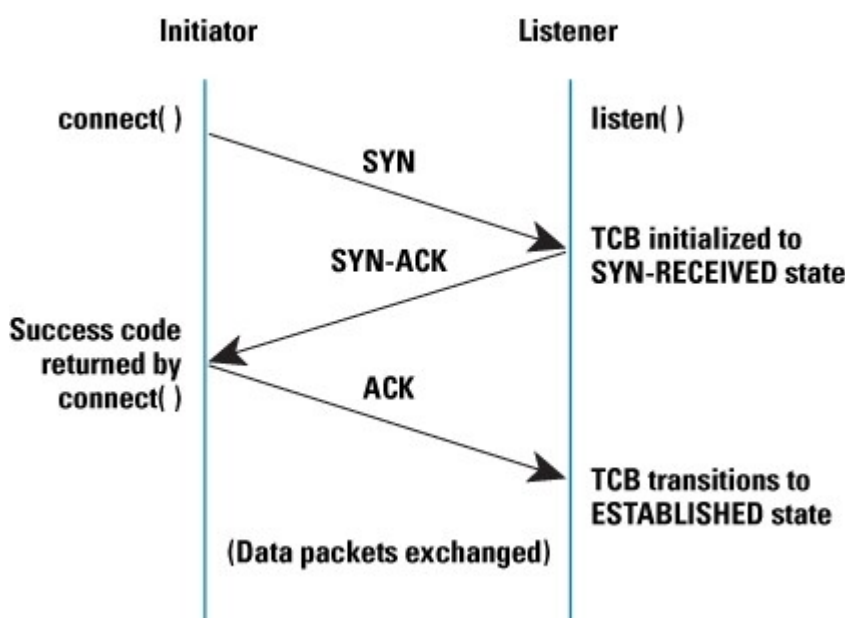
Starting Nmap 7.30 ( https://nmap.org ) at 2018-10-12 16:55 Hora de verano romance
Nmap scan report for 192.168.1.200
Host is up (0.0050s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
873/tcp   open  rsync
2049/tcp  open  nfs
3306/tcp  open  mysql
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
30000/tcp open  ndmps
49152/tcp open  unknown
MAC Address: 24:5E:BE: (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 40.34 seconds
```

## Escaneo mediante TCP Connect

Mientras en el ejemplo anterior (SYN/ACK) dejamos la conexión “a medias”, con este tipo de análisis realizaremos un 3-way-

handshake (saludo de 3 direcciones) o lo que es lo mismo, una conexión completa vía TCP.



Este es el comando para escanear con la opción “conexión TCP”. Si un usuario no cuenta con privilegios elevados sobre paquetes, será el comando a utilizar. Un escaneo de tipo TCP-connect necesita una conexión completa, lo que hace que sea más lento que un escaneo SYN.

Los resultados que veremos serán similares al test anterior. Dado que muchos host estarán configurados para no atender a solicitudes de ping, podría no tener éxito, en cuyo caso utilizaremos la opción `-Pn`. Eso sí, estaremos analizando muchos más posibles host así que el tiempo invertido podría ser mayor.

## Detección de sistema y servicios

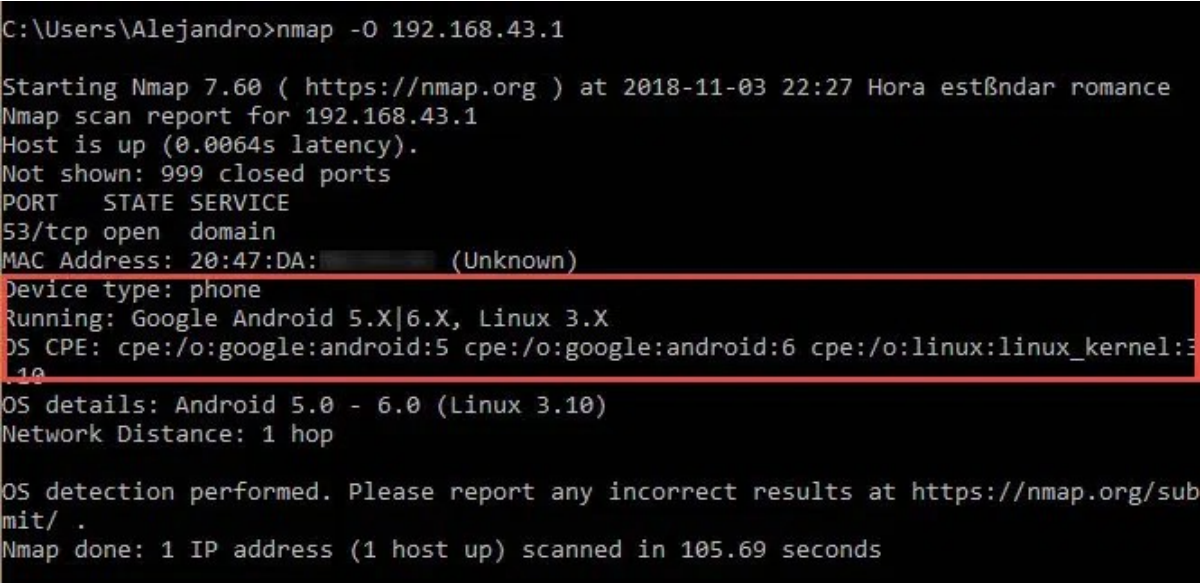
También podemos intentar averiguar el sistema operativo, la versión y los servicios activos en nuestro objetivo gracias a Nmap. No siempre conseguirá darnos una precisión máxima (dependiendo de la visibilidad que tenga sobre ese host) pero siempre es un buen aliado durante cualquier test de penetración.

Los análisis de *sistema operativo* (OS) utilizan el fingerprint o “huella” de la pila **TCP/IP**, mientras la *detección de servicios* funciona comparando las pruebas enviadas por el intérprete contra una base de datos.

## Escaneo de sistema operativo

Escogeremos la opción “O”, como en el ejemplo:

```
nmap -O 192.168.43.45
```



```
C:\Users\Alejandro>nmap -O 192.168.43.1

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-03 22:27 Hora estándar romance
Nmap scan report for 192.168.43.1
Host is up (0.0064s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 20:47:DA: (Unknown)
Device type: phone
Running: Google Android 5.X|6.X, Linux 3.X
OS CPE: cpe:/o:google:android:5 cpe:/o:google:android:6 cpe:/o:linux:linux_kernel:3.10
OS details: Android 5.0 - 6.0 (Linux 3.10)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 105.69 seconds
```

Es una opción simple que se limita a marcar el tipo de dispositivo, sistema operativo y MAC, entre otros datos.

## Escaneo de Sistema Operativo y servicios

Escogeremos la opción “-A/a”:

```
nmap -A 192.168.1.43
```

## Escaneo de servicios estandar

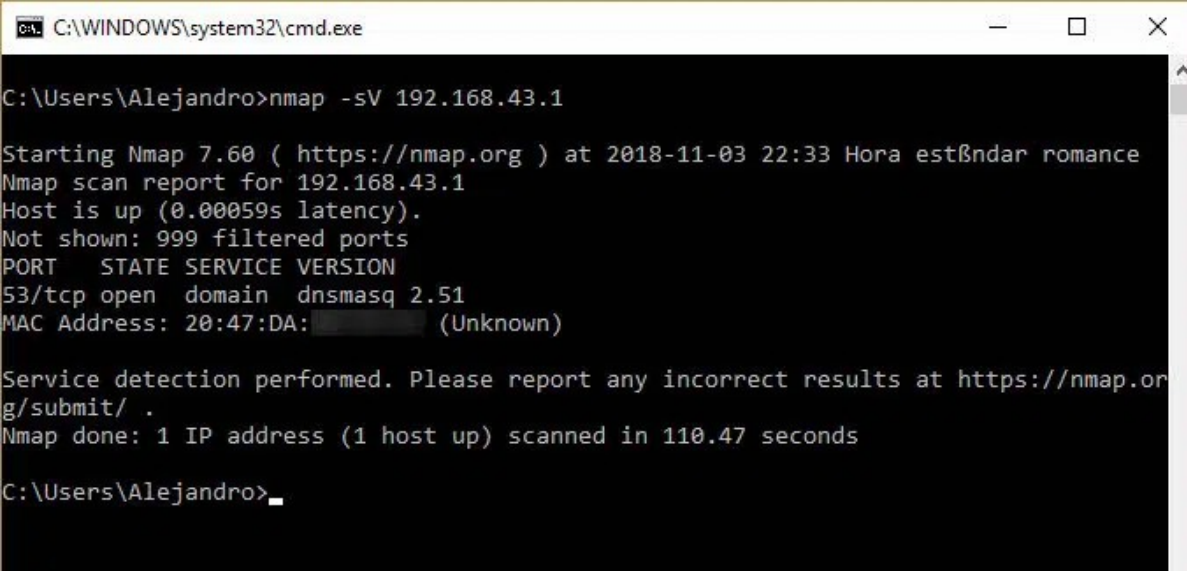
Si queremos evaluar únicamente los servicios con puerto asociado,



es muy posible que la base de datos de Nmap (con más de 2000 entradas) encuentre algo interesante:

```
nmap -sV 192.168.1.43
```

Puertos comunes como SSH (22), DNS (53) o HTTP (80) aparecerán listados.



```
C:\WINDOWS\system32\cmd.exe

C:\Users\Alejandro>nmap -sV 192.168.43.1

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-03 22:33 Hora estándar romance
Nmap scan report for 192.168.43.1
Host is up (0.00059s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.51
MAC Address: 20:47:DA: (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.47 seconds

C:\Users\Alejandro>_
```

## Escaneo de servicios agresivo

Con un análisis de servicios más agresivo podemos obtener más información. Sin embargo, este escaneo deja más trazas en el sistema y en logs de firewalls, por lo que los hackers “black hat” normalmente no utilizan este tipo de escaneo.

```
nmap -sV --version-intensity 5 192.168.43.1
```

Este método es útil para detectar servicios que no se están ejecutando en sus puertos predefinidos.

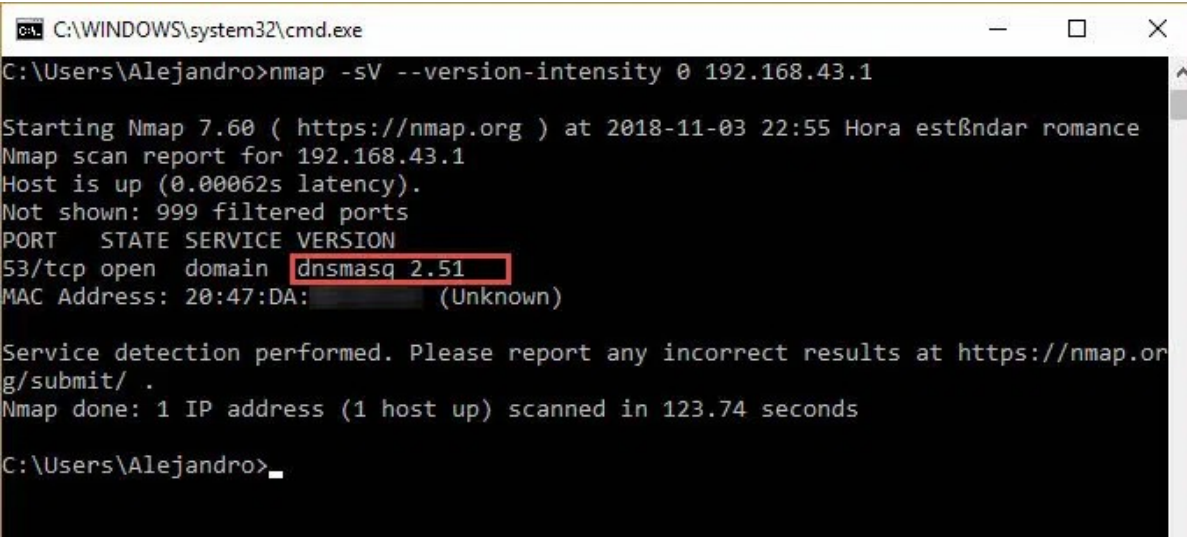
## Escaneo de servicios de banner ligero

Un escaneo ligero de este tipo es usado normalmente por hackers cuando intentan permanecer en la sombra. Es mucho menos



ruidoso que un escaneo agresivo y permite obtener datos sin llamar demasiado la atención, lo que aporta una clara ventaja.

```
nmap -sV --version-intensity 0 192.168.43.1
```



```
C:\WINDOWS\system32\cmd.exe
C:\Users\Alejandro>nmap -sV --version-intensity 0 192.168.43.1

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-03 22:55 Hora estándar romance
Nmap scan report for 192.168.43.1
Host is up (0.00062s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain dnsmasq 2.51
MAC Address: 20:47:DA: (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 123.74 seconds

C:\Users\Alejandro>_
```

Este método no intenta detectar el servicio, sino que se limita a capturar el banner del servicio abierto para averiguar que se está ejecutando.

## ¿Cómo escanear una subred completa usando Nmap?

Nmap es una herramienta extremadamente versátil y seguro que hay quien no la ha usado habitualmente para escanear redes en su conjunto. Pues bien, aquí nos ofrece resultados igual de buenos.

Básicamente, para realizar un escaneo de red completa con nmap tendremos ante todo que indicar el valor de la red como argumento a través del número de *bytes* de su *máscara de red*. Es decir, si cuando analizamos un único host escribimos su dirección IP:

```
nmap xxx.xxx.xxx.xxx
```

Ahora lo que haremos será indicar además la máscara de red

```
nmap xxx.xxx.xxx.xxx/XX
```

Y poco más que decir, porque el resto de opciones siguen aplicando de igual forma que si se tratase de un escaneo convencional.

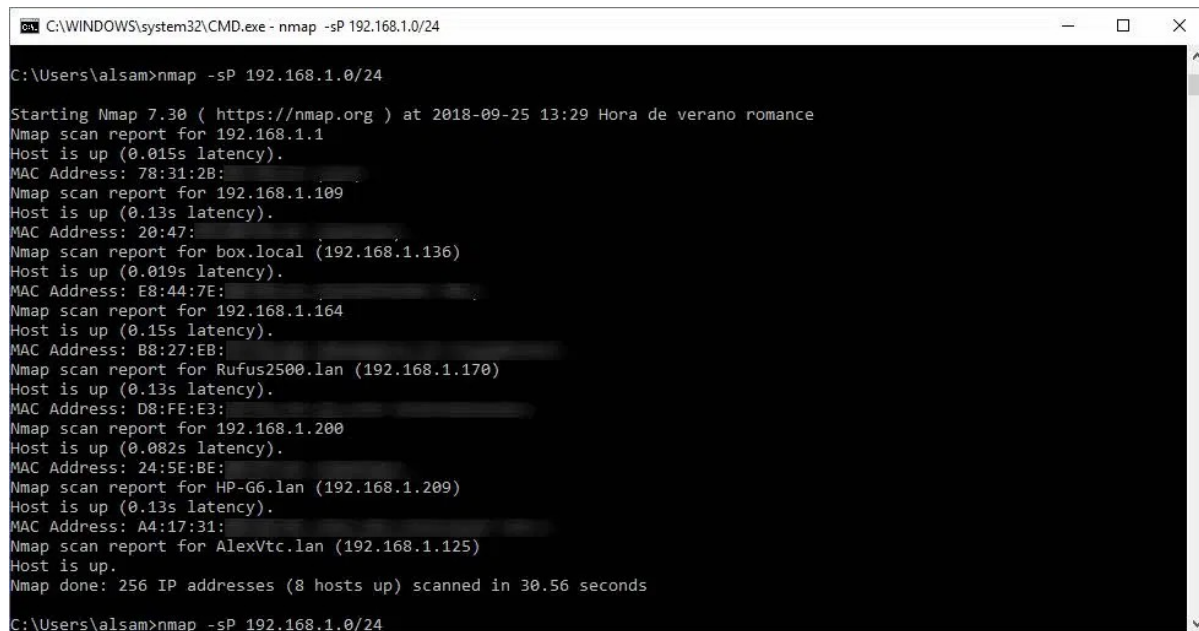
**Relacionado – [¿Cómo calcular máscaras de red?](#)**

## Escaneo de toda la red con Nmap (simple)

Si necesitamos descubrir equipos vivos (es decir, que nos digan “oye, aquí estoy”) en toda la red pero no queremos saber mucho sobre ellos, podemos lanzar un escaneo como el que sigue:

```
nmap -sP <ip/máscara de red>
```

**Ejemplo: nmap -sP 192.168.1.0/24**



```
C:\WINDOWS\system32\CMD.exe - nmap -sP 192.168.1.0/24

C:\Users\alsam>nmap -sP 192.168.1.0/24

Starting Nmap 7.30 ( https://nmap.org ) at 2018-09-25 13:29 Hora de verano romance
Nmap scan report for 192.168.1.1
Host is up (0.015s latency).
MAC Address: 78:31:2B:
Nmap scan report for 192.168.1.109
Host is up (0.13s latency).
MAC Address: 20:47:
Nmap scan report for box.local (192.168.1.136)
Host is up (0.019s latency).
MAC Address: E8:44:7E:
Nmap scan report for 192.168.1.164
Host is up (0.15s latency).
MAC Address: B8:27:EB:
Nmap scan report for Rufus2500.lan (192.168.1.170)
Host is up (0.13s latency).
MAC Address: D8:FE:E3:
Nmap scan report for 192.168.1.200
Host is up (0.082s latency).
MAC Address: 24:5E:BE:
Nmap scan report for HP-G6.lan (192.168.1.209)
Host is up (0.13s latency).
MAC Address: A4:17:31:
Nmap scan report for AlexVtc.lan (192.168.1.125)
Host is up.
Nmap done: 256 IP addresses (8 hosts up) scanned in 30.56 seconds

C:\Users\alsam>nmap -sP 192.168.1.0/24
```

Se nos mostrará el estado del host, su latencia (el tiempo que tarda en responder), su IP y su dirección MAC.

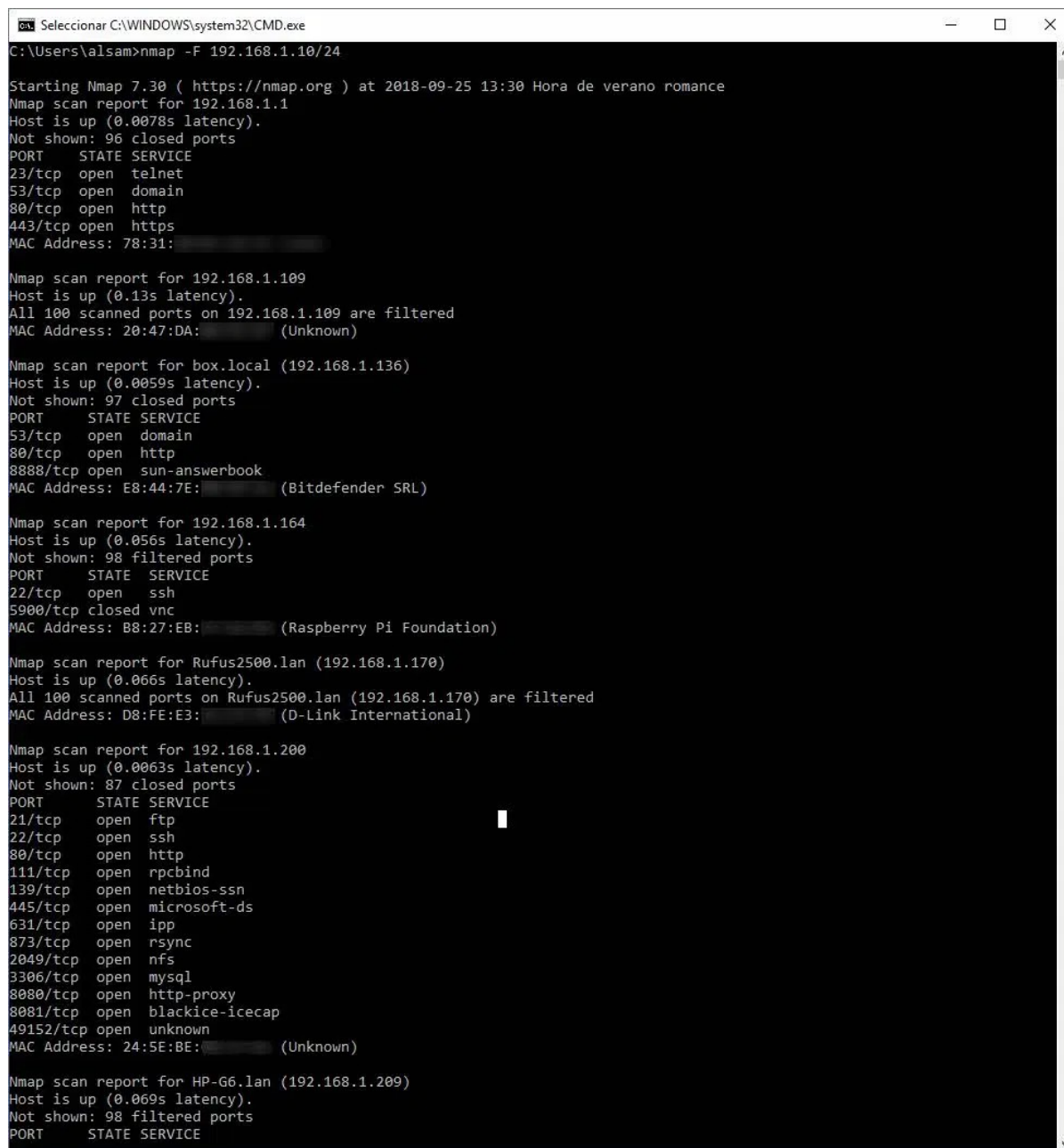
## Escaneo de red con Nmap + puertos (rápido)

Con el siguiente comando podremos analizar toda una red o rango

en busca de hosts. Se nos mostrarán los datos del ejemplo anterior y además el estado de algunos de sus puertos (los más comunes).

```
nmap -F/-f <ip/máscara de red>
```

**Ejemplo:** `nmap -F 192.168.1.0/24`



```
C:\Users\alsam>nmap -F 192.168.1.0/24

Starting Nmap 7.30 ( https://nmap.org ) at 2018-09-25 13:30 Hora de verano romance
Nmap scan report for 192.168.1.1
Host is up (0.0078s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: 78:31: (Unknown)

Nmap scan report for 192.168.1.109
Host is up (0.13s latency).
All 100 scanned ports on 192.168.1.109 are filtered
MAC Address: 20:47:DA: (Unknown)

Nmap scan report for box.local (192.168.1.136)
Host is up (0.0059s latency).
Not shown: 97 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
8888/tcp  open  sun-answerbook
MAC Address: E8:44:7E: (Bitdefender SRL)

Nmap scan report for 192.168.1.164
Host is up (0.056s latency).
Not shown: 98 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
5900/tcp  closed vnc
MAC Address: B8:27:EB: (Raspberry Pi Foundation)

Nmap scan report for Rufus2500.lan (192.168.1.170)
Host is up (0.066s latency).
All 100 scanned ports on Rufus2500.lan (192.168.1.170) are filtered
MAC Address: D8:FE:E3: (D-Link International)

Nmap scan report for 192.168.1.200
Host is up (0.0063s latency).
Not shown: 87 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
873/tcp   open  rsync
2049/tcp  open  nfs
3306/tcp  open  mysql
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
49152/tcp open  unknown
MAC Address: 24:5E:BE: (Unknown)

Nmap scan report for HP-G6.lan (192.168.1.209)
Host is up (0.069s latency).
Not shown: 98 filtered ports
PORT      STATE SERVICE
```

## Detalles

- **F:** la opción **-F** indica que el escaneo sea *Fast* (rápido). Es decir, no se analizarán tantos puertos como con un análisis corriente. Aquí se analizan los 100 puertos más comunes.

## Escaneo de red completa sigiloso con detección de SO

`nmap -sS -O <IP/máscara>`

**Ejemplo:** `nmap -sS -O 192.168.1.0/24`

Este tipo de escaneo se diferencia del anterior en que añade algunos datos adicionales, como son:

- **Tipo de dispositivo (device type):** normalmente aparecerá “general purpose” o propósito general en ambientes domésticos.
- **Sistema operativo:** intentará reconocer el sistema o kernel (en versiones Linux).
- **Distancia de red (network distance):** se lanzará además una traza de red que nos indicará cuantos saltos nos separan del dispositivo/red analizado.

```
C:\Users\alsam>nmap -sS -O 192.168.1.0/24

Starting Nmap 7.30 ( https://nmap.org ) at 2018-10-12 14:59 Hora de verano romance
Nmap scan report for 192.168.1.1
Host is up (0.017s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp    open  https
44443/tcp  filtered coldfusion-auth
52869/tcp  open  unknown
MAC Address: 08:00:27:1C:4E:50 (zte)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.10
Network Distance: 1 hop

Nmap scan report for 192.168.1.109
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.1.109 are filtered (656) or closed (344)
MAC Address: 08:00:27:1C:4E:50 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for box.local (192.168.1.136)
Host is up (0.0083s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
8888/tcp  open  sun-answerbook
MAC Address: 08:00:27:1C:4E:50 (Bitdefender SRL)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.30%E=4%D=10/12%OT=53%CT=1%CU=42791%PV=Y%D=1%DC=D%G=Y%M=E8447E%
OS:TM=5BC09DB9%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=106%TI=Z%CI=I
OS:%TS=U)SEQ(SP=102%GCD=1%ISR=106%TI=Z%CI=I%II=I%TS=U)SEQ(CI=I%II=I)OPS(O1=
OS:M5B4NNSNW3%O2=M5B4NNSNW3%O3=M5B4NNSNW3%O4=M5B4NNSNW3%O5=M5B4NNSNW3%O6=M5B4N
OS:NS)WIN(W1=3908%W2=3908%W3=3908%W4=3908%W5=3908%W6=3908)ECN(R=Y%DF=Y%T=40
OS:%W=3908%O=M5B4NNSNW3%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R
OS:=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
OS:T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%U
OS:N=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

```
Network Distance: 1 hop
Nmap scan report for RedmiNote5A- lan (192.168.1.179)
Host is up (0.024s latency).
All 1000 scanned ports on RedmiNote5A-Lidia.lan (192.168.1.179) are closed
MAC Address: (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

## Detalles

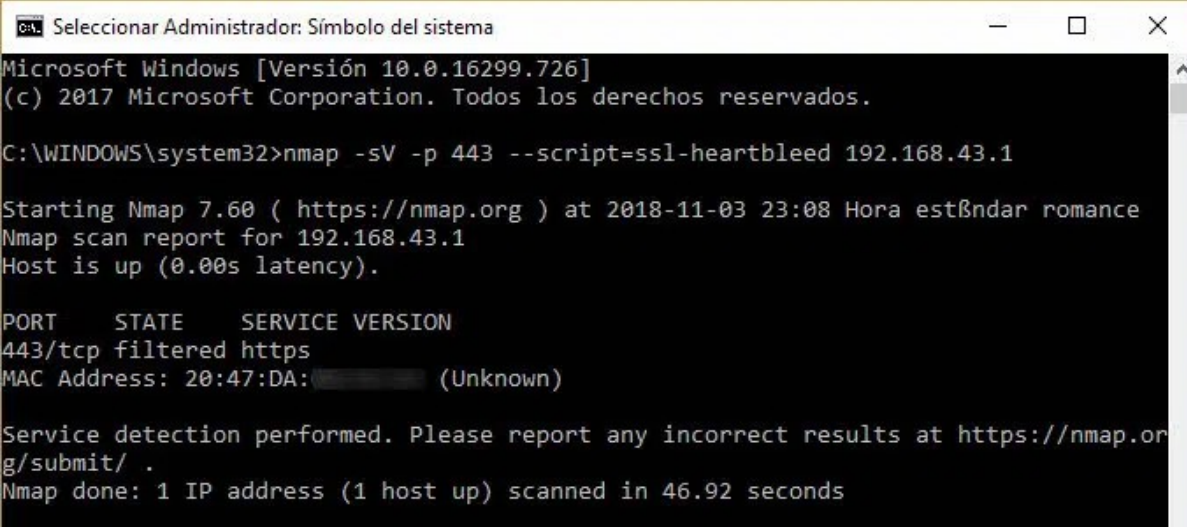
- **Ss**: técnica de escaneo SYN (otras opciones incluyen sT/sA/sW/sM)
- **O**: detección de sistema operativo

## Usar scripts con Nmap

Los scripts son útiles cuando buscamos información sobre diferentes tipos de ataque. Podemos utilizar un único script o incluso un conjunto de ellos (para ahorrar tiempo).

Un ejemplo sería el siguiente script, que busca ataques de tipo heartbleed:

```
nmap -sV -p 443 --script=ssl-heartbleed
192.168.43.1
```



```
Microsoft Windows [Versión 10.0.16299.726]
(c) 2017 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>nmap -sV -p 443 --script=ssl-heartbleed 192.168.43.1

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-03 23:08 Hora estándar romance
Nmap scan report for 192.168.43.1
Host is up (0.00s latency).

PORT      STATE      SERVICE VERSION
443/tcp    filtered  https
MAC Address: 20:47:DA: (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org
g/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.92 seconds
```

Para actualizar la base de datos de scripts de Nmap (actualmente en torno a 500) usaremos el comando:



```
nmap --script-updatedb
```

Para visualizar los scripts disponibles, podemos usar el comando.

## Kali / Linux

```
locate nse | grep script
```

## Windows

```
nmap --script-help *
```

La opción anterior muestra todos los scripts de la base de datos.

Para obtener información sobre uno en concreto usaremos:

```
nmap --script-help=<nombre>
```

```
Administrador: Símbolo del sistema
C:\WINDOWS\system32>nmap --script-help=xmpp-brute

Starting Nmap 7.60 ( https://nmap.org ) at 2018-11-03 23:27 Hora estándar romance

xmpp-brute
Categories: brute intrusive
https://nmap.org/nsedoc/scripts/xmpp-brute.html
  Performs brute force password auditing against XMPP (Jabber) instant messaging servers.
```

Los scripts nos permitirán realizar una gran cantidad de auditorías de seguridad de red y cosas más “chulas”. Si nos tomamos en serio la seguridad de nuestro entorno, será de gran utilidad tomar contacto con estos scripts.

## Evitar el descubrimiento de hosts

Finalmente os dejo un truco que os será de ayuda para no llamar la atención. Nmap normalmente lanza un descubrimiento de red con cada comando, aunque especifiquemos un puerto específico (por ejemplo: `nmap -p 80 ejemplo.com`).

Con el siguiente parámetro es posible evitarlo y así levantaremos menos alarmas:

```
nmap -PN -p 80 ejemplo.com
```

## Palabras finales

Hemos llegado al final de este breve tutorial sobre nmap y hemos demostrado que es uno de los analizadores de red más versátiles y eficientes que existen. Aún hoy. Este software tiene una capacidad de personalización enorme y seguro que algunos de vosotros podéis hacer sugerencias sobre nuevos comandos que no haya tenido en cuenta.

Además, Nmap cuenta con un potente aliado con interfaz gráfica llamado **Zenmap**. Nos despedimos con algo de humor.

