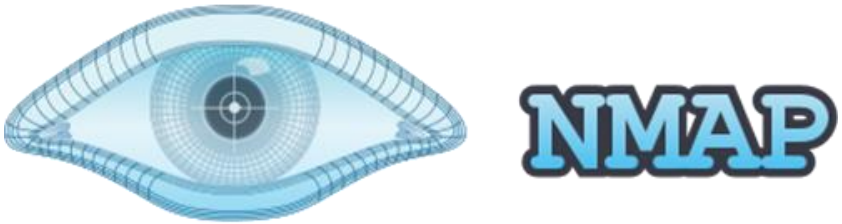
Anexo. Uso de herramienta Nmap

Nmap (“mapeador de redes”) es una **herramienta de código abierto para exploración de red y auditoría de seguridad.** Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. **Nmap utiliza paquetes IP "crudos"** («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, **qué sistemas operativos** (y sus versiones) **ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando**, así como docenas de otras características. Aunque **generalmente se utiliza Nmap en auditorías de seguridad**, muchos **administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos**.

La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la “tabla de puertos interesantes”. Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado. El **estado** puede ser **open** (abierto), **filtered** (filtrado), **closed** (cerrado), o **unfiltered** (no filtrado). **Abierto** significa que **la aplicación en la máquina destino se encuentra esperando** conexiones o paquetes en ese puerto. **Filtrado** indica que **un cortafuegos, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto**, por lo que **Nmap no puede saber si se encuentra abierto o cerrado**. Los puertos **cerrados no tienen ninguna aplicación escuchando en los mismos**, aunque podrían abrirse en cualquier momento. Los clasificados como **no filtrados** son aquellos que responden a los sondeos de Nmap, pero para los que **Nmap no puede determinar si se encuentran abiertos o cerrados**. Nmap informa de las combinaciones de estado open|filtered y closed|filtered cuando no puede determinar en cuál de los dos estados está un puerto. **La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. Nmap** ofrece **información de los protocolos IP soportados**, en vez de puertos abiertos, cuando se solicita un análisis de protocolo IP con la opción (-sO).

Además de la tabla de puertos interesantes, **Nmap** puede dar **información adicional sobre los objetivos**, incluyendo **el nombre de DNS** según la resolución inversa de la IP, **un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC**.

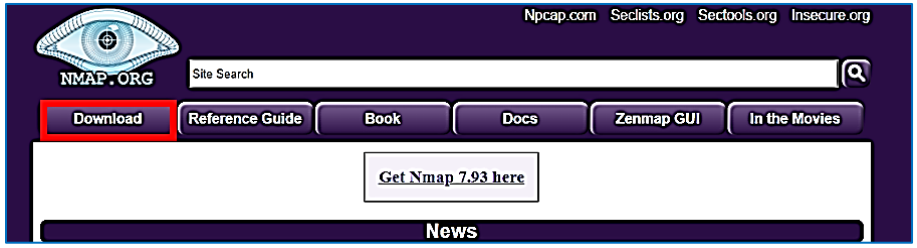


1. **Instalar Nmap**

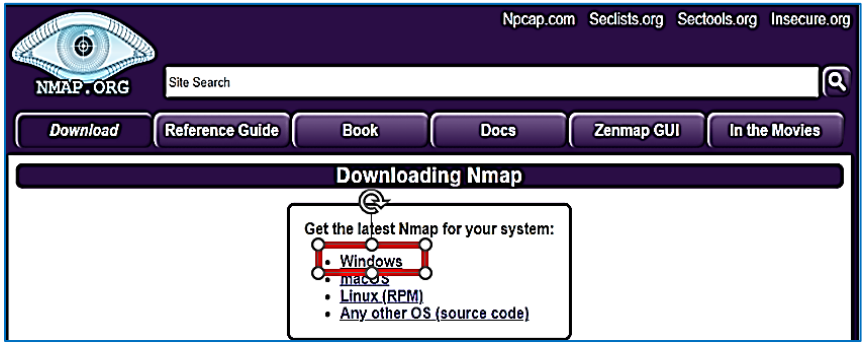
   Windows

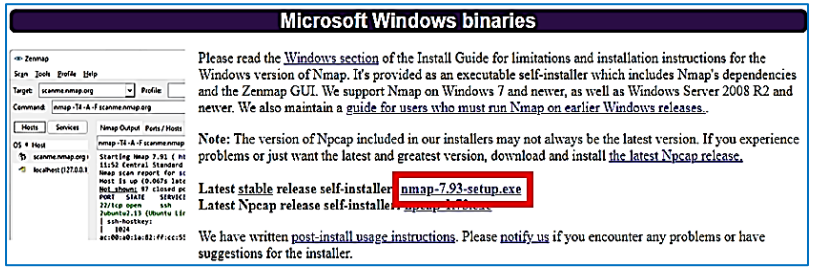
   Acceder al sito de Nmap

   Seleccionar **Download**



   Seleccionar **Windows**





   Descargar e instalar.

Linux

Ya viene instalado en Kali Linux.

```
sudo apt update && sudo apt upgrade
sudo apt install nmap
```

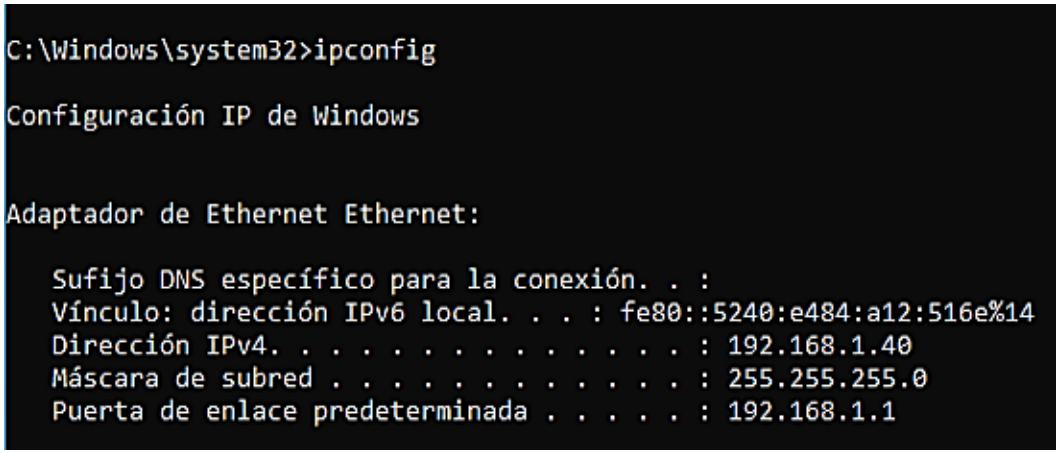
2. Utilizar Nmap

1. Primer escaneo

Vamos a hacer un escaneo de nuestro equipo:

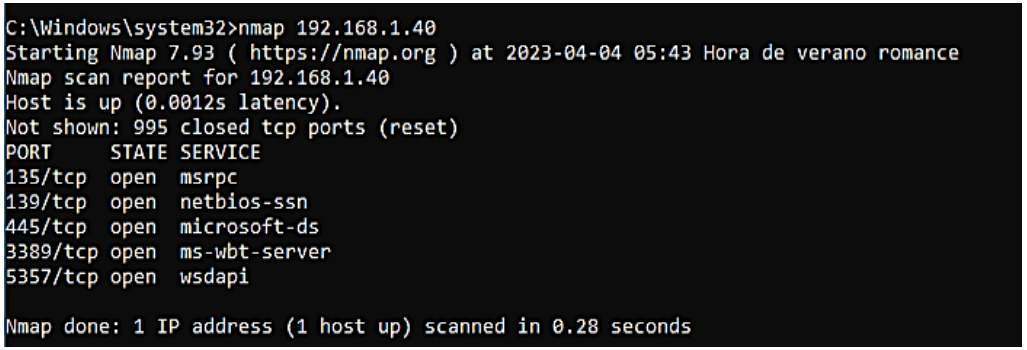
Primero emos cual es nuestra IP:

```
ip address
```



A continuación, hacemos un escaneo a nuestro equipo:

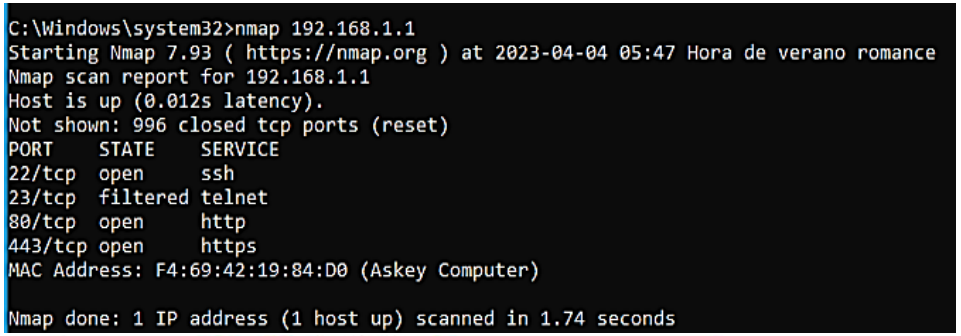
```
Nmap 192.168.1.40
```



2. Escaneos iniciales

A continuación, hacemos un escaneo a nuestro equipo:

```
nmap 192.168.1.1
```



Veamos la versión de **Nmap**

```
nmap --version
```

```
C:\Windows\system32>nmap --version
Nmap version 7.93 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.3.6 openssl-3.0.5 nmap-libssh2-1.10.0 nmap-libz-1.2.12 nmap-libpcre-7.6 Npcap-1.73 nmap-li
dnet-1.12 ipv6
Compiled without:
Available nsock engines: iocp poll select
```

Para escanear un objetivo, con una salida detallada de cada puerto que encuentre, con ***parámetro -vv***

```
nmap -vv IP
```

```
C:\Windows\system32>nmap 10.0.2.1 -vv
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 05:18 Hora de verano romance
Initiating ARP Ping Scan at 05:18
Scanning 10.0.2.1 [1 port]
Completed ARP Ping Scan at 05:18, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:18
Completed Parallel DNS resolution of 1 host. at 05:18, 0.04s elapsed
Initiating SYN Stealth Scan at 05:18
Scanning 10.0.2.1 [1000 ports]
Discovered open port 53/tcp on 10.0.2.1
Completed SYN Stealth Scan at 05:18, 0.23s elapsed (1000 total ports)
Nmap scan report for 10.0.2.1
Host is up, received arp-response (0.0013s latency).
Scanned at 2023-04-05 05:18:54 Hora de verano romance for 1s
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE REASON
53/tcp open  domain  syn-ack ttl 255
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.032KB)
```

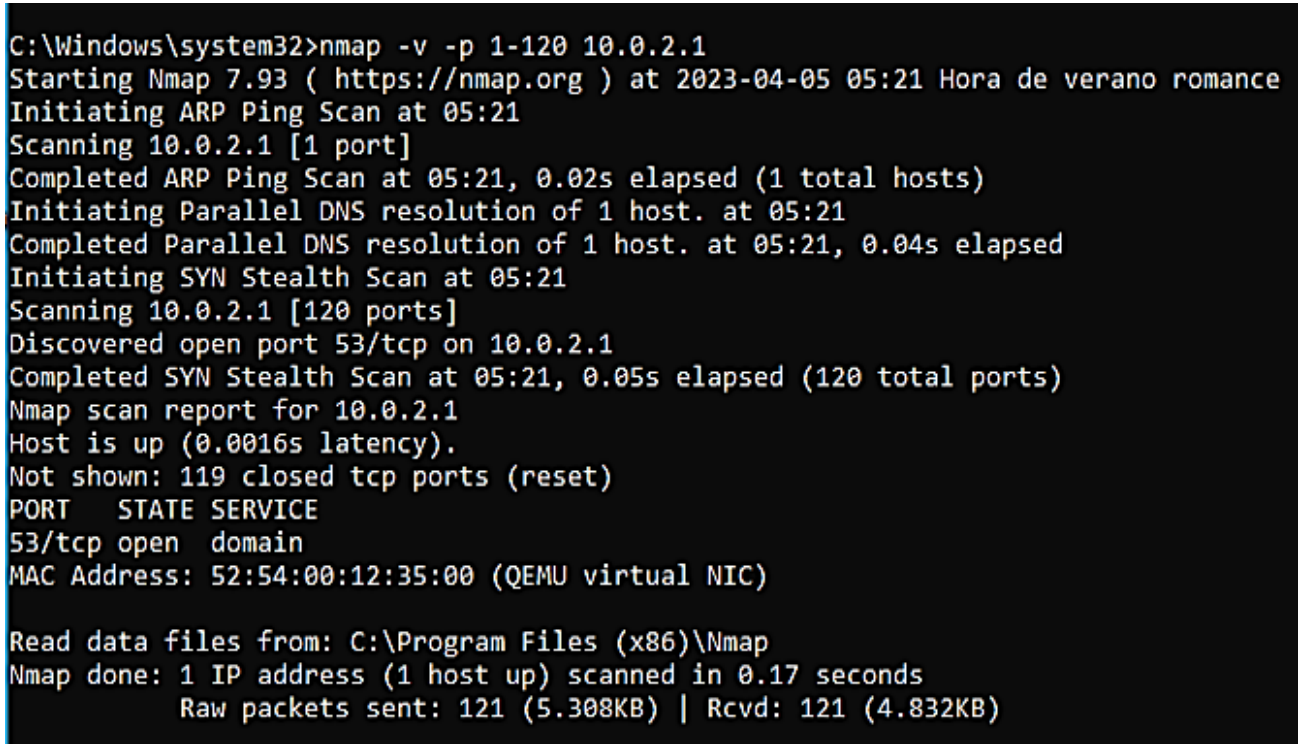
Puede especificar un **nº determinado de puertos**, usando:

-p p_inic-p_fin

```
nmap -v -p 1-120 IP
```

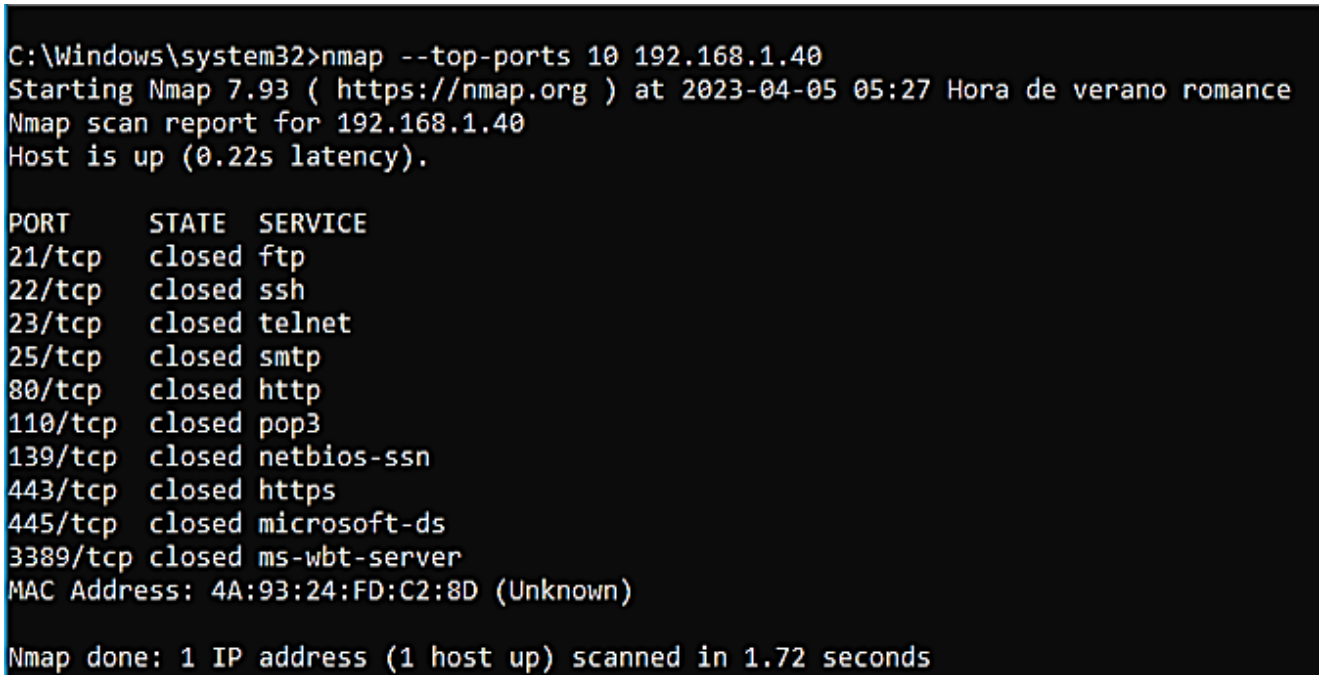
Mostrar **solo puertos abiertos**

```
nmap --open IP
```



Para Escanear los **20 puertos más comunes del objetivo**, podemos variar el 20.

```
nmap --top-ports 20 IP
```



Control de tiempos.

Nmap ofrece un acercamiento más sencillo, basado en **seis plantillas de tiempos**. Puede especificar cualquiera de éstas con la opción -T seguido de un número o su nombre. **Los nombres de las plantillas son**:

paranoico (0), sigiloso (1), amable (2), normal (3), agresivo (4) y loco (5).

Las primeras dos se utilizan para evadir IDS.

El **modo amable reduce el sondeo** para que éste utilice menos ancho de banda y menos recursos de los sistemas analizados.

El **modo normal es el valor por omisión**, así que la opción -T3 no hace nada realmente.

El **modo agresivo** hace que los **sondeos** sean **más rápidos** al asumir que está en una red razonablemente más rápida y fiable.

En **modo loco** asume que está en una **red extraordinariamente rápida** o que está dispuesto a sacrificar fiabilidad por velocidad.

Le recomiendo que empiece siempre con -T4 si está utilizando una conexión de banda ancha o conexión Ethernet decente. Algunas personas adoran la opción -T5 aunque es demasiado agresiva para mi gusto. Otras personas especifican la opción -T2 porque piensan que es menos probable que bloqueen sistemas o porque se consideran a sí mismos amables en general. Muchas veces no se dan cuenta de lo lenta que -T Polite es realmente. Su sondeo puede llegar a tardar diez veces más que un sondeo por omisión. Dado que las caídas de sistemas y problemas de ancho de banda son raros con las opciones de tiempos por omisión (-T3), lo recomiendo habitualmente para las personas cuidadosas. Para reducir estos problemas es más efectivo omitir la detección de versiones que jugar con los valores de tiempos.

Mientras que puede ser útil evitar alarmas de IDS con -T0 y -T1, éste tardará mucho más tiempo para sondear miles de sistemas o puertos. Para este tipo de sondeos puede que prefiera fijar los valores exactos de tiempos que necesita antes que utilizar los valores predefinidos para -T0 y -T1.

Ejemplo:

Escaneo -T5 o loco:

```
C:\Windows\system32>nmap -T Insane 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 05:59 Hora de verano romance
```

```
Nmap done: 256 IP addresses (7 hosts up) scanned in 9.72 seconds
```

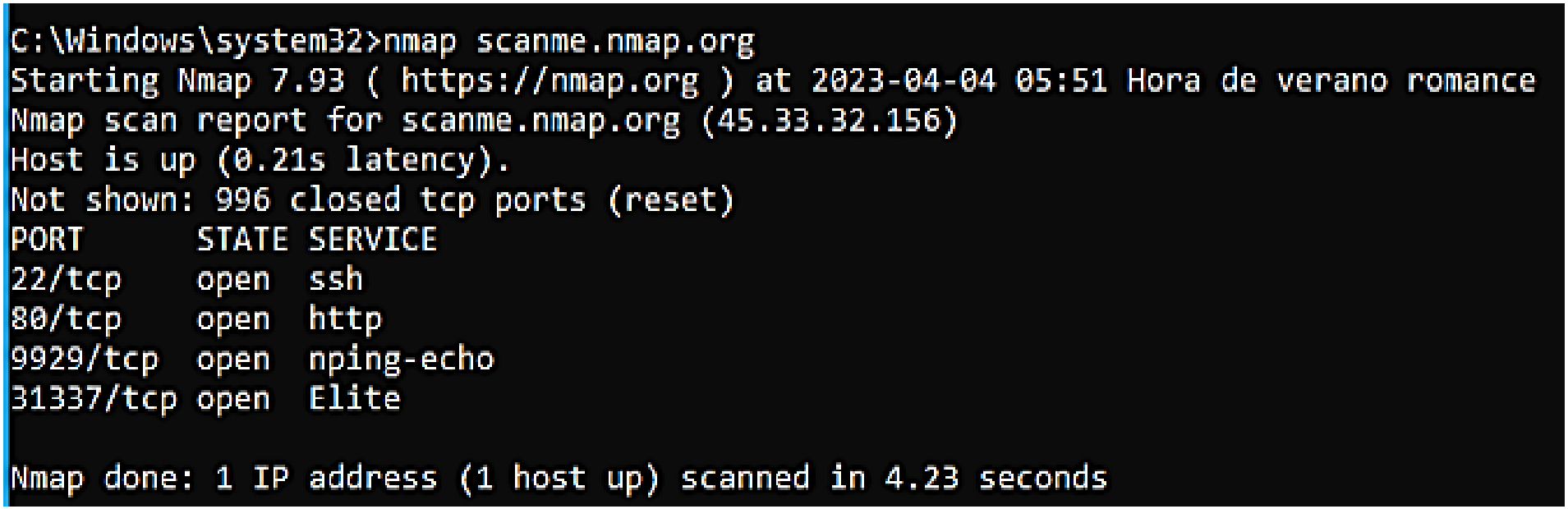
Escaneo -T1 o paranoico:

```
C:\Windows\system32>nmap -T0 192.168.1.0/24
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 06:03 Hora de verano romance
```

3. **Escaneo de hosts**

Al utilizar nmap, estamos haciendo escaneos activos por lo que no podemos hacerlo sin autorización. Vamos a utilizar, a modo de ejemplo, scanme.nmap.org:

```
nmap scanme.nmap.org
```



```
nmap -Pn scanme.nmap.org
```

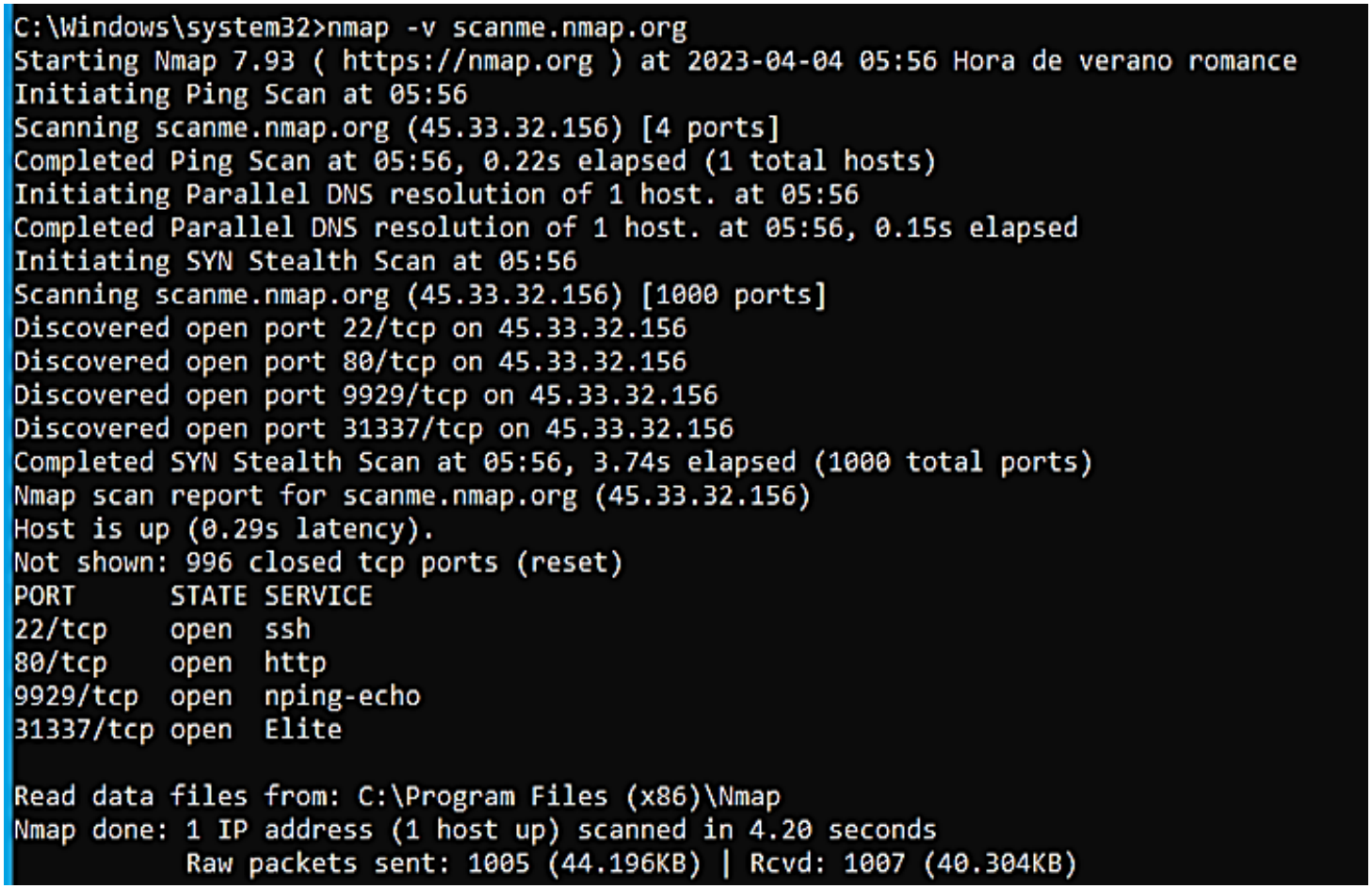
```
C:\Windows\system32>nmap -Pn scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 06:00 Hora de verano romance
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 5.41 seconds
```

-Pn Realiza un escaneo sin utilizar ping

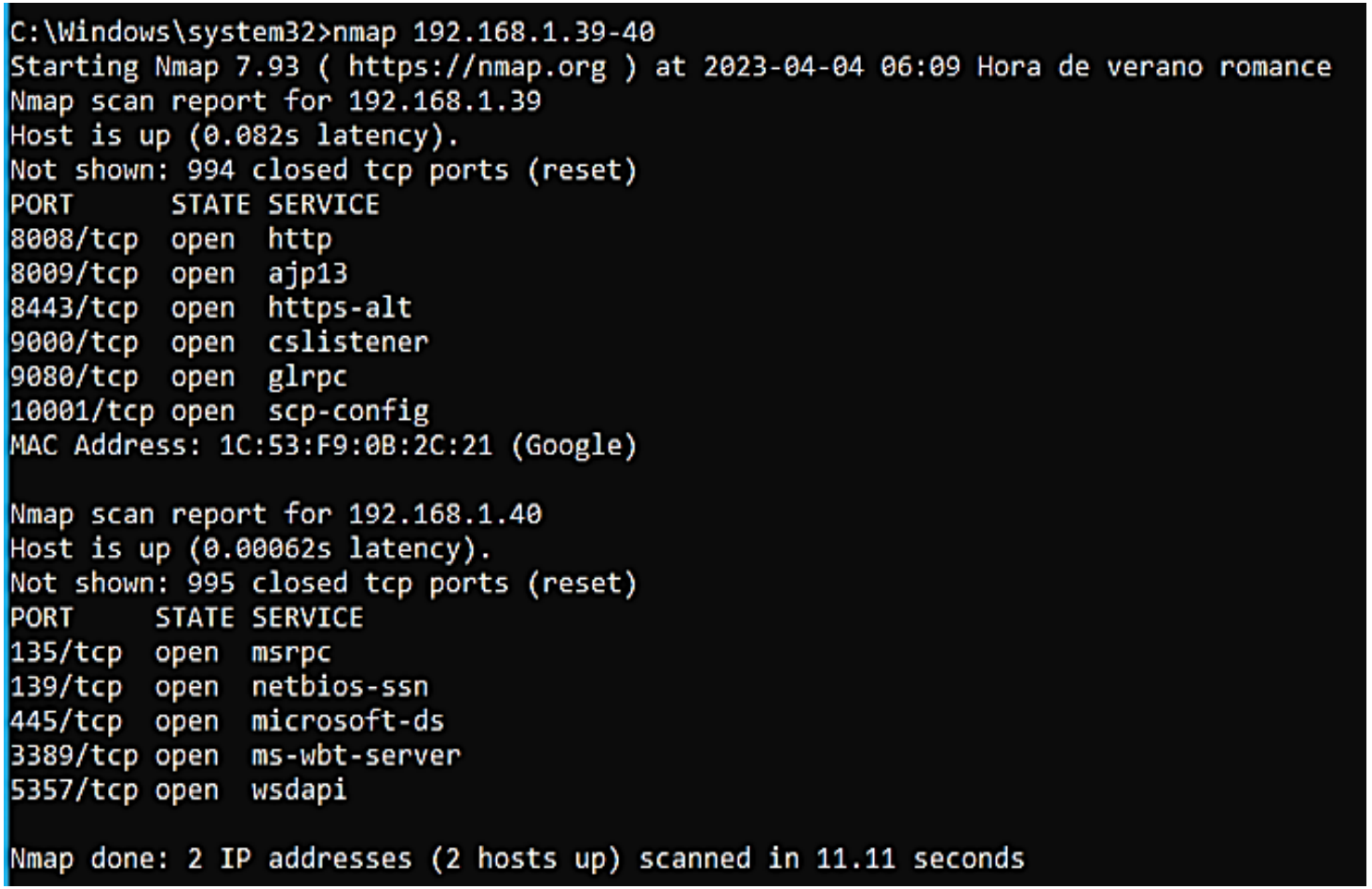
```
nmap -v scanme.nmap.org
```

-v muestra los resultados en pantalla



```
nmap 192.168.1.39-40
```

Se utiliza para escanear un rango de direcciones



```
nmap 192.168.1.0/24
```

Se utiliza para escanear toda la red (clase C)

```
nmap 192.168.1.*
```

Se utiliza para escanear toda la red (clase C)

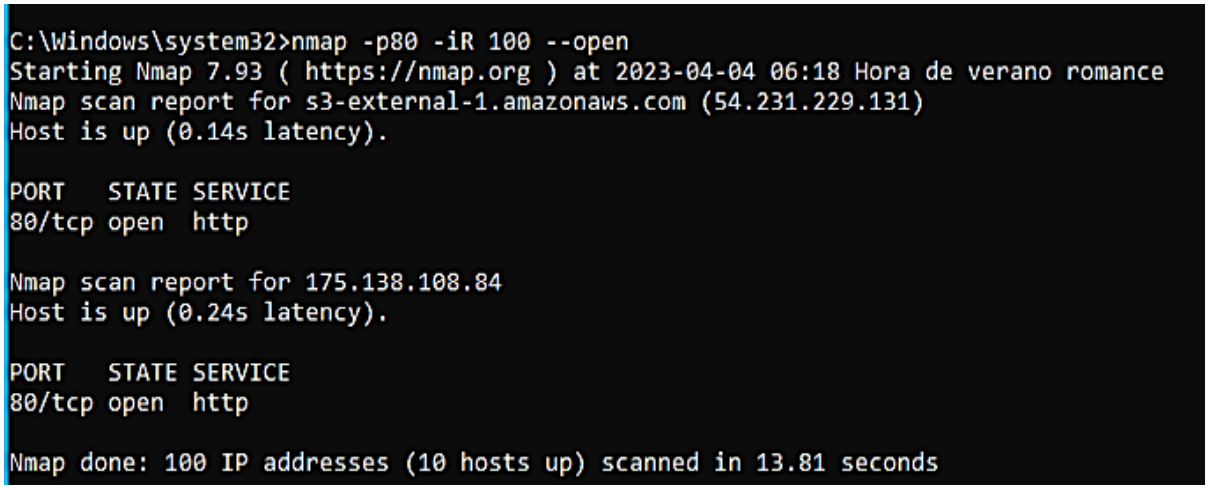
```
nmap 192.168.1.* --exclude 192.168.1.40
```

Escanea toda la red excepto la ip 192.168.1.40

Ejemplo de usos con varios parámetros:

```
nmap -p80 -iR 100 --open
```

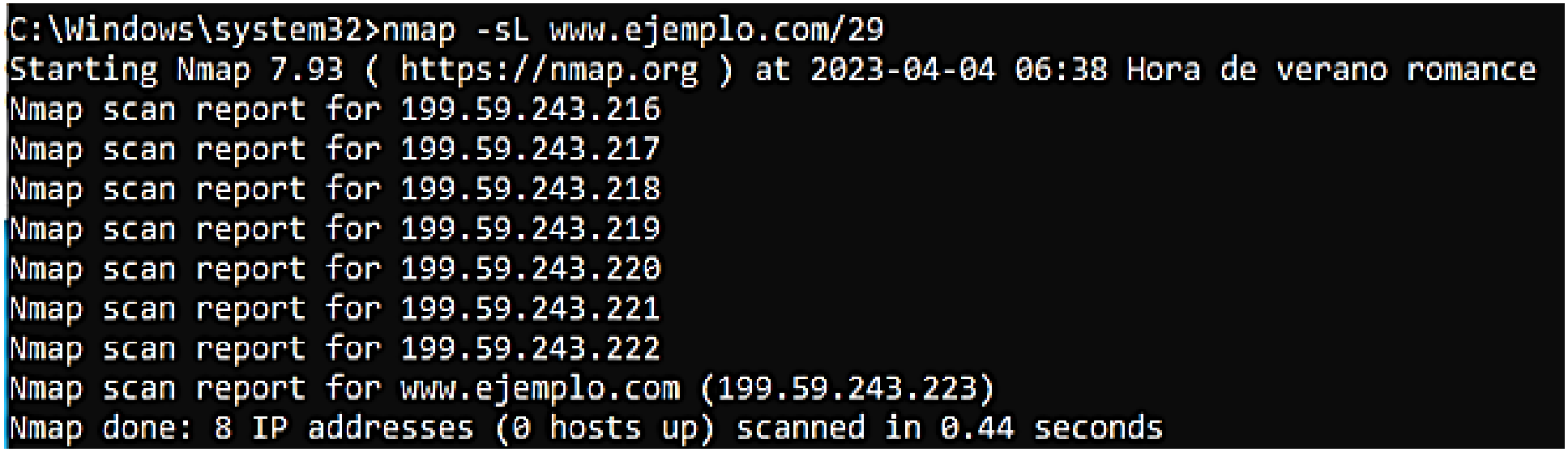
Escanea al azar 100 equipos abiertos por el puerto 80



Descubrimiento de hosts

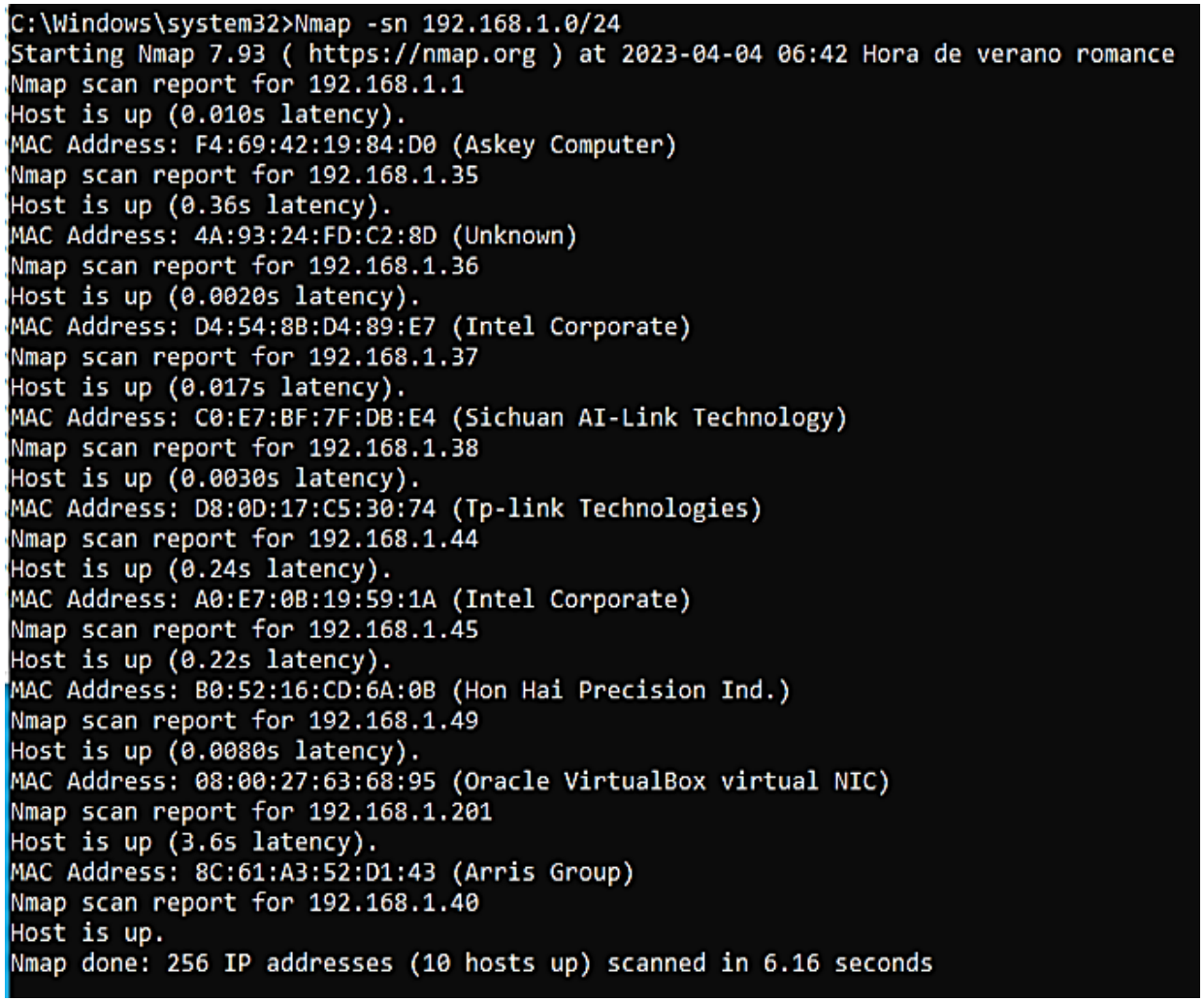
```
nmap -sL www.ejemplo.com/29
```

-sL: List scan. Esta **opción únicamente lista los objetivos dados como argumentos**, sin enviar paquete alguno a éstos. Por defecto, **Nmap realiza una resolución DNS inversa de los equipos a analizar**, así que si se selecciona este método, los paquetes relacionados con esta resolución serán los únicos que se enviarán. Esta **es una opción especialmente sigilosa** (no intrusiva) con la cual obtener información potencialmente valiosa, y que puede servir también para comprobar que no se va a analizar ningún activo fuera de nuestro alcance.



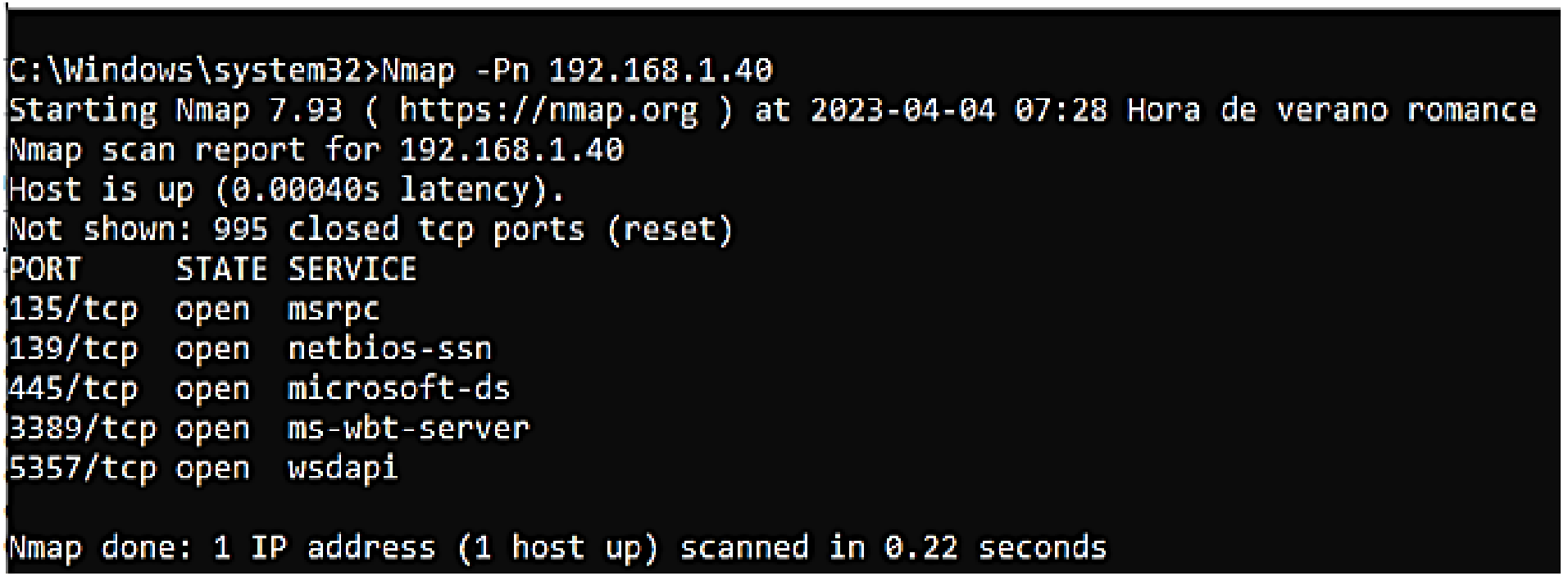
```
nmap -sn 192.168.1.0/24
```

-sn: no port scan. También conocida como **Ping Scan** o **Ping Sweep**. Esta opción, cuando se indica de forma explícita, **instruye a Nmap para que no realice un análisis de los puertos**. Realiza un escaneo ligero. **Realiza una solicitud de Echo ICMP, un TCP SYN al puerto 443, un TCP ACK al puerto 80 y una solicitud de marca de tiempo ICMP**.



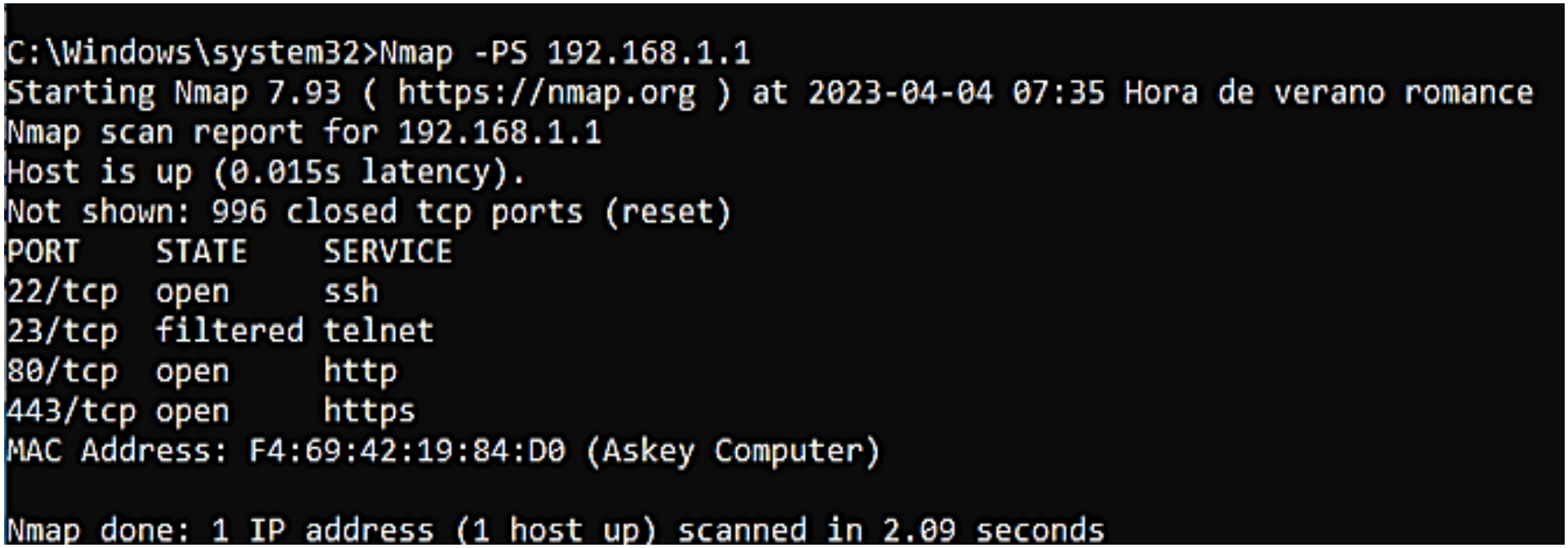
```
nmap -Pn 192.168.1.40
```

-Pn: no Ping scan. Evita completamente que **Nmap** realice la fase de Descubrimiento de Equipos. **Es útil si se desea que todos los objetivos especificados sean considerados como activos, y de este modo se realice un escaneo de puertos en todos ellos, sin excepción**.



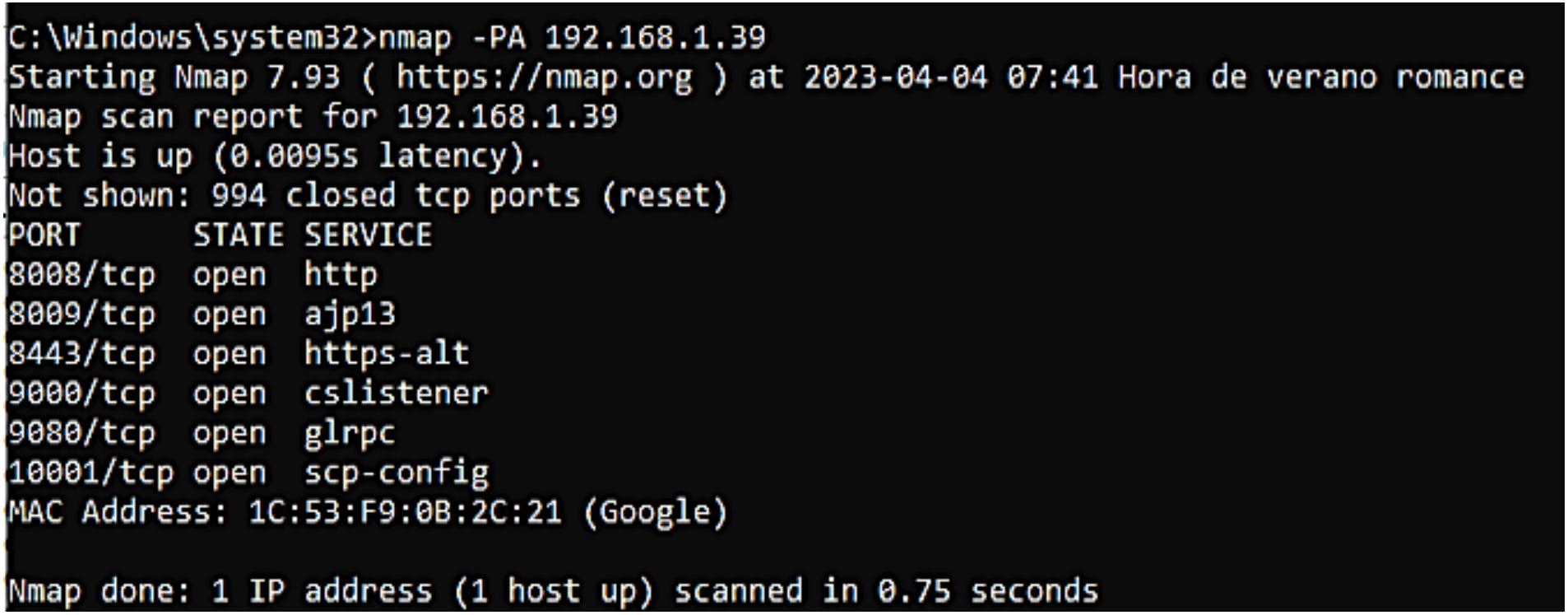
```
nmap -PS 192.168.1.1
```

-PS: Ping TCP SYN. Esta técnica, si no se añade ningún puerto, **envía al objetivo un paquete TCP vacío con el flag SYN activado al puerto 80**. Se puede indicar un listado de puertos sobre los que realizar este análisis, separándolos por comas o introduciendo intervalos separados por un guion.



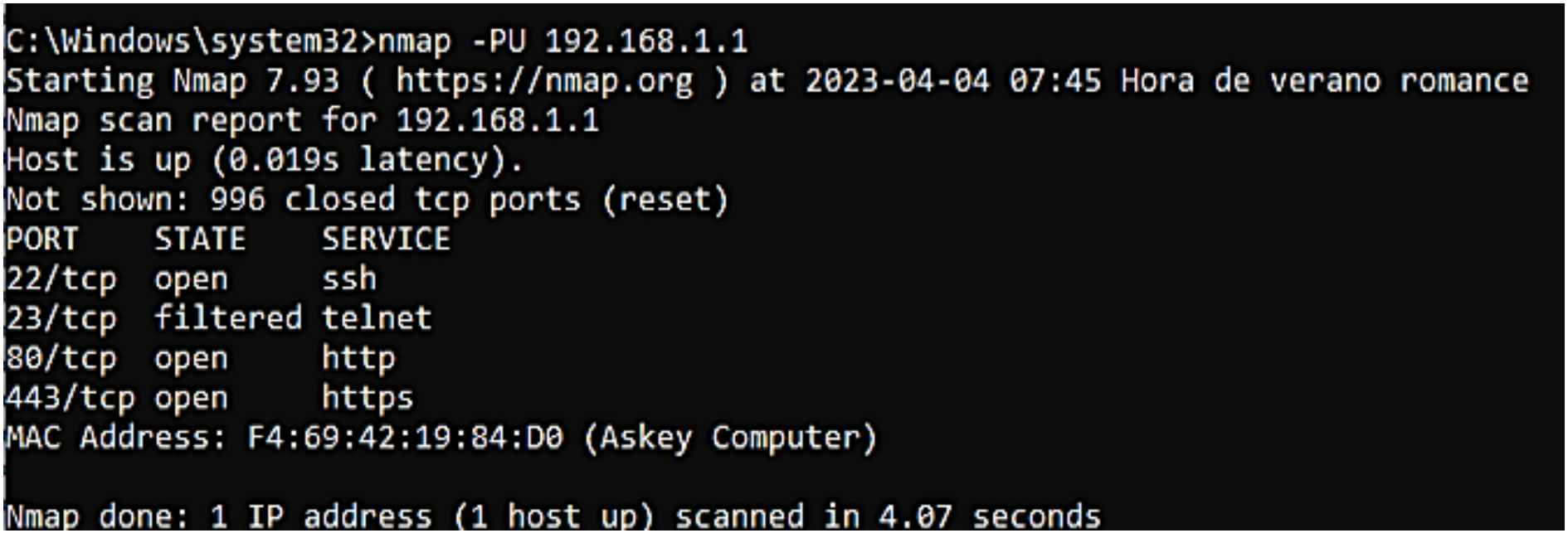
```
nmap -PA 192.168.1.39
```

-PA: Ping TCP ACK esta técnica es **idéntica a la de Ping TCP SYN, con la excepción de que ésta envía un paquete TCP al puerto 80 con el flag ACK activado**. También se pueden añadir más puertos, indicando a continuación el listado de puertos sobre los que realizar este análisis, con el mismo formato que en casos anteriores.



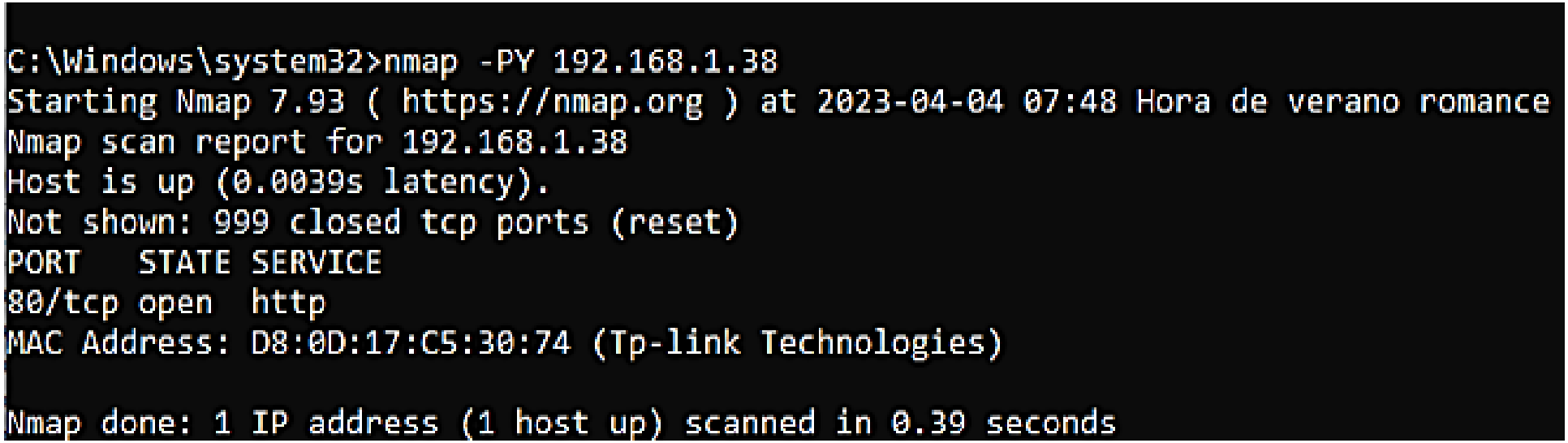
```
nmap -PU 192.168.1.1
```

-PU: Ping UDP. El enfoque de esta técnica es opuesto a las anteriores, por el hecho de que se envía paquetes a puertos que se considera estarán cerrados en el objetivo (por defecto se utiliza el puerto 31338). Esto es así porque, **al ser el protocolo UDP sin conexión, un paquete enviado a un puerto abierto puede no recibir respuesta**, aunque haya algún servicio escuchando en el puerto al que se ha enviado la sonda. Por el contrario, si se utiliza un puerto cerrado, el objetivo debería devolver un paquete ICMP del tipo Puerto Inalcanzable, dejando constancia de su existencia.



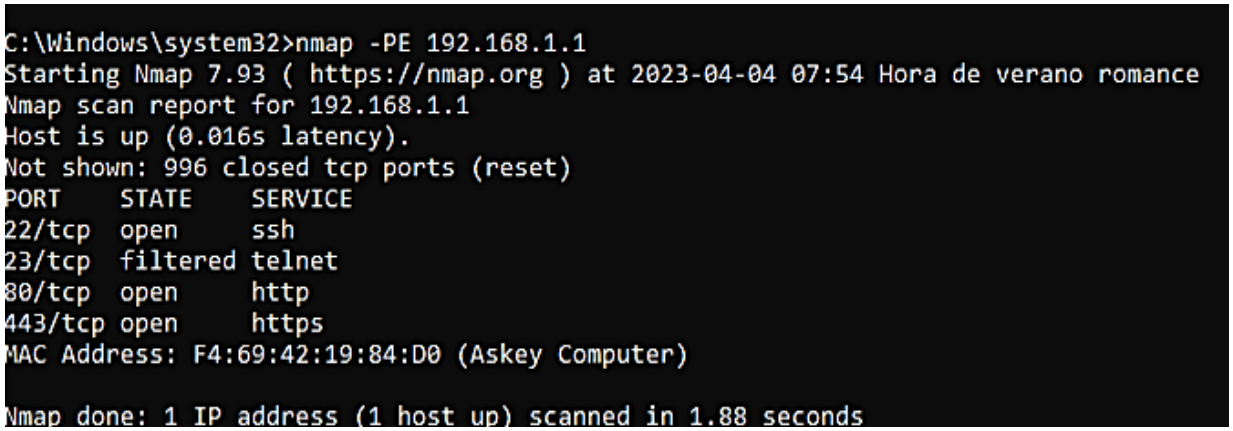
```
nmap -PY 192.168.1.38
```

-PY: Ping SCTP. Este tipo de análisis **envía sondas SCTP INIT al puerto 80**, indicando que se quiere realizar una conexión SCTP con el objetivo. Si el equipo está levantado, responderá o bien con un paquete INIT-ACK (puerto abierto) o bien con un paquete ABORT (puerto cerrado). En cualquier otro caso se considerará el equipo como inactivo.

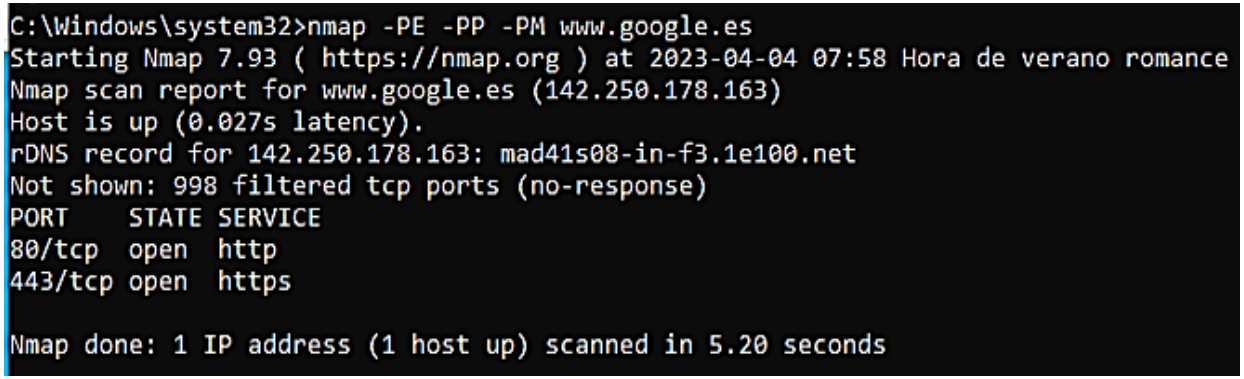


```
nmap -PE 192.168.1.1
```

-PE: Ping ICMP. La forma más extendida de realizar un descubrimiento de equipos es mediante la utilidad ping del sistema operativo, la cual envía paquetes ICMP Echo Request al destino y espera una respuesta ICMP Echo Reply. **Nmap** es capaz de imitar esta técnica mediante la opción -PE.

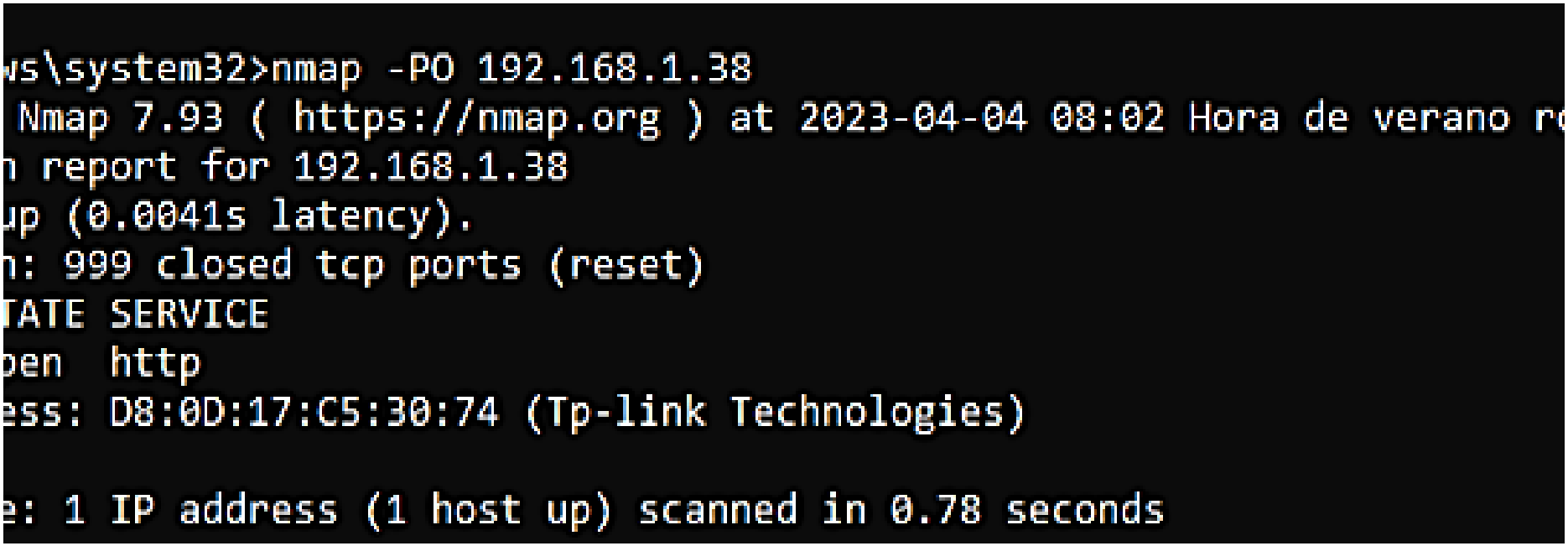


También se puede utilizar -PP y -PM



```
nmap -PO 192.168.1.38
```

-PO: Ping IP PROTOCOL. Una de las técnicas más novedosas para el descubrimiento de equipos **consiste en el envío de paquetes con un protocolo concreto especificado en sus cabeceras**. Por defecto, se envían sondas con los protocolos 1 (ICMP), 2 (IGMP) y 4 (Encapsulado IP), aunque se puede, del mismo modo que en otros casos, introducir un listado de protocolos a utilizar.



Opciones interesantes para estos comandos:

```
nmap -PA 192.168.1.1 --disable-arp-ping
```

Hace un ping sin ARP

```
nmap -PA 192.168.1.1 --traceroute
```

Traza la ruta del host

```
C:\Windows\system32>Nmap -PA scanme.nmap.org --traceroute
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-04 08:14 Hora de verano romance
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   5.00 ms   192.168.1.1
2   ...
3   8.00 ms   129.red-81-41-252.staticip.rima-tde.net (81.41.252.129)
4   38.00 ms  190.red-81-41-252.staticip.rima-tde.net (81.41.252.190)
5   34.00 ms  117.red-80-58-96.staticip.rima-tde.net (80.58.96.117)
6   34.00 ms  46.red-80-58-96.staticip.rima-tde.net (80.58.96.46)
7   80.00 ms  ae12-400-grtmadte1.net.telefonicaglobalsolutions.com (216.184.113.52)
8   34.00 ms  94.142.107.207
9   81.00 ms  prs-bb1-link.ip.twelve99.net (213.155.131.152)
10  120.00 ms 4.14.96.34
11  120.00 ms ae1.r02.iad01.icn.netarch.akamai.com (23.203.152.38)
12  234.00 ms ae5.r01.ord01.icn.netarch.akamai.com (23.32.63.20)
13  130.00 ms ae2.r02.iad01.icn.netarch.akamai.com (23.203.152.40)
14  210.00 ms ae5.r01.ord01.icn.netarch.akamai.com (23.32.63.20)
15  210.00 ms ae2.r11.sjc01.ien.netarch.akamai.com (23.207.232.39)
16  209.00 ms a23-203-158-51.deploy.static.akamaitechnologies.com (23.203.158.51)
17  201.00 ms ae0-100.gw4.scz1.us.linode.com (173.230.159.137)
18  206.00 ms if-0-0-2-997.gw2.fnc1.us.linode.com (213.52.131.188)
19  210.00 ms if-2-4.csw6-fnc1.linode.com (173.230.159.87)
20  205.00 ms scanme.nmap.org (45.33.32.156)

Nmap done: 1 IP address (1 host up) scanned in 9.64 seconds
```

Escaneo de puertos

Nmap entiende que los puertos pueden estar en 6 estados: **abierto, cerrado, filtrado, sin filtro, abierto|filtrado y cerrado|filtrado.**

Cuando un puerto está **abierto**, quiere decir que acepta de forma activa conexiones. Los puertos abiertos muestran los servicios que se están usando.

Cuando un puerto está **cerrado**, quiere decir que recibe y responde a las sondas de los paquetes de **nmap,** pero no encontramos ninguna aplicación a la escucha. Nos sirve para saber que hay un equipo en esa dirección IP.

Cuando un puerto está **filtrado**, quiere decir que **Nmap** no va a saber si está abierto o cerrado. Esto puede ser porque le corta el acceso un firewall, un router o un cortafuegos basado en software.

Cuando un puerto está **sin filtro**, quiere decir que es accesible, pero **Nmap** no va a saber si está abierto o cerrado. Esto puede ser porque le corta el acceso un firewall, un router o un cortafuegos basado en software.

Cuando un puerto está **abierto|filtrado**, quiere decir que es **Nmap** marca a los puertos en este estado cuando no puede determinar si el puerto se encuentra abierto o filtrado. Esto ocurre para tipos de análisis donde no responden los puertos abiertos.

Cuando un puerto está **cerrado|filtrado**, quiere decir que es **Nmap** marca a los puertos en este estado cuando no puede determinar si el puerto se encuentra cerrado o filtrado. Esto ocurre para tipos de análisis donde no responden los puertos abiertos.

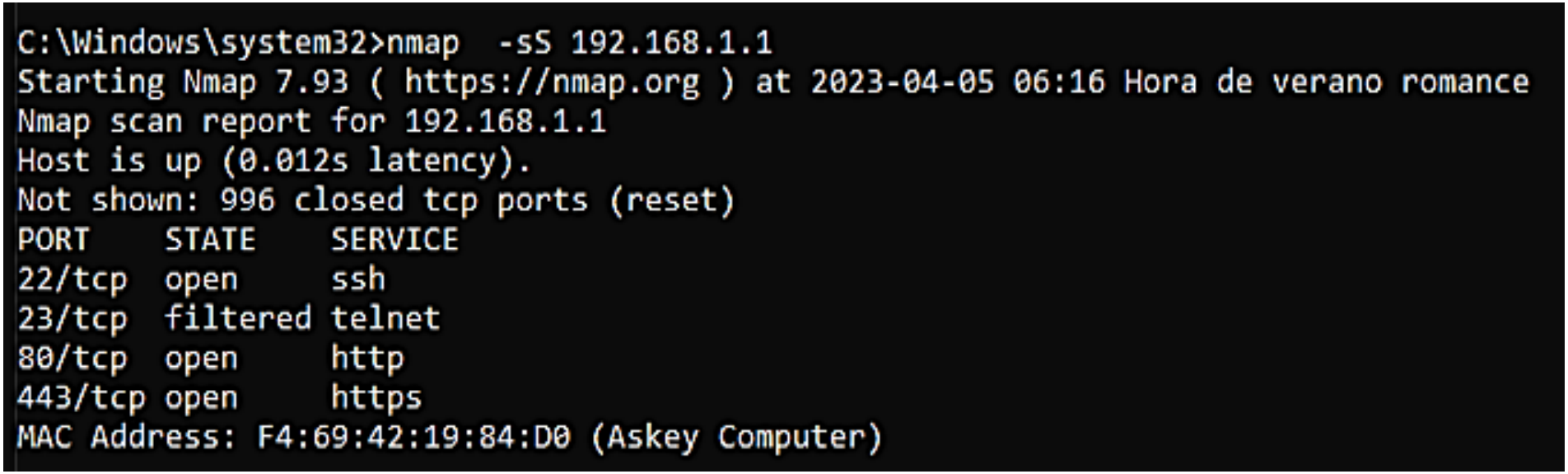
La opción **--reason** Indica la razón por la que se ha concluido el estado de un puerto o equipo. Permite diferenciar el tipo de respuestas que ha generado un puerto cerrado

```
C:\Windows\system32>nmap  --reason 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 05:46 Hora de verano romance
Nmap scan report for 192.168.1.1
Host is up, received arp-response (0.0088s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE REASON
22/tcp  open     ssh     syn-ack ttl 64
23/tcp  filtered telnet  no-response
80/tcp  open     http    syn-ack ttl 64
443/tcp open     https   syn-ack ttl 64
MAC Address: F4:69:42:19:84:D0 (Askey Computer)

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

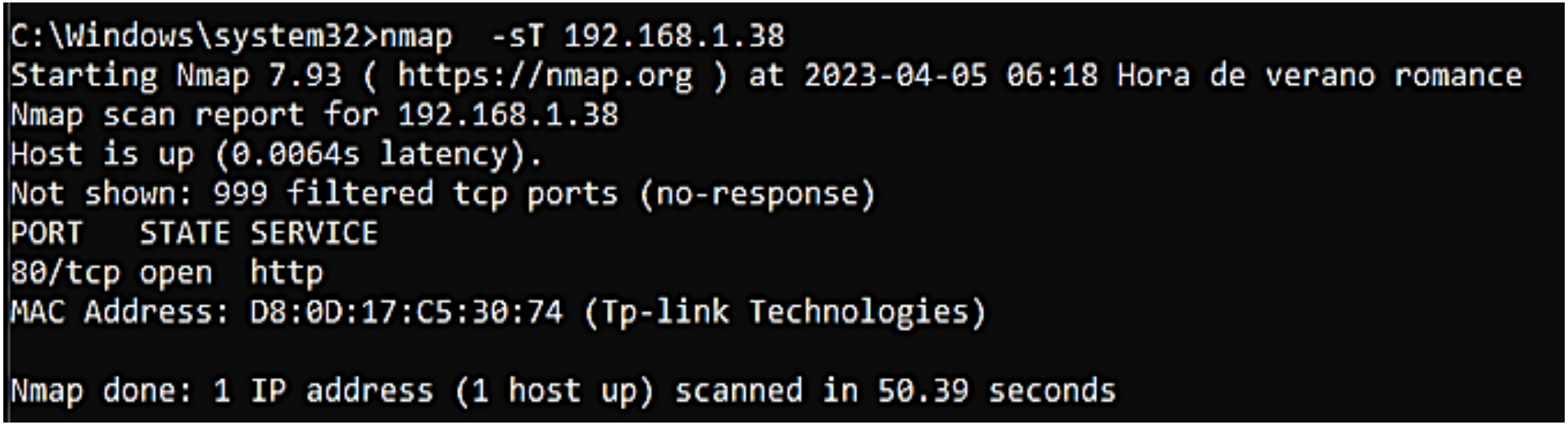
```
nmap -sS 192.168.1.1
```

-sS (sondeo TCP SYN). El sondeo SYN es el utilizado por omisión y el más popular por buenas razones. Puede realizarse rápidamente, sondeando miles de puertos por segundo en una red rápida en la que no existan cortafuegos. El sondeo SYN es relativamente sigiloso y poco molesto. También muestra una clara y fiable diferenciación entre los estados abierto, cerrado, y filtrado.



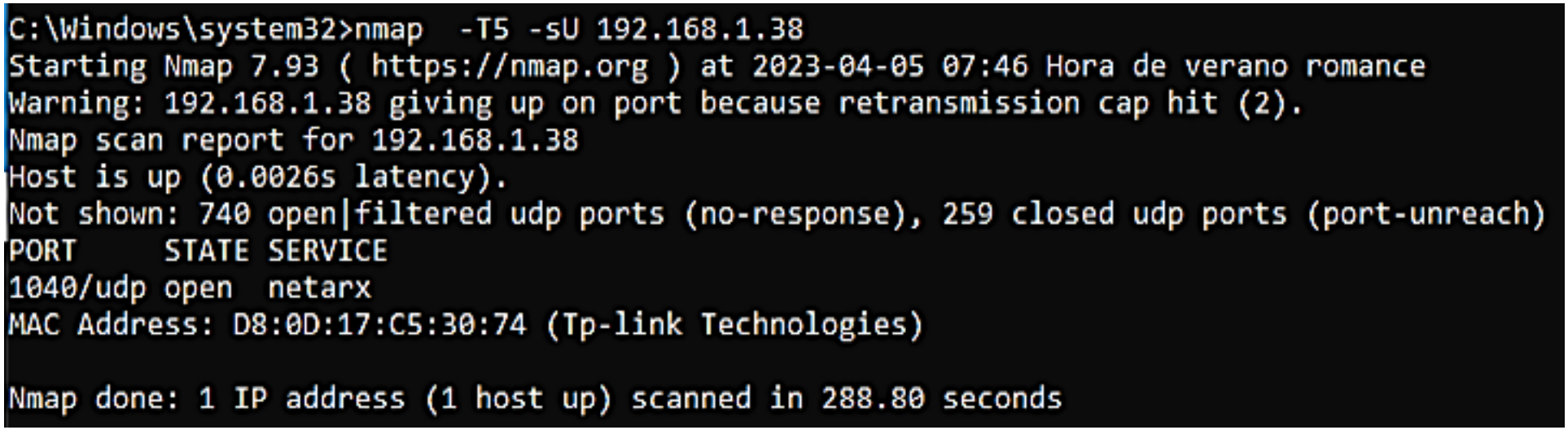
```
nmap -sT 192.168.1.38
```

-sT (sondeo TCP connect()). El sondeo TCP Connect() es el sondeo TCP por omisión cuando no se puede utilizar el sondeo SYN. Esto sucede, por ejemplo, cuando el usuario no tiene privilegios para enviar paquetes en crudo o cuando se están sondeando redes IPv6. Nmap le pide al sistema operativo subyacente que establezcan una conexión con el sistema objetivo en el puerto indicado utilizando la llamada del sistema connect(), a diferencia de otros tipos de sondeo, que escriben los paquetes a bajo nivel..



```
nmap -sU 192.168.1.1
```

-sU sondeos UDP. Aunque la mayoría de los servicios más habituales en Internet utilizan el protocolo TCP, los servicios UDP también son muy comunes. Tres de los más comunes son los servicios DNS, SNMP, y DHCP (puertos registrados 53, 161/162, y 67/68 respectivamente). Dado que el sondeo UDP es generalmente más lento y más difícil que TCP, algunos auditores de seguridad ignoran estos puertos. Esto es un error, porque es muy frecuente encontrarse servicios UDP vulnerables y los atacantes no ignoran estos protocolos. Afortunadamente, Nmap puede utilizarse para hacer un inventario de puertos UDP.



```
nmap -sN 192.168.1.38
```

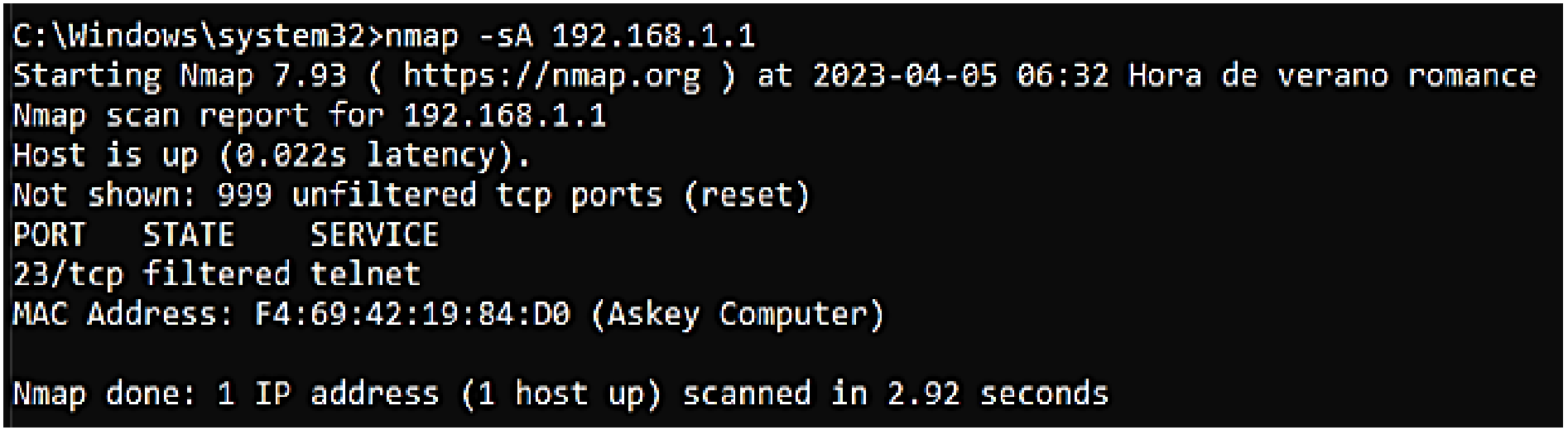
-sN; -sF; -sX (sondeos TCP Null, FIN, y Xmas). Estos tres tipos de sondeos aprovechan una indefinición en la RFC de TCP que diferencia los puertos abiertos y cerrados. Cuando se sondean sistemas que cumplen con el texto de esta RFC, cualquier paquete que no contenga los bits SYN, RST, o ACK resultará en el envío de un RST si el puerto está cerrado. Mientras que no se enviará una respuesta si el puerto está cerrado. La ventaja fundamental de este tipo de sondeos es que pueden atravesar algunos cortafuegos que no hagan inspección de estados o encaminadores que hagan filtrado de paquetes. Otra ventaja es que este tipo de sondeos son algo más sigilosos que, incluso, un sondeo SYN.

```
C:\Windows\system32>nmap -sN 192.168.1.38
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 06:29 Hora de verano romance
Nmap scan report for 192.168.1.38
Host is up (0.0037s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE         SERVICE
80/tcp open|filtered http
MAC Address: D8:0D:17:C5:30:74 (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

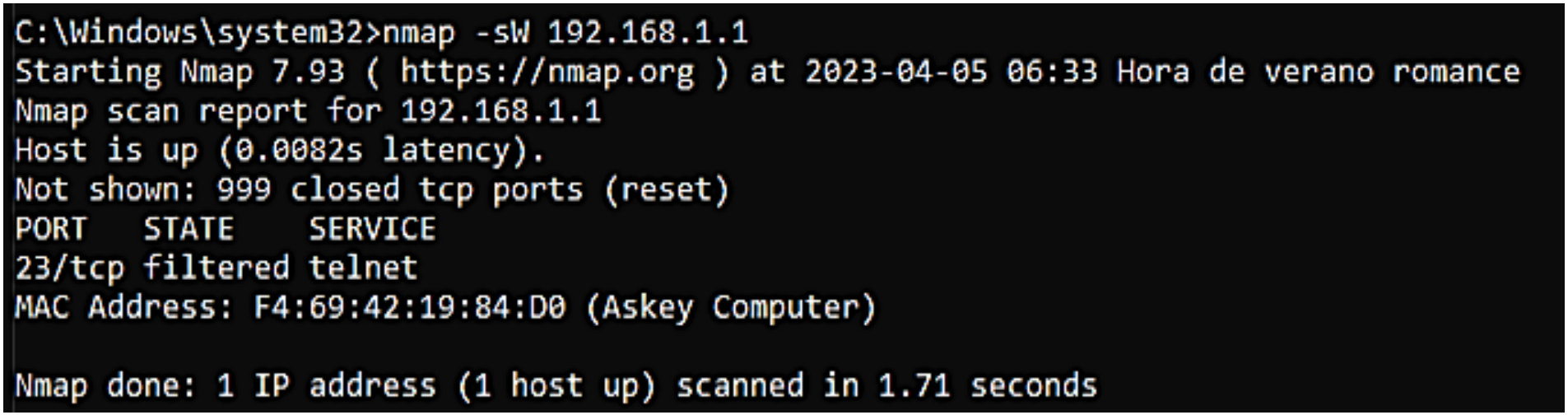
```
nmap -sA 192.168.1.1
```

-sA (sondeo TCP ACK). Este sondeo se utiliza para mapear reglas de cortafuegos, y para determinar si son cortafuegos con inspección de estados y qué puertos están filtrados.



```
nmap -sW 192.168.1.1
```

sW (sondeo de ventana TCP). Este sondeo es exactamente igual al sondeo ACK que se aprovecha de un detalle de implementación de algunos sistemas que permite diferenciar puertos abiertos de los cerrados, en lugar de imprimir no filtrado cuando se devuelve un RST.



```
nmap -sW 192.168.1.1
```

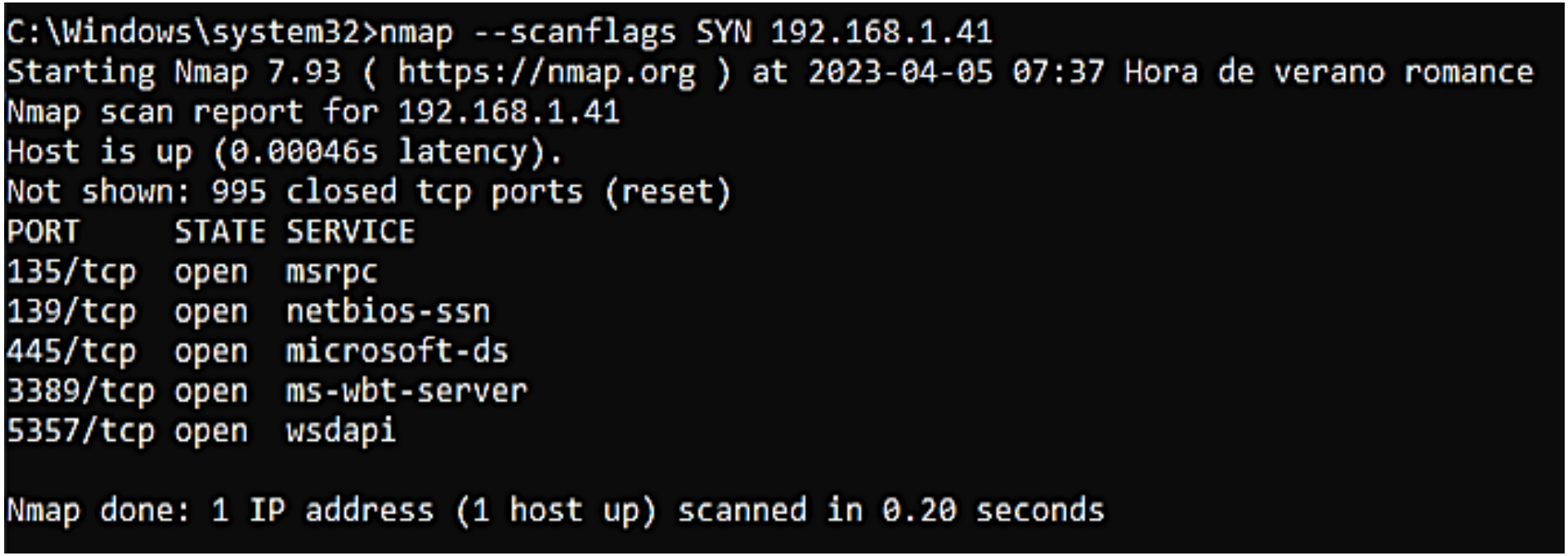
sW (sondeo TCP Maimon). Esta técnica es exactamente la misma a los sondeos Null, FIN, y Xmas, pero en los que se envía una sonda FIN/ACK. Según el RFC 793 (TCP), se debería generar un paquete RST cuando se responde a dicha sonda independientemente de si el puerto está cerrado o abierto. Uriel Maimon se dio cuenta, sin embargo, de que muchos sistemas derivados de BSD simplemente descartan el paquete si el puerto está abierto.

```
C:\Windows\system32>nmap -sW 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 07:31 Hora de verano romance
Nmap scan report for 192.168.1.1
Host is up (0.011s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE
23/tcp filtered telnet
MAC Address: F4:69:42:19:84:D0 (Askey Computer)

Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds
```

```
nmap -sW 192.168.1.1
```

--scanflags (Sondeo TCP a medida). Permite diseñar su propio sondeo mediante la especificación de banderas TCP arbitrarias. Puede ser un valor numérico como el 9 (PSH y FIN), aunque es más sencillo utilizar nombres simbólicos. Sólo tienes que juntar una combinación de URG, ACK, PSH, RST, SYN, y FIN. Ésto le dice a Nmap cómo debe interpretar las respuestas. Por ejemplo, un sondeo SYN considera que si no se recibe respuesta el puerto está filtrado mientras que si no se recibe una respuesta en un sondeo FIN se trata como abierto|filtrado.



Otros

-sI (IDLE SCAN). Esta técnica avanzada explota una "vulnerabilidad" de muchas implementaciones de la pila TCP/IP, consistente en la posibilidad de predecir (simple incremento en peticiones consecutivas) el identificador de fragmento de los paquetes IP (IP ID). Con ello se permite extraer información mediante el análisis de las secuencias predecibles del identificador (IPID) de los paquetes IP.

-sO (Isondeo de protocolos IP). El sondeo de protocolo IP le permite determinar qué protocolos (TCP, ICMP, IGMP, etc.) soportan los sistemas objetivo. Esto no es, técnicamente, un sondeo de puertos, dado que cambia los números de protocolo IP en lugar de los números de puerto TCP ó UDP. Pero también se puede utilizar la opción -p para seleccionar los números de protocolo a analizar, los resultados se muestran en el formato de tabla utilizado para los puertos e incluso utiliza el mismo motor de sondeo que los métodos de sondeo de puertos reales.

```
C:\Windows\system32>nmap -sO -p50 192.168.1.41
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-05 08:14 Hora de verano romance
Nmap scan report for 192.168.1.41
Host is up.

PROTOCOL STATE         SERVICE
50       open|filtered esp

Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

Especificación de puertos y orden de sondeo

Nmap ofrece distintas opciones para especificar los puertos que se van a sondear y si el orden de los sondeos es aleatorio o secuencial. Estas opciones se añaden a los métodos de sondeos que se han discutido previamente. **Nmap**, por omisión, sondea todos los puertos hasta el 1024 además de algunos puertos con números altos listados en el fichero nmap-services para los protocolos que se sondeen.

-p <rango de puertos> (Sólo sondea unos puertos específicos)

Esta opción especifica los puertos que desea sondear y toma precedencia sobre los valores por omisión. Puede especificar tanto números de puerto de forma individual, así como rangos de puertos separados por un guión (p. ej. 1-1023). Puede omitir el valor inicial y/o el valor final del rango. Nmap utilizará 1 ó 65535 respectivamente. De esta forma, puede especificar -p- para sondear todos los puertos desde el 1 al 65535. Se permite sondear el puerto cero siempre que lo especifique explícitamente. Esta opción especifica el número de protocolo que quiere sondear (de 0 a 255) en el caso de que esté sondeando protocolos IP (-sO).

Puede especificar un protocolo específico cuando sondee puertos TCP y UDP si precede el número de puerto con T: o U:. El calificador dura hasta que especifique otro calificador. Por ejemplo, la opción -p U:53,111,137,T:21-25,80,139,8080 sondearía los puertos UDP 53,111, y 137, así como los puertos TCP listados. Tenga en cuenta que para sondear tanto UDP como TCP deberá especificar la opción -sU y al menos un tipo de sondeo TCP (como -sS, -sF, o -sT). Si no se da un calificador de protocolo se añadirán los números de puerto a las listas de todos los protocolos.

-F (Sondeo rápido (puertos limitados))

Indica que sólo quiere sondear los puertos listados en el fichero nmap-services que se incluye con nmap (o el fichero de protocolos si indica -sO). Esto es más rápido que sondear todos los 65535 puertos de un sistema. La diferencia de velocidad con el sondeo TCP por omisión (unos 1650 puertos) no es muy alta dado que esta lista contiene muchos puertos TCP (más de 1200). La diferencia puede ser muy grande si especifica su propio fichero nmap-services más pequeño si utiliza la opción --datadir.

-r (No aleatorizar los puertos)

Nmap ordena de forma aleatoria los puertos a sondear por omisión (aunque algunos puertos comúnmente accesibles se ponen al principio por razones de eficiencia). Esta aleatorización generalmente es deseable, pero si lo desea puede especificar la opción -r para analizar de forma secuencial los puertos.

Detección de servicios y de versiones

Si le indica a **Nmap** que mire un sistema remoto le podrá decir que tiene abiertos los puertos 25/tcp, 80/tcp y 53/udp. Informará que esos puertos se corresponden habitualmente con un servidor de correo (SMTP), servidor de web (HTTP) o servidor de nombres (DNS), respectivamente, si utilizas su base de datos nmap-services con más de 2.200 puertos conocidos. Generalmente este informe es correo dado que la gran mayoría de demonios que escuchan en el puerto 25 TCP son, en realidad, servidores de correo. ¡Pero no debe confiar su seguridad en este hecho! La gente ejecuta a veces servicios distintos en puertos inesperados

Aún en el caso de que Nmap tenga razón y el servidor de ejemplo indicado arriba está ejecutando servidores de SMTP, HTTP y DNS ésto no dice mucho. Cuando haga un análisis de vulnerabilidades (o tan sólo un inventario de red) en su propia empresa o en su cliente lo que habitualmente también quiere saber es qué versión se está utilizando del servidor de correcto y de DNS. Puede ayudar mucho a la hora de determinar qué ataques pueden afectar a un servidor el saber el número de versión exacto de éste. La detección de versiones le ayuda a obtener esta información.

La detección de versiones pregunta para obtener más información de lo que realmente se está ejecutando una vez se han detectado los puertos TCP y/o UDP con alguno de los métodos de sondeo. La base de datos nmap-service-probes contiene sondas para consultar distintos servicios y reconocer y tratar distintas respuestas en base a una serie de expresiones. Nmap intenta determinar el protocolo del servicio (p. ej. ftp, ssh, telnet ó http), el nombre de la aplicación (p. ej. Bind de ISC, http de Apache, telnetd de Solaris), un número de versión, un tipo de dispositivo (p. ej. impresora o router), la familia de sistema operativo (p. ej. Windows o Linux) y algunas veces algunos detalles misceláneos como, por ejemplo, si un servidor X acepta cualquier conexión externa, la versión de protocolo SSH o el nombre de usuario Kazaa). Por supuesto, la mayoría de los servicios no ofrecen toda esta información. Si se ha compilado Nmap con soporte OpenSSL se conectará también a servidores SSL para determinar qué servicio escucha detrás de la capa de cifrado. Se utiliza la herramienta de pruebas RPC de Nmap (-sR) de forma automática para determinar el programa RPC y el número de versión si se descubren servicios RPC. Algunos puertos UDP se quedan en estado open|filtered (N. del T., 'abierto|filtrado') si un barrido de puertos UDP no puede determinar si el puerto está abierto o filtrado. La detección de versiones intentará obtener una respuesta de estos puertos (igual que hace con puertos abiertos) y cambiará el estado a abierto si lo consigue. Los puertos TCP en estado open|filtered se tratan de forma similar. Tenga en cuenta que la opción -A de Nmap actualiza la detección de versiones entre otras cosas. Puede encontrar un documento describiendo el funcionamiento, modo de uso, y particularización de la detección de versiones en https://nmap.org/vscan/.

Cuando Nmap obtiene una respuesta de un servicio pero no encuentra una definición coincidente en la base de datos se imprimirá una firma especial y un URL para que la envíe si sabe lo que está ejecutándose detrás de ese puerto.

La detección de versiones se activa y controla con la siguientes opciones:

-sV (Detección de versiones)

Activa la detección de versiones como se ha descrito previamente. Puede utilizar la opción -A en su lugar para activar tanto la detección de versiones como la detección de sistema operativo.

```
C:\Windows\system32>nmap 192.168.1.1 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-08 06:52 Hora de verano romance
NSOCK ERROR [0.0740s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 192.168.1.1
Host is up (0.0064s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE  VERSION
22/tcp  open     ssh      Dropbear sshd 2019.78 (protocol 2.0)
23/tcp  filtered telnet
80/tcp  open     http     micro_httpd
443/tcp open     ssl/http micro_httpd
MAC Address: 94:91:7F:AC:66:B0 (Askey Computer)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.74 seconds
```

--allports (No excluir ningún puerto de la detección de versiones)

La detección de versiones de Nmap omite el puerto TCP 9100 por omisión porque algunas impresoras imprimen cualquier cosa que reciben en este puerto, lo que da lugar a la impresión de múltiples páginas con solicitudes HTTP get, intentos de conexión de SSL, etc. Este comportamiento puede cambiarse modificando o eliminando la directiva Exclude en nmap-service-probes, o especificando --allports para sondear todos los puertos independientemente de lo definido en la directiva Exclude.

```
C:\Windows\system32>nmap 192.168.1.1 -sV --allports
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-08 06:55 Hora de verano romance
NSOCK ERROR [0.0360s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 192.168.1.1
Host is up (0.016s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE  VERSION
22/tcp  open     ssh      Dropbear sshd 2019.78 (protocol 2.0)
23/tcp  filtered telnet
80/tcp  open     http     micro_httpd
443/tcp open     ssl/http micro_httpd
MAC Address: 94:91:7F:AC:66:B0 (Askey Computer)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.60 seconds
```

--version-intensity <intensidad> (Fijar la intensidad de la detección de versiones)

Nmap envía una serie de sondas cuando se activa la detección de versiones (-sV) con un nivel de rareza preasignado y variable de 1 a 9. Las sondas con un número bajo son efectivas contra un amplio número de servicios comunes, mientras que las de números más altos se utilizan rara vez. El nivel de intensidad indica que sondas deberían utilizarse. Cuanto más alto sea el número, mayor las probabilidades de identificar el servicio. Sin embargo, los sondeos de alta intensidad tardan más tiempo. El valor de intensidad puede variar de 0 a 9. **El valor por omisión es 7**. Se probará una sonda independientemente del nivel de intensidad cuando ésta se registra para el puerto objetivo a través de la directiva nmap-service-probes ports. De esta forma se asegura que las sondas de DNS se probarán contra cualquier puerto abierto 53, las sondas SSL contra el puerto 443, etc.

```
C:\Windows\system32>nmap 192.168.1.1 -sV -version-intensity 9
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-08 06:57 Hora de verano romance
NSOCK ERROR [0.0340s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 192.168.1.1
Host is up (0.0093s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE  VERSION
22/tcp  open     ssh      Dropbear sshd 2019.78 (protocol 2.0)
23/tcp  filtered telnet
80/tcp  open     http     micro_httpd
443/tcp open     ssl/http micro_httpd
MAC Address: 94:91:7F:AC:66:B0 (Askey Computer)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.54 seconds
```

--version-light (Activar modo ligero)

Éste es un alias conveniente para --version-intensity 2. Este modo ligero hace que la detección de versiones sea más rápida pero también hace que sea menos probable identificar algunos servicios.

--version-all (Utilizar todas las sondas)

Éste es un alias para --version-intensity 9, hace que se utilicen todas las sondas contra cada puerto.

--version-trace (Trazar actividad de sondeo de versiones)

Esta opción hace que Nmap imprima información de depuración detallada explicando lo que está haciendo el sondeo de versiones. Es un conjunto de lo que obtendría si utilizara la opción --packet-trace.

-sR (Sondeo RPC)

Este método funciona conjuntamente con los distintos métodos de sondeo de puertos de Nmap. Toma todos los puertos TCP/UDP que se han encontrado y los inunda con órdenes de programa NULL SunRPC con el objetivo de determinar si son puertos RPC y, si es así, los programas y número de versión que están detrás. Así, puede obtener de una forma efectiva la misma información que rpcinfo -p aunque el mapeador de puertos («portmapper», N. del T.) está detrás de un cortafuegos (o protegido por TCP wrappers). Los señuelos no funcionan con el sondeo RPC actualmente. Esta opción se activa automáticamente como parte de la detección de versiones (-sV) si la ha seleccionado. Rara vez se utiliza la opción -sR dado que la detección de versiones lo incluye y es más completa.

```
C:\Windows\system32>nmap 192.168.1.1 -sR
WARNING: -sR is now an alias for -sV and activates version detection as well as RPC scan.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-08 07:00 Hora de verano romance
NSOCK ERROR [0.0560s] ssl_init_helper(): OpenSSL legacy provider failed to load.

Nmap scan report for 192.168.1.1
Host is up (0.013s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE  VERSION
22/tcp  open     ssh      Dropbear sshd 2019.78 (protocol 2.0)
23/tcp  filtered telnet
80/tcp  open     http     micro_httpd
443/tcp open     ssl/http micro_httpd
MAC Address: 94:91:7F:AC:66:B0 (Askey Computer)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.30 seconds
```

Detección de sistema operativo

Uno de los aspectos más conocidos de **Nmap** es la detección del sistema operativo (SO) en base a la comprobación de huellas TCP/IP. Nmap envía una serie de paquetes TCP y UDP al sistema remoto y analiza prácticamente todos los bits de las respuestas. Nmap compara los resultados de una docena de pruebas como puedan ser el análisis de ISN de TCP, el soporte de opciones TCP y su orden, el análisis de IPID y las comprobaciones de tamaño inicial de ventana, con su base de datos nmap-os-fingerprints. Esta base de datos consta de más de 1500 huellas de sistema operativo y cuando existe una coincidencia se presentan los detalles del sistema operativo. Cada huella contiene una descripción en texto libre del sistema operativo, una clasificación que indica el nombre del proveedor (por ejemplo, Sun), el sistema operativo subyacente (por ejemplo, Solaris), la versión del SO (por ejemplo, 10) y el tipo de dispositivo (propósito general, encaminador, conmutador, consola de videojuegos, etc.).

Nmap le indicará una URL donde puede enviar las huellas si conoce (con seguridad) el sistema operativo que utiliza el equipo si no puede adivinar el sistema operativo de éste y las condiciones son óptimas (encontró al menos un puerto abierto y otro cerrado). Si envía esta información contribuirá al conjunto de sistemas operativos que Nmap conoce y la herramienta será así más exacta para todo el mundo.

La detección de sistema operativo activa, en cualquier caso, una serie de pruebas que hacen uso de la información que ésta recoge. Una de estas pruebas es la medición de tiempo de actividad, que utiliza la opción de marca de tiempo TCP (RFC 1323) para adivinar cuánto hace que un equipo fue reiniciado. Esta prueba sólo funciona en sistemas que ofrecen esta información. Otra prueba que se realiza es la clasificación de predicción de número de secuencia TCP. Esta prueba mide de forma aproximada cuánto de difícil es crear una conexión TCP falsa contra el sistema remoto. Se utiliza cuando se quiere hacer uso de relaciones de confianza basadas en la dirección IP origen (como es el caso de rlogin, filtros de cortafuegos, etc.) para ocultar la fuente de un ataque. Ya no se hace habitualmente este tipo de malversación pero aún existen muchos equipos que son vulnerables a ésta. Generalmente es mejor utilizar la clasificación en inglés como: “worthy challenge” («desafío difícil», N. del T.) o “trivial joke” («broma fácil», N. del T.). Esta información sólo se ofrece en la salida normal en el modo detallado (-v). También se informa de la generación de números de secuencia IPID cuando se activa el modo detallado conjuntamente con la opción -O. La mayoría de los equipos estarán en la clase “incremental”, lo que significa que incrementan el campo ID en la cabecera IP para cada paquete que envían. Esto hace que sean vulnerables a algunos ataques avanzados de obtención de información y de falseo de dirección.

La detección de sistema operativo se activa y controla con las siguientes opciones:

-O (Activa la detección de sistema operativo)

Tal y como se indica previamente, activa la detección de sistema operativo. También se puede utilizar la opción -A para activar la detección de sistema operativo y de versiones.

```
C:\Windows\system32>nmap 192.168.1.1 -O
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-08 07:06 Hora de verano romance
Nmap scan report for 192.168.1.1
Host is up (0.0056s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  open     ssh
23/tcp  filtered telnet
80/tcp  open     http
443/tcp open     https
MAC Address: 94:91:7F:AC:66:B0 (Askey Computer)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.31 - 2.6.35
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 3.40 seconds
```

--osscan-limit (Limitar la detección de sistema operativo a los objetivos prometedores)

La detección de sistema operativo funcionará mejor si se dispone de un puerto TCP abierto y otro cerrado. Defina esta opción si no quiere que Nmap intente siquiera la detección de sistema operativo contra sistemas que no cumplan este criterio. Esta opción puede ahorrar mucho tiempo, sobre todo si está realizando sondeos -P0 sobre muchos sistemas. Sólo es de aplicación cuando se ha solicitado la detección de sistema operativo con la opción -O o -A.

--osscan-guess; --fuzzy (Aproximar los resultados de la detección de sistema operativo)

Cuando Nmap no puede detectar un sistema operativo que encaje perfectamente a veces ofrecerá posibilidades que se aproximen lo suficiente. Las opciones tienen que aproximarse mucho al detectado para que Nmap haga esto por omisión. Cualquiera de estas dos opciones (equivalentes) harán que Nmap intente aproximar los resultados de una forma más agresiva.

4. Evasión de cortafuegos/IDS y falsificación

Los filtros de red como los cortafuegos pueden hacer muy difícil el análisis de una red. Esto no va a ser más fácil en el futuro, ya que uno de los objetivos de estos dispositivos es generalmente limitar el reconocimiento casual de la red. En cualquier caso, Nmap ofrece varias funcionalidades para ayudar a entender estas redes complejas, y que también sirven para verificar que los filtros funcionan como se espera de ellos. Incluso tiene mecanismos para saltarse las defensas que no hayan sido implementadas del todo correctamente. Uno de los mejores métodos de entender la posición de la seguridad de su red es intentar comprometerla. Empiece a pensar como un atacante, e intenta utilizar las técnicas de esta sección contra sus propias redes. Lance un sondeo de rebote FTP, un sondeo pasivo, un ataque de fragmentación, o intente realizar un túnel desde una de sus propias pasarelas.

Las compañías, además de restringir la actividad de red, están monitorizando cada vez más el tráfico con sistemas de detección de intrusos (IDS, «Intrusion Detection Systems», N. del T.). Todos los IDS principales vienen preinstalados con reglas diseñadas para detectar sondeos de Nmap porque, a veces, se realizan sondeos previos a un ataque. Muchos de estos productos han mutado recientemente para convertirse en sistemas de prevención de intrusiones (IPS) que bloquean activamente el tráfico reconocido como maligno. Desafortunadamente para los administradores de redes y para los fabricantes de IDS es muy difícil detectar las malas intenciones analizando los datos de los paquetes. Los atacantes con paciencia, habilidad y con la ayuda de ciertas opciones de Nmap pueden, generalmente, esquivar el análisis de los IDS sin ser detectados. Mientras tanto, los administradores deben lidiar con un alto número de falsos positivos debido a que algunas actividades inocentes se diagnostican erróneamente y generan alarmas o se bloquean.

Algunas personas sugieren que Nmap no debería ofrecer funcionalidades de evasión de cortafuegos o para esquivar los IDS, argumentando que es igual de probable que las funcionalidades las utilicen los atacantes como que las utilicen los administradores para mejorar la seguridad. El problema con esta forma de pensar es que los atacantes van a utilizar estos métodos de todas formas: encontrarían otra herramienta para hacerlo o parchearían a Nmap para añadírsela. Al mismo tiempo, los administradores tendrían muchos más problemas para hacer su trabajo. Es mucho mejor defensa utilizar servidores FTP modernos y parcheados que intentar prevenir la distribución de herramientas que permitan la implementación de ataques de rebote FTP.

No hay ninguna herramienta mágica (u opción de Nmap) que permita detectar y evitar cortafuegos y sistemas IDS. Esto requiere habilidad y experiencia. Un tutorial va más allá del alcance de esta guía de referencia, que sólo lista las opciones relevantes y describe lo que hacen.

-f (fragmentar los paquetes); --mtu (utilizar el MTU especificado)

La opción -f hace que el sondeo solicitado (incluyendo los sondeos ping) utilicen paquetes IP fragmentados pequeños. La idea es dividir la cabecera del paquete TCP entre varios paquetes para hacer más difícil que los filtros de paquetes, sistemas de detección de intrusos y otras molestias detecten lo que se está haciendo. ¡Tenga cuidado con esta opción! Algunos programas tienen problemas para manejar estos paquetes tan pequeños. El viejo sniffer llamado Sniffit da un fallo de segmentación inmediatamente después de recibir el primero de estos pequeños fragmentos. Especifica esta opción una sola vez y Nmap dividirá los paquetes en ocho bytes o menos después de la cabecera de IP. De esta forma, una cabecera TCP de veinte bytes se dividiría en 3 paquetes. Dos con ocho bytes de cabecera TCP y uno con los últimos ocho. Obviamente, cada fragmento tiene su propia cabecera IP. Especifica la opción -f otra vez para utilizar fragmentos de dieciséis bytes (reduciendo la cantidad de fragmentos). O puedes especificar tu propio tamaño con la opción --mtu. No utilice la opción -f si utiliza --mtu. El tamaño debe ser múltiplo de ocho. Aunque la utilización de paquetes fragmentados no le ayudará a saltar los filtros de paquetes y cortafuegos que encolen todos los fragmentos IP (como cuando se utiliza la opción CONFIG_IP_ALWAYS_DEFRAG del núcleo de Linux), algunas redes no pueden tolerar la pérdida de rendimiento que esto produce y deshabilitan esa opción. Otros no pueden habilitar esta opción porque los fragmentos pueden tomar distintas rutas para entrar en su red. Algunos sistemas defragmentan los paquetes salientes en el núcleo. Un ejemplo de ésto es Linux con el módulo de seguimiento de conexiones de iptables. Realice un sondeo con un programa de captura de tráfico, como Ethereal, para asegurar que los paquetes que se envían están fragmentándose. Intente utilizar la opción --send-eth, si su sistema operativo le está causando problemas, para saltarse la capa IP y enviar tramas directamente a la capa Ethernet en crudo.

-D <señuelo1 [,señuelo2][,ME],...> (Esconde un sondeo con señuelos)

Realiza un sondeo con señuelos. Esto hace creer que el/los equipo/s que utilice como señuelos están también haciendo un sondeo de la red. De esta manera sus IDS pueden llegar a informar de que se están realizando de 5 a 10 sondeos de puertos desde distintas direcciones IP, pero no sabrán qué dirección IP está realizando el análisis y cuáles son señuelos inocentes. Aunque esta técnica puede vencerse mediante el seguimiento del camino de los encaminadores, descarte de respuesta («response-dropping», N. del T.), y otros mecanismos activos, generalmente es una técnica efectiva para esconder su dirección IP.

Se debe separar cada equipo de distracción mediante comas, y puede utilizar ME («YO», N. del T.) como uno de los señuelos para representar la posición de su verdadera dirección IP. Si pone ME en la sexta posición o superior es probable que algunos detectores de

sondeos de puertos habituales (como el excelente scanlogd de Solar Designer) ni siquiera muestren su dirección IP. Si no utiliza ME, Nmap le pondrá en una posición aleatoria.

Tenga en cuenta que los equipos que utilice como distracción deberían estar conectados o puede que accidentalmente causes un ataque de inundación SYN a sus objetivos. Además, sería bastante sencillo determinar qué equipo está realmente haciendo el sondeo si sólo uno está disponible en la red. Puede que quiera utilizar direcciones IP en lugar de nombres (de manera que no aparezca en los registros del servidor de nombres de los sistemas utilizados como señuelo).

Se utilizan los señuelos tanto para el sondeo de ping inicial (si se utiliza ICMP, SYN, ACK, o cualquier otro) como durante la fase de sondeo. También se utilizan los señuelos durante la detección de sistema operativo (-O). Los señuelos no funcionarán con la detección de versión o el sondeo TCP connect().

Vale la pena tener en cuenta que utilizar demasiados señuelos puede ralentizar el sondeo y potencialmente hacerlo menos exacto. Además, algunos proveedores de acceso a Internet filtrarán los paquetes falsificados, aunque hay muchos que no lo hacen.

-S <Dirección_IP> (Falsifica la dirección de origen)

Nmap puede que no sea capaz de determinar tu dirección IP en algunas ocasiones (Nmap se lo dirá si pasa). En esta situación, puede utilizar la opción -S con la dirección IP de la interfaz a través de la cual quieres enviar los paquetes.

Otro uso alternativo de esta opción es la de falsificar la dirección para que los objetivos del análisis piensen que algún otro los está sondeando. ¡Imagine una compañía a los que les sondea repetidamente la competencia! Generalmente es necesaria la opción -e si lo quiere utilizar así, y también sería recomendable la opción -P0.

-e <interfaz> (Utilizar la interfaz especificada)

Indica a Nmap a través de qué interfaz debe enviar y recibir los paquetes. Nmap debería detectar esto automáticamente, pero se lo dirá si no.

--source-port <número_de_puerto>; -g <número_de_puerto> (Falsificar el puerto de origen)

Un error de configuración sorprendentemente común es confiar en el tráfico basándose únicamente en el número de puerto origen. Es fácil entender por qué pasa esto. Un administrador que está configurando su nuevo y flamante cortafuegos, recibe de repente quejas de

todos sus usuarios desagradecidos que le dicen que sus aplicaciones han dejado de funcionar. En particular, puede romperse el DNS porque las respuestas UDP de DNS de servidores externos ya no pueden entrar en la red. Otro ejemplo habitual es el caso del FTP. En una transferencia activa de FTP, el servidor remoto intenta establecer una conexión de vuelta con el cliente para transferir el archivo solicitado.

Existen soluciones seguras para estos problemas, como las pasarelas en el nivel de aplicación o los módulos de cortafuegos que realizan un análisis del protocolo. Desgraciadamente, también hay soluciones más fáciles y menos seguras. Al darse cuenta que las respuestas de DNS vienen del puerto 53 y que las conexiones activas de FTP vienen del puerto 20, muchos administradores caen en la trampa de configurar su sistema de filtrado para permitir el tráfico entrante desde estos puertos. Generalmente asumen que ningún atacante se dará cuenta de estos agujeros en el cortafuegos ni los aprovechará. En otros casos, los administradores consideran esto una solución a corto plazo hasta que puedan implementar una solución más segura. Y después se olvidan de hacer la mejora de la seguridad.

Los administradores de red con mucho trabajo no son los únicos que caen en esta trampa. Muchos productos se lanzan al mercado con estas reglas inseguras. Hasta Microsoft lo ha hecho. Los filtros de IPsec que se preinstalan con Windows 2000 y Windows XP contienen una regla implícita que permite todo el tráfico TCP o UDP desde el puerto 88 (Kerberos). Otro caso conocido es el de las versiones de Zone Alarm Firewall Personal que, hasta la versión 2.1.25, permitían cualquier paquete entrante UDP desde el puerto 53 (DNS) o 67 (DHCP).

Nmap ofrece las opciones -g y --source-port (son equivalentes) para aprovecharse de estas debilidades. Simplemente indique el número de puerto y Nmap enviará los paquetes desde ese puerto cuando sea posible. Nmap debe utilizar distintos números de puerto para ciertos tipos de prueba en la detección de sistema operativo para que funcionen correctamente, y las solicitudes de DNS ignoran la opción --source-port porque Nmap depende de las librerías del sistema para hacerlas. Esta opción se soporta completamente en muchos sondeos TCP, incluyendo el sondeo SYN, al igual que los sondeos UDP.

--data-length <número> (Añadir datos aleatorios a los paquetes enviados)

Normalmente Nmap envía paquetes mínimos que contienen sólo la cabecera. Así, los paquetes TCP que envía son generalmente de 40 bytes y las solicitudes echo de ICMP son de tan sólo 28. Esta opción le dice a Nmap que añada el número indicado de bytes aleatorios a la mayoría de los paquetes que envía. Esta opción no afecta a los paquetes enviados para la detección de sistema operativo (-O), pero sí

a la mayoría de los paquetes de ping y de sondeo de puertos. Esta opción hace que el sondeo sea un poco más lento, pero también que el sondeo sea un poco más difícil de detectar.

--ttl <valor> (Indica el valor del campo tiempo-de-vida de la cabecera IP)

Establece el campo tiempo-de-vida («time-to-live», N. del T.) en la cabecera de los paquetes IPv4 al valor especificado.

--randomize-hosts (Mezclar aleatoriamente la lista de equipos a sondear)

Indica a Nmap que debe mezclar aleatoriamente cada grupo de hasta 8096 equipos antes de hacer un sondeo. Esto puede hacer que el sondeo sea menos obvio para algunos sistemas de monitorización de la red, especialmente cuando se combina con las opciones que ralentizan el sondeo. Si quiere mezclar aleatoriamente listas más grandes, incremente el valor de la constante PING_GROUP_SZ en nmap.h y recompile el programa. Una solución alternativa es generar la lista de sistemas a sondear con un sondeo de lista (-sL -n -oN <fichero>), ordenarlo aleatoriamente con un script de Perl, y luego darle a Nmap la lista entera con la opción -iL.

--spoof-mac <dirección MAC, prefijo o nombre del fabricante> (Falsifica la dirección MAC)

Solicita a Nmap que utilice la MAC dada para todas las tramas de Ethernet enviadas. Esta opción activa implícitamente la opción --send-eth para asegurar que Nmap envía los paquetes del nivel Ethernet. La MAC dada puede tener varios formatos. Nmap elegirá una MAC completamente aleatoria para la sesión si se utiliza el valor “0”. Nmap utilizará la MAC indicada si el parámetro es un número par de dígitos hexadecimales (separando opcionalmente cada dos dígitos con dos puntos). Nmap rellenará los 6 bytes restantes con valores aleatorios si se dan menos de 12 dígitos hexadecimales. Si el argumento no es ni 0 ni un conjunto de dígitos hexadecimales, Nmap mirará en nmap-mac-prefixes para encontrar un fabricante cuyo nombre coincida con el parámetro utilizado (en esta búsqueda no diferenciará entre mayúsculas y minúsculas). Si se encuentra algún fabricante, Nmap utilizará el OUI del fabricante (prefijo de 3 bytes) y rellenará los otros 3 bytes aleatoriamente. Ejemplos de argumentos --spoof-mac son: Apple, 0, 01:02:03:04:05:06, deadbeefcafe, 0020F2, y Cisco.

--badsum (Envía paquetes con sumas de comprobación TCP/UDP erróneas)

Esta opción le indica a Nmap que debe generar sumas de comprobación inválidas para los paquetes que se envíen a los equipos objetivos. Cualquier respuesta que se reciba vendrá de un cortafuegos o un IDS que no comprobó la suma, dado que la mayoría de las pilas IP descartan estos paquetes. Para obtener más información de esta técnica puede consultar https://nmap.org/p60-12.txt

5. Opciones misceláneas

Esta sección describe algunas opciones importantes (y no tan importantes) que no encajan realmente en ningún otro sitio.

-6 (Activa el sondeo IPv6)

Nmap tiene soporte IPv6 para la mayoría de sus funcionalidades más populares desde 2002. En particular, tiene soporte de: sondeo ping (TCP-only), sondeo connect() y detección de versiones. La sintaxis de las órdenes es igual que las habituales salvo que debe especificar la opción -6 Por supuesto, debe utilizarse la sintaxis IPv6 si se indica una dirección en lugar de un nombre de sistema. Una dirección IPv6 sería parecida a 3ffe:7501:4819:2000:210:f3ff:fe03:14d0, por lo que se recomienda utilizar nombres de equipo. La salida es igual que en los otros casos. Lo único que distingue que esta opción está habilitada es que se muestran las direcciones IPv6 en la línea que indica los "puertos de interés".

Aunque IPv6 no se está utilizando en todo el mundo, sí que se utiliza mucho en algunos países (generalmente asiáticos) y muchos sistemas operativos modernos lo soportan. Tanto el origen como el objetivo de su sondeo deben estar configurados para utilizar IPv6 si desea utilizar Nmap con IPv6. Si su ISP (como sucede con la mayoría) no le da direcciones IPv6, puede encontrar gestores de túneles gratuitos en muchos sitios y funciona bien con Nmap. Una lista de gestores está en Wikipedia. Los túneles IPv6 a IPv4 («6to4») son también otro método muy popular y gratuito.

-A (Opciones de sondeos agresivos)

Esta opción activa algunas opciones avanzadas y agresivas. Aún no he decidido qué significa exactamente. Actualmente esto activa la detección de sistema operativo (-O) y el análisis de versiones (-sV). Aunque se añadirán más opciones en el futuro. La idea es que esta opción active un conjunto de opciones para evitar que los usuarios de Nmap tengan que recordar un número de opciones muy elevado. Esta opción sólo activa funcionalidades, no afecta a las opciones de temporización (como -T4) o de depuración (-v) que quizás desee activar también.

--datadir <nombre_directorio> (Indica la ubicación de un archivo de datos de Nmap)

Nmap obtiene algunos datos especiales al ejecutarse de los archivos llamados nmap-service-probes, nmap-services, nmap-protocols, nmap-rpc, nmap-mac-prefixes, y nmap-os-fingerprints. Nmap buscará primero estos ficheros en el directorio que se especifique con la opción --datadir (si se indica alguno). Los archivos que no se encuentren allí se buscarán en el directorio especificado por la variable de

entorno NMAPDIR. A continuación se buscará en ~/.nmap tanto para el identificador (UID) real como el efectivo (sólo en sistemas POSIX) o la ubicación del ejecutable de Nmap (sólo sistemas Win32), y también en una ubicación compilada en la aplicación como pudiera ser /usr/local/share/nmap o /usr/share/nmap. Nmap, por último, buscará en el directorio actual.

--send-eth (Enviar tramas Ethernet en crudo)

Le indica a Nmap que debe enviar paquetes en la capa Ethernet en crudo (enlace de datos) en lugar de en la capa IP (red). Por omisión, Nmap elegirá cuál utilizar en función de lo que sea mejor para la plataforma donde esté ejecutándose. Los sockets crudos (capa IP) son generalmente más eficientes para sistemas UNIX, mientras que las tramas Ethernet son necesarias en sistemas Windows ya que Microsoft deshabilitó el soporte de sockets crudos. Nmap seguirá utilizando paquetes IP crudos en UNIX, aunque se especifique esta opción, cuando no se pueda hacer de otra forma (como es el caso de conexiones no Ethernet).

--send-ip (Enviar al nivel crudo IP)

Indica a Nmap que debe enviar utilizando sockets IP crudos en lugar de enviar tramas Ethernet de bajo nivel. Esta opción es complementaria a la opción --send-eth descrita previamente.

--privileged (Asumir que el usuario tiene todos los privilegios)

Esta opción le dice a Nmap que simplemente asuma que el usuario con el que se ejecuta tiene suficientes privilegios para trabajar con sockets crudos, capturar paquetes y hacer otras operaciones similares que generalmente sólo puede hacerla en sistemas UNIX el usuario root. Por omisión, Nmap aborta si se han solicitado esas operaciones pero el resultado de geteuid() no es cero. La opción --privileged es útil con las capacidades del núcleo Linux y sistemas similares que pueden configurarse para permitir realizar sondeos con paquetes crudos a los usuarios no privilegiados. Asegúrese de indicar esta opción antes de cualquier otra opción que pueda requerir de privilegios específicos (sondeo SYN, detección de SO, etc.). Una forma alternativa a --privileged es fijar la variable de entorno NMAP_PRIVILEGED.

-V; --version (Mostrar el número de versión)

Imprime el número de versión de Nmap y aborta.

-h; --help (Mostrar la página resumen de ayuda)

Imprime una pequeña pantalla de ayuda con las opciones de órdenes más habituales. Pasa lo mismo si ejecuta Nmap sin argumentos.

Nmap Cheat Sheet

Network Mapper (Nmap) es un escáner de red de código abierto y gratuito que se utiliza para auditorías de seguridad y descubrimiento de redes.

Es una de las herramientas más confiables y poderosas para los profesionales de redes y seguridad durante pruebas de penetración y evaluación de vulnerabilidad.

Y conocer su uso es esencial, dada la flexibilidad, facilidad de uso, precisión y alto rendimiento de Nmap. Nmap es útil para monitorear el tiempo de actividad y los hosts del servicio, el inventario de la red y más. Nmap Scripting Engine (NSE) también es una gran herramienta para ayudarlo a escribir scripts rápidos y automatizar muchas actividades de red.

Con tantas opciones y comandos, es difícil para los profesionales recordar todo. Es por eso por lo que hemos seleccionado esta lista de las mejores hojas de trucos de.

Nmap Cheat Sheet 2023: All the Commands, Flags & Switches

NMAP Cheat Sheet

nmap Cheat Sheet

NMAP CHEAT-SHEET (Nmap Scanning Types, Scanning Commands , NSE Scripts)

Nmap Cheat Sheet

Nmap Cheat Sheet

Nmap Cheat Sheet

Nmap Cheat Sheet

1. **NSE (Nmap Scripting Engine)**

   Nmap incorpora un potente sistema de scripts conocido como NSE (Nmap Scripting Engine) que permite a los usuarios extender las capacidades de Nmap usando los diversos scripts que incorpora (actualmente hay más de 500 disponibles) que permiten desde la detección avanzada de versiones a la explotación de vulnerabilidades, o creando nuevos scripts que podemos compartir con el resto de usuarios (para los script se utiliza el lenguaje de programación LUA).

   SCRIPTS EN NMAP

   Ejemplos de scripts:

```
Nmap --script ssh-brute IP
```

```
Nmap --script ftp-brute IP
```