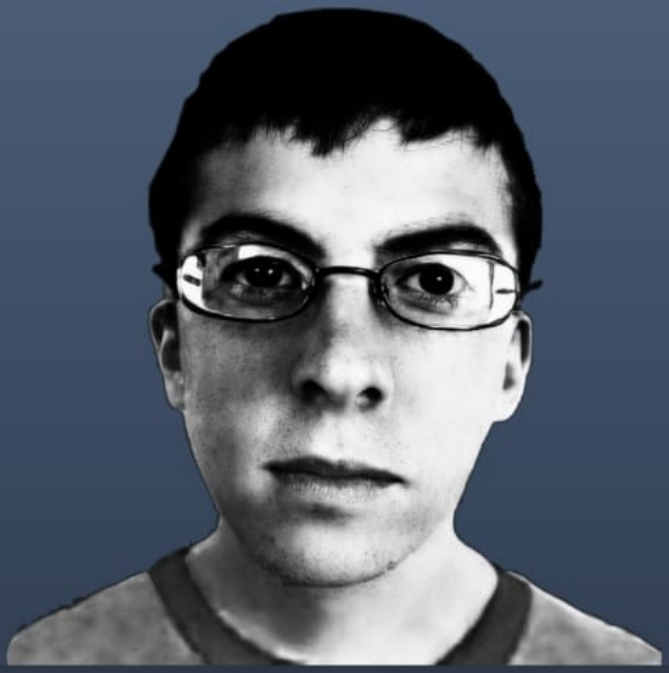

GUIA PARA NOVATOS

NMAP

<NMAP>
<guia de Hacking>
<here>

Hola, mi nombre es Matteo, soy el autor de esta guía y decidí crearla con fines educativos. Su propósito es exclusivamente el aprendizaje, por lo que no me hago responsable del mal uso que se le pueda dar. Es importante recordar que escanear puertos sin autorización puede ser ilegal. Para evitar problemas legales, en esta guía utilizaremos *scanme.nmap.org*, un servicio proporcionado por Nmap para fines de prueba y práctica.

INDICE.....

Cap 1.....

¿Que es y para que sirve?

¿Qué es Nmap?

Nmap (**Network Mapper**) es una herramienta de código abierto utilizada para el escaneo y auditoría de redes. Su principal función es descubrir dispositivos, servicios y puertos abiertos en una red, permitiendo analizar su estado y detectar posibles vulnerabilidades. Es ampliamente utilizada en el ámbito de la ciberseguridad, administración de sistemas y pruebas de penetración.

¿Para qué sirve Nmap?

Estas van a ser alguno de los usos que le vamos a dar a Nmap en esta guia

-Descubrimiento de hosts: Identifica dispositivos conectados a una red.

-Escaneo de puertos: Detecta puertos abiertos y servicios en los dispositivos.

-Detección de sistemas operativos: Intenta identificar el sistema operativo y su versión.

-Reconocimiento de servicios: Determina qué servicios y versiones están corriendo en los puertos abiertos.

-Auditoría de seguridad: Permite detectar configuraciones inseguras y posibles vulnerabilidades.

-Automatización con scripts (NSE - Nmap Scripting Engine): Ejecuta scripts para detectar vulnerabilidades, realizar ataques simulados y mucho más.

Cap 2.....

Requisitos y instalacion

Para comenzar con esta guía, debemos preparar nuestro laboratorio de manera ordenada y limpia.
Empezaremos por la instalación de la herramienta. Lo primero que debemos saber es en qué entorno vamos a trabajar. En mi caso, será desde Kali Linux, donde Nmap ya viene preinstalado.
Si queremos comprobar si Nmap está instalado, podemos ejecutar el siguiente comando:

```
m47730 ~ nmap --version
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.0.13 libssh2-1.11.0
libz-1.3 libpcre2-10.42 libpcap-1.10.4 nmap-libdnet-1.12
ipv6
Compiled without:
Available nsock engines: epoll poll select
```

Como podemos ver, cuento con la versión 7.94.

En caso de no tener Nmap instalado, podemos hacerlo de la siguiente manera:

```
m47730 ~ sudo apt install nmap -y
```

La opcion `-y` se utiliza para aceptar automáticamente los términos de instalación, ahorrándonos tiempo en el proceso.

Una vez instalado, podemos comprobar la instalación con el comando mencionado anteriormente o ejecutando la herramienta con:

```
m47730 ~ nmap
```

¡Perfecto! Ya tenemos instalada nuestra herramienta. Ahora, ¿cómo la utilizamos?

Cap 3.....

Como usar Nmap

Bien, antes que nada, necesitamos una víctima para probar las opciones que veremos más adelante. En este caso, los mismos creadores de Nmap nos ofrecen una víctima (ellos mismos), cuya URL es http://scanme.nmap.org/ . Si contamos con una máquina personal para pruebas, usaríamos su dirección IP. En mi caso, utilizaré *scanme.nmap.org*.

Una vez que tengamos nuestra víctima, debemos explorar las opciones disponibles hasta encontrar la que nos interese, algo que veremos en más detalle más adelante. Por ahora, utilizaremos la opción -sS, la cual, en pocas palabras, nos permite identificar qué puertos están abiertos de manera rápida y sigilosa.

Ahora que ya tenemos la víctima y la opción a ejecutar, lo siguiente es combinar ambos elementos y ejecutar la herramienta.

El orden correcto de los parámetros es el siguiente:

- **Permisos (en caso de no estar como root):** sudo
- **Nombre de la herramienta:** nmap
- **Opción:** -sS
- **IP o URL:** scanme.nmap.org

En la terminal, el comando quedaría de la siguiente manera:

```
m47730 ~ sudo nmap -sS scanme.nmap.org
```

bien ya acomodamos todo, que les parece si ejecutamos el comando y vemos que nos dice:

```
m47730 ~ sudo nmap -sS scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-11 18:52
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
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 2.51 seconds
```

perfecto, antes de darte la respuesta me gustaria que por cuenta propia intentes de analizarlo y en tu cabeza te respondas las siguientes preguntas

1)Que version de nmap tengo o tenes?
2)Que direccion ip usa scanme.nmap.org?
3)Cuantos puertos estan cerrados?
4)Que puertos estan abiertos y cuales son sus servicios?
5)Cuanto tardo en escanear?

Espero que puedas responderlas. Si no es así, no te preocupes, en la siguiente página podrás ver las respuestas.

Si lograste responderlas, ¡felicidades! Si no es el caso, no te preocupes, ya lo reforzaremos más adelante y, de ser necesario, vuelve a leer las veces necesarias.

Las respuestas son:
1)¿Qué versión de Nmap tienes? La versión de Nmap que tienes es 7.94SVN.

2)¿Qué dirección IP usa scanme.nmap.org? La dirección IP de scanme.nmap.org es 45.33.32.156.

3)¿Cuántos puertos están cerrados? Hay 996 puertos cerrados según el reporte.

4)¿Qué puertos están abiertos y cuáles son sus servicios? Los puertos abiertos son:

-22/tcp (servicio: ssh)

-80/tcp (servicio: http)

-9929/tcp (servicio: nping-echo)

-31337/tcp (servicio: Elite)

5)¿Cuánto tardó en escanear? El escaneo tardó 2.51 segundos.

Cap 4.....

Conceptos esenciales antes de usar Nmap

Bien, esta parte es importante para entender lo que sucede al momento de lanzar nuestro escaneo. Nmap funciona enviando y analizando paquetes de red. Dependiendo del tipo de escaneo, utilizará diferentes protocolos y tipos de paquetes.
Tranquilo, aquí te dejo una pequeña lista de los protocolos y los paquetes de red:

Protocolos de comunicación

Los protocolos definen cómo se comunican los dispositivos en una red. Nmap utiliza principalmente estos:

Protocolo	Descripción
TCP (Transmission Control Protocol)	Protocolo orientado a conexión, lo que significa que garantiza la entrega de los datos en el orden correcto. Usa el "Three-Way Handshake" (SYN, SYN-ACK, ACK) para establecer una conexión.
UDP (User Datagram Protocol)	Protocolo sin conexión, es más rápido que TCP, pero no garantiza la entrega de los datos ni verifica si han llegado correctamente. Se usa en servicios como DNS, VoIP y streaming.
Escaneo SCTP (Stream Control Transmission Protocol)	Se usan para detectar puertos abiertos en servicios que emplean el protocolo SCTP, común en telecomunicaciones, LTE/5G, VoIP y sistemas de señalización. Permiten descubrir servicios activos, evaluar la seguridad de infraestructuras y evadir detecciones basadas en TCP/UDP

Cap 5.....

Opciones y su descripcion.

Bien, ha llegado el momento de ver las opciones que ofrece Nmap.
Intentaremos revisar todas y daremos una descripción de cada una.
Estos son los parámetros básicos de Nmap:

-sS (SYN Scan)	También llamado **escaneo sigiloso**, es la opción por defecto de Nmap cuando se ejecuta con privilegios de administrador. Envía paquetes SYN para iniciar una conexión, pero no la completa, lo que lo hace menos detectable en los registros del sistema. Rápido y efectivo.
-sT (TCP Connect Scan)	Escaneo en el que se establece una conexión completa con el objetivo. Es más fácil de detectar en los logs del sistema, pero funciona sin privilegios de root.
-sU (UDP Scan)	Escaneo de puertos UDP. Más lento que el escaneo TCP debido a la falta de confirmaciones en los paquetes UDP y la posible necesidad de esperar respuestas ICMP de "puerto inalcanzable".
-sA (ACK Scan)	Envío de paquetes TCP con la bandera ACK para determinar si un firewall está filtrando puertos. No detecta puertos abiertos, solo identifica filtrado.
-sW (Window Scan)	Similar al escaneo -sA, pero se basa en el tamaño de la ventana TCP para diferenciar puertos filtrados de no filtrados.
-sM (Maimon Scan)	Variante del escaneo FIN que intenta evadir algunas implementaciones de firewall.
-sN (NULL Scan)	Envía paquetes TCP sin ninguna bandera activada. Puede ayudar a evadir ciertas configuraciones de firewall.
-sF (FIN Scan)	Envía paquetes con la bandera FIN activada, lo que puede eludir algunos sistemas de detección.
-sX (Xmas Scan)	Envía paquetes con las banderas **FIN, PSH y URG** activadas, lo que puede revelar puertos filtrados. Se llama "Xmas Scan" porque las banderas forman un patrón similar a un árbol de Navidad.
-sY (SCTP INIT Scan)	Similar a SYN Scan, pero para el protocolo SCTP en lugar de TCP.
-sZ (SCTP COOKIE ECHO Scan)	Variante del escaneo SCTP para detectar puertos abiertos utilizando la verificación de cookies.

Tambien podemos saber que version y sistema operativo cuenta la victima:

-O	Intenta detectar el sistema operativo del objetivo analizando los paquetes de respuesta.
--osscan-guess	Fuerza una estimación más agresiva del sistema operativo en caso de incertidumbre.
-sV	Escaneo de versión de servicios. Identifica la versión específica de los servicios en los puertos abiertos.
--version-intensity <nivel>	Ajusta la agresividad del escaneo de versión. Va de 0 (mínimo) a 9 (máximo).

Cap 6.....

Poniendo a prueba las opciones.

-Opciones para el protocolo TCP(-sS,-sT,-sA,-sW y -sM).

¿Que es TCP?

TCP (Transmission Control Protocol):

Orientado a la conexión: Establece una conexión antes de transmitir datos y garantiza la entrega ordenada y sin errores.

Fiabilidad: Si un paquete se pierde o llega corrupto, TCP se encarga de reintentarlo.

Control de flujo y congestión: Evita que la red se sobrecargue con demasiados datos.

Uso: Ideal para aplicaciones que requieren fiabilidad, como la navegación web (HTTP), correos electrónicos (SMTP) y transferencia de archivos (FTP).

-Opcion -sT.

Bien, ahora que hemos visto los principales, pongamos a prueba algunas opciones y veamos sus resultados.
Iremos en orden. Ya probamos la opción `-sS`, ahora probemos la opción `-sT`, que es un poco más fácil de rastrear, pero la ventaja es que no requerimos permisos de root.

```
m47730 ~ nmap -sT scanme.nmap.org
```

Bien una vez lanzado el comando debemos esperar a tener una respuesta.

```
m47730 ~ nmap -sT scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-12 14:11
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
25/tcp    filtered smtp
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo
31337/tcp open     Elite

Nmap done: 1 IP address (1 host up) scanned in 24.47 seconds
```

bien en mi caso logramos conseguir el siguiente resultado, anteriormente practicamos el analizáis de los resultados, por ello voy a obviar esta parte y acomodar los resultados que podemos ver.

Bueno el escaneo tardo 24.47 segundos, tuvo un total de 992 puertos cerrados, 4 puertos abiertos y 4 filtrados.

Bien empezando por los puertos abiertos tenemos:

Puerto	Estado	Servicio
22/tcp	abierto	ssh
80/tcp	abierto	http
9929/tcp	abierto	nping-echo
31337/tcp	abierto	Elite

Ahora acomodemos los puertos filtrados, pero antes de ello,¿que significa que el puerto este filtrado?

Bueno lo mas probable que el puerto este custodiado por un firewall lo cual bloquea o restringe el acceso a estos servicios.

Puerto	Estado	Servicio
25/tcp	filtrado	smtp
135/tcp	filtrado	msrpc
139/tcp	filtrado	netbios-ssn
445/tcp	filtrado	microsoft-ds

-Opcion -sA.

Llego el momento de usar la opción -sA

```
m47730 ~ sudo nmap -sA scanme.nmap.org
```

esperamos el resultado...

Ok, recibimos un resultado donde se nos indica que hay 1000 puertos filtrados, lo que sugiere que hay algún tipo de sistema de seguridad.
Como aclaración, podemos encontrar variantes en el resultado como: Not shown: 1000 filtered tcp ports (no-response).
Podemos recibir los siguientes resultados:

Filtrado → Cuando Nmap muestra que los puertos están filtrados, significa que los paquetes enviados no han recibido respuesta o han sido bloqueados por un Firewall. Esto sugiere que el sistema de seguridad está eliminando los paquetes ACK sin devolver un RST.

No filtrado → Si un puerto es detectado como "no filtrado", significa que el paquete ha recibido una respuesta RST, lo que indica que el puerto está accesible pero no necesariamente abierto.

Sin respuesta → Si no se recibe ninguna respuesta, es probable que un Firewall esté descartando los paquetes silenciosamente (DROP).

En nuestro caso, recibimos una respuesta de "sin respuesta".

Una opción útil por si queremos indagar sobre la presencia de un Firewall en un puerto específico es:

```
m47730 ~ sudo nmap -sA -p 80,443 scanme.nmap.org
```

Especificamos los puertos que queremos escanear(-p) que en este caso son los 80 y 443, para saber si estos 2 puertos presentan algún tipo de Firewall.

```
m47730 ~ sudo nmap -sA -p 80,443 scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15 17:51
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f

PORT    STATE    SERVICE
80/tcp  filtered http
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 4.82 seconds
```

Y en el resultado nos presenta que el puerto esta filtrado lo que nos da a entender que tenemos un tipo de sistema de seguridad.

-Opcion -sW.

Una opción algo similar al -sA visto con anterioridad pero nos permite ser un poco mas ordenados y sobre todo diferenciar entre filtrados y no filtrados.

```
m47730 ~ sudo nmap -sW scanme.nmap.org
```

Enter y a ver que sale

```
m47730  ~  sudo nmap -sW scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15 20:17
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.28s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in
ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 286.76 seconds
```

Podemos ver una respuesta similar al -sA pero apliquemos lo mismo que antes, determinemos ya sea los puertos que queremos escanear o el rango, esta vez vamos a escanear un rango, que van a ir de los puertos

```
m47730  ~  sudo nmap -sW -p 20-100  scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15 20:29
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.31s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
All 81 scanned ports on scanme.nmap.org (45.33.32.156) are in
ignored states.
Not shown: 81 filtered tcp ports (no-response)
```

okey se ve que dentro del rango todos los puestos están filtrados lo que indica que Nmap no recibió respuesta, esto como vimos con anterioridad indica la presencia de un Firewall, ¿podemos hacer algo mas?

Si, cambiar el parámetro por un -sA o cambiar el rango, lo del rango lo use para que vean las diferentes cosas que podemos hacer, por si no te diste cuenta

al momento de indicar los puertos que queremos analizar, podemos darle rango(ejemplo: 10-20) o indicarlo(ejemplo:10,20,30).

-Parametro -sM

este parámetro evita ciertas implementaciones del Firewall, pero sin mas preámbulos lanzamos este parámetro.

```
m47730  ~  sudo nmap -sM scanme.nmap.org
```

Veamos el resultado...

```
m47730 ~ sudo nmap -sM scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-15 20:39
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
All 1000 scanned ports on scanme.nmap.org (45.33.32.156) are in
ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 236.61 seconds
```

perfecto, a este punto seguramente te preguntes el por que recibimos el mismo resultado, ¿verdad?

El escaneo Maimon (-sM) muestra todos los puertos como **"open|filtered"** porque no recibe respuestas del objetivo. Esto ocurre porque:

Un Firewall está bloqueando los paquetes FIN+ACK sin responder.

El sistema operativo ignora este tipo de paquetes.

El método -sM **no es efectivo en sistemas modernos.**

Mi consejo utiliza las opciones SNY(-sS) o ACK(-sA).

Ya que los parámetro -sW y -sM, resultaron no ser tan efectivos con sistemas modernos, pero pueden llegar a ser útiles en otros casos.

-Opción para el protocolo UDP(-sU).

UDP (User Datagram Protocol):

Sin conexión: No establece una conexión antes de enviar los datos, lo que lo hace más rápido, pero no garantiza que los datos lleguen correctamente o en el orden correcto.
Sin fiabilidad: No hay reintentos si los paquetes se pierden o llegan desordenados.
Uso: Se utiliza cuando la velocidad es más importante que la fiabilidad, como en aplicaciones de transmisión en vivo (video o audio), juegos en línea o consultas DNS.

Ahora nos toca la opcion -sU, para ello vamos a lanzarlo y analizar el resultado.

```
m47730  ~  sudo nmap -sU scanme.nmap.org
```

Ahora analizamos el resultado.

```
m47730  ~  sudo nmap -sU scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-13 12:38
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.26s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 998 closed udp ports (port-unreach)
PORT    STATE         SERVICE
68/udp  open|filtered dhcpc
123/udp open          ntp

Nmap done: 1 IP address (1 host up) scanned in 1114.77 seconds
```

Bien ahora veamos que presenta este resultado.

Como pueden ver este resultado tardo mucho mas de lo habitual con 1114.77 segundos unos 18 minutos y 34 segundos, contamos con un total de 998 puertos cerrados y 2 puertos abiertos

Puerto	Estado	Servicio
68/udp	abierto|filtrado	dhcpc
123/udp	abierto	ntp

Por si te preguntas que significa que el puerto 68/udp esta abierto y filtrado a la vez, esto indica que no pudo determinar con certeza si el puerto está realmente abierto o si está siendo filtrado por un Firewall u otro mecanismo de seguridad.

Es algo así como gato de Schrödinger, realmente no se sabe si esta o no custodiado por algún sistema de seguridad, ¿podemos indagar mas a profundidad para saber realmente?, obviamente pero en esta primera edición no lo vamos a ver

(*pero data adicional, podríamos saber analizando el trafico con Wireshark, para saber si realmente hay una respuesta de nuestro amigo el puerto 68 ;)*)

-Opciones para el protocolo SCTP(-sY y -sZ).

SCTP (Stream Control Transmission Protocol):

Orientado a la conexión: Al igual que TCP, SCTP establece una conexión antes de transmitir datos.
Multihoming: Permite que una conexión utilice múltiples direcciones IP, lo que mejora la tolerancia a fallos.

Multistreaming: Permite el envío de múltiples flujos de datos dentro de una sola conexión, lo que ayuda a evitar bloqueos en uno de los flujos si otro tiene problemas.
Uso: Se utiliza principalmente en aplicaciones de telecomunicaciones, como en redes de telefonía móvil o en protocolos como SIP (Session Initiation Protocol).

Llego el momento de usar opciones de Namp en base al protocolo SCTP

probemos la primera opción -sY

```
m47730  ~  sudo nmap -sY scanme.nmap.org
```

```
m47730  ~  sudo nmap -sY scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 12:23
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.22s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
All 52 scanned ports on scanme.nmap.org (45.33.32.156) are in
ignored states.
Not shown: 52 closed sctp ports (abort)

Nmap done: 1 IP address (1 host up) scanned in 5.15 seconds
```

Bien viendo el resultado ya sabemos que los 52 puertos SCTP esta cerrados, lo que indica que el host respondió con un mensaje de aborto, esto nos indica que no hay servicios SCTP en ejecución en los puertos escaneados

pero no nos quedemos con los brazos cruzados, de paso agregamos opciones.

```
m47730  ~  sudo nmap -sY -p- scanme.nmap.org
```

Acá agregamos un -p- para escanear **los 65,535 puertos posibles**, asegurando que no nos perdemos nada.

```
m47730 ~ sudo nmap -sY -p- scanme.nmap.org
Starting Nmap 7.94 ( https://nmap.org ) at 2025-02-28 12:34 UTC
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.12s latency).
Scanned at 2025-02-28 12:34 UTC with SCTP INIT scan (-sY)

PORT      STATE         SERVICE
1/sctp    closed        tcpmux
7/sctp    closed        echo
9/sctp    closed        discard
13/sctp   closed        daytime
17/sctp   closed        qotd
19/sctp   closed        chargen
22/sctp   closed        ssh
23/sctp   closed        telnet
25/sctp   closed        smtp
53/sctp   open          domain
80/sctp   open          http
443/sctp  closed        https
500/sctp  open|filtered isakmp
3306/sctp closed        mysql
3389/sctp closed        ms-wbt-server
5060/sctp closed        sip
8080/sctp closed        http-proxy

Nmap done: 1 IP address (1 host up) scanned in 34.12 seconds
```

Acá ya recibimos nuestro resultado donde tenemos un total de 14 puertos cerrados, 2 puertos abiertos y 1 abierto/filtrado.

Pero podemos ir más allá: si el objetivo tiene un Firewall que bloquea los pings, podríamos agregar `-Pn` para evitar la detección de host.

También podemos usar --open para ver solo los puertos abiertos y evitar resultados innecesarios.

```
m47730 ~ sudo nmap -sY -p- --open -Pn scanme.nmap.org
```

Lanzamos...

```
m47730 ~ sudo nmap -sY -p- --open -Pn scanme.nmap.org
[sudo] contraseña para m47730:
Lo siento, pruebe otra vez.
[sudo] contraseña para m47730:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 11:22
-03
Nmap done: 1 IP address (1 host up) scanned in 75.89 seconds
```

El escaneo no presento resultados de puertos abiertos, lo que indica que:

No hay puertos SCTP abiertos en scanme.nmap.org.

El host sigue estando activo, ya que no hubo errores de conectividad.

Podría haber un Firewall bloqueando el tráfico SCTP, lo que haría que todos los puertos parezcan cerrados o filtrados.

Interpretación del resultado:

El escaneo con -sY y -p- --open no encontró puertos SCTP abiertos en scanme.nmap.org. Esto puede significar dos cosas:

El host no tiene servicios SCTP en ejecución → No hay procesos escuchando en este protocolo.
Un Firewall o política de red está bloqueando el tráfico SCTP → Algunos sistemas deshabilitan completamente este protocolo por razones de seguridad.

Opciones para investigar más:

Si queremos asegurarnos de que no sea un Firewall bloqueando, podemos forzar la detección de servicios:

```
m47730 ~ sudo nmap -sY -p- -Pn --reason scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 11:25
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up, received user-set (0.20s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
All 65535 scanned ports on scanme.nmap.org (45.33.32.156) are in
ignored states.
Not shown: 65535 closed sctp ports (abort)

Nmap done: 1 IP address (1 host up) scanned in 1242.36 seconds
```

En este caso, Nmap escaneó todos los puertos SCTP (-p-), pero encontró que todos estaban cerrados (closed) y respondieron con ABORT, lo que confirma que scanme.nmap.org no tiene servicios SCTP en ejecución. Además, como no se encontraron puertos filtrados (filtered), es poco probable que haya un Firewall bloqueando el tráfico SCTP.

Bien ya nos extendimos mucho ya es hora de dar un ultimo salto a la opción -sZ

pero antes de ellos que es?

El escaneo `-sZ` usa un enfoque distinto al `-sY`: en lugar de enviar un paquete SCTP INIT, envía un SCTP COOKIE-ECHO para verificar si hay servicios esperando completar la autenticación SCTP. Este método es útil para detectar si un servicio requiere verificación antes de establecer una conexión.

```
m47730  ~  sudo nmap -sZ scanme.nmap.org
```

```
m47730  ~  sudo nmap -sZ scanme.nmap.org
[sudo] contraseña para m47730:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 12:08
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.20s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
All 52 scanned ports on scanme.nmap.org (45.33.32.156) are in
ignored states.
Not shown: 52 closed sctp ports (abort)

Nmap done: 1 IP address (1 host up) scanned in 2.12 seconds
```

En este caso, todos los puertos respondieron con ABORT, lo que confirma que scanme.nmap.org no tiene servicios SCTP esperando completar autenticación. Esto coincide con los resultados obtenidos en -sY, reafirmando que SCTP no está en uso en este host.

Podríamos probar un escaneo de servicios para ver que servicios esta corriendo el host

```
m47730  ~  sudo nmap -sV scanme.nmap.org
```

```
m47730  ~  sudo nmap -sV scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-06 11:19
-03
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 991 closed tcp ports (reset)
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 6.6.1p1 Ubuntu
2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open     http         Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
9929/tcp  open     nping-echo   Nping echo
31337/tcp open     tcpwrapped
49163/tcp filtered unknown
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 45.59 seconds
```

bien ahora que sabemos que puertos están corriéndose en el hots podemos analizarlos con las diferentes opciones que vimos en esta guía.

Y con esto concluimos esta guía introductoria sobre el uso básico de Nmap. Hemos cubierto los comandos esenciales para empezar a escanear redes y puertos. A medida que avances, podrás explorar más opciones avanzadas para aprovechar todo el potencial de esta herramienta. Recuerda siempre practicar de manera ética y legal. ¡Gracias por leer y espero que te haya sido útil!