

## ARQUITECTURA Y SISTEMAS OPERATIVOS

### Que es NMAP y cómo utilizarlo

*Nmap (Network Mapper) es una herramienta de código abierto ampliamente utilizada para el escaneo de puertos y el mapeo de redes. Nmap puede ser utilizado para identificar hosts y servicios en una red, así como para determinar la vulnerabilidad de los sistemas.*

Nmap es una herramienta de línea de comandos, lo que significa que se ejecuta a través de la línea de comandos en un terminal. Aunque puede parecer intimidante para los usuarios sin experiencia en la línea de comandos, Nmap es una herramienta muy útil para los profesionales de la seguridad informática y para cualquier persona interesada en conocer más sobre su red.

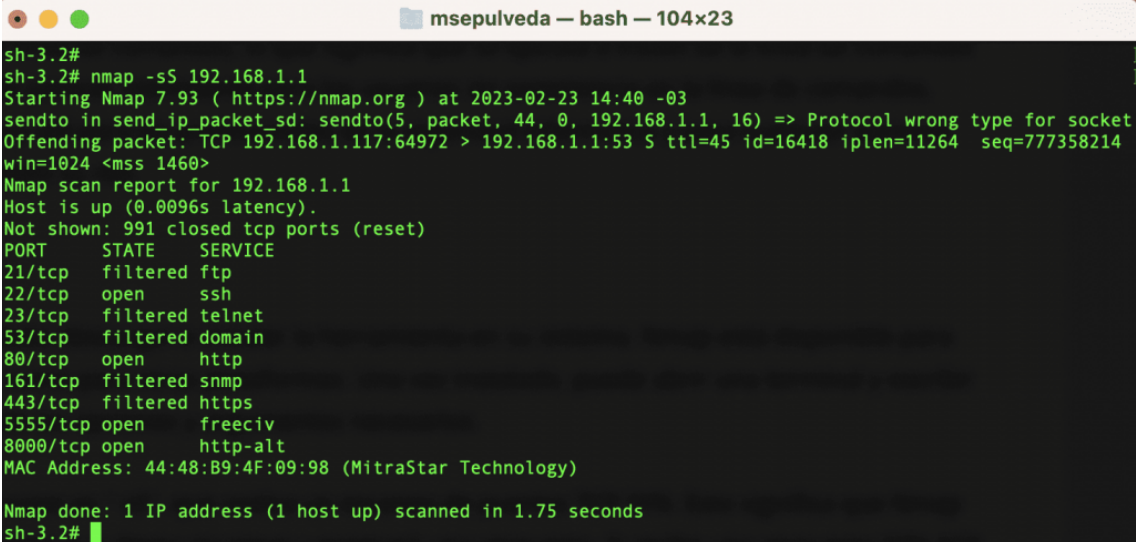
### 1. Cómo utilizar Nmap

Para utilizar Nmap, primero debe descargar e instalar la herramienta en su sistema. Nmap está disponible para Windows, Linux y macOS, así como para otras plataformas. Una vez instalado, puede abrir una terminal y escribir el comando «nmap» seguido de las opciones y argumentos necesarios.

Una de las opciones más comunes es «-sS», que realiza un escaneo de puertos TCP SYN. Esto significa que Nmap enviará un paquete SYN al puerto que desea escanear y esperará una respuesta. Si recibe una respuesta SYN-ACK, significa que el puerto está abierto. Si recibe una respuesta RST, significa que el puerto está cerrado.

Por ejemplo, para escanear los puertos de un host, puede ejecutar el siguiente comando:

***nmap -sS 192.168.1.1***



```
sh-3.2# nmap -sS 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-23 14:40 -03
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 192.168.1.1, 16) => Protocol wrong type for socket
Offending packet: TCP 192.168.1.117:64972 > 192.168.1.1:53 S ttl=45 id=16418 iplen=11264 seq=777358214
win=1024 <mss 1460>
Nmap scan report for 192.168.1.1
Host is up (0.0096s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    filtered ftp
22/tcp    open  ssh
23/tcp    filtered telnet
53/tcp    filtered domain
80/tcp    open  http
161/tcp   filtered snmp
443/tcp   filtered https
5555/tcp  open  freeciv
8080/tcp  open  http-alt
MAC Address: 44:48:B9:4F:09:98 (MitraStar Technology)

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
sh-3.2#
```

Este comando escaneará los puertos del host con dirección IP 192.168.1.1 utilizando un escaneo de puertos TCP SYN.

Nmap también tiene varias opciones para la identificación de servicios. Por ejemplo, la opción «-sV» se utiliza para identificar los servicios que se ejecutan en los puertos abiertos. Esta opción enviará una solicitud al servicio para obtener información sobre su versión y otros detalles.

Otra opción útil es «-A», que activa el escaneo de detección de sistemas operativos, identificación de servicios y detección de scripts de NSE (Nmap Scripting Engine). Esta opción proporciona información detallada sobre el sistema operativo y los servicios que se ejecutan en el host escaneado.

Además de las opciones que mencioné anteriormente, Nmap tiene varias opciones adicionales que pueden ser utilizadas para personalizar el escaneo y obtener información detallada sobre la red. A continuación, se presentan algunas opciones comunes:

Opción	Descripción	Ejemplo / Notas
<b>-O</b>	Detección del sistema operativo. Nmap envía paquetes específicos y analiza las respuestas para identificar la plataforma del host.	nmap -O <target>
<b>-p</b>	Especifica el rango o lista de puertos a escanear.	nmap -sS -p 1-100 192.168.1.1
<b>-T</b>	Define el nivel de agresividad del escaneo, de <b>-T0</b> (muy lento y furtivo) a <b>-T5</b> (rápido y agresivo). La opción predeterminada es <b>-T3</b> .	nmap -T4 <target>
<b>-f</b>	Activa la fragmentación de paquetes para evadir algunos firewalls o IDS.	nmap -f <target>
<b>--script</b>	Permite ejecutar scripts del Nmap Scripting Engine (NSE) para obtener información adicional (vulnerabilidades, configuraciones, etc.).	nmap --script vuln <target>
<b>-sU</b>	Realiza un escaneo de puertos UDP, útil para identificar servicios basados en UDP como DNS, DHCP y SNMP.	nmap -sU <target>
<b>-sS</b>	Realiza un escaneo SYN (half-open), el modo por defecto para escanear puertos TCP de manera rápida y relativamente furtiva.	nmap -sS <target>
<b>-sT</b>	Realiza un escaneo de conexión TCP completa (TCP Connect Scan), útil cuando el SYN scan no es posible.	nmap -sT <target>
<b>-sV</b>	Realiza la detección de versiones, identificando qué servicios y versiones están corriendo en los puertos abiertos.	nmap -sV <target>
<b>-A</b>	Escaneo agresivo que combina detección de OS, detección de versiones, ejecución de scripts NSE y traceroute. Este comando recopila mucha información, pero puede ser más ruidoso.	nmap -A <target>
<b>-Pn</b>	Desactiva el ping previo, asumiendo que el host está activo. Es útil en redes con firewalls que bloquean los pings.	nmap -Pn <target>
<b>-iL</b>	Lee la lista de objetivos desde un archivo, permitiendo escanear múltiples hosts en un solo comando.	nmap -iL targets.txt
<b>-oN, -oX, -oG</b>	Permite guardar la salida en distintos formatos: normal (-oN), XML (-oX) o grepable (-oG), facilitando su posterior análisis o integración con otras herramientas.	nmap -oN output.txt <target>

## Aclaraciones adicionales sobre Nmap:

### Detección de OS (-O):

Es recomendable utilizar esta opción con precaución, ya que puede generar tráfico adicional que algunos IDS/IPS consideren sospechoso. Además, algunos sistemas pueden limitar la precisión de la detección debido a configuraciones de red o firewalls.

### Niveles de agresividad (-T):

Dependiendo del entorno y de los requerimientos, puedes ajustar este parámetro. En entornos de producción, niveles más bajos (como -T0 o -T1) pueden ser preferibles para evitar la detección o causar interrupciones.

### Uso de scripts (--script):

El Nmap Scripting Engine (NSE) incluye una amplia variedad de scripts para tareas específicas, como detección de vulnerabilidades, descubrimiento de configuraciones erróneas o recolección de información. Es aconsejable revisar la documentación de NSE para elegir los scripts que se ajusten a tu objetivo.

### Fragmentación (-f):

La fragmentación de paquetes puede ayudar a evadir algunas medidas de seguridad, pero también puede provocar falsos negativos o generar tráfico anómalo que llame la atención en entornos monitorizados.

## Ejemplos de Uso de Nmap:

- **Descubrimiento de Dispositivos en una Red:**

### **nmap -sn 192.168.1.0/24**

Este comando realiza un escaneo de hosts vivos en la red especificada (en este caso, 192.168.1.0/24), sin realizar una exploración de puertos, útil para descubrir qué dispositivos están activos.

- **Escaneo de Puertos en un Host:**

### **nmap 192.168.1.1**

Analiza los puertos abiertos en el host con la dirección IP 192.168.1.1, proporcionando información detallada sobre los servicios en ejecución.

- **Escaneo Completo de Puertos en un Rango de IP:**

### **nmap -p 1-65535 192.168.1.0**

Explora todos los puertos posibles en el host con la dirección IP 192.168.1.0, permitiendo una evaluación exhaustiva de la superficie de ataque.

- **Identificación de Versiones de Servicios:**

#### **nmap -sV 192.168.1.100**

Realiza un escaneo de servicios en el host 192.168.1.100, identificando las versiones de los servicios que están en ejecución.

- **Escaneo de Red para Descubrir Sistemas Operativos:**

#### **nmap -O 192.168.1.0/24**

Intenta determinar los sistemas operativos de los dispositivos en la red especificada (192.168.1.0/24), proporcionando información valiosa sobre la diversidad de sistemas en la infraestructura.

Estas son solo algunas de las opciones disponibles en Nmap. Para obtener una lista completa de opciones y argumentos, consulte la documentación oficial de Nmap en el siguiente [enlace](#).

### **Conclusión**

Nmap es una herramienta poderosa y ampliamente utilizada en la seguridad informática y el mapeo de redes. Aunque puede parecer intimidante al principio, Nmap ofrece una gran cantidad de opciones y argumentos que pueden ser utilizados para personalizar el escaneo y obtener información detallada sobre la red. Si está interesado en aprender más sobre la seguridad informática y el mapeo de redes, Nmap es una herramienta que debe conocer y utilizar.