INTRODUCCIÓN

🛰️ ¿Qué es Nmap y para qué sirve?

Nmap (Network Mapper) es la herramienta de escaneo de redes más famosa y utilizada en el mundo del hacking ético. Su función principal es descubrir qué dispositivos están conectados a una red, qué puertos tienen abiertos y qué servicios están ejecutando.

🧠 La Importancia del Escaneo en el Hacking Ético

En la fase de reconocimiento (OSINT), recopilamos información pasiva. Ahora entramos en la fase activa. Nmap nos permite "tocar" la red del objetivo para ver qué responde. Es como tocar la puerta de una casa para ver si hay alguien dentro y qué tipo de cerradura tiene.

Nmap es una herramienta de línea de comandos (aunque tiene una interfaz gráfica llamada Zenmap). Se ejecuta en Kali Linux (y en la mayoría de distribuciones de Linux).

> 💡 **Dato Clave**
>
> Nmap fue creado por Gordon Lyon (Fyodor) en 1997. Ha aparecido en películas como *Matrix Reloaded* y *El Cuarto Poder*. Es el estándar de la industria para escaneo de redes.

PASO 01

🔍 Descubrimiento de Hosts (Ping Sweep)

Antes de escanear puertos, necesitamos saber qué IPs están activas en nuestra red. Este proceso se conoce como "Ping Sweep" (barrido de ping).

🏓 ¿Cómo funciona?

Nmap envía paquetes ICMP (ping) o paquetes TCP/UDP a un rango de IPs. Si el dispositivo responde, sabemos que está encendido. Si no responde, puede estar apagado o tener el firewall bloqueando el ping.

Terminal

```
kali@root:~$ nmap -sn 192.168.56.0/24
Starting Nmap 7.92 ( https://nmap.org )
Nmap scan report for 192.168.56.1
Host is up (0.00050s latency).
Nmap scan report for 192.168.56.102
Host is up (0.00080s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.34 seconds
```

Explicación del comando: `-sn` significa "No port scan" (solo descubrimiento de hosts). El `/24` indica que estamos escaneando todo el rango de la red (desde la IP .1 hasta la .254).

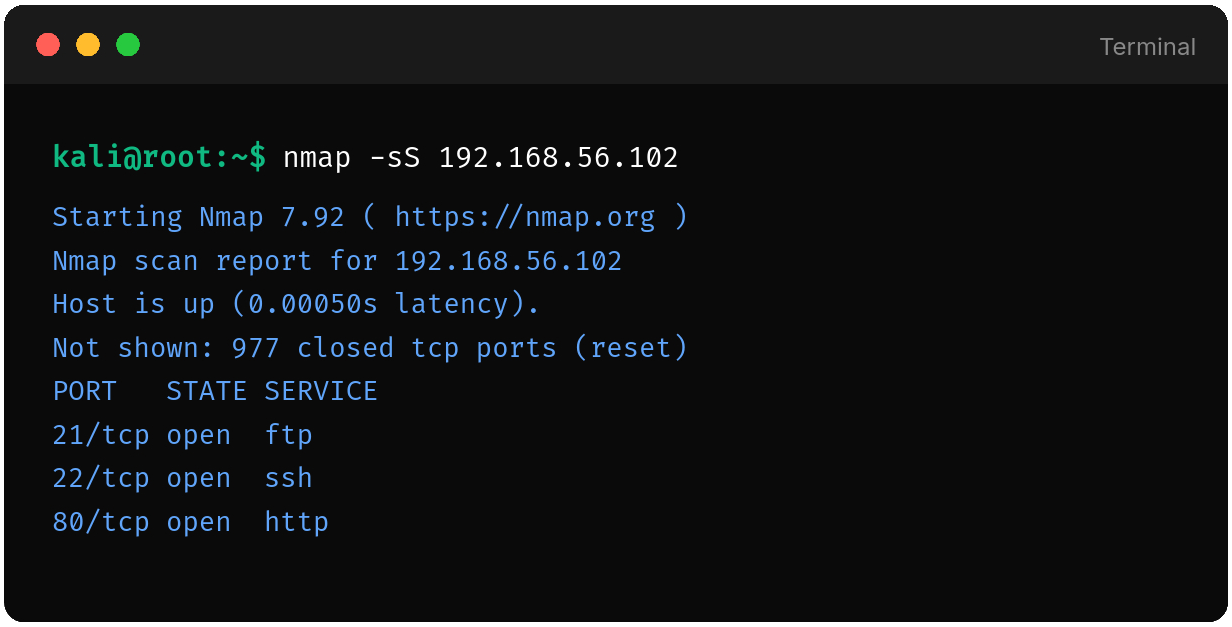
PASO 02

🚪 Escaneo de Puertos (TCP/UDP)

Una vez que sabemos qué hosts están activos, el siguiente paso es descubrir qué puertos tienen abiertos. Los puertos son como las "puertas" de un edificio. Cada servicio (web, correo, SSH) usa un puerto específico.

📡 Escaneo TCP (El más común)

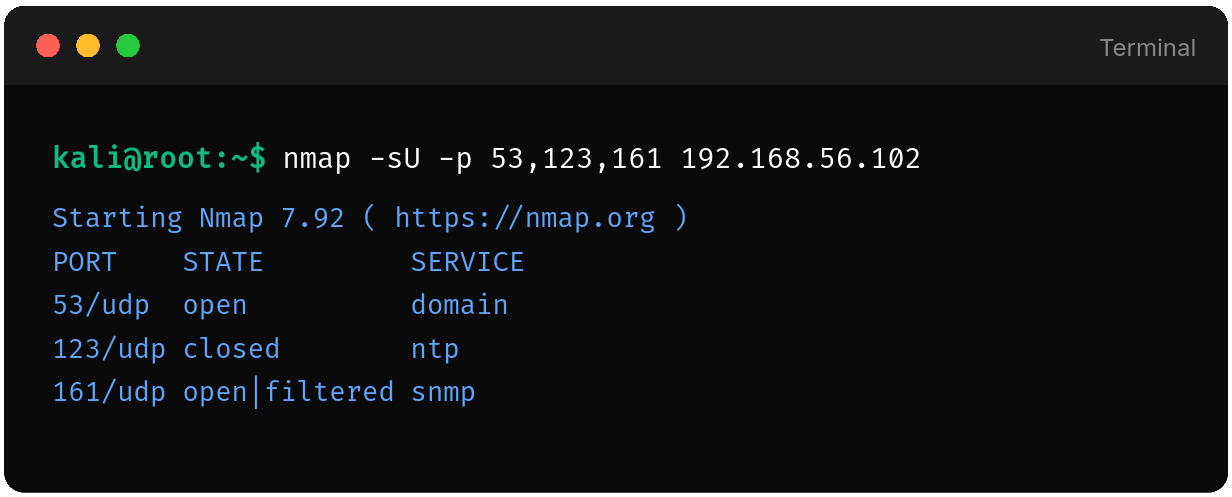
TCP es un protocolo orientado a conexión. Nmap utiliza el "Three-Way Handshake" (apretón de manos de tres vías) para determinar si un puerto está abierto.



Explicación del comando: `-sS` es un escaneo "SYN Stealth" (sigiloso). Es el más rápido y el que menos rastro deja en los logs del servidor.

📡 Escaneo UDP

UDP es un protocolo sin conexión. Es más difícil de escanear porque los puertos abiertos no responden con un "OK", sino que simplemente no envían error. Nmap usa técnicas especiales para detectarlos.



Explicación del comando: `-sU` activa el escaneo UDP. `-p` especifica los puertos a escanear (en este caso, DNS, NTP y SNMP).

PASO 03

⚙️ Detección de Servicios y Versiones

Saber que el puerto 80 está abierto es bueno, pero saber que está corriendo Apache 2.4.41 en Ubuntu es mucho mejor. Esta información nos dice qué vulnerabilidades explotar.

🔍 El parámetro -sV

La bandera `-sV` (Service Version) le dice a Nmap que no solo detecte el puerto, sino que intente determinar el software exacto y su versión. Esto lo logra enviando paquetes de "sondeo" (probes) y comparando las respuestas con su base de datos de firmas.

Terminal

```
kali@root:~$ nmap -sV 192.168.56.102
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

Ahora sabemos que el servidor FTP tiene la versión **vsftpd 2.3.4**, que es famosa por tener una puerta trasera (backdoor) que permite ejecutar comandos remotamente. Sin `-sV`, nunca lo habríamos sabido.

PASO 04

💻 Fingerprinting de Sistema Operativo

Nmap puede adivinar qué sistema operativo está usando el objetivo analizando cómo responde a ciertos paquetes (TTL, tamaño de ventana, etc.).

🖥️ El parámetro -O

La bandera `-O` (OS Detection) activa la detección de sistema operativo. Nmap envía una serie de paquetes malformados a propósito para ver cómo reacciona el kernel del objetivo. Cada sistema operativo (Windows, Linux, macOS) reacciona de forma distinta.

Terminal

```
kali@root:~$ sudo nmap -O 192.168.56.102
Running (JUST GUESSING): Linux 2.6.X (88%)
Aggressive OS guesses: Linux 2.6.9 - 2.6.33 (88%), Linux 2.6.18 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Nota: La detección de SO requiere privilegios de root (por eso usamos `sudo`). Los resultados no son 100% exactos, pero te dan una idea muy cercana del sistema que estás atacando.

PASO 05

📜 Scripts NSE (Nmap Scripting Engine)

Nmap no es solo un escáner; es una plataforma de scripting. Los scripts NSE permiten automatizar tareas avanzadas: desde detectar vulnerabilidades hasta hacer fuerza bruta a un login.

🚀 ¿Qué son los scripts NSE?

Nmap trae cientos de scripts escritos en el lenguaje Lua. Se clasifican por categorías: `auth`, `broadcast`, `brute`, `default`, `discovery`, `dos`, `exploit`, `external`, `fuzzer`, `intrusive`, `malware`, `safe`, `version`, `vuln`.

Terminal

```
kali@root:~$ nmap --script vuln 192.168.56.102
PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-vsftpd-backdoor: VULNERABLE
|   State: VULNERABLE
|   IDs:  CVE:CVE-2011-2523
|   This server is running vsftpd 2.3.4, which is vulnerable to a
backdoor command execution.
```

Explicación del comando: `--script vuln` ejecuta todos los scripts de la categoría "vulnerabilidad". En este caso, detectó automáticamente que el servidor FTP tiene la puerta trasera.

🛠️ Otros scripts útiles

- `--script default`: Ejecuta los scripts básicos de detección (es lo mismo que usar `-sC`).
- `--script http-enum`: Enumera directorios y archivos ocultos en un servidor web.
- `--script smb-vuln-ms17-010`: Verifica si el servidor es vulnerable a EternalBlue (WannaCry).
- `--script ssh-brute`: Intenta fuerza bruta contra el servicio SSH.

REFERENCIA RÁPIDA

📋 Todos los Comandos de Nmap

Una tabla completa con los flags más utilizados de Nmap, su función y un ejemplo práctico.

FLAG / COMANDO	FUNCIÓN Y EJEMPLO
`-sn`	Descubrimiento de hosts (Ping Sweep). No escanea puertos. `$ nmap -sn 192.168.1.0/24`
`-sS`	Escaneo TCP SYN (sigiloso y rápido). Requiere root. `$ sudo nmap -sS 192.168.1.10`
`-sT`	Escaneo TCP Connect. No requiere root, pero deja más rastro. `$ nmap -sT 192.168.1.10`
`-sU`	Escaneo UDP. Más lento y ruidoso. `$ nmap -sU -p 53,161 192.168.1.10`
`-sV`	Detección de versiones de servicios. `$ nmap -sV 192.168.1.10`
`-O`	Detección de sistema operativo. `$ sudo nmap -O 192.168.1.10`
`-p-`	Escanea todos los puertos (1-65535). Muy lento. `$ nmap -p- 192.168.1.10`
`-p 80,443`	Escanea puertos específicos. `$ nmap -p 80,443 192.168.1.10`
`-A`	Modo "Aggressive". Combina -sV, -O, -sC y traceroute.

	`$ sudo nmap -A 192.168.1.10`
`-T4`	Aumenta la velocidad del escaneo (0 a 5). T4 es agresivo pero seguro. `$ nmap -T4 -F 192.168.1.10`
`-F`	Escaneo rápido (solo los 100 puertos más comunes). `$ nmap -F 192.168.1.10`
`--script`	Ejecuta scripts NSE. Puede ser un script específico o una categoría. `$ nmap --script vuln 192.168.1.10`
`-oN`	Guarda el resultado en un archivo de texto normal. `$ nmap -oN resultado.txt 192.168.1.10`
`-oX`	Guarda el resultado en formato XML (para importar a otras herramientas). `$ nmap -oX resultado.xml 192.168.1.10`
`-v`	Modo verbose. Muestra más detalles durante el escaneo. `$ nmap -v 192.168.1.10`

🎓 ¡Fin de la Clase 1.4!

Ya dominas los fundamentos de Nmap. En la próxima clase veremos cómo usar esta información para explotar vulnerabilidades con Metasploit.