

Chuleta de comandos de Nmap

Los comandos de uso diario, agrupados por tarea. Cambia `scanme.nmap.org` o el rango de ejemplo por tus propios objetivos.

Escanea solo redes y equipos que sean tuyos o para los que tengas permiso por escrito. Para practicar, usa `scanme.nmap.org` (unos pocos escaneos al día) o `127.0.0.1`.

Escaneos básicos y objetivos

Comando	Qué hace
<code>nmap --version</code>	Muestra la versión de Nmap instalada.
<code>nmap scanme.nmap.org</code>	Escaneo por defecto: los 1.000 puertos TCP más comunes.
<code>nmap 127.0.0.1</code>	Escanea tu propio equipo.
<code>nmap 192.168.1.10 192.168.1.20</code>	Escanea varias direcciones.
<code>nmap 192.168.1.0/24</code>	Escanea una red entera en notación CIDR.
<code>nmap 192.168.1.1-50</code>	Escanea un rango de direcciones.
<code>nmap -iL objetivos.txt</code>	Lee los objetivos desde un archivo, uno por línea.
<code>nmap 192.168.1.0/24 --exclude 192.168.1.1</code>	Escanea la red excepto la dirección indicada.
<code>nmap -v scanme.nmap.org</code>	Muestra más detalle durante el escaneo (-vv para aún más).

Descubrimiento de equipos y puertos

Comando	Qué hace
<code>nmap -sn 192.168.1.0/24</code>	Descubre qué equipos están encendidos, sin escanear puertos.
<code>nmap -Pn 192.168.1.10</code>	Se salta la comprobación de equipo encendido y escanea igual.
<code>nmap -n 192.168.1.0/24</code>	No resuelve nombres DNS (va más rápido).
<code>nmap -p 22 scanme.nmap.org</code>	Escanea un puerto.
<code>nmap -p 22,80,443 scanme.nmap.org</code>	Escanea una lista de puertos.
<code>nmap -p 1-1024 scanme.nmap.org</code>	Escanea un rango de puertos.
<code>nmap -p- 127.0.0.1</code>	Escanea los 65.535 puertos TCP.
<code>nmap -F scanme.nmap.org</code>	Modo rápido: los 100 puertos más comunes.
<code>nmap --top-ports 200 scanme.nmap.org</code>	Los N puertos más comunes.
<code>sudo nmap -sS scanme.nmap.org</code>	Escaneo SYN (necesita privilegios).
<code>nmap -sT scanme.nmap.org</code>	Escaneo connect (sin privilegios).
<code>sudo nmap -sU -p 53,161 192.168.1.1</code>	Escaneo UDP de puertos concretos.
<code>nmap --open scanme.nmap.org</code>	Muestra solo los puertos abiertos.
<code>nmap --reason scanme.nmap.org</code>	Explica por qué cada puerto tiene su estado.
<code>nmap -T4 scanme.nmap.org</code>	Plantilla de tiempo rápida, para redes propias.

Servicios, sistema operativo, scripts y salida

Comando	Qué hace
<code>nmap -sV scanme.nmap.org</code>	Detecta el programa y la versión de cada servicio.
<code>sudo nmap -O 192.168.1.10</code>	Estima el sistema operativo (necesita privilegios).
<code>sudo nmap -A scanme.nmap.org</code>	Sistema operativo, versiones, scripts por defecto y traceroute.
<code>nmap -sC scanme.nmap.org</code>	Ejecuta los scripts NSE por defecto.
<code>nmap -sV --script vuln 127.0.0.1</code>	Busca vulnerabilidades conocidas en tu equipo.
<code>nmap --script safe 127.0.0.1</code>	Ejecuta solo scripts de la categoría segura.
<code>nmap --script-help vuln</code>	Describe los scripts sin ejecutarlos.
<code>nmap -oN resultado.txt scanme.nmap.org</code>	Guarda en formato normal.
<code>nmap -oX resultado.xml scanme.nmap.org</code>	Guarda en XML.
<code>nmap -oA resultado scanme.nmap.org</code>	Guarda en .nmap, .xml y .gnmap a la vez.