REFERENCIA RÁPIDA DE NMAP

Escaneo de puertos, descubrimiento de hosts, detección de servicios y scripts NSE

Escaneos básicos

Objetivos del escaneo

```
nmap 192.168.1.1              # single host
nmap 192.168.1.0/24           # entire subnet
nmap 192.168.1.1-50           # IP range
nmap -iL targets.txt          # hosts from file
```

Especificación de objetivos

`192.168.1.1`	Dirección IP individual
`192.168.1.0/24`	Notación CIDR (256 hosts)
`192.168.1.1-254`	Rango de IPs
`example.com`	Nombre de host (resuelto a IP)
`-iL file.txt`	Leer objetivos desde archivo
`--exclude 192.168.1.1`	Excluir hosts específicos
`--excludefile skip.txt`	Excluir hosts desde archivo

Escaneo de puertos

Tipos de escaneo

`-sS`	Escaneo TCP SYN (por defecto, sigiloso, requiere root)
`-sT`	Escaneo TCP connect (handshake completo, sin root)
`-sU`	Escaneo UDP (lento, frecuentemente filtrado)
`-sA`	Escaneo TCP ACK (detectar firewalls)
`-sN`	Escaneo TCP NULL (sin flags)
`-sF`	Escaneo TCP FIN (solo flag FIN)
`-sX`	Escaneo Xmas (flags FIN+PSH+URG)

Selección de puertos

```
nmap -p 80,443 target         # specific ports
nmap -p 1-1000 target         # port range
nmap -p- target               # all 65535 ports
nmap --top-ports 100 target   # most common 100 ports
```

Estados de puerto

`open`	La aplicación acepta conexiones
`closed`	Puerto accesible pero sin servicio
`filtered`	Firewall bloqueando, no se puede determinar estado
`unfiltered`	Puerto accesible, abierto/cerrado desconocido
`open|filtered`	No se puede determinar si abierto o filtrado

Descubrimiento de hosts

Métodos de descubrimiento

`-sn`	Solo escaneo de ping (sin escaneo de puertos)
`-Pn`	Omitir descubrimiento (tratar todos como activos)
`-PS 80,443`	Descubrimiento TCP SYN en puertos
`-PA 80`	Descubrimiento TCP ACK
`-PU 53`	Descubrimiento UDP
`-PE`	Petición de echo ICMP
`-PR`	Descubrimiento ARP (red local)

Barrido de red

```
nmap -sn 192.168.1.0/24       # ping sweep subnet
nmap -sn -n 10.0.0.0/24       # sweep, skip DNS
nmap -sn -PR 192.168.1.0/24   # ARP scan (fastest)
```

Detección de servicios

Detección de versiones

```
nmap -sV target               # detect service versions
nmap -sV --version-intensity 5 target  # deeper probing
nmap -sV --version-all target  # try every probe (slow)
nmap -A target                 # OS + version + scripts + traceroute
```

Flags de servicio

`-sV`	Sondear puertos abiertos para servicio/versión
`--version-intensity 0-9`	Intensidad de sondeo (7 por defecto)
`--version-light`	Sondeo ligero (intensidad 2)
`--version-all`	Probar todas las sondas (intensidad 9)
`-A`	Agresivo: -sV -O --script=default -traceroute
`-sC`	Ejecutar scripts NSE por defecto

Detección de SO

Fingerprinting de SO

```
nmap -O target                # OS detection (needs root)
nmap -O --osscan-limit target # only scan promising hosts
nmap -O --osscan-guess target # aggressive OS guessing
nmap -A target                # includes OS detection
```

Flags de detección de SO

`-O`	Habilitar detección de SO
`--osscan-limit`	Omitir hosts sin puertos TCP abiertos+cerrados
`--osscan-guess`	Adivinar SO de forma más agresiva
`--max-os-tries N`	Máximo de intentos de detección de SO por host

Scripts (NSE)

Uso de scripts

```
nmap --script=default target   # default category
nmap --script=vuln target      # vulnerability scripts
nmap --script=http-headers target
nmap --script="http-*" target  # wildcard match
```

Categorías de scripts

`default`	Scripts seguros y útiles (atajo -sC)
`vuln`	Verificar vulnerabilidades conocidas
`safe`	Scripts no intrusivos
`intrusive`	Puede crashear objetivos o activar IDS
`discovery`	Descubrimiento de red y servicios
`auth`	Verificaciones de autenticación
`brute`	Prueba de credenciales por fuerza bruta
`exploit`	Intentos de explotación activa

Scripts útiles

`http-title`	Obtener títulos de páginas web
`ssl-cert`	Mostrar detalles del certificado SSL
`ssh-hostkey`	Mostrar huellas de clave de host SSH
`dns-brute`	Enumerar subdominios DNS
`smb-os-discovery`	Detectar SO Windows via SMB
`vuln`	Ejecutar todas las verificaciones de vulnerabilidades

Formatos de salida

Opciones de salida

```
nmap -oN scan.txt target      # normal text output
nmap -oX scan.xml target      # XML output
nmap -oG scan.gnmap target    # grepable output
nmap -oA scan_all target      # all formats at once
```

Flags de salida

`-oN file`	Salida normal a archivo
`-oX file`	Salida XML (para herramientas/parsing)
`-oG file`	Salida grepable (un host por línea)
`-oA basename`	Los tres formatos (basename.nmap/xml/gnmap)
`-v`	Aumentar verbosidad (-vv para más)
`-d`	Salida de depuración (-dd para más)
`--open`	Mostrar solo puertos abiertos
`--reason`	Mostrar razón del estado del puerto

Temporización y rendimiento

Plantillas de temporización

`-T0 (paranoid)`	Muy lento, evasión de IDS (5 min entre sondas)
`-T1 (sneaky)`	Lento, evasión de IDS (15 seg entre sondas)
`-T2 (polite)`	Velocidad reducida, menos ancho de banda
`-T3 (normal)`	Temporización por defecto
`-T4 (aggressive)`	Rápido, asume red confiable
`-T5 (insane)`	Más rápido, puede perder resultados

Ajuste fino

`--min-rate 1000`	Enviar al menos 1000 paquetes/seg
`--max-rate 500`	Limitar a 500 paquetes/seg
`--max-retries 2`	Máximo de retransmisiones de sonda
`--host-timeout 30m`	Omitir host si el escaneo supera 30 min
`--scan-delay 1s`	Retraso entre sondas
`--min-parallelism 10`	Mínimo de grupos de sondas en paralelo

Evasión de firewall

Técnicas de evasión

`-f`	Fragmentar paquetes (trozos de 8 bytes)
`-D RND:5`	Escaneo señuelo con 5 IPs aleatorias
`-S spoof_ip`	Falsificar IP de origen (requiere paquetes raw)
`-e eth0`	Usar interfaz de red específica
`--source-port 53`	Usar puerto de origen específico (p. ej. DNS)
`--data-length 25`	Agregar datos aleatorios a los paquetes
`--spoof-mac 0`	Aleatorizar dirección MAC

Ejemplos de evasión

```
nmap -f -D RND:3 target       # fragments + decoys
nmap --source-port 53 target  # DNS port (often allowed)
nmap -T1 --scan-delay 5s target  # slow to evade IDS
```

Patrones comunes

Reconocimiento rápido

```
nmap -T4 -F target            # fast common ports
nmap -T4 -A -v target         # OS + service detection
nmap -sV --top-ports 1000 target  # top 1000 + versions
```

Escaneo exhaustivo

```
# Full TCP + service + OS + scripts
nmap -sS -sV -O -sC -p- -T4 -oA full target
# UDP scan on common ports
nmap -sU --top-ports 50 target
```

Auditoría de servidor web

```
nmap -p 80,443 --script=http-title,http-headers,\
ssl-cert,http-methods target
# Check for open proxies and vulns
nmap -p 80,443,8080 --script=http-open-proxy,vuln target
```

Inventario de red

```
# Discover all live hosts with OS info
nmap -sn 192.168.1.0/24 -oG - | grep "Up"
# Service inventory for subnet
nmap -sV -T4 192.168.1.0/24 -oX inventory.xml
```