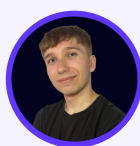


Domina Nmap

Aprende sus comandos clave para pentesting

Descubrimiento de hosts

Parámetro	Ejemplo	Descripción
-sn	nmap -sn 192.168.1.1/24	Descubrimiento de hosts sin escanear puertos
-Pn	nmap -Pn 192.168.1.10	Trata al host como activo aunque no responda a ICMP
-PE	nmap -PE 192.168.1.10	Descubrimiento usando ICMP Echo Request
-PS	nmap -PS22,80 192.168.1.10	Descubrimiento mediante TCP SYN en puertos específicos
-PA	nmap -PA80 192.168.1.10	Descubrimiento mediante paquetes TCP ACK
-PU	nmap -PU53,161 192.168.1.10	Descubrimiento usando paquetes UDP



Saúl Ruiz Plaza
PlaSysX



Escaneo de Puertos

Parámetro	Ejemplo	Descripción
-p-	nmap -p- 192.168.1.10	Escanea todos los puertos (1-65535)
-p	nmap -p 80 192.168.1.10	Escanea un puerto específico
-p rango	nmap -p 1-1000 192.168.1.10	Escanea un rango de puertos
-F	nmap -F 192.168.1.10	Escaneo rápido de los 100 puertos más comunes
-sS	nmap -sS 192.168.1.10	Escaneo SYN (más sigiloso)
-sT	nmap -sT 192.168.1.10	Escaneo TCP completo
-sU	nmap -sU 192.168.1.10	Escaneo de puertos UDP
-sA	nmap -sA 192.168.1.10	Detecta si un puerto está filtrado



Detección de servicios y sistema

Parámetro	Ejemplo	Descripción
-sV	<code>nmap -sV 192.168.1.10</code>	Detecta versiones de servicios
-O	<code>nmap -O 192.168.1.10</code>	Detecta el sistema operativo
--osscan-guess	<code>nmap --osscan-guess 192.168.1.10</code>	Fuerza detección agresiva de SO
-A	<code>nmap -A 192.168.1.10</code>	Escaneo completo (SO + versión + scripts + traceroute)



NSE (Scripts)

Parámetro	Ejemplo	Descripción
-sC	<code>nmap -sC 192.168.1.10</code>	Ejecuta scripts básicos de enumeración
--script	<code>nmap --script=http-title 192.168.1.10</code>	Ejecuta un script específico
--script-help	<code>nmap --script-help=http-title</code>	Muestra información del script
--script-args	<code>nmap --script=smb-enum-shares --script-args smbusername=admin,smbpassword=pass 192.168.1.10</code>	Pasa argumentos a scripts

ls -la /usr/share/nmap/scripts para ver los scripts disponibles



Evación y Bypass

Parámetro	Ejemplo	Descripción
-f	nmap -f 192.168.1.10	Fragmenta paquetes. Muy utilizado para evadir firewalls
--mtu	nmap --mtu 8 192.168.1.10	Define tamaño de fragmentación (Unidad Máxima de Transmisión)
-D	nmap -D 192.168.1.1,ME 192.168.1.10	Usa decoy para ocultar IP origen (ME)
-g	nmap -g 53 192.168.1.10	Define puerto origen
--data-length	nmap --data-length 192.168.1.10	Define el tamaño del paquete



Rendimiento

Parámetro	Ejemplo	Descripción
-T0 a -T5	nmap -T4 192.168.1.10	Ajusta velocidad del escaneo. Mayor velocidad = Mayor agresividad + Más detectable
-v	nmap -v 192.168.1.10	Muestra más información
--host-timeout	nmap --host-timeout 30m 192.168.1.10	Limita tiempo por host
--min-rate	nmap --min-rate 1000 192.168.1.10	Establece el mínimo de paquetes enviados por segundo para acelerar el escaneo

Guardado de Resultados

Parámetro	Ejemplo	Descripción
-oN	nmap -oN resultado.txt 192.168.1.10	Guarda salida en texto
-oX	nmap -oX resultado.xml 192.168.1.10	Guarda en XML
-oG	nmap -oG resultado.txt 192.168.1.10	Formato grepable (comando grep)
-oA	nmap -oA resultado 192.168.1.10	Guarda en todos los formatos



Estado de Puertos

Estado	Descripción
open	Puerto abierto
closed	Puerto cerrado
filtered	Filtrado por firewall



Combos Recomendados

“

Nota importante: en entornos Windows es común que ICMP esté bloqueado, por lo que -sn puede no detectar hosts activos. En estos casos se recomienda complementar con TCP/UDP ping (-PS, -PA, -PU) o usar -Pn.

”

Comando	Descripción
nmap -sn -T4 192.168.1.0/24	Descubrimiento rápido de hosts activos en redes donde ICMP responde
nmap -PS22,80,445 -PA80,445 -PU53 -T4 192.168.1.0/24	Descubrimiento más fiable en entornos Windows (ICMP filtrado)
nmap -Pn -T4 192.168.1.10	Trata el host como activo (útil cuando -sn no detecta máquinas Windows)
nmap -p- -sS -T4 -Pn 192.168.1.10	Escaneo completo (SO + versión + scripts)
nmap -sS -sV -sC -O -T4 -Pn 192.168.1.10	Enumeración profesional completa (puertos, , enumeración de servicios, versiones, SO)
nmap -A -T4 -Pn 192.168.1.10	Escaneo agresivo todo en uno (reconocimiento completo automatizado)
nmap -p80,443,8080,8000 -sV --script=http-title,http-headers -T4 192.168.1.10	Enumeración de servicios web y obtención de información relevante
nmap -sC -sV -p- --script=vuln -T4 192.168.1.10	Enumeración de servicios y versiones con vulnerabilidades conocidas
nmap -p445 -sV --script=smb-os-discovery,smb-enum-shares,smb-enum-users -T4 192.168.1.10	Enumeración SMB en entornos Windows (shares, usuarios, SO)
nmap -sU -p 53,67,68,69,123,161 192.168.1.10	Escaneo UDP de servicios críticos



Saúl Ruiz Plaza

PlaSysX