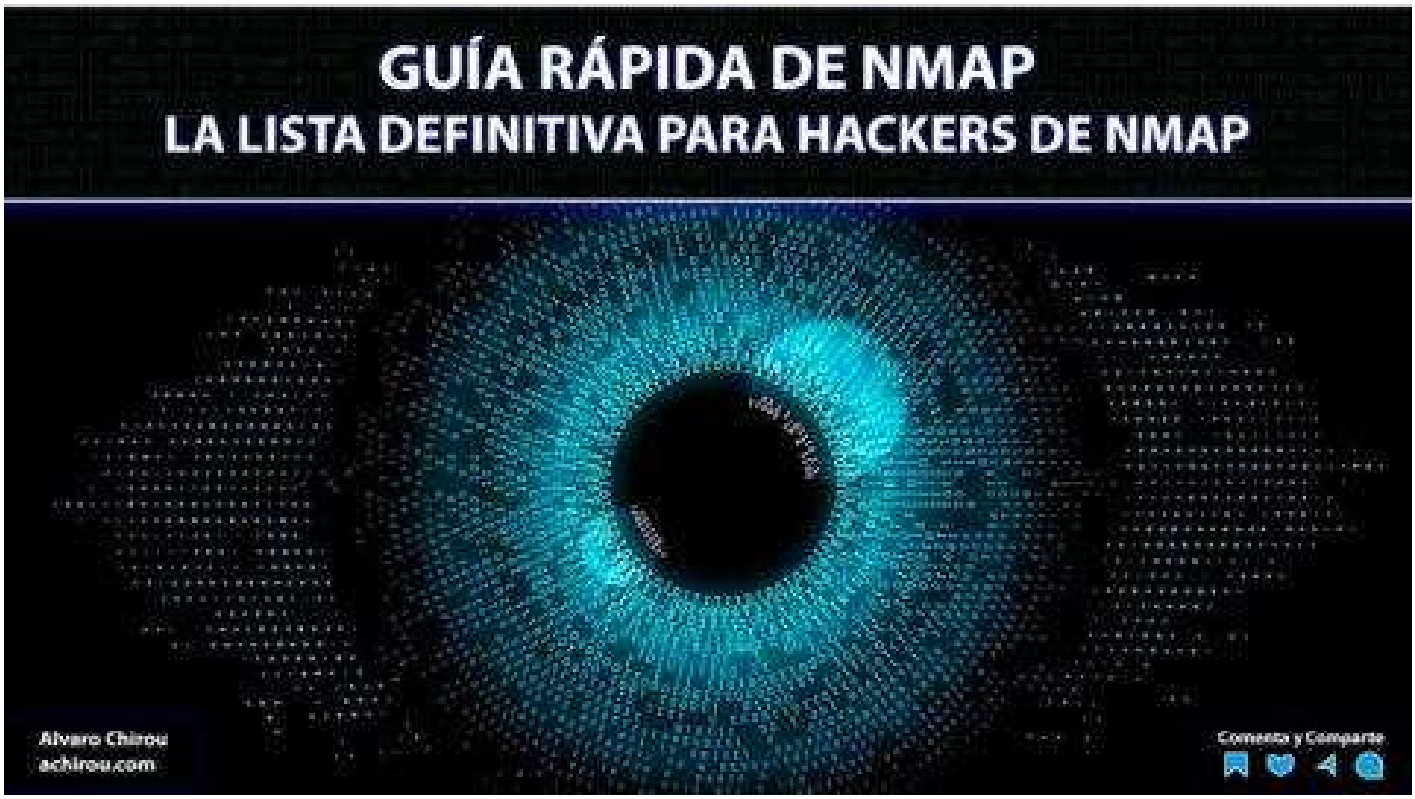
Guía Rápida de NMAP – La lista definitiva para hackers de NMAP

por Carlos Laprovittera | Dic 22, 2023 | Hacking | 0 Comentarios



Como hacker ético, NMAP se convierte en tu aliado estratégico. Este artículo te llevará a través de sus funcionalidades, tácticas avanzadas y te proporcionará la destreza necesaria para potenciar tu habilidad en la evaluación de redes y sistemas.

La única desventaja de una herramienta tan robusta y poderosa como Nmap es recordar tantos comandos. Incluso muchos profesionales experimentados de la industria no logran aprovechar Nmap al máximo simplemente porque mantener un registro de todas sus banderas puede resultar todo un desafío.

Table of Contents

Hemos compilado y organizado esta hoja de trucos de Nmap para ayudarlo a dominar lo que posiblemente sea la herramienta más útil en el arsenal de cualquier evaluador de penetración. Ya sea que lo use para memorizar las opciones de Nmap, como referencia rápida para tener cerca o como hoja de estudio para su examen CEH/Pentest+, estamos seguros de que lo ayudará a convertirse en un profesional de Nmap.

Especificación de destino

CAMBIAR	EJEMPLO	DESCRIPCIÓN
	nmap 192.168.1.1	Escanea una sola IP
	nmap 192.168.1.1 192.168.2.1	Escanear IP específicas
	nmap 192.168.1.1-254	Escanear un rango
	nmap scanme.nmap.org	Escanear un dominio
	nmap 192.168.1.0/24	Escanear usando notación CIDR
-Illinois	nmap -iL targets.txt	Escanear objetivos desde un arch
-ir	nmap -iR 100	Escanea 100 hosts aleatorios
-excluir	nmap -exclude 192.168.1.1	Excluir hosts listados

Técnicas de escaneo de Nmap

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-SS	nmap 192.168.1.1 -sS	Exploración del puerto TCP SYN (predeterminado)
-calle	nmap 192.168.1.1 -st	Exploración del puerto de conexión TCP (predetermi privilegios de root)
-su	nmap 192.168.1.1 -sU	escaneo de puertos UDP
-sa	nmap 192.168.1.1 -	Escaneo de puerto TCP ACK

CAMBIAR	EJEMPLO	DESCRIPCIÓN
	sA	
-sudoeste	nmap 192.168.1.1 -sW	Escaneo de puerto de ventana TCP
-sM	nmap 192.168.1.1 -sM	Escaneo del puerto TCP Maimon

Descubrimiento de host

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-sL	nmap 192.168.1.1-3 -sL	Sin escaneo. Listar solo objetivos
-sn	nmap 192.168.1.1/24 -sn	Deshabilite el escaneo de puertos. Solo descubrimiento de host.
-Pn	nmapn 192.168.1.1-5 -Pn	Deshabilite el descubrimiento de host. S escaneo de puertos.
-PD	nmap 192.168.1.1-5 -PS22-25,80	Descubrimiento TCP SYN en el puerto Puerto 80 por defecto
-PENSILVANIA	nmap 192.168.1.1-5 -PA22-25,80	Descubrimiento de TCP ACK en el puer Puerto 80 por defecto
-PU	nmap 192.168.1.1-5 -PU53	Descubrimiento de UDP en el puerto x. Puerto 40125 por defecto
-PR	nmap 192.168.1.1-1/24 -PR	Descubrimiento de ARP en la red local
-norte	nmap 192.168.1.1 -n	Nunca hagas resolución DNS

Especificación del puerto

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-pag	nmap 192.168.1.1 -p 21	Escaneo de puertos para el puerto x
-pag	nmap 192.168.1.1 -p 21-100	Rango de puertos
-pag	nmap 192.168.1.1 -p U:53,T:21-25,80	Escaneo de puertos múltiples puertos TC
-pag	nmap 192.168.1.1 -p-	Escanear todos los puertos
-pag	nmap 192.168.1.1 -p http,https	Escaneo de puertos desde el nombre del
-F	nmap 192.168.1.1 -F	Escaneo rápido de puertos (100 puertos)
-puertos-superiores	nmap 192.168.1.1 -top-ports 2000Copied	Escaneo de puertos en los x puertos sup

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-p-65535	nmap 192.168.1.1 -p-65535	Dejar fuera el puerto inicial dentro del rar que el escaneo comience en el puerto 1
-p0-	nmap 192.168.1.1 -p0-	Dejar el puerto final dentro del alcance ha el escaneo pase al puerto 65535

Detección de servicio y versión

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-sV	nmap 192.168.1.1 -sV	Intenta determinar la versión del servicio ejecuta en el puerto.
-sV -versión-intensidad	nmap 192.168.1.1 -sV -version-intensity 8	Nivel de intensidad de 0 a 9. Un número r aumenta la posibilidad de corrección
-sV -versión-luz	nmap 192.168.1.1 -sV -version-light	Habilita el modo de luz. Menor posibilidad corrección. Más rápido
-sV -versión-todo	nmap 192.168.1.1 -sV -version-all	Habilitar nivel de intensidad 9. Mayor posi de corrección. Más lento
-A	nmap 192.168.1.1 -A	Permite la detección de sistema operativo detección de versiones, escaneo de script traceroute.

Detección del sistema operativo

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-O	nmap 192.168.1.1 -O	Detección remota del sistema operativo mediant dactilares de pila TCP/IP
-O -osscan-límite	nmap 192.168.1.1 -O -osscan-limit	Si no se encuentran al menos un puerto TCP abi uno cerrado, no intentará la detección del sistem operativo en el host.
-O -osscan-guess	nmap 192.168.1.1 -O -osscan-guess	Hace que Nmap adivine de forma más agresiva
-O -max-os-tries	nmap 192.168.1.1 -O -max-os-tries 1	Establecer el número máximo x de intentos de d del sistema operativo contra un objetivo
-A	nmap 192.168.1.1 -A	Permite la detección de sistema operativo, detec versiones, escaneo de scripts y traceroute.

Tiempo y rendimiento

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-T0	nmap 192.168.1.1 -T0	Paranoico (0) Evasión del sistema de detección de intru
-T1	nmap 192.168.1.1 -T1	Evasión furtiva del sistema de detección de intrusos (1)
-T2	nmap 192.168.1.1 -T2	Cortés (2) ralentiza el análisis para utilizar menos ancho banda y menos recursos de la máquina de destino
-T3	nmap 92.168.1.1 -T3	Normal (3) que es la velocidad predeterminada
-T4	nmap 192.168.1.1 -T4	Exploraciones de velocidades agresivas (4); asume que en una red razonablemente rápida y confiable
-T5	nmap 192.168.1.1 -T5	Loco (5) velocidades de escaneo; asume que estás en muyrápida

Interruptores de sincronización y rendimiento

CAMBIAR	ENTRADA DE EJEMPLO	DESCRIPCIÓN
-host-timeout	1s; 4m; 2h	Renuncia al objetivo después de tar tiempo.
-min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout	1s; 4m; 2h	Especifica el tiempo de ida y vuelta sonda.
-min-hostgroup/max-hostgroup	50; 1024	Tamaños de grupos de exploración paralelos
-min-parallelism/max-parallelism	10; 1	Paralelización de sondas
-max-retries	3	Especificar el número máximo de retransmisiones de sondas de escar puertos
-min-rate	100	Enviar paquetes a una velocidad no <número> por segundo
-max-rate	100	Enviar paquetes a una velocidad no a <número> por segundo

Guiones NSE

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-sC	nmap 192.168.1.1 -sC	Escanee con scripts NSE predeterminados. Se considera el descubrimiento y seguro.

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-script default	nmap 192.168.1.1 -script default	Escanee con scripts NSE predeterminados. Se considera u el descubrimiento y seguro.
-script	nmap 192.168.1.1 -script=banner	Escanee con un solo script. Ban ejemplo
–script	nmap 192.168.1.1 -script=http*	Escanee con un comodín. Ejemp
-script	nmap 192.168.1.1 -script=http,banner	Escanee con dos guiones. Ejem banner
-script	nmap 192.168.1.1 -script «not intrusive»	Escanee de forma predetermina elimine los scripts intrusivos
-script-args	nmap -script snmp-sysdescr -script-args snmpcommunity=admin 192.168.1.1	Script NSE con argumentos

Ejemplos útiles de scripts NSE

DOMINIO	DESCRIPCIÓN
nmap -Pn -script=http-sitemap-generator scanme.nmap.org	generador de mapas del sit
nmap -n -Pn -p 80 -open -sV -vvv -script banner,http-title -iR 1000	Búsqueda rápida de servido aleatorios
nmap -Pn -script=dns-brute dominio.com	Fuerzas brutas nombres de DNS adivinando subdomini
nmap -n -Pn -vv -O -sV -script smb-enum*,smb-ls,smb-mbenum,smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv 192.168.1.1	Scripts SMB seguros para e
nmap -script whois* dominio.com	consulta whois
nmap -p80 -script http-unsafe-output-escaping scanme.nmap.org	Detectar vulnerabilidades d secuencias de comandos e sitios
nmap -p80 -script http-sql-injection scanme.nmap.org	Comprobar inyecciones SQ

Firewall / Evasión y suplantación de identidad (IDS)

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-F	nmap 192.168.1.1 -f	Los análisis solicitados (in los análisis de utilizan peque paquetes IP fragmentados

CAMBIAR	EJEMPLO	DESCRIPCIÓN
		difícil para los de paquetes
-mtu	nmap 192.168.1.1 -mtu 32	Establece tu tamaño de compensació
-D	nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1	Enviar escane desde IP falsi
-D	nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip	Ejemplo ante explicado
-S	nmap -S www.microsoft.com www.facebook.com	Escanee Fac desde Micros posible que s requiera -e et
-g	nmap -g 53 192.168.1.1	Utilice el núm puerto de orig proporcionad
-proxies	nmap -proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1	Retransmitir conexiones a de servidores HTTP/SOCK
-data-length	nmap -data-length 200 192.168.1.1	Agrega datos aleatorios a lo paquetes env

Ejemplo de comando de evasión IDS

nmap -f -t 0 -n -Pn –longitud-datos 200 -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1

Producción

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-en	nmap 192.168.1.1 -oN normal.file	Salida normal al archivo normal.file
-oX	nmap 192.168.1.1 -oX xml.file	Salida XML al archivo xml.file
-oG	nmap 192.168.1.1 -oG grep.file	Salida grepable al archivo grep.file
-oA	nmap 192.168.1.1 -oA results	Salida en los tres formatos principales a la
-oG-	mapa nm 192.168.1.1 -oG –	Salida Grepable a la pantalla. -oN -, -oX – ta utilizable

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-append-output	nmap 192.168.1.1 -oN file.file -append-output	Agregar un escaneo a un archivo de escane anterior
-v	nmap 192.168.1.1 -v	Aumente el nivel de detalle (use -vv o más p obtener un mayor efecto)
-d	nmap 192.168.1.1 -d	Aumentar el nivel de depuración (use -dd o para un mayor efecto)
-reason	nmap 192.168.1.1 -reason	Muestra el motivo por el que un puerto se e en un estado particular, el mismo resultado
-open	nmap 192.168.1.1 -open	Mostrar solo puertos abiertos (o posiblemer abiertos)
-packet-trace	nmap 192.168.1.1 -T4 -packet-trace	Mostrar todos los paquetes enviados y recib
-iflist	nmap -iflist	Muestra las interfaces y rutas del host.
-resume	nmap -resume results.file	Reanudar un escaneo

Ejemplos útiles de salida de Nmap

DOMINIO	DESCRIPCIÓN
nmap -p80 -sV -oG – -open 192.168.1.1/24 | grep open	Busque servidores web y grep para mostra están ejecutando servidores web
nmap -iR 10 -n -oX out.xml | grep «Nmap» | cut -d » » -f5 > live-hosts.txt	Generar una lista de las IP de los hosts er
nmap -iR 10 -n -oX out2.xml | grep «Nmap» | cut -d » » -f5 >> live-hosts.txt	Agregar IP a la lista de hosts en vivo
ndiff scanl.xml scan2.xml	Comparar la salida de nmap usando ndif
xsltproc nmap.xml -o nmap.html	Convertir archivos nmap xml a archivos ht
grep » open » results.nmap | sed -r ‘s/ +/ /g’ | sort | uniq -c | sort -rn | less	Lista ordenada inversa de la frecuencia co aparecen los puertos

Banderas varias de Nmap

CAMBIAR	EJEMPLO	DESCRIPCIÓN
-6	nmap -6 2607:f0d0:1002:51::4	Habilitar el escaneo IPv6
-h	nmap -h	pantalla de ayuda de nmap

Otros comandos útiles de Nmap

DOMINIO	DESCRIPCIÓN
nmap -iR 10 -PS22-25,80,113,1050,35000 -v -sn	Descubrimiento solo en los puertos x, sin escaneo d puertos
nmap 192.168.1.1-1/24 -PR -sn -vv	Descubrimiento de Arp solo en la red local, sin esca puertos
nmap -iR 10 -sn -traceroute	Traceroute a objetivos aleatorios, sin escaneo de pu
nmap 192.168.1.1-50 -sL -dns-server 192.168.1.1	Consultar el DNS interno para hosts, enumerar solo
nmap 192.168.1.1 –packet-trace	Muestre los detalles de los paquetes que se envían durante un escaneo y capture el tráfico.

Nmap es la primera herramienta que utilizará en la etapa de escaneo y enumeración de muchas evaluaciones, sentando las bases para el resto de su pentest. Al concluir esta guía rápida de NMAP, te has armado con conocimientos cruciales para enfrentar cualquier desafío en el ámbito de la ciberseguridad. La maestría en el uso de NMAP te proporcionará la capacidad de explorar y asegurar redes con precisión, consolidando tu posición como un experto en ciberseguridad.