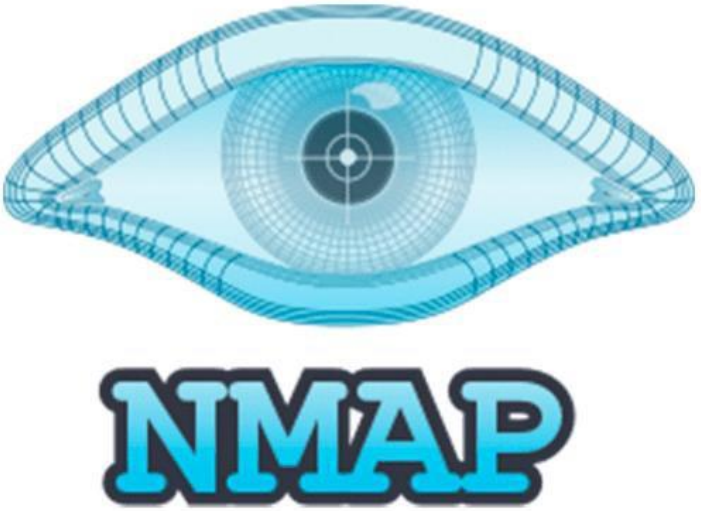
MANUAL DE COMANDOS NMAP



WEB: https://elhackeretico.com/

EL HACKER ETICO

Contenido

NMAP – TÉCNICAS BÁSICAS DE ESCANEO

Escaneo TCP SYN – Requiere privilegios root

Sintaxis del comando	sudo nmap –sS <target_IP / hostname>
Ejemplos de comandos	**sudo nmap –sS scanme.nmap.org** **sudo nmap –sS 192.168.1.1** **sudo nmap –sS 192.168.56.100-110 (escanea todas las IP en el rango 100-110)**
Escanear puertos seleccionados	**sudo nmap –sS –p <port_no.> <target_IP_address / hostname>** **sudo nmap –sS –p 80 scanme.nmap.org** **sudo nmap –sS –p 80,22,25,443 192.168.56.103** **sudo nmap –sS –p 1-500 192.168.56.103**

Escaneo Conexión TCP – No requiere privilegios root

Sintaxis del comando	nmap <target_IP_address / hostname> nmap –sT <target_IP_address / hostname>
Ejemplos de comandos	**nmap scanme.nmap.org** **nmap 192.168.56.103** **nmap 192.168.56.100-110 (escanea todas las IP en el rango 100-110)**
Escanear puertos seleccionados	**nmap –p <port_no.> <target_IP_address / hostname>** **nmap –p 80 scanme.nmap.org** **nmap –p 80,22,25,443 192.168.56.103** **nmap –p 1-500 192.168.56.103**

Escaneo FIN, NULL & XMAS - Requiere privilegios root

Sintaxis del comando	sudo nmap -sF <target_IP_address /hostname> -- ESCANEO FIN sudo nmap -sN <target_IP_address /hostname> -- ESCANEO NULL sudo nmap -sX <target_IP_address /hostname> -- ESCANEO XMAS
Ejemplos de comando	sudo nmap -sF scanme.nmap.orgsudo nmap -sN 192.168.56.103 sudo nmap -sX 192.168.56.100-110 (Escanealas direcciones IP entre 192.168.56.100 - 192.168.56.110)
Escanear puertos seleccionados	sudo nmap -sN –p <port_no.> <target_IP_address / hostname> nmap –sX –p 80 scanme.nmap.org nmap -sF –p 80,22,25,443 192.168.56.103 nmap -sN –p 1-500 192.168.56.103

Escaneo UDP - Requiere privilegios root

Sintaxis del comando	sudo nmap –sU <target_IP/Hostname>
Ejemplos de comando	sudo nmap –sU 192.168.56.103 sudo nmap –sU scanme.nmap.org
Escanear puertos seleccionados	sudo nmap -sN –p <port_no.> <sudo nmap –sU –p161 192.168.56.103 sudo nmap –sU –p161,53 scanme.nmap.org

Escaneo SCTP INIT – Requiere privilegios root

Sintaxis del comando	sudo nmap –sY <target_IP/Hostname>
Ejemplos de comando	sudo nmap –sY 192.168.56.103 sudo nmap –sY scanme.nmap.org

Más tipos de escaneos con NMAP

Nombre	¿Requiere privilegios elevados?	Comando	Sintaxis
Escaneo SCTP INIT	SI	-sY	sudo nmap –sY <target_IP/hostname> sudo nmap –sY scanme.nmap.org

Escaneo ACK	**SI**	**-sA**	**sudo nmap –sA <target_IP/hostname> sudo nmap –sA scanme.nmap.org NOTA: Para obtener más información de este escaneo, utilizar - -reason.**
Escaneo Maimon	**SI**	**-sM**	**sudo nmap –sM < target_IP/hostname > sudo nmap –sM scanme.nmap.org NOTA: Para obtener más información de este escaneo, utilizar - -reason.**
Escaneo de protocolo IP	**SI**	**-sO**	**sudo nmap –sO < target_IP/hostname > sudo nmap –sO scanme.nmap.org sudo nmap –sO –p25 scanme.nmap.org**

NMAP - VERSIÓN DE SERVICIO Y HUELLAS DACTILARES DELSISTEMA OPERATIVO

Detección de servicio

Sintaxis del comando	**nmap –sV <target_IP_address / hostname>**
Ejemplos de comando	**nmap –sV scanme.nmap.org nmap –sV 192.168.56.103**
Escanear puertos seleccionados	**nmap –sV –p <port_no.> <target_IP_address /hostname> nmap –sV –p 80 scanme.nmap.org**

Otros parámetros de detección

Nombre	¿Requiere privilegios elevados?	Comando	Sintaxis
All ports	**NO**	**--allports**	**nmap –sV --allports <target_IP / Hostname>**
Versión intensity	**NO**	**-- version-intensity**	**nmap –sV --version-intensity <#> <target_IP /Hostname> nmap –sV --version-intensity 5 scanme.nmap.org nmap –sV --version-intensity 5 –p80 scanme.nmap.org**

Versión light	**NO**	**--version-light**	**nmap –sV --version-light <target_IP / Hostname> nmap –sV --version-light scanme.nmap.org nmap –sV --version-light –p80 scanme.nmap.org**
Versión all	**NO**	**--version-all**	**nmap –sV --version-all <target_IP / Hostname>eg. nmap –sV --version-all scanme.nmap.org nmap –sV --version-all –p80 scanme.nmap.org**
Versión trace	**NO**	**--versión -trace**	**nmap –sV --version-trace <target_IP / Hostname> nmap –sV --version-trace scanme.nmap.org nmap –sV --version-trace –p80 scanme.nmap.org**

DETECCIÓN DEL SISTEMA OPERATIVO

Sintaxis del comando	**sudo nmap –O <target_IP_address / hostname>**
Ejemplos de comando	**sudo nmap –O scanme.nmap.org**

Más comandos para la detección del sistema operativo

Nombre	¿Requiere privilegios elevados?	Comando	Sintaxis
Detección de Sistema Operativo	**SI**	**--osscan-guess --fuzzy**	**sudo nmap –O - -osscan-guess <target_IP / Hostname> sudo nmap –O - -fuzzy <target_IP / Hostname> sudo nmap –O - -osscan-guess scanme.nmap.org sudo nmap –O - -fuzzy scanme.nmap.org**
Número de intentos para detección de sistema operativo	**SI**	**--max-os-tries**	**sudo nmap –O - -max-os-tries <#><target_IP /Hostname> sudo nmap –O - -max-os-tries 2 scanme.nmap.org**

Opción agresiva	**NO**	**-A**	**nmap –A <target_IP/Hostname>** **nmap –A scanme.nmap.org Nmap –A –p80 scanme.nmap.org**

ESPECIFICACIÓN DE PUERTO A ESCANEAR

Opciones de especificación de puerto

Descripción	Comando	Sintaxis	Ejemplo de comando
Especificar un únicopuerto	**-p**	**nmap –p22 <target_IP/Hostname>**	**nmap –p22 scanme.nmap.org**
Especificar múltiples puertos		**nmap –p <n1,n2,n3….nm> <target_IP/Hostname>**	**nmap –p21,22,23,25,80 scanme.nmap.org**
Especificar un rango depuertos		**nmap –p<n1-nm> <target_IP/Hostname>**	**nmap –p10-100 scanme.nmap.org**
Especifique y escaneepuertos con múltiples protocolos (requiere elevado / root privilegios)		**sudo nmap –sS –sU –p T:<t1,t2,..tn>,U:<u1,u2,…un> <target_IP/Hostname>**	**sudo nmap –sS –sU –p T:21,22,25,80,U:53,161 scanme.nmap.org**
Especifique protocolos para escanear (requiereelevado / privilegios de root - Dependiendo de protocolos solicitados.)		**sudo nmap –sS –p <protocol_name> <target_IP/Hostname>**	**sudo nmap –sS –p ftp,ssh,telnet,http,https scanme.nmap.org**
Escaneo con límite superior de puertos		**nmap –p [-1024] <target_IP/Hostname>**	**nmap –p [-1024] scanme.nmap.org**
Escanea los 65535 en el sistema de destino	**-p-**	**nmap –p- <target_IP/Hostname>**	**nmap –p- scanme.nmap.org**
Excluyendo puertos únicos / múltiples de un escaneo.	**--exclude-ports**	**nmap - -exclude-ports <port_no> <target_IP/Hostname>**	**nmap - -exclude-ports 80 scanme.nmap.org** **nmap - -exclude-ports 1-100 scanme.nmap.org**
Escaneo rápido	**-F**	**nmap –F <target_IP/Hostname>**	**nmap –F scanme.nmap.org**
No aleatorización depuertos durante el escaneo.	**-r**	**nmap –r <target_IP/Hostname>**	**nmap –r scanme.nmap.org**

Escanea los puertos principales	**- -top-ports**	**nmap - -top-ports <n> <target_IP/Hostname>**	**nmap - -top-ports 50 scanme.nmap.org**

Escaneo por especificaciones de destino

Tipo de escaneo	Comando	Sintaxis	Ejemplo
Incluir objetivos en archivo	**-iL**	**nmap –iL <filename_with_targets_to_scan>**	**nmap –iL targets_in_scope.txt**
Excluir objetivos	**--excludefile**	**nmap --excludefile <filename_with_targets_to_exclude> <target_IP/Hostname>**	**nmap –excludefiledo_not_scan.txt 192.168.56.1/24**
	--exclude	**nmap --exclude <IP_address_to_exclude> <target_IP/Hostname/range>**	**nmap --exclude 192.168.56.100,192.168.56.101, 192.168.56.1/24**

NMAP – DESCUBRIMIENTO DE HOSTS ACTIVOS

Descripción	Comando	Sintexis	Ejemplo de uso
Lista de escaneo	**-sL**	**nmap –sL <target_network_range>**	**nmap –sL 192.168.56.1/24**
Escaneo de red	**-sn**	**nmap –sn <target_network_range>**	**nmap –sn 192.168.56.1/24**
Sin utilizar PIN	**-Pn**	**nmap –Pn <target_network_range>**	**nmap –sn 192.168.56.1/24**
TCP SYN Ping	**-PS**	**nmap –PS *<port_list> <target_network_range>**	**nmap –PS 192.168.56.1/24** **nmap –PS 21,22,25 192.168.56.1/24**
TCP ACK Ping	**-PA**	**nmap –PA *<port_list> <target_network_range>**	**nmap –PA 192.168.56.1/24** **nmap –PA 21,22,25 192.168.56.1/24** **nmap –PS –PA 192.168.56.1/24**
UDP Ping	**-PU**	**nmap –PU <target_network_range>**	**sudo nmap –PU 192.168.56.1/24**
ICMP Pings	**-PE** **-PP**	**nmap –PE (-PP, -PM) <target_network_range>**	**nmap –sn –PE 192.168.56.1/24** **nmap –sn –PP 192.168.56.1/24**

	-PM		nmap –sn –PM 192.168.56.1/24
Disable ARPPings	- -disable-arp-ping	nmap - -disable-arp-ping <target_network_range>	nmap –sn - -disable-arp-ping 192.168.56.1/24

NMAP – ESCANEO MEDIANTE EL USO DE SCRIPTS

Nombre de script	Categoría	Ejemplo
DNS brute	intrusive, discovery	sudo nmap –p80 - -script dns-brute scanme.nmap.org
Traceroute geolocation	safe, external, discovery	sudo nmap - -traceroute - -script traceroute-geolocation.nse –p80 scanme.nmap.org
Detectar versión PHP	discovery, safe	sudo nmap –sV –p80 - -script http-php-version 192.168.56.103
Banner grabbing	discovery, safe	sudo nmap –sV –p80 - -script banner scanme.nmap.org
Obtener cabeceras HTTPS	discovery, safe	sudo nmap –Pn –p80 - -script http-headers scanme.nmap.org
Enumeración servidor HTTP	discovery, intrusive, vuln	sudo nmap –p80 - -script http-enum scanme.nmap.org sudo nmap –p80 - -script http-enum - -script-args http-enum.basepath=dvwa 192.168.56.103
Obtener cabeceras deseguridad de servidor web	discovery, safe	sudo nmap –p80 - -script http-security-headers scanme.nmap.org
Generar sitemap	discovery, intrusive	sudo nmap –p80 - -script http-sitemap-generator scanme.nmap.org
Prueba de los useragents permitidos	discovery, safe	sudo nmap –p80 - -script http-useragent-tester scanme.nmap.org
Prueba de todos los métodos HTTP	default, safe	nmap –p80 - -script http-methods scanme.nmap.org
Prueba del cifrado SSL	discovery, intrusive	nmap –p443 - -script ssl-enum-ciphers sslsite.com
Realizar análisis de vulnerabilidades	vuln, safe, external	nmap –sV - -script vulners 192.168.56.103 nmap –sV –p80 - -script vulners scanme.nmap.orgnmap –sV - -script vulners - -script-args mincvss=5scanme.nmap.org
FTP – Prueba del login anonymous	default, auth, safe	sudo nmap –p21 - -script ftp-anon 192.168.56.103

FTP – fuerza bruta de contraseñas	**intrusive, brute**	**nmap –p21 - -script ftp-brute - -script-args userdb=/path/to/username/file,passdb=/path/to/password/file 192.168.56.103**
SSH – fuerza bruta de contraseñas	**intrusive brute**	**nmap –p22 - -script ssh-brute - -script-args userdb=/path/to/username/file,passdb=/path/to/password/file 192.168.56.103**

NMAP – EVASIÓN Y PRUEBA DE FIREWALL

Nombre del comando	Comando	Ejemplo de uso
Fragmentación de paquetes	**-f**	**sudo nmap –sS –f scanme.nmap.org** **sudo nmap –sS –f –p80,22 scanme.nmap.org**
Cambio del MTU de los paquetes	**--mtu**	**sudo nmap –sS - -mtu 16 192.168.56.103**
Uso de tramas sin procesar	**--send-eth**	**sudo nmap –sS –f - -send-eth –p22,80 192.168.56.103**
Envío de señuelos	**-D**	***Envía señuelos especificos*** **sudo nmap –sS –p22,23,80 –D 192.168.56.105,192.168.56.110 1922.168.56.103** ***Envía señuelos aleatorios*** **sudo nmap –sS –p22 –D RND:3 192.168.56.103** **RND:3 == Envía 3 señuelos aleatorios**
Falsificación de la IP de origen	**-S**	**sudo nmap –sS –S 192.168.56.110 -Pn –e vboxnet0 –p80 192.168.56.103**
Falsificación de la dirección MAC	**--spoof-mac**	**sudo nmap –sS –p80 –Pn –e vboxnet0 –S 192.168.56.115 - -spoof-mac 00:5a:4c:5d:ff:00192.168.56.103** ***Falsificación de MAC basada en fabricante*** **sudo nmap –sS –p80 - -spoof-mac dell 192.168.56.103s** **sudo nmap –sS –p80 - -spoof-mac apple 192.168.56.103** ***Falsificación de MAC aleatoria*** **sudo nmap –sS –p80 - -spoof-mac 0 192.168.56.103**
Falsificación del Puerto origen	**--source-port**	**sudo nmap –sS –p80 - -source-port 88 192.168.56.103**

NMAP – ESCANEO DE TIEMPO Y RENDIMIENTO

Nombre de comando	¿Requiere privilegios root?	Comando	Ejemplo de uso
Establecer pruebas en paralelo	SI	--min-parallelism	sudo nmap –sS - -min-parallelism1192.168.56.1/24
		--max-parallelism	sudo nmap –sS - -max- parallelism 5 192.168.56.1/24
Establecer tiempo de espera en host	SI	--host-timeout	sudo nmap - -host-timeout 2m192.168.56.1/24
Configurar grupos de hosts para escaneo paralelo	SI	--min-hostgroup	sudo nmap - -min-hostgroup2192.168.56.1/24
		--max-hostgroup	sudo nmap - -max hostgroup10 192.168.56.1/24
Establecer intervalo de retardo entre sondas	SI	--scan-delay	sudo nmap - -scan-delay 2s192.168.56.1/24 sudo nmap - -scan-delay 2s –p 20-100scanme.nmap.org
		--max -scan-delay	sudo nmap - -max-scan-delay2s192.168.56.1/24 sudo nmap - -max-scan-delay 2s –p20-100 scanme.nmap.org
Establecer la velocidad de escaneo	SI	--min-rate	sudo nmap - -min-rate 100192.168.56.1/24 sudo nmap - -min-rate 100 –p 1-100scanme.nmap.org
	SI	--max-rate	sudo nmap - -max-rate2192.168.56.1/24 sudo nmap - -max-rate 2 –p 1-100scanme.nmap.org

NMAP – REPORTE DEL ESCANEO

Tipo de formato	Comando	Ejemplo de uso
Formato nmap	**-oN**	**nmap –oN nmap_format.nmap scanme.nmap.org** **nmap –oN nmap_format.txt scanme.nmap.org**
Formato XML	**-oX**	**nmap –oX xml_format.xml scanme.nmap.org**
Formato Fancy	**-oS**	**nmap –oS script_kiddie.txt scanme.nmap.org**
Formato grepable	**-oG**	**nmap –oG grepable_demo scanme.nmap.org**
Todos los formatos	**-oA**	**nmap –oA all_formats scanme.nmap.org**