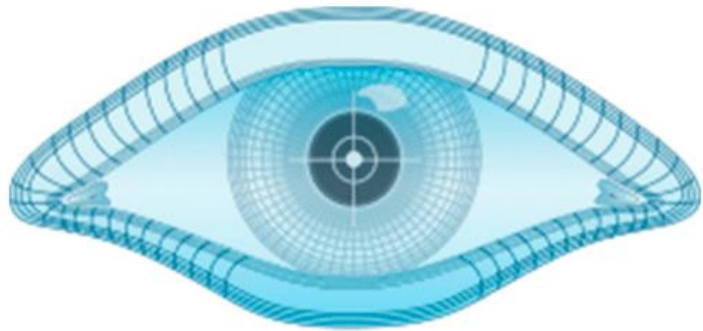


MANUAL DE COMANDOS NMAP



NMAP

WEB: <https://elhackeretico.com/>

EL HACKER ETICO



AUDITORIA DE SEGURIDAD EN RED CON NMAP

Contenido

NMAP – TÉCNICAS BÁSICAS DE ESCANEEO.....	2
Escaneo TCP SYN – Requiere privilegios root.....	2
Escaneo Conexión TCP – No requiere privilegios root.....	2
Escaneo FIN, NULL & XMAS - Requiere privilegios root.....	2
Escaneo UDP - Requiere privilegios root	4
Escaneo SCTP INIT – Requiere privilegios root	4
Más tipos de escaneos con NMAP	4
NMAP - VERSIÓN DE SERVICIO Y HUELLAS DACTILARES DEL SISTEMA OPERATIVO .	5
Detección de servicio	5
Otras parámetros de detección.....	5
DETECCIÓN DEL SISTEMA OPERATIVO	6
Más comandos para la detección del sistema operativo	6
ESPECIFICACIÓN DE PUERTO A ESCANEAR.....	7
Opciones de especificación de puerto.....	7
Escaneo por especificaciones de destino	8
NMAP – DESCUBRIMIENTO DE HOSTS ACTIVOS	9
NMAP – ESCANEEO MEDIANTE EL USO DE SCRIPTS	10
NMAP – EVASIÓN Y PRUEBA DE FIREWALL.....	11
NMAP – ESCANEEO DE TIEMPO Y RENDIMIENTO	12
NMAP – REPORTE DEL ESCANEEO	13





AUDITORIA DE SEGURIDAD EN RED CON NMAP

NMAP – TÉCNICAS BÁSICAS DE ESCANEO

Escaneo TCP SYN – Requiere privilegios root

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

Escaneo Conexión TCP – No requiere privilegios root

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

Escaneo FIN, NULL & XMAS - Requiere privilegios root

Sintaxis del comando	<code>sudo nmap -sF <target_IP_address / hostname> -- ESCANEO FIN</code> <code>sudo nmap -sN <target_IP_address / hostname> -- ESCANEO NULL</code> <code>sudo nmap -sX <target_IP_address / hostname> -- ESCANEO XMAS</code>
Ejemplos de comando	<code>sudo nmap -sF scanme.nmap.org</code> <code>sudo nmap -sN 192.168.56.103</code> <code>sudo nmap -sX 192.168.56.100-110 (Escanea las direcciones IP entre 192.168.56.100 - 192.168.56.110)</code>





AUDITORIA DE SEGURIDAD EN RED CON NMAP

Escanear puertos seleccionados	<pre>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</pre>
---------------------------------------	--





AUDITORIA DE SEGURIDAD EN RED CON NMAP

Escaneo UDP - Requiere privilegios root

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

Escaneo SCTP INIT – Requiere privilegios root

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

Más tipos de escaneos con NMAP

Name	¿Requiere privilegios elevados?	Comando	Sintaxis
Escaneo SCTP INIT	SI	-sY	<code>sudo nmap -sY <target_IP/hostname></code> <code>sudo nmap -sY scanme.nmap.org</code>
Escaneo ACK	SI	-sA	<code>sudo nmap -sA <target_IP/hostname></code> <code>sudo nmap -sA scanme.nmap.org</code> NOTA: Para obtener más información de este escaneo, utilizar - -reason.
Escaneo Maimon	SI	-sM	<code>sudo nmap -sM < target_IP/hostname ></code> <code>sudo nmap -sM scanme.nmap.org</code> NOTA: Para obtener más información de este escaneo, utilizar - -reason.
Escaneo de protocol IP	SI	-sO	<code>sudo nmap -sO < target_IP/hostname ></code> <code>sudo nmap -sO scanme.nmap.org</code> <code>sudo nmap -sO -p25 scanme.nmap.org</code>





AUDITORIA DE SEGURIDAD EN RED CON NMAP

NMAP - VERSIÓN DE SERVICIO Y HUELLAS DACTILARES DEL SISTEMA OPERATIVO

Detección de servicio

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

Otras parámetros de detección

Name	¿Requiere privilegios elevados?	Comando	Sintaxis
All ports	NO	- -allports	<code>nmap -sV --allports <target_IP / Hostname></code>
Version intensity	NO	- -version-intensity	<code>nmap -sV --version-intensity <#> <target_IP / Hostname></code> <code>nmap -sV --version-intensity 5 scanme.nmap.org</code> <code>nmap -sV --version-intensity 5 -p80 scanme.nmap.org</code>
Version light	NO	- -version-light	<code>nmap -sV --version-light <target_IP / Hostname></code> <code>nmap -sV --version-light scanme.nmap.org</code> <code>nmap -sV --version-light -p80 scanme.nmap.org</code>
Version all	NO	- -version-all	<code>nmap -sV --version-all <target_IP / Hostname>eg.</code> <code>nmap -sV --version-all scanme.nmap.org</code> <code>nmap -sV --version-all -p80 scanme.nmap.org</code>
Version trace	NO	- -version-trace	<code>nmap -sV --version-trace <target_IP / Hostname></code> <code>nmap -sV --version-trace scanme.nmap.org</code> <code>nmap -sV --version-trace -p80 scanme.nmap.org</code>





AUDITORIA DE SEGURIDAD EN RED CON NMAP

DETECCIÓN DEL SISTEMA OPERATIVO

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

Más comandos para la detección del sistema operativo

Name	¿Requiere privilegios elevados?	Comando	Sintaxis
Detección de Sistema Operativo	SI	<code>--osscan-guess</code> <code>--fuzzy</code>	<code>sudo nmap -O - -osscan-guess <target_IP / Hostname></code> <code>sudo nmap -O - -fuzzy <target_IP / Hostname></code> <code>sudo nmap -O - -osscan-guess scanme.nmap.org</code> <code>sudo nmap -O - -fuzzy scanme.nmap.org</code>
Número de intentos para detección de sistema operativo	SI	<code>--max-os-tries</code>	<code>sudo nmap -O - -max-os-tries <#><target_IP / Hostname></code> <code>sudo nmap -O - -max-os-tries 2 scanme.nmap.org</code>
Opción agresiva	NO	<code>-A</code>	<code>nmap -A <target_IP/Hostname></code> <code>nmap -A scanme.nmap.org</code> <code>Nmap -A -p80 scanme.nmap.org</code>





AUDITORIA DE SEGURIDAD EN RED CON NMAP

ESPECIFICACIÓN DE PUERTO A ESCANEAR

Opciones de especificación de puerto

Descripción	Comando	Sintaxis	Ejemplo de comando
Especificar un único puerto	-p	nmap -p22 <target_IP/Hostname>	nmap -p22 scanme.nmap.org
Especificar multiples puertos		nmap -p <n1,n2,n3....nm> <target_IP/Hostname>	nmap -p21,22,23,25,80 scanme.nmap.org
Especificar un rango de puertos		nmap -p<n1-nm> <target_IP/Hostname>	nmap -p10-100 scanme.nmap.org
Especifique y escanee puertos con múltiples protocolos (requiere elevado / root privilegios)		sudo nmap -sS -sU -p T:<t1,t2,...tn>,U:<u1,u2,...u n> <target_IP/Hostname>	sudo nmap -sS -sU -p T:21,22,25,80,U:53,161 scanme.nmap.org
Especifique protocolos para escanear (requiere elevado / 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 de puertos 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





AUDITORIA DE SEGURIDAD EN RED CON NMAP

Escaneo por especificaciones de destino

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





AUDITORIA DE SEGURIDAD EN RED CON NMAP

NMAP – DESCUBRIMIENTO DE HOSTS ACTIVOS

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





AUDITORIA DE SEGURIDAD EN RED CON NMAP

NMAP – ESCANEO MEDIANTE EL USO DE SCRIPTS

Nombre de script	Categoría	Ejemplo
DNS brute	intrusive, discovery	<code>sudo nmap -p80 -script dns-brute scanme.nmap.org</code>
Traceroute geolocation	safe, external, discovery	<code>sudo nmap -traceroute -script traceroute-geolocation.nse -p80 scanme.nmap.org</code>
Detectar version PHP	discovery, safe	<code>sudo nmap -sV -p80 -script http-php-version 192.168.56.103</code>
Banner grabbing	discovery, safe	<code>sudo nmap -sV -p80 -script banner scanme.nmap.org</code>
Obtener cabeceras HTTPS	discovery, safe	<code>sudo nmap -Pn -p80 -script http-headers scanme.nmap.org</code>
Enumeración servidor HTTP	discovery, intrusive, vuln	<code>sudo nmap -p80 -script http-enum scanme.nmap.org</code> <code>sudo nmap -p80 -script http-enum -script-args http-enum.basepath=dvwa 192.168.56.103</code>
Obtener cabeceras de seguridad de servidor web	discovery, safe	<code>sudo nmap -p80 -script http-security-headers scanme.nmap.org</code>
Generar sitemap	discovery, intrusive	<code>sudo nmap -p80 -script http-sitemap-generator scanme.nmap.org</code>
Prueba de los useragents permitidos	discovery, safe	<code>sudo nmap -p80 -script http-useragent-tester scanme.nmap.org</code>
Prueba de todos los métodos HTTP	default, safe	<code>nmap -p80 -script http-methods scanme.nmap.org</code>
Prueba del cifrado SSL	discovery, intrusive	<code>nmap -p443 -script ssl-enum-ciphers sslsite.com</code>
Pruebas de servicios inusuales	safe	<code>nmap -sV -script unusual-port 192.168.56.103</code>
Realizar análisis de vulnerabilidades	vuln, safe, external	<code>nmap -sV -script vulners 192.168.56.103</code> <code>nmap -sV -p80 -script vulners scanme.nmap.org</code> <code>nmap -sV -script vulners -script-args mincvss=5 scanme.nmap.org</code>
FTP – Prueba del login anonymous	default, auth, safe	<code>sudo nmap -p21 -script ftp-anon 192.168.56.103</code>
FTP – fuerza bruta de contraseñas	intrusive, brute	<code>nmap -p21 -script ftp-brute -script-args userdb=/path/to/username/file,passdb=/path/to/password/file 192.168.56.103</code>





AUDITORIA DE SEGURIDAD EN RED CON NMAP

SSH – fuerza bruta de contraseñas	intrusive brute	<code>nmap -p22 -script ssh-brute -script-args userdb=/path/to/username/file,passdb=/path/to/password/file 192.168.56.103</code>
-----------------------------------	-----------------	--

NMAP – EVASIÓN Y PRUEBA DE FIREWALL

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





AUDITORIA DE SEGURIDAD EN RED CON NMAP

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-parallelism 1192.168.56.1/24
		--max-parallelism	sudo nmap -sS - -max-parallelism 5192.168.56.1/24
Establecer tiempo de espera en host	SI	--host-timeout	sudo nmap - -host-timeout 2m 192.168.56.1/24
Configurar grupos de hosts para escaneo paralelo	SI	--min-hostgroup	sudo nmap - -min-hostgroup 2192.168.56.1/24
		--max-hostgroup	sudo nmap - -max-hostgroup 10192.168.56.1/24
Establecer intervalo de retardo entre sondas	SI	--scan-delay	sudo nmap - -scan-delay 2s 192.168.56.1/24 sudo nmap - -scan-delay 2s -p 20-100 scanme.nmap.org
		--max-scan-delay	sudo nmap - -max-scan-delay 2s 192.168.56.1/24 sudo nmap - -max-scan-delay 2s -p 20-100 scanme.nmap.org
Establecer la velocidad de escaneo	SI	- -min-rate	sudo nmap - -min-rate 100 192.168.56.1/24 sudo nmap - -min-rate 100 -p 1-100 scanme.nmap.org
		- -max-rate	sudo nmap - -max-rate 2192.168.56.1/24 sudo nmap - -max-rate 2 -p 1-100 scanme.nmap.org



AUDITORIA DE SEGURIDAD EN RED CON NMAP

NMAP – REPORTE DEL ESCaneo

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

