Basque CyberSecurity Centre

Nmap cheat sheet

Herramienta de código abierto usada para **escaneo de redes, puertos y la búsqueda de vulnerabilidades.** Se utiliza en auditorías de seguridad para monitorizar redes.

1. Opciones de especificación de puertos

Sintaxis	Ejemplo	Descripción
-p	nmap -p 23 172.15.10.1	Escaneo de puertos en el puerto especificado
-p	nmap -p 23-100 172.16.1.1	Escaneo de puertos en el rango de puertos especificado
-p	nmap -pU:110,T:23-25,43 172.15.10.1	Diferentes tipos de escaneo U-UDP T-TCP
-p-	nmap -p 172.15.10.1	Escanea todos los puertos
-p	nmap -p -smtp,https 172.16.1.1	Escaneo de protocolos específicos
-F	nmap -F 172.15.10.1	Escaneo rápido de puertos
-p "*"	nmap -p "*" ftp 172.16.1.1	Escaneo de puertos con nombre
-r	nmap -r 172.15.10.1	Escaneo de puertos secuencial

2. Tipos de escaneo

Sintaxis	Ejemplo	Descripción
-sS	nmap 172.15.10.1 -sS	Escaneo puerto TCP SYN
-sT	nmap 172.15.10.1 -sT	Escaneo conexión a puerto TCP
-sA	nmap 172.15.10.1 -sA	Escaneo puerto TCP ACK
-sU	nmap 172.15.10.1 -sU	Escaneo puerto UDP
-Sf	nmap 172.15.10.1 -Sf	Escaneo TCP FIN
-sX	nmap 172.15.10.1 -sX	Escaneo XMAS
-sP	nmap 172.15.10.1 -sP	Escaneo PING
-Su	nmap 172.15.10.1 -sU	Escaneo UDP
-sA	nmap 172.15.10.1 -sA	Escaneo TCP ACK
-SL	nmap 172.15.10.1 -SL	Lista cada host de la red

Basque CyberSecurity Centre

3. Comandos diversos	
nmap -6	Escaneo IPV6 de los objetivos
nmap –proxies proxy 1 URL, proxy 2 URL	Corre en los objetivos con proxies
nmap –open	Muestra sólo puertos abiertos

4. Formatos de salida en nmap	
Por defecto	nmap -oN scan.txt 172.15.10.1
XML	nmap -oX scanr.xml 172.15.10.1
Formato Grepable	nmap -oG grep.txt 172.15.10.1
Todos los formatos	nmap -oA 172.15.10.1

5. Comandos de escaneo/Sintaxis
nmap [tipo de escaneo] [opciones] {171.20.20.1 especificación}

6. Especificación 172.16.1.1	
nmap 172.16.1.1	Escaneo simple de IP
nmap 172.16.1.1 172.16.100.1	Escaneo específico de IP´s
nmap 172.16.1.1 -254	Escaneo de un rango de IP´s
nmap xyz.org	Escaneo de un dominio
nmap 10.1.1.0/8	Escaneo usando notación CIDR
nmap –iL scan.txt	Escaneo 172.16.1.1 de un archivo
nmap –exclude 172.16.1.1	IP específica excluida del escaneo

Basque CyberSecurity Centre

7. Scripts NSE en nmap

nmap --script= test script	Ejecuta el script contra la dirección IP objetivo
nmap --script-update-db	Actualiza la bb.dd desde scripts/script.db
nmap -sV -sC	Usar scripts por defecto para escaneo
nmap –script-help=" Test script"	Ayuda de la herramienta para scripts

8. Opciones de escaneo

nmap -sP 172.15.10.1	Sólo escaneo de ping
nmap -PU 172.15.10.1	Escaneo ping UDP
nmap -PE 172.15.10.1	Echo ping ICMP
nmap -PO 172.15.10.1	Ping protocolo IP
nmap -PR 172.15.10.1	Ping ARP
nmap -Pn 172.15.10.1	Escano sin ping
nmap -traceroute 172.15.10.1	Traceroute

9. Opciones de timing en nmap

nmap -T0 172.15.10.1	Escaneo más lento
nmap -T1 172.15.10.1	Escaneo para evitar IDS
nmap -T2 172.15.10.1	Escaneo oportuno
nmap -T3 172.15.10.1	Escaneo con temporizador por defecto
nmap -T4172.15.10.1	Escaneo agresivo
nmap -T5 172.15.10.1	Escaneo muy agresivo