Documentación de Nmap

Tabla de Comandos de Nmap

Objetivo	Comando	Descripción
Escaneo básico de red local	nmap -sn 192.168.1.0/24	Detecta todos los dispositivos activos en la red.
Escaneo de puertos abiertos	nmap 192.168.1.100	Escanea los puertos abiertos en un dispositivo espec
Escaneo rápido de puertos	nmap -F 192.168.1.100	Escanea los puertos más comunes rápidamente.
Escaneo de todos los puertos	nmap -p- 192.168.1.100	Escanea todos los puertos (0-65535).
Detectar versión del servicio	nmap -sV 192.168.1.100	Detecta la versión de los servicios en los puertos.
Detectar sistema operativo	nmap -O 192.168.1.100	Intenta identificar el sistema operativo.
Escaneo agresivo	nmap -A 192.168.1.100	Combina detección de servicios, versiones, scripts y
Escaneo sigiloso (TCP SYN)	nmap -sS 192.168.1.100	Escaneo sigiloso sin completar la conexión TCP.
Escaneo UDP	nmap -sU 192.168.1.100	Escanea puertos UDP.
Escaneo con script NSE	nmap --script=default 192.168.1.100	Ejecuta scripts NSE predeterminados.
Script específico	nmap --script=vuln 192.168.1.100	Ejecuta scripts de vulnerabilidad.
Exportar a archivo	nmap -oN resultado.txt 192.168.1.100	Guarda los resultados en archivo de texto.
Exportar a XML	nmap -oX resultado.xml 192.168.1.100	Guarda los resultados en XML.
Red completa + puertos	nmap -p 1-1000 -T4 192.168.1.0/24	Escanea los primeros 1000 puertos en la red.
Escaneo lento y sigiloso	nmap -T2 -sS -p 1-1000 192.168.1.100	Escaneo lento para evitar detección.

Explicación de los Parámetros Comunes

- -sn: Realiza un "ping sweep" sin escanear puertos.
- -p: Especifica puertos a escanear (ej: -p 1-1000 o -p 80,443).
- -p-: Escanea todos los puertos (0-65535).
- -sS: Escaneo TCP SYN (sigiloso).
- -sU: Escaneo UDP.
- -sV: Detecta versión de servicios.
- -O: Identifica sistema operativo.
- -A: Modo agresivo (servicios, scripts, SO).
- -T: Ajusta velocidad (T0 a T5).
- --script: Ejecuta scripts NSE.
- -oN: Guarda en texto plano.
- -oX: Guarda en XML.

Pasos Recomendados para Explorar tu Red Local

1. Detectar dispositivos activos:
   nmap -sn 192.168.1.0/24

2. Escaneo rápido de puertos:
   nmap -F 192.168.1.100

3. Escaneo completo de puertos y servicios:
   nmap -p- -sV 192.168.1.100

4. Identificar SO y vulnerabilidades:

Documentación de Nmap

nmap -A --script=vuln 192.168.1.100

5. Guardar resultados:
nmap -p- -sV -oX resultado.xml 192.168.1.100

Nota Importante

- Permisos: Algunos comandos requieren sudo.
- Ética: Solo escanea redes con autorización.