NMAP

CHEAT SHEET

Simple Cheat Sheet de Nmap

Objetivos y Rango de Escaneo

Opción Nmap	Descripción
10.10.10.0/24	Escanea una red completa (en este caso, la subred 10.10.10.0 con máscara /24).
-sn	Desactiva el escaneo de puertos (solo hace "ping" para ver qué hosts están activos).
-Pn	No hace ping (ICMP), asume que todos los hosts están activos. Útil cuando los pings están bloqueados.
-n	Desactiva la resolución DNS (no intenta convertir IPs en nombres).

Técnicas de Detección / Ping /Reconocimiento

Opción Nmap	Descripción
-PE	Realiza escaneo tipo ping mediante solicitudes ICMP Echo (equivalente a ping).
--disable-arp-ping	Desactiva el uso de ARP para detectar dispositivos en red local.
--packet-trace	Muestra todos los paquetes enviados y recibidos (útil para análisis técnico o debugging).
--reason	Muestra la razón por la cual un puerto o servicio ha sido marcado como tal (por ejemplo, por una respuesta TCP RST).

Opciones de Puertos

Opción Nmap	Descripción
--top-ports=<num>	Escanea los <num> puertos más comunes (según estadísticas de Nmap).
-p-	Escanea todos los puertos TCP (del 1 al 65535)
-p22-110	Escanea todos los puertos comprendidos entre 22 y 110.
-p22,25	Escanea solo los puertos 22 (SSH) y 25 (SMTP).
-F	Escaneo rápido: analiza los 100 puertos más comunes.

Técnicas de Escaneo de Puertos

Opción Nmap	Descripción
-sS	Escaneo TCP SYN (rápido y sigiloso, no completa la conexión).
-sA	Escaneo TCP ACK (sirve para detectar si hay un firewall que bloquea).
-sU	Escaneo de puertos UDP. Más lento pero detecta servicios diferentes.
-sV	Detecta versiones de servicios descubiertos.
-sC	Ejecuta scripts de Nmap por defecto (detección básica de servicios).
--script <script>	Ejecuta scripts personalizados (por nombre, categoría o ruta).

Evasión, Spoofing y Engaño

Opción Nmap	Descripción
-D RND:5	Usa 5 direcciones IP falsas aleatorias como señuelos (decoys). Oculta tu IP real.
-e <interfaz>	Especifica la interfaz de red que se usará para el escaneo (ej. eth0).
-S 10.10.10.200	Define una IP de origen falsa para el escaneo (IP spoofing).
-g <puerto>	Define el puerto de origen que se usará para los paquetes enviados.
--dns-server <ns>	Utiliza un servidor DNS específico para la resolución de nombres.

Opciones de salida

Opción Nmap	Descripción
-oA <nombre>	Guarda los resultados en todos los formatos disponibles: .nmap, .xml, .gnmap.
-oN <nombre>	Guarda los resultados en formato normal (legible para humanos).
-oG <nombre>	Guarda los resultados en formato grepable (para búsquedas o parseos).
-oX <nombre>	Guarda los resultados en formato XML. Útil para herramientas de análisis.

Rendimiento y Tiempo

Opción Nmap	Descripción
--max-retries <num>	Número máximo de reintentos por puerto antes de darlo por no disponible.
--stats-every=5s	Muestra el progreso del escaneo cada 5 segundos.
-v / -vv	Salida detallada durante el escaneo (-vv = más detallado aún).
--initial-rtt-timeout 50ms	Define el tiempo de espera inicial (RTT) en 50 milisegundos.
--max-rtt-timeout 100ms	Tiempo máximo de espera para recibir respuestas.
--min-rate 300	Envia al menos 300 paquetes por segundo (acelera el escaneo

Detección de Sistema Operativo y Servicios Avanzados

Opción Nmap	Descripción
-O	Detecta el sistema operativo del objetivo (basado en huellas de red).
-A	Escaneo agresivo: incluye detección de OS, servicios, traceroute y scripts.