Cheat sheet comandos/parámetros de Nmap

Escaneos básicos/principales

Comando/Parámetro	Descripción	Cuándo usarlo
-sS	TCP SYN scan *(inicia una conexión TCP. Este escaneo envía solo ese primer paso, sin completarla, para mantenerlo sigiloso)*	Rápido, más sigiloso porque no establece conexión completa.
-sT	TCP connect scan *(completa toda la conexión TCP [SYN, SYN-ACK, ACK]. Es como un cliente normal conectándose)*	Cuando no hay privilegios para usar -sS
-sU	UDP scan *(busca servicios que usen UDP como DNS o SNMP, que no responden igual que TCP)*	Para encontrar servicios UDP como DNS, SNMP o DHCP
-sN	TCP NULL scan *(no tiene ningún flag TCP activo, por lo que es un paquete "en blanco")*	Puede evadir IDS/firewalls simples.
-sF	TCP FIN scan *(cierra una conexión TCP. Aquí se usa solo ese flag para confundir sistemas de detección)*	Se parece a -sN, evasión de firewalls.
-sX	Xmas scan *(tiene múltiples flags encendidos como FIN, URG, PSH)*	Contra sistemas que no siguen RFC correctamente

Detectar hosts

Comando/Parámetro	Descripción	Cuándo usarlo
-Pn	No se hace ping, ya se asume que los hosts están activos	Cuando haya firewalls que bloqueen ICMP o cuando ya se sabe que el host está activo.
-sn	Hace ping	Solo para saber qué hosts están activos.
-PS	Ping TCP SYN (con puerto especificado)	Para evitar ICMP bloqueado.
-PA	Ping TCP ACK (*Envía un paquete TCP con ACK para ver si el host responde, sin iniciar conexión)*	Se parece al -PS pero sirve más para pillar hosts con firewalls.
-PU	Ping UDP *(Envía un paquete UDP para ver si el host responde o devuelve un error)*	Para buscar hosts con servicios UDP activos.
-PE, -PP, -PM	Ping ICMP Echo, Timestamp y Netmask	Cuando se quiere encontrar hosts ICMP.

Detección de servicios y versiones

Comando/Parámetro	Descripción	Cuándo usarlo
-sV	Detectar servicios y versiones. Es muy común.	Cuando se necesita saber que programa y versión corre en los puertos.

**He visto otros parámetros como –version-all pero nunca los he usado o su efectividad, así que no los pongo.*

Detectar sistemas operativos

Comando/Parámetro	Descripción	Cuándo usarlo
-O	Detectar sistemas operativos. Es muy común.	Cuando se quiere saber que sistema operativo tiene el host, puede servir para saber hacer ataques más específicos.

**He visto otros parámetros para complementar este pero tampoco los he usado, así que no los pongo.*

Especificar puertos

Comando/Parámetro	Descripción	Cuándo usarlo
-p o -p-	-p para especificar puertos -p- escanea los 65535 puertos	Cuando se quiere escanear todos los puertos (-p) o cuando se desea escanear puertos específicos (ej: -p 21,80,443)

**Hay parámetros para escanear los "n" puertos más comunes o más utilizados en frecuencia. Pero, esos no los he usado, y en lo personal prefiero elegir yo cuales escanear por rapidez sabiendo lo que busco o explorarlos todos.*

Salida y archivos

Comando/Parámetro	Descripción	Cuándo usarlo
-oN archivo.txt	Genera una salida en archivo de texto	Para guardarlo, puede servir para después hacer el informe y no tener que estar escaneando todo el tiempo.
-oX archivo.xml	Genera una salida en archivo XML	Si es que se quiere integrar con otras herramientas
-oG archivo.gnmap	Genera una salida en archivo grepable	Cuando se quiera usar con scripts

Scripting NSE

Comando/Parámetro	Descripción	Cuándo usarlo
-sC	Ejecuta scripts NSE por defecto (son scripts que nmap automatiza para detectar vulnerabilidades, enumerar servicios, recolección de información, etc.)	Cuando se quieran detectar de forma común los servicios.
–script=nombre_script	Ejecuta un script específico	Cuando se quiera usar un script específico, situacional.
–script=vuln	Ejecuta scripts de detección de vulnerabilidades	Para hacer un escaneo de vulnerabilidades, es útil.

**Suelo usar -sC en un escaneo básico. El comando de detección de vulnerabilidades lo he usado menos veces. El del script específico creo que nunca lo he usado, pero puede ser útil en algunos casos.*

Otros relacionados a evasión y ofuscación

Comando/Parámetro	Descripción	Cuándo usarlo
-T[0-5]	Timing template 0 = paranoico 5 = agresivo	Cuando se quiera controlar la velocidad vs evasión
-f	Fragmenta paquetes	Cuando se quiera evadir IDS de forma básica

** Hay un par más, pero no los he usado ni los comprendo del todo. Así que no los colocaré.*