Chuleta rápida de Nmap

Guía compacta y lista para imprimir con los parámetros y ejemplos más útiles de Nmap — orientada a hacking ético.

---

1. Uso básico

- `nmap <IP>` — Escaneo por defecto (1000 puertos TCP más comunes).
- `nmap 192.168.1.0/24` — Escanear subred completa.
- `nmap -iL objetivos.txt` — Leer lista de hosts desde archivo.

2. Selección de puertos

- `-p 80` — Puerto específico.
- `-p 22,80,443` — Varios puertos.
- `-p 1-1000` — Rango de puertos.
- `-p-` — Todos los puertos (0-65535).

3. Tipos de escaneo (TCP/UDP)

- `-sT` — TCP Connect (útil si no se tienen privilegios raw).
- `-sS` — SYN scan (half-open, el más usado para sigilo).
- `-sU` — Escaneo UDP.
- Combinado: `-sS -sU`.

4. Detección de servicios y SO

- `-sV` — Detección de versión de servicios.
- `-O` — Detección de sistema operativo.
- `-A` — Modo agresivo (equivale a `-sV -O --traceroute --script=default`).

5. Escaneo sigiloso / evasión

- `-T0` a `-T5` — Timing templates (0 más lento, 5 más rápido). Ej: `-T2` para ser más cauteloso.
- `-f` — Fragmentar paquetes IP.
- `--source-port <puerto>` — Falsificar puerto origen (e.g. 53).
- `--randomize-hosts` — Orden aleatorio de hosts.
- `--badsum` — Enviar paquetes con checksum malo (pruebas específicas).

Nota: la evasión puede ser ilegal en redes que no posees. Usa siempre con autorización.

6. Nmap Scripting Engine (NSE)

- `-sC` — Ejecuta los scripts por defecto (equivalente a `--script=default`).
- `--script <script|category>` — Ejecutar script/s específico/s. Ejemplos:
- `--script smb-enum-shares` — Enumerar shares SMB.

- `--script vuln` — Ejecutar scripts de vulnerabilidad.
- Lista de scripts: `/usr/share/nmap/scripts/` (en muchas distros).

7. Salida y formatos

- `-oN archivo.txt` — Salida normal en texto.
- `-oX archivo.xml` — Salida en XML.
- `-oG archivo.gnmap` — Salida grepable.
- `-oA prefijo` — Guardar en los tres formatos (normal, XML, grepable).

8. Ejemplos combinados (prácticos)

- Escaneo rápido con versión y OS:
  `nmap -sS -sV -O 192.168.1.10`

- Escaneo profundo de puertos + guardar resultado:
  `nmap -sS -p- -T4 -sV -oA host_completo 192.168.1.10`

- Escaneo sigiloso con fragmentación y puerto fuente DNS:
  `nmap -sS -f --source-port 53 -T2 192.168.1.10`

- Escaneo UDP enfocado (puertos 1-200):
  `nmap -sU -p 1-200 -T3 -oN udp_scan.txt 192.168.1.10`

- Escaneo con scripts de vulnerabilidad en un rango:
  `nmap -sV --script vuln 192.168.1.0/24 -oN vuln_scan.txt`

9. Trucos útiles

- `--open` — Mostrar solo puertos abiertos.
- `--reason` — Mostrar la razón del estado (RESET, ACK, etc.).
- `--script-args` — Pasar argumentos a scripts NSE.
- `--top-ports <n>` — Escanear los n puertos más comunes (ej: `--top-ports 1000`).
- `-Pn` — No hacer ping previo (tratar hosts como up).

10. Buenas prácticas éticas

1. Obtén permiso por escrito antes de escanear.
2. Escanea en ventanas de baja actividad cuando sea posible.
3. Documenta los comandos y resultados.
4. No uses técnicas destructivas sin autorización.

Exportar / Imprimir

Si quieres que convierta esta chuleta a **PDF** listo para imprimir o una **tabla A4** con diseño, dime: `PDF` o `Tabla`. También puedo añadir más ejemplos concretos, categorías de scripts NSE o una versión para **cheat-sheet A5**.

Fin de la chuleta.