🧠 GUÍA COMPLETA DE NMAP

🎯 COMANDOS DE ESCANEO MÁS USADOS

1. Escaneo rápido (100 puertos más comunes)
```
nmap -F 192.168.1.20
```
✅ Ideal para análisis rápidos en red local.

2. Escaneo completo (todos los puertos TCP)
```
nmap -p- 192.168.1.20
```
🔍 Escanea desde el puerto 1 al 65535.

3. Escaneo con detección de servicios y sistema operativo
```
nmap -sS -sV -O 192.168.1.20
```
📦 Muestra puertos abiertos, versiones de servicios y sistema operativo.

4. Escaneo agresivo completo
```
nmap -A 192.168.1.20
```
💥 Combina -O, -sV, scripts NSE y traceroute.

5. Escaneo silencioso (evasión básica)
```
nmap -sS -Pn -T2 192.168.1.20
```
🕶️ Sin ping, más sigiloso, ideal para entornos protegidos.

6. Descubrimiento de hosts activos (sin escanear puertos)
```
nmap -sn 192.168.1.0/24
```
📡 Detecta qué dispositivos están activos en la red.

7. Escaneo de vulnerabilidades HTTP
```
nmap --script http-vuln* -p 80,443 192.168.1.20
```
🔐 Ejecuta scripts NSE de vulnerabilidad sobre servidores web.

8. Escaneo UDP específico (DNS y SNMP)
```
nmap -sU -p 53,161 192.168.1.20
```
📮 Verifica servicios comunes en puertos UDP.

9. Guardar resultado en múltiples formatos
```
nmap -sS -oA escaneo_final 192.168.1.20
```
🗂️ Guarda `.nmap`, `.xml` y `.gnmap` al mismo tiempo.

10. Escaneo evasivo con MAC spoof y fragmentación
```
nmap -sS --spoof-mac 0 -f 192.168.1.20
```
👻 Evade detección usando técnicas básicas de ofuscación.

Diego Alexis Villafuerte

🔍 DESCUBRIMIENTO DE HOSTS (PING SCANS)

`-Pn`
No realiza ping. Supone que todos los hosts están activos.

`-sn`
Solo detecta si el host está activo. No escanea puertos.

`-sL`
Solo lista los hosts, sin enviar paquetes (resuelve nombres si puede).

Tipos de Ping:

- `-PR` → ARP Ping (solo en redes locales)
- `-PE` → ICMP Echo Request
- `-PP` → ICMP Timestamp
- `-PM` → ICMP Address Mask
- `-PO1,2` → Ping por protocolo IP (ej: ICMP, IGMP)
- `-PS80` → TCP SYN Ping al puerto 80
- `-PA443` → TCP ACK Ping al puerto 443
- `-PU53` → UDP Ping al puerto 53
- `-PY123` → SCTP INIT Ping

🔓 ESCANEO DE PUERTOS

📡 Modos TCP

- `-sS` → SYN Stealth Scan
- `-sT` → TCP Connect (visible, sin root)
- `-sA` → ACK Scan (detecta filtrado)
- `-sN` → NULL Scan (sin flags)

- `-sF` → FIN Scan
- `-sX` → Xmas Scan
- `-sW` → Window Scan
- `-sM` → Maimon Scan

📬 Modos UDP y SCTP

- `-sU` → Escaneo de puertos UDP
- `-sY` → SCTP INIT Scan
- `-sZ` → SCTP Cookie Echo

🎯 Especificar puertos

- `-p 22,80,443` → Escanear puertos específicos
- `-p-` → Escanear todos los puertos (1–65535)
- `--top-ports 100` → Los 100 puertos más comunes
- `--port-ratio 0.9` → Puertos con alta probabilidad de estar abiertos

⚡ Escaneo rápido

- `-F` → Solo los 100 puertos más populares

🧪 DETECCIÓN DE SERVICIOS Y SISTEMA OPERATIVO

Servicios

- `-sV` → Detección de versiones de servicios
- `--version-intensity 0–9` → Controla la profundidad del escaneo
- `--version-light` → Equivale a intensidad 2

Diego Alexis Villafuerte

- `--version-all` → Equivale a intensidad 9
- `--version-trace` → Muestra trazas detalladas

Sistema operativo

- `-O` → Detección del sistema operativo
- `--osscan-guess` → Adivina si no tiene certeza
- `--osscan-limit` → Solo analiza si lo ve viable
- `--max-ostries 3` → Número máximo de intentos

Análisis agresivo

- `-A` → Combina `-O -sV -sC --traceroute`

👻 EVASIÓN Y SPOOFING

Fragmentación y tamaño

- `-f` → Fragmentar paquetes
- `--mtu 24` → Tamaño personalizado (múltiplos de 8)
- `--data-length 50` → Añadir 50 bytes aleatorios

Cambiar identidad

- `--spoof-mac 0` → MAC aleatoria
- `-D 1.2.3.4,ME` → Añadir señuelos
- `-S 10.0.0.100` → Falsificar dirección origen
- `--source-port 53` → Cambiar puerto fuente

Otros

- `--ttl 5` → TTL personalizado
- `--badsum` → Enviar paquetes con checksum inválido
- `--adler32` → Usar resumen Adler32 (SCTP)

⚙️ SCRIPTS NSE

- `-sC` → Scripts por defecto
- `--script nombre` → Script individual o categoría (e.g. vuln, auth)
- `--script-args clave=valor` → Argumentos para scripts
- `--script-argsfile archivo.txt` → Cargar args desde archivo
- `--script-trace` → Mostrar comunicación del script
- `--script-help nombre` → Mostrar ayuda específica
- `--script-updatedb` → Actualizar base de datos de scripts

💾 SALIDA Y REPORTES

- `-oN salida.txt` → Salida normal
- `-oX salida.xml` → XML estructurado
- `-oG salida.gnmap` → Grepeable (deprecated)
- `-oA base` → Genera `.nmap`, `.xml` y `.gnmap` al mismo tiempo

Extras

- `--reason` → Explica por qué el puerto está "open", "closed", etc.
- `--open` → Solo mostrar puertos abiertos
- `--append-output` → Añadir resultados a un archivo existente

Diego Alexis Villafuerte

- `--resume archivo` → Continuar escaneo interrumpido
- `--iflist` → Ver interfaces y rutas locales

⏱️ RENDIMIENTO Y VELOCIDAD

Plantillas de velocidad

- `-T0` → 🐢 Paranoico
- `-T1` → 🐌 Sneaky
- `-T2` → 🧊 Polite
- `-T3` → ⚖️ Normal (default)
- `-T4` → ⚡ Agresivo
- `-T5` → 🚀 Insane (rápido, pero ruidoso)

Control fino

- `--min-rate 100` → Mínimo 100 paquetes por segundo
- `--max-rate 300` → Límite superior
- `--min-parallelism 10` → Mínimo tareas simultáneas
- `--max-retries 2` → Reintentos por puerto
- `--host-timeout 30s` → Tiempo máximo por host
- `--scan-delay 1s` → Pausa entre sondas
- `--defeat-rst-ratelimit` → Ignorar límites RST

💡 COMBINACIONES PRÁCTICAS (TOP 10)

1. Escaneo rápido básico:

```
nmap -F 192.168.1.1
```

2. Detección completa (servicios + SO):

```
nmap -sS -sV -O 192.168.1.1
```

3. Análisis agresivo total:

```
nmap -A -T4 192.168.1.1
```

4. Buscar vulnerabilidades web:

```
nmap --script http-vuln* -p 80,443 192.168.1.1
```

5. Ver solo puertos abiertos con razones:

```
nmap -sS --open --reason 192.168.1.1
```

6. Escanear una red completa:

```
nmap -sn 192.168.0.0/24
```

7. Escaneo total de puertos + versiones:

```
nmap -p- -sV 192.168.1.1
```

8. Escaneo UDP profesional:

```
nmap -sU -p 53,161 -sV 192.168.1.1
```

9. Evasión básica (MAC spoof + fragmentación):

```
nmap -sS -f --spoof-mac 0 192.168.1.1
```

10. Guardar todo en archivos:

```
nmap -sS -sV -O -oA reporte_final 192.168.1.1
```

Diego Alexis Villafuerte