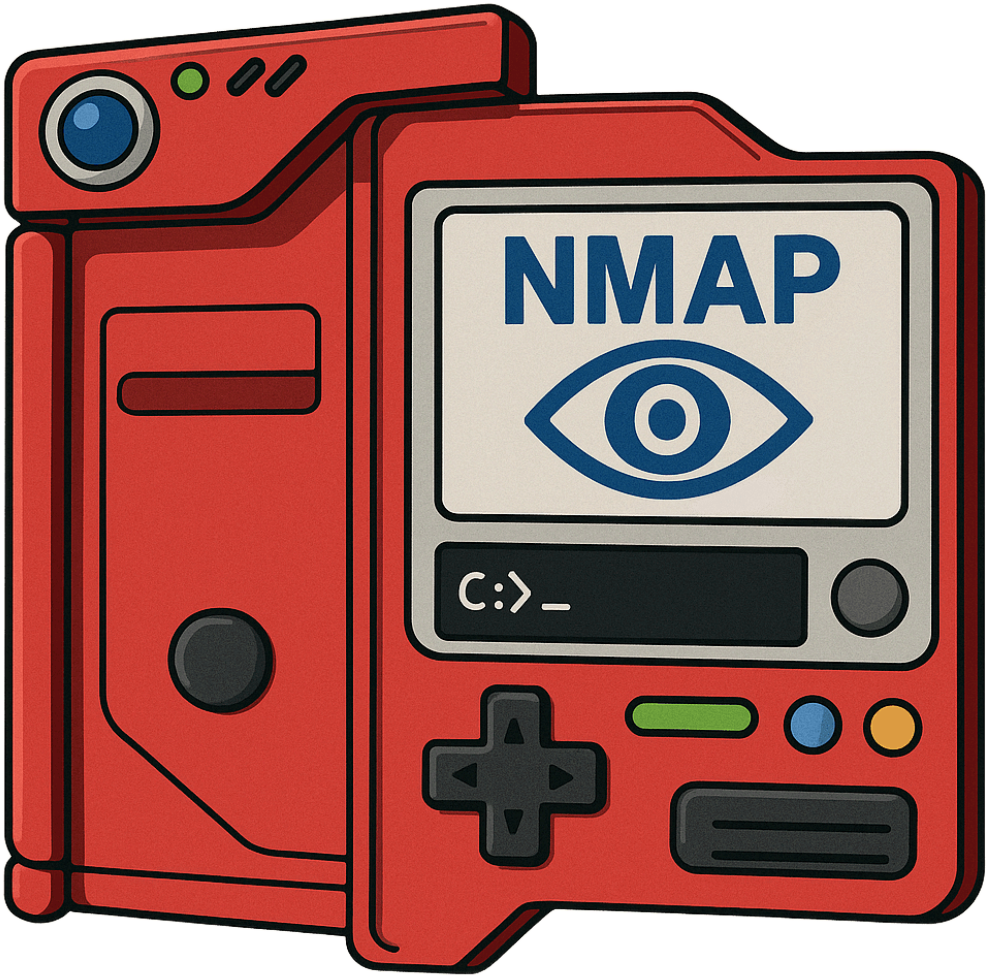
# Guía básica de Nmap con Pokémon




👌🏻 Nmap es una poderosa herramienta que te permite utilizarla como si fuera una pokedex y así poder escanear redes y encontrar Pokémons. Con esta guía te convertirás en el mejor maestro Pokémon. Así que... ¡Atrápalos a todos!

## 🔄 Analogía: Mundo Pokémon 🆚 Mundo Hacking Ético

| Mundo Pokémon | Mundo Hacking Ético | Descripción |
|---|---|---|
| **Pokémon** | **Puerto** | Cada puerto abierto es como un Pokémon: tiene un tipo (servicio) y habilidades (versión). |
| **Hábitat/Zona** | **Host / Dispositivo** | Un hábitat es un lugar donde habitan los Pokémon. En ciberseguridad, es una IP o un host. |
| **Tipo de Pokémon** | **Protocolo / Servicio** | SSH, HTTP, DNS, FTP... cada uno tiene un comportamiento y vulnerabilidades. |
| **Gimnasio** | **Sistema de Defensa / Firewall** | Cada red tiene barreras: firewalls, detección de intrusos, como un líder de gimnasio. |

## 🔍 COMANDOS NMAP: POKEDEX

### 🎯 1. `nmap <IP>`

> Tipo: Normal
>
> **Nombre**: *Escaneo Básico*
>
> **Técnica**: `nmap + dirección IP`
>
> **Descripción Técnica**:
>
> Envía paquetes TCP a los 1000 puertos más comunes de la IP objetivo para ver cuáles están abiertos.

```
nmap 192.168.1.1
```

> Usado para: Detectar rápidamente puertos abiertos de un host.

### 🕊️ 2. `nmap -sP <rango_IP>` → *(ahora se usa `sn`)*

> Tipo: Volador
>
> **Nombre**: *Detección de Pokémon salvajes*
>
> **Técnica**: `Ping Scan`
>
> **Descripción Técnica**:
>
> No escanea puertos, solo hace ping y análisis ARP para ver qué dispositivos (hábitats) están activos.

```
nmap -sn 192.168.1.0/24
```

> Usado para: Enumerar qué IPs están vivas dentro de un rango.

---

### 👻 3. `nmap -sS <IP>`

> Tipo: Fantasma
>
> **Nombre**: *Sombra Silenciosa*
>
> **Técnica**: `TCP SYN Stealth Scan`
>
> **Descripción Técnica**:
>
> Envía paquetes SYN (como si fuera a iniciar una conexión), pero nunca la completa. Si el host responde con SYN-ACK, sabemos que el puerto está abierto.

```
nmap -sS 192.168.1.1
```

> Usado para: Detectar puertos abiertos sin establecer conexión completa, útil contra firewalls o IDS.

## 🔐 4. `nmap -sT <IP>`

> Tipo: Acero
>
> **Nombre**: *Conexión Directa*
>
> **Técnica**: `TCP Connect Scan`
>
> **Descripción Técnica**:
>
> Usa llamadas del sistema para abrir conexiones completas (SYN-SYN/ACK-ACK). Más detectable pero más fiable si no tienes privilegios.

```
nmap -sT 192.168.1.1
```

> Usado cuando: No tienes permisos para hacer SYN scan (como usuario sin root).

---

## 🧠 5. `nmap -O <IP>`

> Tipo: Psíquico
>
> **Nombre**: *Lectura de Sistema*
>
> **Técnica**: `OS Detection`
>
> **Descripción Técnica**:
>
> Intenta adivinar el sistema operativo observando cómo responde a ciertos paquetes TCP/IP.

```
nmap -O 192.168.1.1
```

> Usado para: Identificar si el enemigo es tipo Windows, Linux, etc.

---

### 🧬 6. `nmap -A <IP>`

> Tipo: Dragón
>
> **Nombre**: *Análisis Total*
>
> **Técnica**: Aggressive Scan
>
> **Descripción Técnica**:
>
> Combina: detección de sistema operativo (`-O`), detección de versiones (`-sV`), traceroute y NSE scripts comunes.

```
nmap -A 192.168.1.1
```

> Usado para: Obtener el máximo de información. Pero es ruidoso
> Precaución fácilmente detectable.

---

### 🌀 7. `nmap -sV <IP>`

> Tipo: Hada
>
> **Nombre**: *Revelación de Tipos*
>
> **Técnica**: Version Detection
>
> **Descripción Técnica**:
>
> Detecta la versión de los servicios corriendo en cada puerto.

```
nmap -sV 192.168.1.1
```

> Usado para: Saber si el puerto 80 corre Apache 2.4.7 o Nginx 1.18, etc.

---

### 💥 8. `nmap -p- <IP>`

> Tipo: Lucha
>
> **Nombre**: *Puño Infinito*
>
> **Técnica**: `Full Port Scan`
>
> **Descripción Técnica**:
>
> Escanea absolutamente **todos** los puertos TCP (1 al 65535).

```
nmap -p- 192.168.1.1
```

> Usado para: No dejar ningún puerto oculto, incluso los no estándar.

---

### 📜 9. `nmap --script <script> <IP>`

> Tipo: Legendario
>
> **Nombre**: *Ataque con Movimiento Personalizado*
>
> **Técnica**: `Nmap Scripting Engine (NSE)`
>
> **Descripción Técnica**:
>
> Ejecuta scripts para tareas especiales: vulnerabilidades, autenticación, enumeración de servicios.

```
nmap --script vuln 192.168.1.1
```

🧪 Ejemplos de scripts útiles:

- `vuln`: Busca vulnerabilidades conocidas.
- `http-enum`: Enumera rutas en un servidor web.
- `smb-os-discovery`: Identifica sistema operativo vía SMB.

---

## 🧠 BANDERAS ADICIONALES (ATRIBUTOS)

| Bandera | Significado | Tipo Pokémon |
|---|---|---|
| `-T0` a `-T5` | Nivel de velocidad del escaneo (T0 = más lento/sigiloso, T5 = más rápido/ruidoso) | Eléctrico (velocidad) ⚡ |
| `-Pn` | No hace ping antes de escanear (como entrar sin llamar) | Siniestro 👤 |
| `-F` | Escaneo rápido (100 puertos comunes) | Volador 🕊️ |
| `-v` / `-vv` | Modo verbose (más información en tiempo real) | Psíquico 🧠 |

---

## 🧩 EJEMPLOS COMPLETOS

### 🔎 Búsqueda de Pokémon raros en toda la región:

```
nmap -p- -sS -sV -O -T4 192.168.1.1
```

➡️ Escaneo completo, agresivo y detallado.

---

### 🤫 Infiltración sigilosa en un gimnasio:

```
nmap -sS -Pn -T1 192.168.1.1
```

➡️ Para evitar ser detectado por firewalls o IDS.

---

### 🧪 Detección de vulnerabilidades en un pokémon legendario:

```
nmap -sV --script vuln 192.168.1.1
```

---