Martín Losada

Qué ve un atacante cuando escanea tu red con Nmap

Ciberseguridad

🔍 ¿Qué ve un atacante cuando escanea tu red con Nmap?

Cuando hablamos de ciberseguridad, muchas veces asumimos que "todo está bien configurado". Pero… ¿realmente sabes qué está expuesto en tu red?
Con Nmap, cualquier persona (incluso sin acceso previo) puede escanear tu infraestructura y obtener información crítica.

En este documento simulamos un escaneo típico que haría un atacante para detectar vulnerabilidades rápidamente.

-

🧠 ¿Qué es Nmap?

Nmap (Network Mapper) es una herramienta gratuita y de código abierto utilizada para descubrir hosts, servicios, puertos abiertos y sistemas operativos en una red.
Es ampliamente utilizada tanto por profesionales de la ciberseguridad como por atacantes en la fase de reconocimiento.

-

🛠️ Escaneos más utilizados

✅ Escaneo Básico

```
nmap 192.168.1.1
```

Muestra puertos abiertos y si el host está activo. Ideal para comprobar qué está mínimamente accesible desde fuera.

-

✅ Detección de Servicios

```
nmap -sV 192.168.1.1
```

Detecta versiones de servicios (Apache, SSH, MySQL…)
🔎 Si encuentra versiones antiguas, el atacante buscará exploits públicos asociados.

-

✅ Detección de Sistema Operativo

```
nmap -O 192.168.1.1
```

Intenta identificar el sistema operativo objetivo.
🔧 Saber si es Linux, Windows o una versión concreta ayuda a preparar ataques más efectivos.

-

✅ Búsqueda de Vulnerabilidades

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

Ejecuta scripts NSE para descubrir vulnerabilidades conocidas.
⚠️ ¡En muchos casos, sin necesidad de autenticarte ya puedes ver posibles fallos críticos!

-

📊 Tabla resumen de escaneos

Tipo de Escaneo	Comando	¿Qué te dice?	Riesgo si está expuesto
Escaneo básico	`nmap IP`	Puertos abiertos	Medio
Detección de servicios	`nmap -sV IP`	Versiones de servicios	Alto
Sistema Operativo	`nmap -O IP`	Probable sistema operativo	Medio
Vulnerabilidades	`nmap --script vuln IP`	Vulnerabilidades asociadas a los servicios	Muy alto

-

🚨 Riesgos comunes detectables

- Servicios web con versiones antiguas (Apache, PHP…)
- Puertos de administración abiertos (SSH, RDP)
- Servidores de bases de datos accesibles externamente
- Uso de protocolos inseguros (Telnet, FTP)
- Firewalls mal configurados

-

🧰 Herramientas complementarias

- **Wireshark** – para analizar el tráfico de red
- **OpenVAS / Nessus** – escáneres de vulnerabilidades profundos
- **Nikto** – para escaneo web más específico
- **Zenmap** – interfaz gráfica de Nmap
- **Shodan** – búsqueda de dispositivos expuestos públicamente

-

✅ Recomendaciones tras un escaneo

- Cierra puertos innecesarios
- Desactiva servicios antiguos o sin uso
- Aplica parches de seguridad pendientes
- Aísla los servicios internos con firewalls
- Configura autenticación fuerte
- Monitoriza la actividad tras cada cambio
- Documenta los resultados de forma periódica

-

📚 Recursos para aprender más

- 📖 Manual oficial de Nmap: https://nmap.org/book/
- 💻 TryHackMe – Curso gratuito de Nmap
- 🧪 Hack The Box – Máquinas para practicar escaneos

-

🎯 Conclusión

> “El primer paso hacia una red segura es verla con los ojos del atacante.”
> Hazte escaneos internos. Aprende a leer lo que ve un intruso. Y actúa.