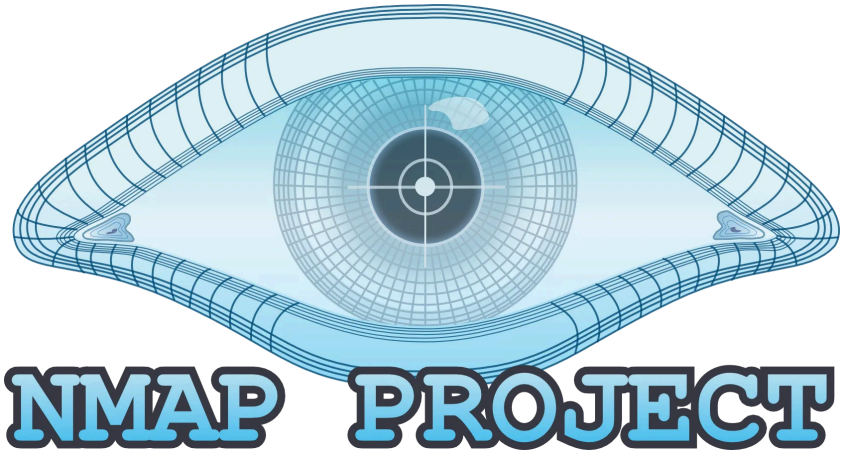

Aprende a Usar NMAP

Aquí tienes tu guía sobre la herramienta **Nmap**. En ella encontrarás:

- Qué es NMAP y sus principales usos.
- Los **comandos** esenciales.
- Una lección **gratis** del curso de Nmap de la academia.
- Un **vídeo** demostración de mi canal de YouTube.

Así que... ¡Vamos al lío!

1. Qué es y para qué se usa

NMAP (Network Mapper) es una herramienta de **código abierto** para la exploración de redes y auditoría de seguridad.

Es muy utilizada por profesionales de la ciberseguridad y administradores de sistemas para detectar dispositivos activos, escanear puertos y servicios, y evaluar la seguridad de la red.

Nos permitirá:

- Descubrir hosts en una red
- Identificar puertos y servicios activos
- Realizar fingerprinting de versiones y sistemas operativos
- Análisis de vulnerabilidades sobre los activos descubiertos

2. Comandos para descubrir Hosts

Para el descubrimiento de activos en una red con NMAP debemos utilizar la opción **-sn**, que deshabilitará el escaneo de puertos y se centrará SÓLO en detectar equipos conectados a la red.

Comandos útiles:

- ***nmap -sn <dirección_IP_o_nombre_de_host>***
    - detecta si existe un host en la red
- ***nmap -sn <IP1-IP2>***
    - encuentra los host en un rango de IPs
- ***nmap -sn <subred>/máscara_de_red***
    - escanea la subred en busca de hosts

3. Tipos de escaneo

Existen varios tipos de escaneos, cada uno con sus ventajas y desventajas. Los tres más comunes y usados son los siguientes:

- ***nmap -sT <dirección_IP>***
    - escaneo TCP Connect, se ejecuta por defecto
- ***nmap -sS <dirección_IP>***
    - escaneo TCP SYN, más sigiloso e indetectable
- ***nmap -sU <dirección_IP>***
    - escanea los protocolos y servicios UDP

4. Comandos para escanear puertos

Una vez tenemos los hosts activos de una red, el siguiente paso es detectar qué puertos y servicios tiene habilitados. Para ello usaremos el parámetro **-p**.

Comandos útiles:

- ***nmap -p <puerto1,puerto2,puerto3,...> <dirección_IP>***
    - escaneamos los puertos especificados
- ***nmap -p- <dirección_IP>***
    - escaneamos todos los puertos del activo

5. Identificación de Versiones y Sistemas Operativos

Con los servicios enumerados, procederemos a detectar las versiones de los mismos, así como el sistema operativo del hosts objetivo.

- ***nmap -O <dirección_IP>***
    - detección del sistema operativo
- ***nmap -p <puerto1,puerto2,puerto3,...> -sV <dirección_IP>***
    - detección de la versión de los servicios ejecutándose en los puertos especificados

6. Detección de vulnerabilidades con NSE

Por último, podemos ver si las versiones de los servicios se encuentran afectadas por alguna vulnerabilidad o alguna configuración insegura. Para ello podemos usar los scripts por defecto de NSE (NMAP Search Engine).

Estos scripts nos detectarán de forma automática si el activo presenta alguna de las vulnerabilidades "**más comunes**".

- ***nmap -p <puerto1,puerto2,puerto3,...> -sV <dirección_IP> -sC***

NOTA: Existen muchísimos tipos de scripts en función a su objetivo, incluso los puedes crear tú mismo.

7. Ajustar los tiempos de escaneo

Los escaneos con NMAP son altamente personalizables. Un claro ejemplo de esto es el parámetro **-TX**, que especifica lo rápido que tiene que ser un escaneo.

A continuación te dejo las opciones que tiene:

- ***nmap -T0 <dirección_IP>***
    - Paranoid (Paranoid, más lento)
- ***nmap -T1 <dirección_IP>***
    - Sneaky (Sigiloso)
- ***nmap -T2 <dirección_IP>***
    - Polite (Cortés)
- ***nmap -T3 <dirección_IP>***
    - Normal (Normal, el que se ejecuta si no se pone nada)
- ***nmap -T4 <dirección_IP>***
    - Aggressive (Agresivo)

- ***nmap -T5 <dirección_IP>***
    - Insane (Insano, más rápido)

8. Guardar escaneo en un archivo

Si queremos guardar los resultados de nuestro escaneo en un archivo, solo tenemos que usar una de las siguientes opciones:

- ***nmap -oA <dirección_IP>***
    - lo guarda en todos los formatos posibles
- ***nmap -oN <dirección_IP>***
    - lo guarda en formato legible por terminal

9. Extras

Y cómo te he dicho, aquí tienes una lección gratuita de nuestro curso **NMAP PROFESSIONALS** y el vídeo práctico de YouTube.

- **Lección gratis** 👇

  https://www.contandobits.com/lecciones/introduccion-al-curso-de-nmap/

- **Vídeo de YouTube** 👇

  Cómo Usar NMAP y WIRESHARK para Escanear y Ver el Tráfico de Red Local con Ka...