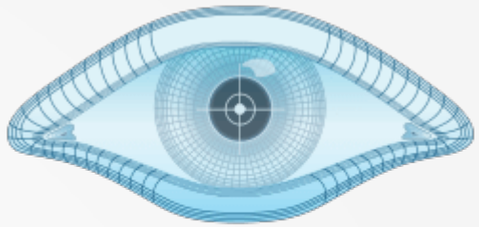

NMAP

Javier Galera Garrido
Antonio Miguel Morillo Chica

Indice

1. ¿Qué es Nmap?

- Es una herramienta de código abierto para el rastreo de puertos.
  - Método para conocer el nivel de seguridad de la configuración de los servivios que se ofrecen.
  - Una de las primeras etapas que realiza un atacante contra una victima.

Índice

2. ¿Qué permite hacer nmap?

- Entre muchas cosas nos ayuda a:
  - Descubrir e identificar equipos en la red.
  - Identificar puertos abiertos.
  - Conocer los servivios que ofrecen los equipos.
  - Sistema operativo de los equipos y versión del mismo.
  - Conocer si se está usando cortafuegos.
  - Conocer algunas caracteristicas del hardware de la red.

Indice

3. ¿Cómo funciona?

- Su funcionamiento se basa en el envió de paquetes IP en formato raw (crudos)
  - Paquetes que no han sufrido modificaciones y por tanto originales sea cual sea el protocolo.

3.1 ¿Cómo funciona?

- Nmap usa diferentes tipos de sondeos
  - TCP SYN (-sS):

    Envio de paquete SYS para recibir una respuesta ACK, RST, ICMP o ninguno.
    - ACK: Acuse de recibo (puerto está abierto)
    - RST: Reset (puerto está cerrado)
    - ICMP: Internet Control Message Protocol (filtrado)
  - TCP connect() (-sT)
  - UDP (-sU)
  - Otros TCP Null, FIN, Xmas, TCP ACK (-sN, -sF, -sX y -sW) entre otros.

Índice

4. ¿Cómo se usa? (entrada)

- Tenemos dos opciones:
  - Zenmap interfaz grafica.
  - Por terminal:

    nmap <tipo de sondeo> <Opciones> <especificaciones>

4.1 ¿Cómo se usa? (salida)

- Nmap nos dará como salida un listado de objetivos analizados. La parte más impotante es la “tabla de puertos interesantes”.

- Dicha tabla lista el numero de puerto, el protocolo, el nombre más común del servicio y su estado.

  - Estados: open, filtered, colsed y unfiltered.

Open (abierto)	Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Es decir, que hay una aplicación aceptando conexiones de algún tipo.
Filtered (filtrado)	Filtrado indica que un firewall (cortafuegos), filtro de reglas del router, u otro obstaculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto.
Closed (Cerrado)	Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos aunque podrían abrirse en cualquier momento.
Unfiltered (no filtrado)	Los clasificados como no filtrados son aquellos que responden a los sondeos de Nmap, pero para los que Nmap no puede determinar si se encuentran abiertos o cerrados.

Indice

5. Demo

- Para la demo usaremos los siguientes comandos:
  - namp <ip_máquina>
  - namp -o <ip_máquina>
  - namp -A <ip_máquina>
  - nmap -n -Pn <ip_máquina> -p - --script=vuln

6. Conclusión

Esta herramienta es sumamente poderosa, solo hemos tocado algunos aspectos. Saber que está expuesto en nuestra red es el primer paso para poder protegerla, si se encuentran puertos extraños que deberían estar abiertos, debemos cerralos, estos pueden ser entradas para los atacantes e incluso virus. Algunos puertos normales como el SSH si no se usa, lo mejor es cerrarlo o redireccionarlo a otro puerto. Mientras más controlado esté nuestro sistema menos oportunidades daremos para que este sea roto por un acante.