



NMAP

Javier Galera Garrido
Antonio Miguel Morillo Chica

Indice

1. ¿Qué es nmap?
2. ¿Cómo funciona?
3. ¿Qué permite hacer?
4. ¿Cómo se usa? (Entrada)
 - 4.1 ¿Cómo se usa? (Salida)
5. Demo

1. ¿Que 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 servicios que se ofrecen.
 - Una de las primeras etapas que realiza un atacante contra una víctima.

Indice

1. ¿Qué es nmap?
2. ¿Cómo funciona?
3. ¿Qué permite hacer?
4. ¿Cómo se usa? (Entrada)
 - 4.1 ¿Cómo se usa? (Salida)
5. Demo

2. ¿Cómo funciona?

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

Indice

1. ¿Qué es nmap?
2. ¿Cómo funciona?
3. ¿Qué permite hacer?
4. ¿Cómo se usa? (Entrada)
 - 4.1 ¿Cómo se usa? (Salida)
5. Demo

3. ¿Que permite hacer nmap?

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

Indice

1. ¿Qué es nmap?
2. ¿Cómo funciona?
3. ¿Qué permite hacer?
4. ¿Cómo se usa? (Entrada)
 - 4.1 ¿Cómo se usa? (Salida)
5. Demo

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 importante es la “tabla de puertos interesantes”.
- Dicha tabla lista el número de puerto, el protocolo, el nombre más común del servicio y su estado.
 - Estados: open, filtered, closed 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

1. ¿Qué es nmap?
2. ¿Cómo funciona?
3. ¿Qué permite hacer?
4. ¿Cómo se usa? (Entrada)
 - 4.1 ¿Cómo se usa? (Salida)
5. Demo

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`