

HERRAMIENTA PARA EL MAPEO DE LA RED



Network mapper...

Network mapper... >nmap

TITULO: NETWORK MAPPING FROM LINUX OS (PARTE 1)

AUTOR: Luis Miguel Castañeda Ibañez

ESTUDIANTE DE LA FACULTAD #2, 4TO AÑO

Network Mapper, más conocida como **Nmap**, es una de las herramientas más avanzadas para realizar exploración de puertos desde sistemas GNU/Linux.

Nmap básico>...

Nmap brinda posibilidades como que, implementa la gran mayoría de técnicas conocidas para exploración de puertos y permite descubrir información de los servicios y sistemas encontrados, así como el reconocimiento de huellas identificativas de los sistemas escaneados...

..permite hacer una auditoría de nuestra red. Nmap permite una rápida visualización de puertos inseguros o abiertos por equivocación en los equipos de nuestra red.

...permite comprobar la configuración de los elementos de seguridad. Nmap puede ser de gran utilidad para comprobar la configuración de los elementos de seguridad de nuestra red como, por ejemplo, sistema cortafuegos, sistemas de detección de intrusos, etc.

...permite comprobar la configuración de los elementos de red. Mediante Nmap podemos realizar una serie de comprobaciones de los dispositivos de conectividad y enrutamiento de nuestra red y detectar así si hay algún malfuncionamiento o, al contrario, si todo funciona con normalidad.

Nmap es más que un simple escáner de puertos y algunas de las funcionalidades más interesantes que han hecho de Nmap una de las herramientas de exploración más importantes y populares son las siguientes:

-Alta velocidad de exploración. Nmap ofrece una extraordinaria velocidad a la hora de realizar una comprobación de sistemas activos y servicios ofrecidos por dichos sistemas.

-Descubrimiento de huellas identificativas. Nmap no hace más que una predicción del sistema operativo que se esconde detrás del equipo que está explorando.

¿Cómo lo hace...? Pues sencillo, basa la predicción en contrastar la información recibida frente a una gran base de datos de respuestas basadas en tráfico IP, ICMP, UDP y TCP de centenares de sistemas operativos existentes en la actualidad.

-Funciones para realizar suplantación. Es posible que un atacante pueda hacerse pasar por otros equipos de confianza con el objetivo de atravesar la protección que ofrece el sistema cortafuegos de una red. Nmap puede ayudar a modificar la configuración de estos sistemas cortafuegos disminuyendo, así, la posibilidad de recibir un ataque de suplantación.

-**Posibilidad de guardar y leer ficheros de texto.** Nmap ofrece la posibilidad de guardar sus resultados en forma de ficheros de texto de salida así como la posibilidad de leer la información de exploraciones anteriores por parte del propio Nmap.

☺...Y así muchachos, muchas opciones más como estas...!

Nmap puede ser utilizado tanto para una sencilla exploración rutinaria contra los equipos de nuestra red, como para realizar una compleja predicción de números de secuencia y descubrimiento de la huella identificativa de sistemas remotos protegidos por sistemas cortafuegos. Por otro lado, puede ser utilizado para la realización de una única exploración o de forma interactiva, para poder realizar múltiples exploraciones desde un mismo equipo.

Nmap desde consola>...

```
^ v x root@bt: ~
File Edit View Terminal Help
root@bt:~# nmap 192.168.1.1
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2012-01-05 19:49 ART
Nmap scan report for 192.168.1.1
Host is up (0.051s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
80/tcp    open  http
1900/tcp  open  upnp
49152/tcp open  unknown
MAC Address: D8:5D:4C:C7:DC:EE (Tp-link Technologies Co.)

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
root@bt:~#
```

nmap [param] [host]

Zona de puertos con sus estados:

- Closed> cerrado
- Open> abierto
- Filtred> filtrado
- Unfiltred> no filtrado

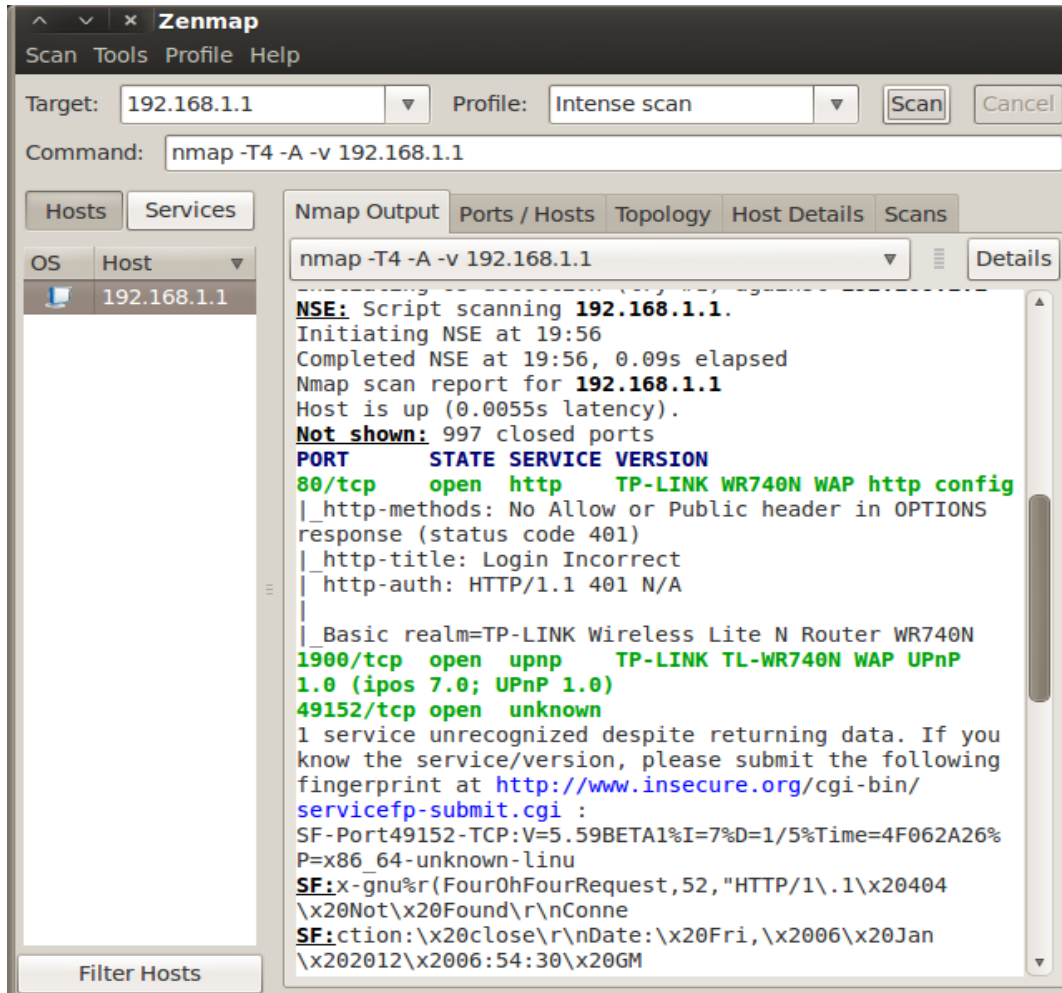
PORT	STATE	SERVICE
80/tcp	open	http
1900/tcp	open	upnp
49152/tcp	open	unknown

📄 Lo primordial es su tabla de puertos con sus estados que son los siguientes:

- CLOSED:** Cerrado (no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento)
- OPEN:** Abierto (la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto)
- FILTRED:** Filtrado (indica que un cortafuego, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto)
- UNFILTRD:** No Filtrado (responden a los sondeos de Nmap, pero no puede determinar si se encuentran abiertos o cerrados.)

Respetar parámetros en mayúsculas y minúsculas porque varía su función.

Nmap desde interfaz gráfica>...





Aclaro que **Zenmap** es lo mismo que Nmap pero de esta forma incluye interfaz gráfica.


Nmap en práctica>...


Ejemplos de cómo trabaja NMAP directamente desde la consola de Linux. Espero les ayude en conocimiento.


 `nmap [Parámetro] [Host] | nmap 10.51.19.229`

 En este caso no tenemos parámetros ya que es solo un simple mapeo IP para observar los puertos abiertos.


 `nmap -p [Puertos] [Host] | nmap -p 80,135,2000,8080 10.51.19.229`


 Para escanear puertos que nosotros queramos.


 `nmap -O [Host] | nmap -O 10.51.19.229`


 Ver el sistema operativo que tiene el equipo instalado.

 `nmap -sP [Puerta de enlace] | nmap -sP 192.168.1.1-255`


 Es para ver hosts activos en una red y para ello debemos saber la puerta de enlace; o sea, sabemos que en una red solo se alojan máximo 255 hosts, lo que se hará será un **ping scan** para saber cuántos host hay en la red.


 `nmap -sV [Host] | nmap -sV 10.51.19.229`

 Para ver puertos, servicios y la versión de los servicios de un host.

 `nmap -sV -O [Host] | nmap -sV -O 10.51.19.229`

 Para sacar Servicios, versiones y sistema operativo.

 `nmap -sV [Host] -oN [dirección para guardar archivo .txt] | nmap -sV [192.168.1.3] -oN [Desktop/archive.txt]`

 Nmap permite exportar escaneos en formato *.TXT o *.XML. Los parámetros para ello son: **-oN** (txt) y **-oX** (xml).

Bueno muchachos, son estos los primeros pasos para trabajar con NMAP. Por lo que han visto es una herramienta muy poderosa, directamente desde la consola o el terminal de nuestro OS Linux y espero que les haya gustado.

¡Seguiremos en contacto! 😊

P.D.: Ah! Eso sí, todos estos ejemplos pude comprobarlos desde mi PC pero como pudieron observar los IP puestos y demás parámetros de red (puerta de enlace) no son aquí reales. Pórtense bien y no hagan travesuras...