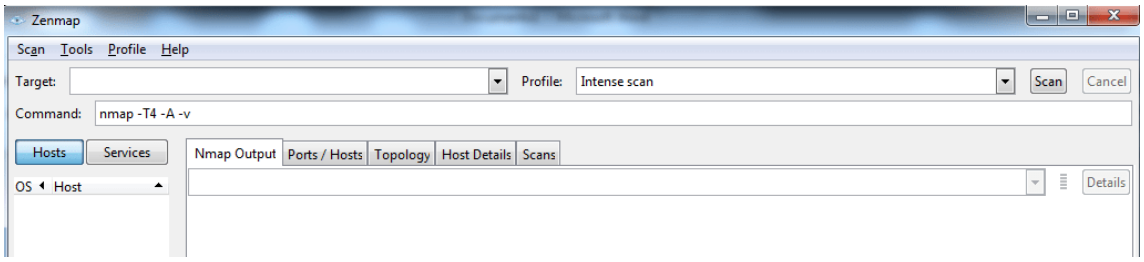
Ejercicios resueltos nmap

NMAP es una herramienta para escanear puertos, servicios, versiones, sistemas operativos, …, esta herramienta Open Source permite a los auditores de Seguridad realizar un completo escaneo de puertos, detectar si un host se encuentra activo, además permite detectar servicios con sus respectivas versiones. Por otro lado esta herramienta no es solo un simple escáner de puertos, ya que permite detectar vulnerabilidades a través de sus scripts personalizados en lenguaje LUA.

Lo primero de todo hay que tener en cuenta que NMAP es una herramienta para escanear la red, por lo tanto, hay herramientas que si estás escaneando red, es posible que te metan en **listas negras** (porque si estás escaneando la red, es posible que no sea para nada bueno), si meten tu IP en listas negras podrías tener problemas para conectarte a diversas web's, no poder enviar correos electrónicos en sistemas de correo como Gmail, hotmail, …

Lo ideal es lanzar escaneos sobre un laboratorio echo por nosotros, en nuestra LAN, probar sobre nuestros propios servidores, o bien probar en la url siguiente de NMAP que está indicada para ello, http://scanme.nmap.org/

Tiene 2 modos de ejecución, bien en modo gráfico (**ZENMAP**) o bien en modo comandos, explicaremos el modo comandos, y gracias a este entenderemos mucho mejor el modo gráfico.



NMAP tiene muchísimas funcionalidades, nos centraremos solamente en algunos ejemplos para ver su potencia.

Nmap utiliza varios enfoques de escaneo de puertos. La siguiente tabla resume los tipos de análisis «enlatados» y los indicadores de línea de comando correspondientes:

- **-sT: Escaneo de** Conexión TCP ()
- **-sS:** Escaneo SYN
- **-sA:** ACK Scan
- **-sW:** Ventana
- **-sN:** escaneo nulo
- **-sF:** escaneo FIN
- **-sX:** Escaneo de **Navidad**
- **-sU:** Escaneo UDP
- **-sM:** Escaneo de Maimón
- **-sO:** Escaneo de protocolo IP
- **-sI:** host: escaneo inactivo del puerto
- **-b:** Escaneo de rebote de FTP

Ejercicios:

Ejercicio 1. Escaneo básico sobre equipo o red.

Equipo: # **nmap 172.16.0.132**

Red: # **nmap 172.16.0.0/24**

Ejercicio 2. Filtrado de puertos.

Por defecto, Nmap escanea los 1000 puertos más usados: 21 (ftp), 22 (ssh), 80 (http), 53 (DNS), …

Se puede seleccionar puertos y rangos de los mismos.

➢ Puertos concretos **# nmap -p 21,22,80 172.16.0.132**

➢ Rango de puertos **# nmap -p 20-100 172.16.0.132**

➢ Escaneos UDP **# nmap -p 53,123 -sU 172.16.0.132**

Ejercicio 3. Deshabilitar la resolución inversa de nombres. Con esto conseguimos una respuesta más rápida del escaneo.

 # nmap -n 172.16.0.132

Ejercicio 4. Modo Debug (-v/-vv…), vemos lo que está haciendo internamente el programa.

#nmap -vv 172.16.0.132

Ejercicio 5. Descubrimiento de servicios.

Conocer qué servicio escucha detrás de un puerto.

➢ Versión del servicio usando los banners de respuesta

#nmap -sV 172.16.0.132

➢ Intensidad del escaneo

#nmap -version-intensity 9 172.16.0.132

Mayor intensidad → más pruebas → pero más visibles

➢ Sistemas Operativos

#nmap -O 172.16.0.132

Ejercicio 6. Escaneo TCP SYN (-sS) al puerto 443.

El método más común de escaneo TCP, es el escaneo SYN. Esto implica crear una conexión parcial al host en el puerto de destino por medio de un paquete SYN y luego evaluando la respuesta del host. Si el paquete de solicitud no es filtrado o bloqueado por un firewall, entonces el host responderá enviando un paquete SYN/ACK si el puerto está abierto, de lo contrario enviará un paquete RST.

#nmap -sS -p 443 172.16.0.1

Con la línea de comando anterior, solo se escaneará el puerto 443. Para escanear todos los puertos de la máquina, use el indicador *-p* :

#nmap -sS 192.168.1.100 -p1-65535

Ejercicio 7. Para escanear una gran cantidad de máquinas, puedes usar rangos y comodines.

#nmap -sA 192.168. *. 1-10,250-254

Lo anterior escaneará todo lo que comience con **192.168** y termine con **1–10** o **250–254**. También se puede utilizar la notación CIDR menos flexible. A continuación, se muestra un ejemplo sobre cómo realizar un escaneo UDP en una subred de clase C:

#nmap -sU 192.168.0.0/24

Consejos para realizar Pentesting

Para realizar un Pentesting a una entidad en particular, es importante dejar la menor cantidad de rastros, por esta razón a continuación se explicará, como realizar un Pentesting adecuado con la herramienta nmap.

Lo primero que es importante mencionar es que nmap posee un rango de escaneo, el cual está definido dentro de los números del 0 al 5. ¿Para qué sirve esto?, principalmente cuando se requiere hacer un Pentesting, la forma más óptima de realizarlo es siendo sigiloso, de tal manera que cada uno de estos números representan la agresividad con la que se envían los paquetes hacía el(los) host(s). Un ejemplo de esto es lo siguiente.

Estructura:

nmap -T[0-5] target

Rango	Nombre	Detalle
–T0	Paranoico	Muy lento - No recomendable
–T1	Sigiloso	Útil para la evasión de IDS - Lento
–T2	Educado	No interfiere con el objetivo - Lento pero recomendable
–T3	Normal	Escaneo por defecto
–T4	Agresivo	Escaneo rápido y agresivo - No recomendable
–T5	Demente	Escaneo muy rápido y muy agresivo - No recomendable

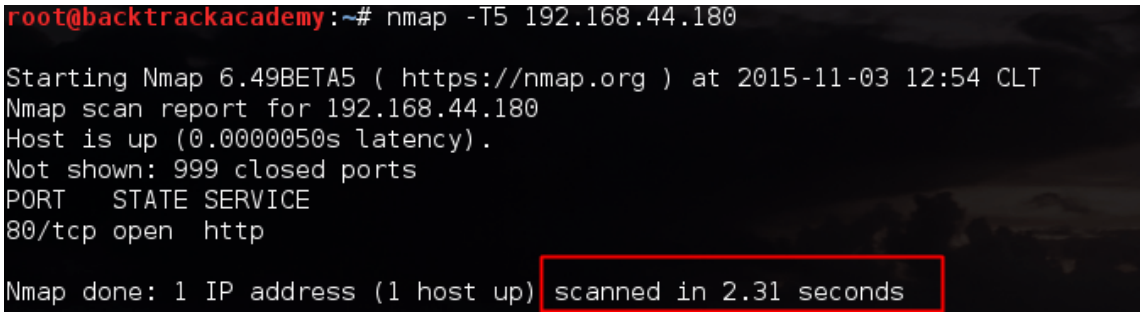
Estructura de agresividad en Nmap

Al escanear un host con la opción -T0 se tiene lo siguiente

Escaneo agresividad 0 nmap

El escaneo no tiene sentido ya que tardaría demasiado tiempo en ejecutarse.

Ahora se realizó un escaneo con el nivel de agresividad más alto.



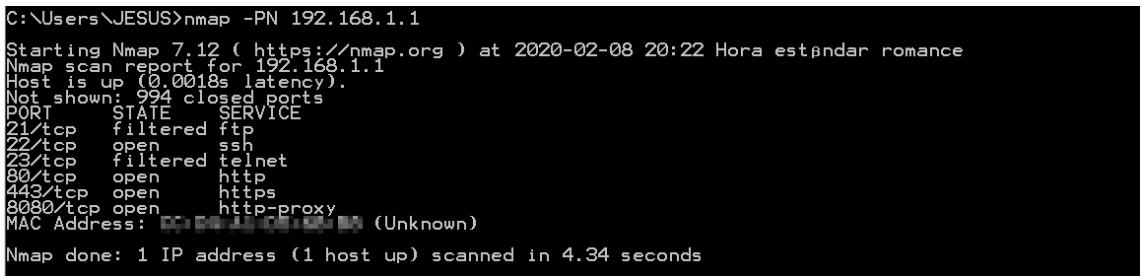
Escaneo agresividad 5 nmap

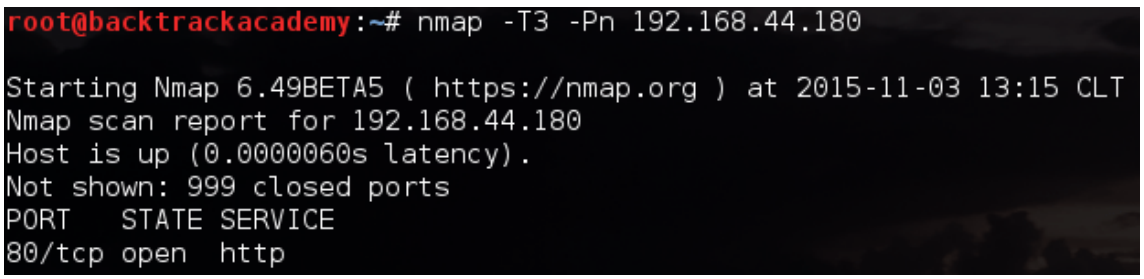
El escaneo finalizó en 2.31 segundos, el problema de este escaneo es que deja muchos logs en el servidor auditado, por esta razón no se recomienda utilizar esta opción, lo más óptimo es realizar un escaneo entre los rangos T2 y T3.

Otra medida de realizar un escaneo sigiloso, es realizar un escaneo sin ping. Por defecto nmap realiza un ping al host antes de realizar un escaneo, en algunos casos se presentan dos escenarios, el primero es que nmap al ejecutar un escaneo por ping puede ser detectado por un IPS y esto es un problema, ya que al momento de realizar un escaneo se requiere la mayor cautela posible, el segundo caso es que en algunos casos al detectar que el escaneo por ping no fue exitoso hacia el host, nmap automáticamente envía un mensaje diciendo que el host no se encuentra habilitado, y no siempre es así. Por esta razón lo ideal es siempre realizar un escaneo que no verifique ping.

Opción	Detalle
–Pn	No verifica el ping para realizar el escaneo

Opción para evitar el ping durante el escaneo





Combinando opciones de escaneo sigiloso.

Otra forma de realizar un escaneo sigiloso es agregar la opción *–f*, esta opción permite fragmentar los paquetes enviados, de tal manera que esto permitirá regularizar el tráfico enviado hacía el host.

Opción	Detalle
–f	Opción para fragmentar paquetes

Opción para fragmentar los paquetes enviados

```
root@backtrackacademy:~# nmap -T3 -Pn -f 192.168.44.180

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-03 13:22 CLT
Nmap scan report for 192.168.44.180
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
```

Métodos de escaneo sigiloso

Anexo a esto es importante conocer los servicios habilitados en dicho host y por supuesto sus respectivas versiones, para esto se encuentra disponible la opción *–sV,* la cual permite enumerar las versiones de los servicios que se encuentran corriendo en la máquina objetivo.

Opción	Detalle
–sV	Permite mostrar información sobre el banner de un servicio

Opción para obtener información de banner de los servicios del host

```
root@backtrackacademy:~# nmap -T3 -Pn -f -sV 192.168.44.180

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-11-03 13:28 CLT
Nmap scan report for 192.168.44.180
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
```

Servicio apache httpd 2.4.10 (Debian)

Estos son solo algunos de los métodos de escaneo sigiloso con nmap, además es posible obtener información sensible sobre los servicios que están corriendo en el host objetivo y de esta manera poder buscar si existen *exploit*s asociados a cada uno de estos servicios.

Más alternativas NMAP

ZMAP (https://zmap.io)

Escáner Open-Source orientado a redes grandes. Teóricamente podría escanear internet en una hora aproximadamente pero solo está orientado a IPv4.

MASSCAN (http://tools.kali.org/information-gathering/masscan)

Teóricamente puede escanear internet en 6 minutos. Funciona parecido a otras herramientas como scanrand, unicornscan o zmap. Además de su velocidad es más flexible permitiendo rangos de direcciones IP y puertos.

SHODAN

Escáner pasivo online. Es un tercero quien escanea la red, y nosotros consultamos sobre su motor de búsqueda.

Registro y uso gratuito, pero si pagamos por este servicio nos va a devolver más resultados.

Subdividido por categorías, con buen conjunto de filtros. Escaneo de IP's, puertos y servicios.

A modo de prueba, tienes permiso de sondear el servidor scanme.nmap.org. Este permiso sólo incluye sondear mediante Nmap y no para probar "exploits" o ataques de denegación de servicio. Por favor, para conservar el ancho de banda no inicie más de una docena de sondeos contra este servidor el mismo día. Si se abusa de este servicio de sondeo se desconectará y Nmap reportará Failed to resolve given hostname/IP: scanme.nmap.org ("No se pudo resolver la dirección IP o nombre datos: scanme.nmap.org"). Este permiso también se aplica a los servidores analizame2.nmap.org, analizame3.nmap.org, y así sucesivamente, aunque esos servidores actualmente no existen.

```
nmap -v scanme.nmap.org
```

Esta opción sondea todos los puertos TCP reservados en el servidor scanme.nmap.org. La opción -v activa el modo detallado (también llamado verboso).

```
nmap -sS -O scanme.nmap.org/24
```

Lanza un sondeo de tipo SYN sigiloso contra cada una de las 255 máquinas en la "clase C" de la red donde está el sistema "analizame". También intenta determinar cual es el sistema operativo que se ejecuta en cada máquina que esté encendida. Esto requiere permisos de root por la opción de sondeo SYN y por la de detección de sistema operativo.

```
nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127
```

Lanza una enumeración de equipos y un sondeo TCP a cada uno de la primera mitad de las 255 posibles subredes de 8 bit en la red de clase B 198.116. Esto probará si los sistemas están ejecutando sshd, DNS, pop3d, imapd o tienen un servidor en el puerto 4564. Para cualquier puerto que se encuentre abierto, se realizará una detección de versión para determinar qué aplicación se está ejecutando.

```
nmap -v -iR 100000 -P0 -p 80
```

Solicita a Nmap que elija 100.000 sistemas aleatoriamente y los sondee buscando servidores web (puerto 80). La enumeración de sistemas se deshabilita con -P0 ya que es un desperdicio enviar un par de pruebas para determinar si el sistema debe ser analizado cuando de todas maneras sólo se va a analizar un puerto.

```
nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap
216.163.128.20/20
```

Esto sondea 4096 IPs para buscar cualquier servidor web (sin enviar sondas ICMP) y guarda la salida en formato para grep y en XML.