

Uso del Escaner de puertos Nmap

1. Copyleft 2004 debianitas.net

Emilio Guirado Hernández

Se puede copiar, modificar o distribuir este manual bajo las condiciones de la licencia **GNU General Public License (GNU GPL)**

Si se desea hacer una copia total o parcial del documento se deberá adjuntar debidamente la identidad del autor así como la dirección www.debianitas.net en las partes superior e inferior del manual.

El autor no se hace responsable de los daños producidos por la utilización de la información del documento.

www.debianitas.net Copyleft 2004 **GeeSeCillo** geesecillo@debianitas.net

2. Introducción y Objetivos

- ¿Que es **Nmap**? Es una herramienta para administradores de sistemas y gente interesada en el escaneo de grandes o pequeñas redes para determinar los equipos que se encuentran activos y cuales son sus servicios.

En definitiva un escáner de puertos muy potente.

- El objetivo sería poder determinar si un servidor o máquina está en uso y que servicios ofrece.

3. Conceptos Previos

Muy brevemente para que los usuarios poco adentrados en el tema puedan seguir con facilidad el manual debemos tener claras algunas ideas.

¿Que es un puerto?:

Un puerto es una zona en la que dos ordenadores (hosts) intercambian información

¿Que es un servicio?:

Un servicio es el tipo de información que se intercambia con una utilidad determinada como ssh o telnet.

¿Que es un Firewall?:

Un firewall acepta o no el tráfico entrante o saliente de un ordenador.

¿Que son paquetes SYN?:

Así por encima, pueden ser paquetes que abren un intento de establecer una conexión TCP.

4. Instalación

Para instalar **Nmap** en debian podemos recurrir a **Apt**, tan fácil como siempre.

```
bash# apt-get install nmap
```

Si deseamos instalarlo bajándonos las fuentes del programa, iremos a la dirección:
http://www.insecure.org/nmap/nmap_download.html

Una vez bajadas las fuentes solo nos queda descomprimirlas y compilarlas.

```
Bash$ bzip2 -cd nmap-VERSION.tar.bz2 | tar xvf -  
Bash$ cd nmap-VERSION  
Bash$ ./configure  
Bash$ make  
Bash$ su  
Bash# make install
```

Una vez compilado tendremos el ejecutable "nmap" y podremos usarlo como detallaremos posteriormente.

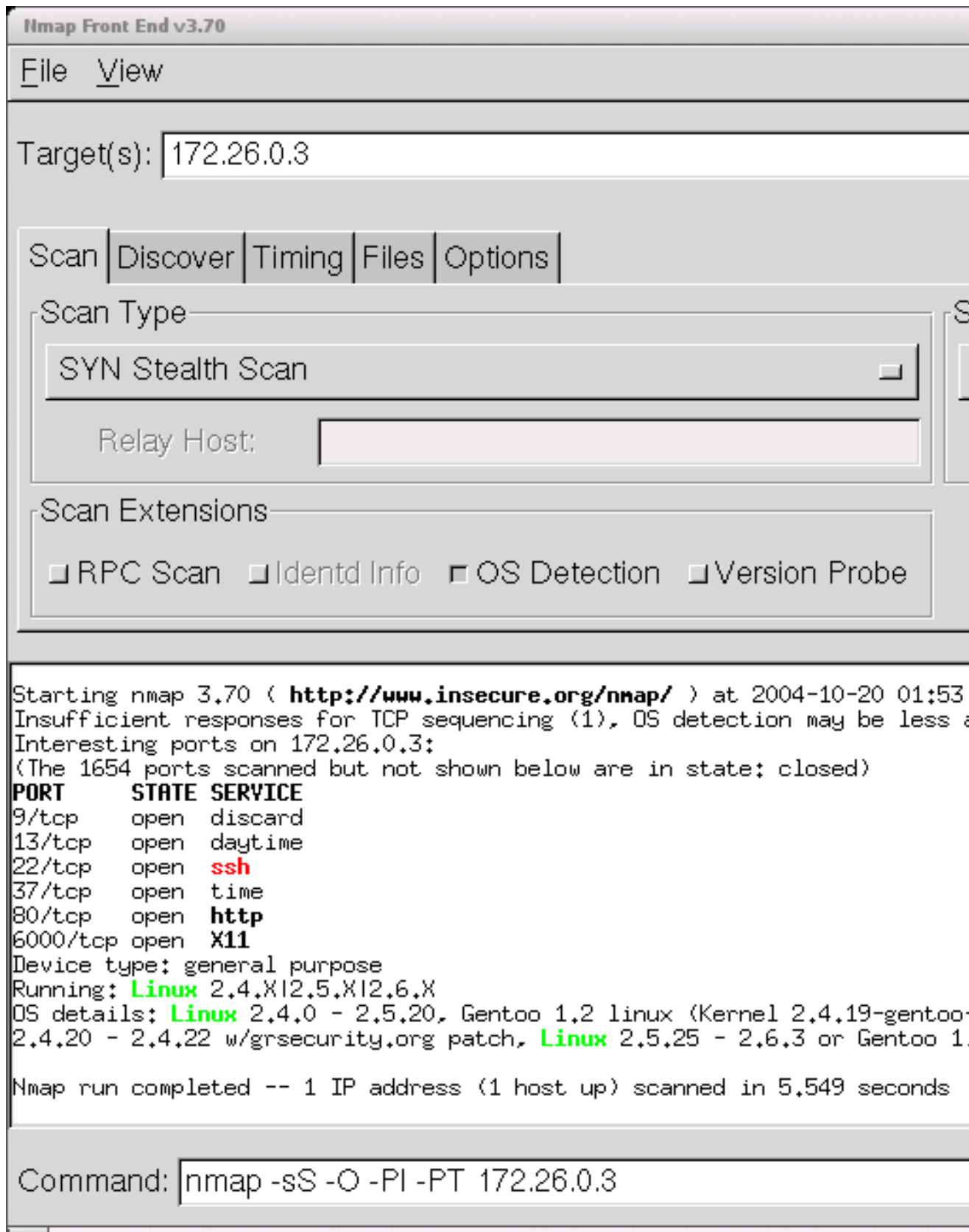
4.1. Aplicación Gráfica para Nmap (NMAPFE)

Si queremos una utilidad gráfica a click de ratón, podemos instalar este interprete y usarlo fácilmente.

Para instalarlo simplemente lo descargamos por apt de la siguiente manera.

```
bash# apt-get install nmapfe
```

Aquí podemos ver la utilidad y lo fácil que nos será manejarla, gracias a poder ver todas las opciones en visual.



5. Usando Nmap

Vamos ahora a entrar un poco en la practica y a ver como se usa básicamente el **Nmap**.

Lo ejecutamos seguido de la ip que nos gustaría escanear.

```
Bash$ nmap 172.26.0.3
```

```
Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2004-10-20 02:13 CEST
Interesting ports on 172.26.0.3:
```

```
(The 1654 ports scanned but not shown below are in state: closed)
```

PORT	STATE	SERVICE
9/tcp	open	discard
13/tcp	open	daytime
22/tcp	open	ssh
37/tcp	open	time
74/tcp	filtered	netrjs-4
80/tcp	open	http
349/tcp	filtered	mftp
6000/tcp	open	X11

```
Nmap run completed -- 1 IP address (1 host up) scanned in 2.529 seconds
```

Como podéis observar la salida del programa tras escanear es bastante simple y se entiende perfectamente,

Nos dice que la ip 172.26.0.3, tiene los puertos 9,13,22,37,80 y 6000 abiertos y al servicio a los cuales pertenecen.

Esto es un scaneo básico, empecemos a introducir opciones y comentar para que es cada una.

5.1. Escaneando Rango de puertos.

Para escanear un rango determinado de puertos para una ip lo haremos de la siguiente manera. Opción -p

```
bash$ nmap -p 1-80 172.26.0.3
```

```
Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2004-10-20 02:29 CEST
Interesting ports on 172.26.0.3
```

```
(The 74 ports scanned but not shown below are in state: closed)
```

PORT	STATE	SERVICE
9/tcp	open	discard
13/tcp	open	daytime
22/tcp	open	ssh
25/tcp	open	smtp
37/tcp	open	time
80/tcp	open	http

```
Nmap run completed -- 1 IP address (1 host up) scanned in 3.612 seconds
```

La opción `-p` nos permite acotar un rango de puertos incluyendo el primero y el ultimo, muy útil para tardar menos escaneando si sabemos que solo nos interesa unos determinados puertos.

También con `-p 22,53,110,143` así escanearemos solo los puertos especificados.

5.2. Escaneando un rango de ips para un puerto determinado.

Si estamos en una red donde nos interesa saber que ordenadores tienen por ejemplo el puerto 139 abierto lo haríamos de la siguiente manera.

```
bash# nmap -p 139 172.26.0.1-10

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2004-10-20 02:35 CEST
Interesting ports on 172.26.0.2:
PORT      STATE      SERVICE
139/tcp   filtered  netbios-ssn

Interesting ports on 172.26.0.9):
PORT      STATE      SERVICE
139/tcp   open      netbios-ssn

Nmap run completed -- 10 IP addresses (2 hosts up) scanned in 4.002 second
```

La información que obtenemos sería la de dos ordenadores encendidos en ese rango de ips como bien podemos leer abajo del todo y que uno de ellos tiene abierto el servicio de netbios perteneciente al puerto 139.

5.3. Escanear un host sin hacerle ping

La opción `-p0` Puede servirnos si no queremos que intente hacer ping a un servidor antes de escanearlo, es muy útil para maquinas que tienen firewall o no responden a ping.

5.4. Escaneando Host por ping

Usando la opción `-sP` le diremos al Nmap que nos haga un escaneo de los hosts haciendo ping.

5.5. Escaneando y sacando Versiones de los servicios

Si queremos sacar las versiones de los servicios, por ejemplo la versión de ssh que se está usando en una determinada ip o host, debemos usar la opción `-sV`.

```
bash# # nmap -sV 172.26.0.3

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2004-10-20 02:44 CEST
Interesting ports on 172.26.0.3:
```

```
(The 1654 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
9/tcp     open  discard
13/tcp    open  daytime
22/tcp    open  ssh      OpenSSH 3.8.1p1 (protocol 2.0)
37/tcp    open  time
80/tcp    open  http     Apache httpd 1.3.31 ((Debian GNU/Linux))
6000/tcp  open  X11      (access denied)

Nmap run completed -- 1 IP address (1 host up) scanned in 103.108 seconds
```

Es tan útil saber que se esta ejecutando en una maquina como cuanto tiempo hace que actualizan algún tipo de servicio.

Como podemos ver nos dice la versión de OpenSsh y de Apache.

5.6. Como saber el sistema operativo que esta instalado en un host

Con la opción **-O** podemos saber que sistema tiene un host.

```
bash# nmap -O 172.26.0.6
Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2004-10-20 02:50 CEST
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on 172.26.0.6:
(The 1654 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
9/tcp     open  discard
13/tcp    open  daytime
22/tcp    open  ssh
37/tcp    open  time
80/tcp    open  http
6000/tcp  open  X11
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.0 - 2.5.20, Gentoo 1.2 linux (Kernel 2.4.19-gentoo-rc5), Linux 2.4.20
Uptime 0.132 days (since Tue Oct 19 23:41:15 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 4.572 seconds
```

Dice que tiene un núcleo 2.4 y lleva Gentoo instalado, muy útil para ciertas cosas.

En un ordenador con windows, nos saldría un mensaje similar a este:

```
Device type: general purpose
Running: Microsoft Windows 2003/.NET|NT/2K/XP
OS details: Microsoft Windows Server 2003, Microsoft Windows 2000 SP3
```

Este seria un ordenador con Windows Server 2003

Decir también que puede equivocarse el Nmap y decirnos que es una gentoo y ser una debian pero no fallan de windows a linux o freebsd.

5.7. Escaneando a velocidades variables

Para escanear mas o menos velocidad para no ser detectados o bien si no nos importa que a un administrador le salga si esta mirando o monitorizando la red un escaneo de puertos desde nuestra ip.

-T seguido de Paranoid, Sneaky, Polite, Normal, Aggressive, Insane

De mayor a menor nivel de cuidado o paranoia como dice una de las opciones.

5.8. Escaneos con opciones avanzadas I

Opción **-sS**

Escaneo TCP SYN se envían **paquetes SYN**, denominada como escaneo medio abierto porque envía paquetes como si se fuese a abrir una conexión.

Este método requiere ser Root para el envio de estos paquetes.

5.9. Escaneo con opciones avanzadas II

Opciones **-sF -sX -sN**

Modos Stealth FIN, Xmas Tree o Nul scan respectivamente.

Con estos modos podremos ser suficientemente clandestinos por si hay un firewall o filtros que no dejan enviar paquetes SYN a determinados puertos.

Debemos ser root para poder usar estas opciones.

5.10. Otras Opciones de interés

-v modo de información ampliada de lo que va haciendo el **Nmap**

-h Nos da los comandos de ayuda general.

6. Referencias

man nmap

<http://www.insecure.org/nmap/>

En el man encontrareis ejemplos y ayuda a las opciones que no comento en este manual.

7. Sobre el autor

<http://www.debianitas.net> **Emilio Guirado Hernández.**

Documento bajo Licencia GNU | GPL geesecillo@debianitas.net

Este documento esta siempre en revisión, si ves algún error, tienes algún consejo o quieres darnos tu opinión, escribeme.

Agradecimientos a **Roció Rubio** ;)

Gracias a *los Debianitas* por la ayuda en la elaboración de este manual.