La exploración de puertos suele ser utilizada bajo dos puntos de vista diferentes:

Como forma de conocer el nivel de seguridad de la configuración de los servicios que se ofrecen. Y...

Como una de las primeras etapas que un posible atacante lleva a cabo, dentro del plan de ataque, para investigar o enumerar qué servicios tiene la víctima activados.

Existen muchas herramientas para hacer exploración de puertos, pero nosotros utilizaremos las más conocidas en entornos académicos: nmap para la línea de orden y Zenmap en entorno gráfico.

Comenzamos con nmap para conocer las diferentes opciones y así poder luego interpretar los comandos generados por Zenmap al hacer la selección de acciones que ofrece la herramienta. Por otro lado, también es posible que en un entorno de administración se disponga únicamente de consola, en cuyo caso es indispensable conocer bien los parámetros utilizados.

# Nmap
## Introducción

Nmap, cuyo nombre significa mapeador de redes, es software libre y puede redistribuirse y/o

modificarse bajo los términos de la Licencia Publica General GNU.

La web oficial es http://nmap.org de la que puede bajarse la herramienta. En concreto Ubuntu la incluye en su Centro de Software y en la web hay también versión disponible para Windows y otros sistemas operativos.

La versión actual es la 5.6. En http://nmap.org/man/es/ existe un manual oficial que detalla su funcionamiento.

Nmap ha sido diseñada para permitir a administradores de sistemas y a usuarios curiosos en general, explorar y realizar auditorías de seguridad de redes para determinar qué servidores se encuentran activos y qué servicios ofrecen.

Su funcionamiento se basa en el envío de paquetes IP en formato raw (crudo), es decir paquetes que no han sufrido ningún tipo de modificación, y por lo tanto son originales sea cual sea el protocolo utilizado.

¿Qué permite nmap?

- Descubrir e identificar equipos en la red.
- Identificar puertos abiertos en estos equipos.
- Conocer los servicios concretos que están ofreciendo estos equipos.
- El sistema operativo que tienen instalado, incluida la versión.
- Conocer si se está utilizando cortafuegos.
- Conocer algunas características del hardware de red de los equipos detectados.

Es compatible con un gran numero de técnicas de escaneo como: UDP, TCP connect(), TCP SYN (half open), ICMP (ping sweep), FIN, ACK sweep, Xmas Tree y Null scan.

De todas estás técnicas comentaremos aquellas de las cuales se incluyan ejemplos concretos de uso.

La salida que genera nmap es un listado de hosts/redes analizadas, con información específica para cada uno ellos dependiendo de las opciones utilizadas. De ellas la mas importante es la tabla que muestra el número de puertos, el nombre del servicio asociado y su estado.

El estado puede ser:

- open (abierto): la máquina destino se encuentra esperando conexiones o paquetes en ese puerto.
- filtered (filtrado): un cortafuegos, filtro o algún obstáculo en la red está bloqueando el acceso a ese puerto y nmap no puede saber si se está abierto o cerrado. closed (cerrado): son puertos que no tienen ninguna aplicación escuchando en ellos, aunque podrían abrirse en cualquier momento.
- unfiltered (no filtrado): son puertos que responden a la exploración de nmap, pero para ellos nmap no puede determinar si se están abiertos o cerrados. Nmap, cuando no puede determinar en cual de dos estados está un puerto, informa indicando una combinación de estados, como open|filtered y closed|filtered.

La tabla de puertos también puede informar sobre la versión de la aplicación si se le pide. Y mucha mas información que dependerá de las opciones utilizadas.

Además de la tabla de puertos con nmap, se puede obtener información sobre los hosts/redes como son el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, tipos de dispositivo y direcciones MAC.

A lo largo de la explicación de los ejemplos de uso se hace referencia a conceptos relacionados con la seguridad. Algunos de ellos se describen a continuación:

- Decoy: significa señuelo y es utilizado para esconder la IP de la máquina origen que está realizando la exploración.
- Fingerprinting: significa identificación por huella y se utiliza para detectar el sistema operativo de las máquinas que se están explorando.
- Scan: se utiliza en el sentido de sondeo, análisis o exploración, no de escaneo de documentos.
- Spoof: significa falsificar y va relacionado con algún tipo de servicio o protocolo que se

quiere falsear.

Sintaxis de la herramienta

```
nmap [Tipos(s)de analisis] [Opciones] <servidor o red #1... [#N]>
```

En general para obtener ayuda ejecutar:

$nmap -h

La red que se utilizará para algunos de los ejemplos será 192.168.0.0/24. En otros se utilizarán IPs de dominios públicos.

---

# Tipos de exploración soportados

## Ejecución simple

Ejecutamos nmap sobre una IP para conocer los puertos activos.

**$nmap 192.168.0.101**

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-03 12:57 CEST

Interesting ports on servidor (192.168.0.101):

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

23/tcp open telnet

80/tcp open http

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

Si queremos conocer qué tipo de sistema operativo se está ejecutando en el host explorado añadimos la opción -O. Observar que la orden se ejecuta como root, o también con privilegios (sudo).

**#nmap -O 192.168.0.101**

No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).

TCP/IP fingerprint:

OS:SCAN(V=5.00%D=5/3%OT=22%CT=1%CU=36744%PV=Y%DS=0%G=Y%TM=4FA264D9%P=i686-p

OS:c-linux-gnu)SEQ(SP=FF%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=8)SEQ(SP=FF%GCD=2%

….....

OS:RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G) OS:IE(R=Y%DFI=N%T=40%CD=S)

Toda esta salida es la huella TCP/IP (TCP/IP fingerprint) que tiene cada Sistema Operativo en particular. Y, como se puede observar, nmap muestra esta información porque no consigue identificar con exactitud qué Sistema Operativo se está ejecutando en el host explorado.

## Identificar hosts activos en la red: Ping scan

Si se quiere conocer los hosts activos en la red, 192.168.0.0/24 utilizamos un Ping Scan. En realidad lo que se envía son peticiones de respuesta ICMP a cada una de las IPs dadas. Si un host contesta significa que está activo.

Puede ocurrir que el host destino sea un servidor que tenga bloqueada la recepción de paquetes ICMP, en cuyo caso no es posible explorarlo. Es decir, nmap sólo explora aquellos servidores de los que obtiene respuesta.

Ejemplo:

$nmap -sP 192.168.0.1-255

## Sondeo básico TCP/UDP

Las opciones a utilizar son: -sT / -sU escaneo TCP/UDP connect()

Utiliza la llamada de sistema connect() (disponible para cualquier usuario sin privilegios) para establecer una conexión con todos los puertos posibles de la máquina.

Si el puerto está a la escucha, connect() tendrá éxito.

Sino, el puerto es inalcanzable.

Es una exploración muy fácil de detectar ya que proporciona mucha información de la conexión, incluidos mensaje de error.

Ejemplos:

**$ nmap -sT 62.41.70.186**

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-03 13:06 CEST

Interesting ports on static-ip-62-41.eurorings.net (62.41.70.186):

Not shown: 997 filtered ports P

ORT STATE SERVICE

80/tcp open http

443/tcp open https

8000/tcp closed http-alt

**$ sudo nmap -sU 62.41.70.186**

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-03 13:08 CEST

Interesting ports on static-ip-62-41.eurorings.net (62.41.70.186):

Not shown: 692 open|filtered ports, 307 closed ports

PORT STATE SERVICE

161/udp filtered snmp

Nmap done: 1 IP address (1 host up) scanned in 1229.36 seconds

**NOTA**:

Observar que en algunas órdenes se ejecuta nmap como usuario y en otras se incluye sudo para obtener privilegios. Esto es así porque no todas las opciones de exploración están permitidas a los usuarios.

## Realizar Stealth Scans (escaneos sigilosos)

Si se quiere no ser detectado por software de detección de sondeos con nmap se envían paquetes a los hosts con ciertos 'flags' TCP activados o desactivados para evitarlo.

El uso mas típico es el stealth Xmas Tree Scan (-sX). Es muy útil para conocer que hosts se encuentran activos sin que seamos detectados.

Ejemplo: un stealth scan del tipo Xmas Tree, y además queremos conocer qué sistema operativo se está ejecutando en el host destino:

**#nmap -sX -O 192.168.0.102**

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-04 17:30 CEST

Note: Host seems down. If it is really up, but blocking our ping probes, try -PN

Nmap done: 1 IP address (0 hosts up) scanned in 0.50 seconds

## Sondeo TCP SYN

También se llama 'half open' porque no abre una conexión TCP completa. El procedimiento consiste en abrir una conexión real enviando un paquete SYN y se espera a que llegue una respuesta ACK (puerto escuchando) para enseguida enviar un RST y cortar la conexión.

Se llama sondeo silencioso. De esta forma hay menos probabilidades de que este sondeo se haya registrado en las máquinas destino y se necesitan privilegios de root para hacerlo.

**#nmap -sS 173.194.34.49**

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-08 15:41 CEST

Interesting ports on par03s03-in-f17.1e100.net (173.194.34.49):

Not shown: 997 filtered ports

PORT STATE SERVICE

80/tcp open http

113/tcp closed auth

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 42.97 seconds

## Guardar los resultados de la exploración

Podemos guardar los resultados de una exploración en archivos con varios formatos como txt, XML, etc. Para ello utilizamos la opción -oN indicando a continuación el nombre del archivo.

En el ejemplo anterior, podemos hacer el stealth scan del tipo Xmas Tree, intentar conocer el sistema operativo y ahora guardamos los resultados en el archivo resultado.txt:

**#nmap -sX -O 192.168.0.102 -oN resultado.txt**

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-04 17:44 CEST

Note: Host seems down. If it is really up, but blocking our ping probes, try -PN

Nmap done: 1 IP address (0 hosts up) scanned in 0.51 seconds

Comprobamos que se genera un archivo con el mismo contenido mostrado en pantalla.

Si lo que queremos es que no salga nada por pantalla, simplemente redirigimos la salida de la orden al archivo:  #nmap -sX -O 192.168.0.102 > resultado.txt

## Ejemplos de utilización de nmap

### Sondeo silencioso a toda una red con detección del sistema operativo

**#nmap -sS -O 192.168.0.0/24**

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-08 16:10 CEST

Interesting ports on 192.168.0.100:

Not shown: 998 closed ports

PORT STATE SERVICE 80/tcp open http

5431/tcp open park-agent

MAC Address: 00:14:BF:15:FE:09 (Cisco-Linksys)

Device type: general purpose

Running: Linux 2.4.X

OS details: Linux 2.4.18 - 2.4.35 (likely embedded)

Network Distance: 1 hop

Interesting ports on 192.168.0.102:

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

23/tcp open telnet

80/tcp open http

443/tcp open https

TCP/IP fingerprint:

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 256 IP addresses (2 hosts up) scanned in 19.42 seconds

Ejecuta una exploración SYN oculto (-sS) contra cada una de las máquinas activas de las 255 maquinas de la red de clase 'C' 192.168.0.0. Intenta determinar el sistema operativo (-O) usado en cada una de las máquinas activas.

## Sondeo Xmas Tree al host 74.125.230.216 con detección de ciertos puertos y enmascarando el origen de la exploración

#nmap -p 25,53 -sX -P0 -D 1.2.3.4,5.6.7.8 74.125.230.216

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-08 16:16 CEST

Interesting ports on par08s09-in-f24.1e100.net (74.125.230.216):

PORT STATE SERVICE

25/tcp open|filtered smtp

53/tcp open|filtered domain

Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds

Ejecuta una exploración Xmas Tree (-sX) al host 74.125.230.216 de los puertos 25 (SMTP) y 53 (DNS) sin enviar pings (-P0) y enmascarando el origen de la exploración (-D) detrás de las IPs 1.2.3.4 y 5.6.7.8.

La opción -D intenta engañar al host explorado haciéndole creer que los sondeos se están haciendo desde otros hosts que se indican por su IP detrás de -D.

La opción -P0 evita que nmap envíe mensajes ICMP (pings) para comprobar si la maquina está activa.

## Sondeo TCP al puerto 80 de la máquina local , sin envío de pings y que muestre mucha información

**#nmap -sT -P0 -v -p 80 127.0.0.1**

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-08 16:20 CEST

NSE: Loaded 0 scripts for scanning.

Initiating Connect Scan at 16:20

Scanning localhost (127.0.0.1)

Discovered open port 80/tcp on 127.0.0.1

Completed Connect Scan at 16:20, 0.00s elapsed (1 total ports)

Host localhost (127.0.0.1) is up (0.00015s latency).

Interesting ports on localhost (127.0.0.1):

PORT STATE SERVICE

80/tcp open http

Read data files from: /usr/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds

Como vemos la exploración vuelca mas información del proceso.

### Listar servidores con un puerto especifico abierto

#nmap -sT -p 80 -oG - 192.168.0.*|grep open

Host: 192.168.0.100 () Ports: 80/open/tcp//http///

Host: 192.168.0.102 () Ports: 80/open/tcp//http///

## Entorno de pruebas

Nmap pone a disposición de los usuarios un dominio de pruebas llamado scanme.nmap.org. Pero sólo para explorar con nmap, no para hacer otro tipo de pruebas como ataques de denegación de servicio o pruebas con exploits.

Hay que tener en cuenta en este caso que, si se lanzan múltiples exploraciones simultáneamente, se puede colapsar el servidor y nmap nos dirá que 'Failed to resolve given hostname/IP: scanme.nmap.org
'.

**$sudo nmap -sX -O scanme.nmap.org**

Starting Nmap 5.00 ( http://nmap.org ) at 2012-05-04 17:48 CEST

Interesting ports on scanme.nmap.org (74.207.244.221):

Not shown: 994 closed ports

PORT STATE SERVICE

22/tcp open|filtered ssh

80/tcp open|filtered http

135/tcp open|filtered msrpc

139/tcp open|filtered netbios-ssn

445/tcp open|filtered microsoft-ds

1720/tcp open|filtered H.323/Q.931

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

Running: Linux 2.6.X

OS details: Linux 2.6.25 (Arch Linux), Linux 2.6.5-7.283-smp (SuSE Enterprise Server 9, x86)

Network Distance: 12 hops

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 12.43 seconds

Esta opción sondea todos los puertos TCP reservados en el servidor scanme.nmap.org.

## Zenmap

Zenmap es la interfaz gráfica oficial de nmap, válida tanto para Windows como para Ubuntu y otros sistemas (MAC OS, BSD,...), es gratuita y de código abierto.

Proporciona la ventaja de ser mas intuitiva para los usuarios que no conocen nmap y sus posibilidades y por otro lado, proporciona mas opciones de ejecución a los usuarios mas avanzados.

Zenmap permite la creación de perfiles de ejecución y de esa forma hacer mas sencilla la repetición de órdenes. También permite guardar los informes obtenidos de la exploración en una base de datos.

Nmap (y Zenmap) permite trabajar con scripts (pestaña *Scripting*) que amplían la funcionalidad de nmap más allá de la exploración. Con estos scripts nmap puede hacer, incluso, análisis de vulnerabilidades. Pero hay que recordar que no es esta la finalidad de nmap. Esta funcionalidad está disponible tanto en GNU/Linux ( /usr/share/nmap/scripts

) como en Windows (
Archivos de ProgramaNmapscripts
).

Los scripts están clasificados por categorías: safe, intrusive, malware, discovery, vuln, auth, external, default, y all .La extensión es .nse.

El script whois, por ejemplo, permite hacer una consulta a las bases de datos whois para obtener información acerca de una organización, país de origen, nombre de red, etc de los hosts explorados.

### Instalación

Zenmap está disponible en el repositorio de Ubuntu y la podemos instalar directamente desde Synaptic o desde el Centro de Software de Ubuntu (según versiones de Ubuntu).

Una vez instalada está disponible en *Aplicaciones > Internet* o en el *Centro de Software de Ubuntu* (Ubuntu 12.04)

La ejecución conviene hacerla con privilegios de administrador. En cuyo caso lanzamos la aplicación desde una terminal de la forma:

**$ sudo zenmap**

## Utilización de Zenmap

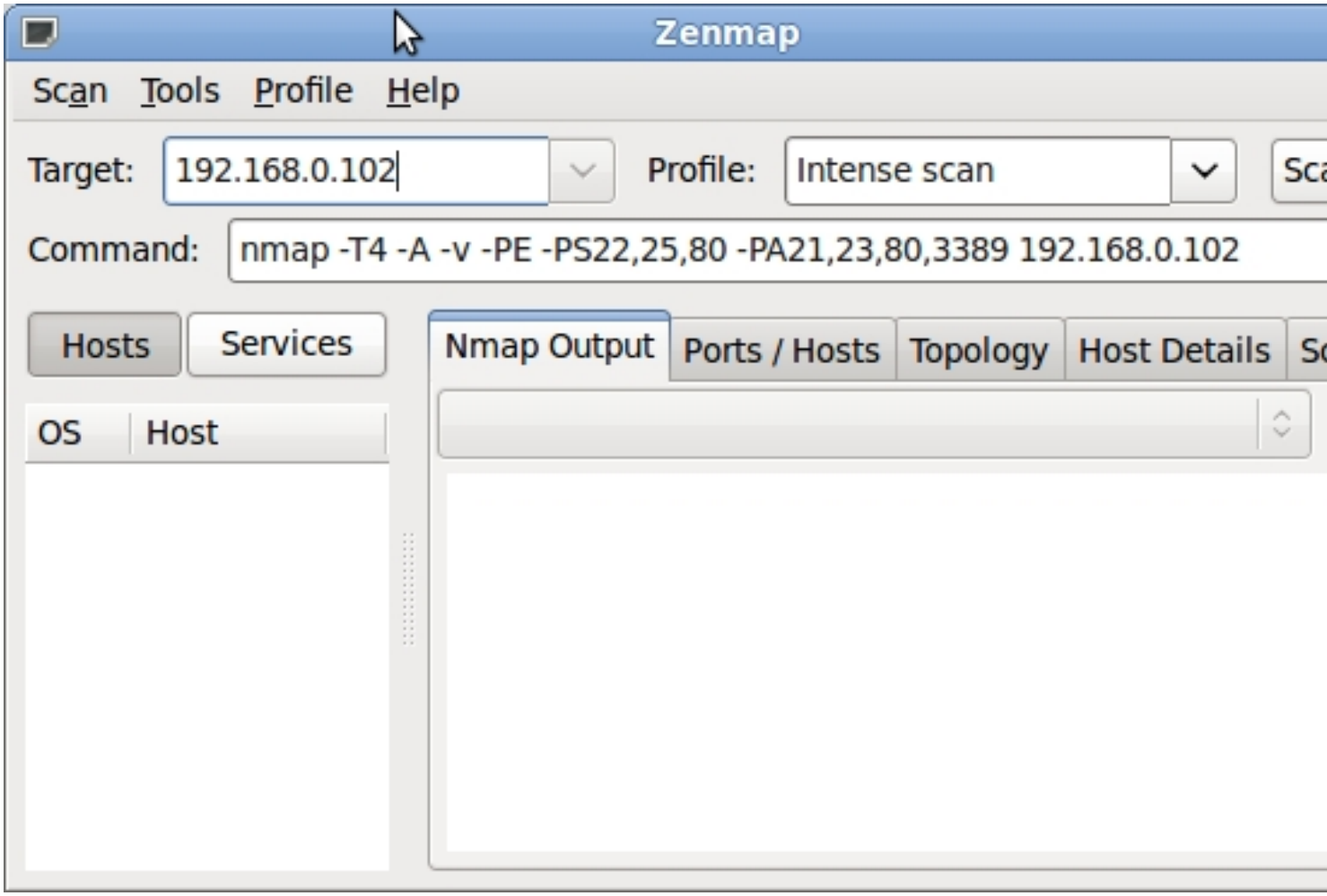
En la interfaz gráfica destacamos las zonas siguientes:

- Target: indicamos la IP del objetivo de nuestra exploración, o un rango de IPs.
- Profile: es una lista desplegable que contiene una serie de perfiles de exploración predeterminados. De ellos el mas usual es el 'Regular scan'. Pero lo mas interesante de esta zona es que nos permite editar estos perfiles e incluso crear nuestros propios perfiles.

- Command: en esta zona va apareciendo la orden nmap que estamos generando al ir

indicando el perfil seleccionado y opciones añadidas.

La interfaz de Zenmap tiene el siguiente aspecto:



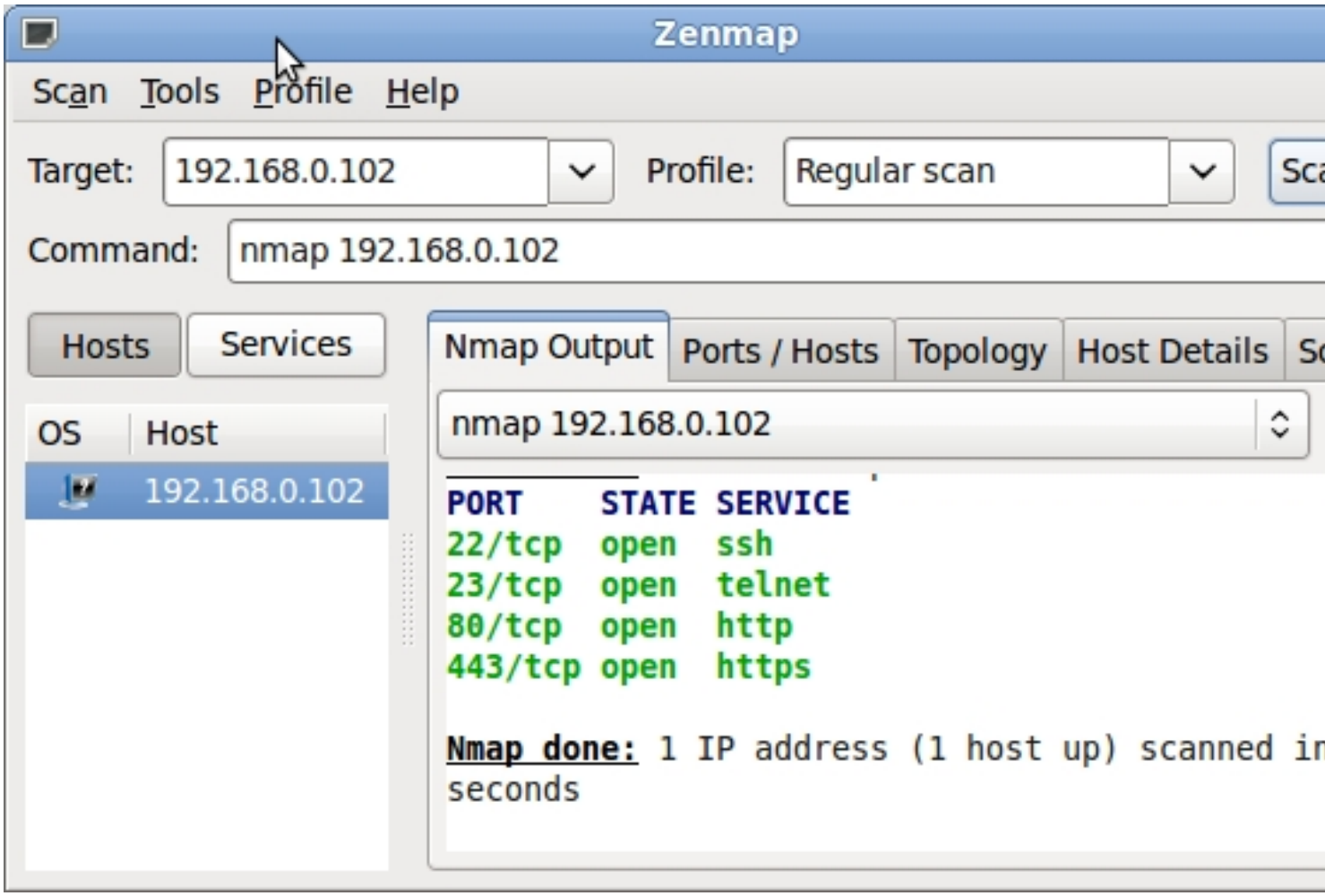

Vemos que la parte inferior está dividida en dos zonas. La zona de la izquierda tiene las pestañas Hosts y Services que muestran los hosts escaneados y los servicios detectados para cada uno de ellos, respectivamente.

La zona de la derecha muestra la salida generada por la orden nmap e información relacionada con la exploración realizada agrupada en diferentes pestañas (Nmap Output, Ports/Hosts, Topology, Host Details y Scans).

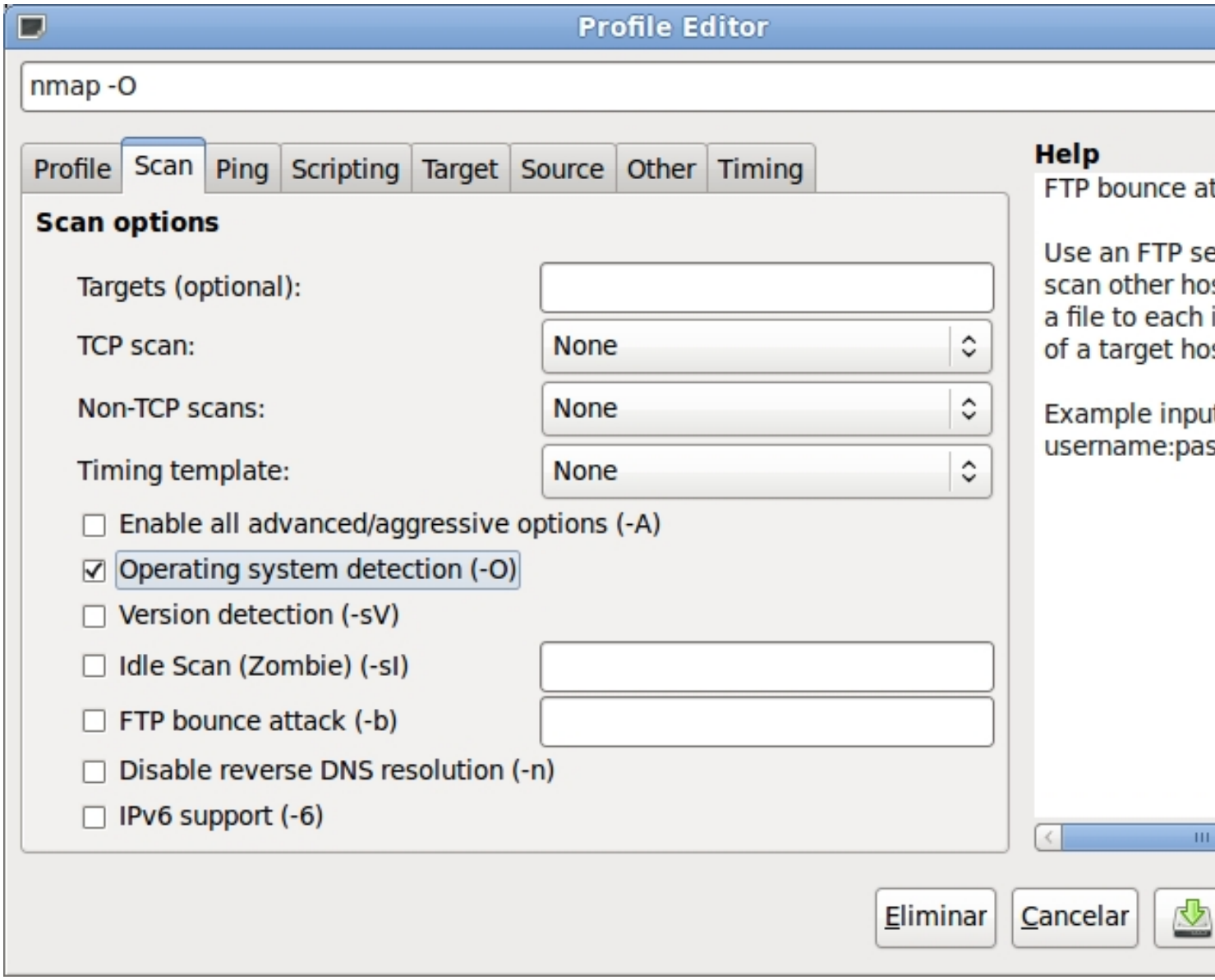
Como ejemplos de utilización podemos reproducir los ejemplos anteriores de la línea de orden.

## Ejemplo 1. Ejecución simple

Se trata de explorar una IP con el perfil 'Regular scan'. La salida mostrada es:




Si en una exploración sencilla queremos detectar siempre el sistema operativo podemos editar el perfil 'Regular scan' (*Profile > Edit Selected Profile*) y seleccionar la opción que detecta el sistema operativo.Guardamos y a partir de este momento cualquier exploración regular intentará detectar el sistema operativo.




**Ejemplo 2. Identificar hosts activos en la red:Ping scan**

Utilizamos el perfil Ping Scan y en la línea de orden comprobamos que escribe:

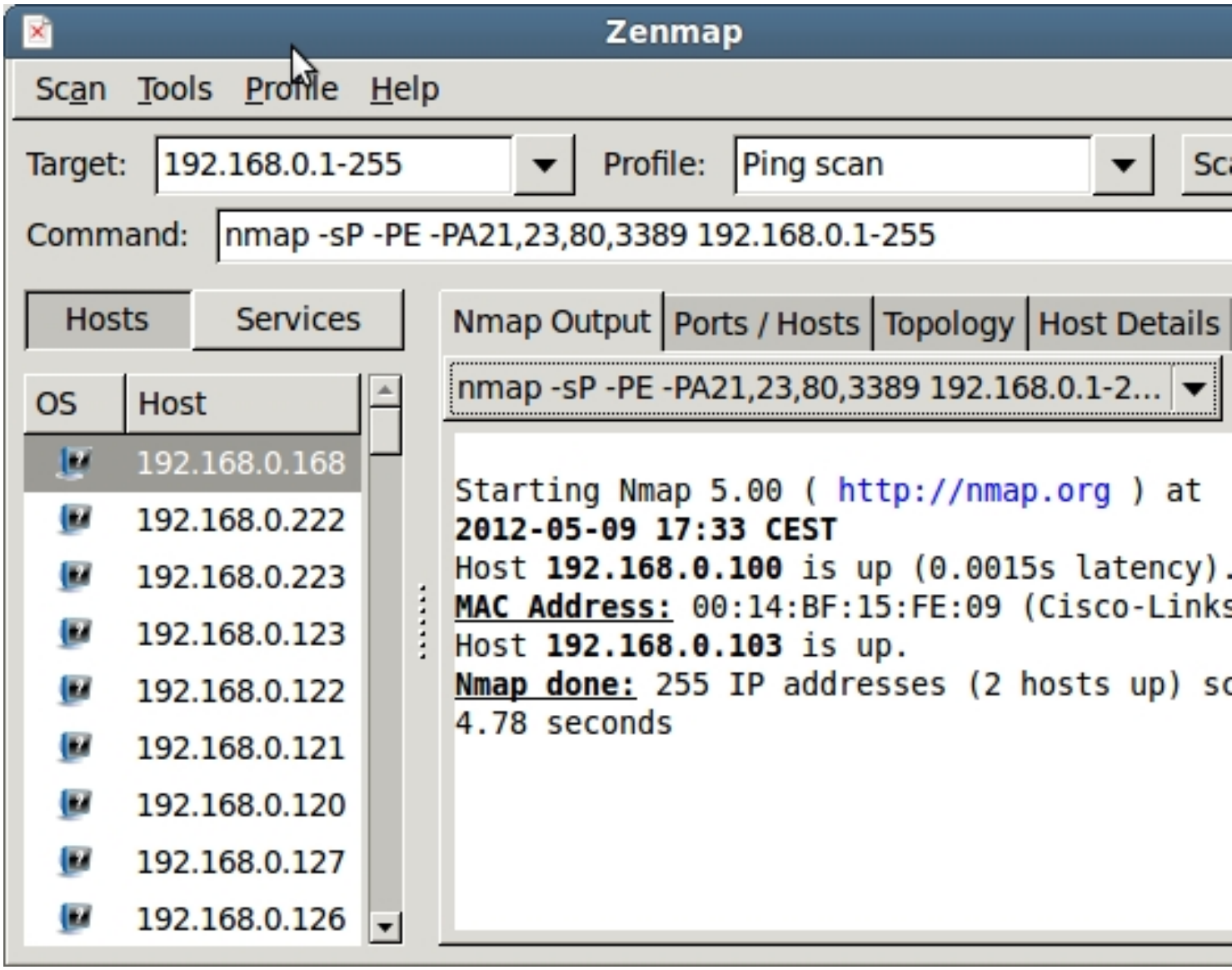
**#nmap -sP -PE -PA21,23,80,3389 192.168.0.1-255**

Si comparamos la orden con la del ejemplo en linea de orden vemos que el perfil estándar Ping Scan añade las opciones -PE y -PA.

-PE indica que se hace envío de paquetes ICMP Ping. El protocolo ICMP se utiliza para manejar mensajes de error y de control de la red, e informa al host origen para que evite o corrija algún problema detectado.

-PA indica que se hace envío de paquetes ACK Ping a los puertos 21, 23, 80, 3389 por defecto. El paquete ACK indica reconocimiento afirmativo por parte del destino de la conexión.

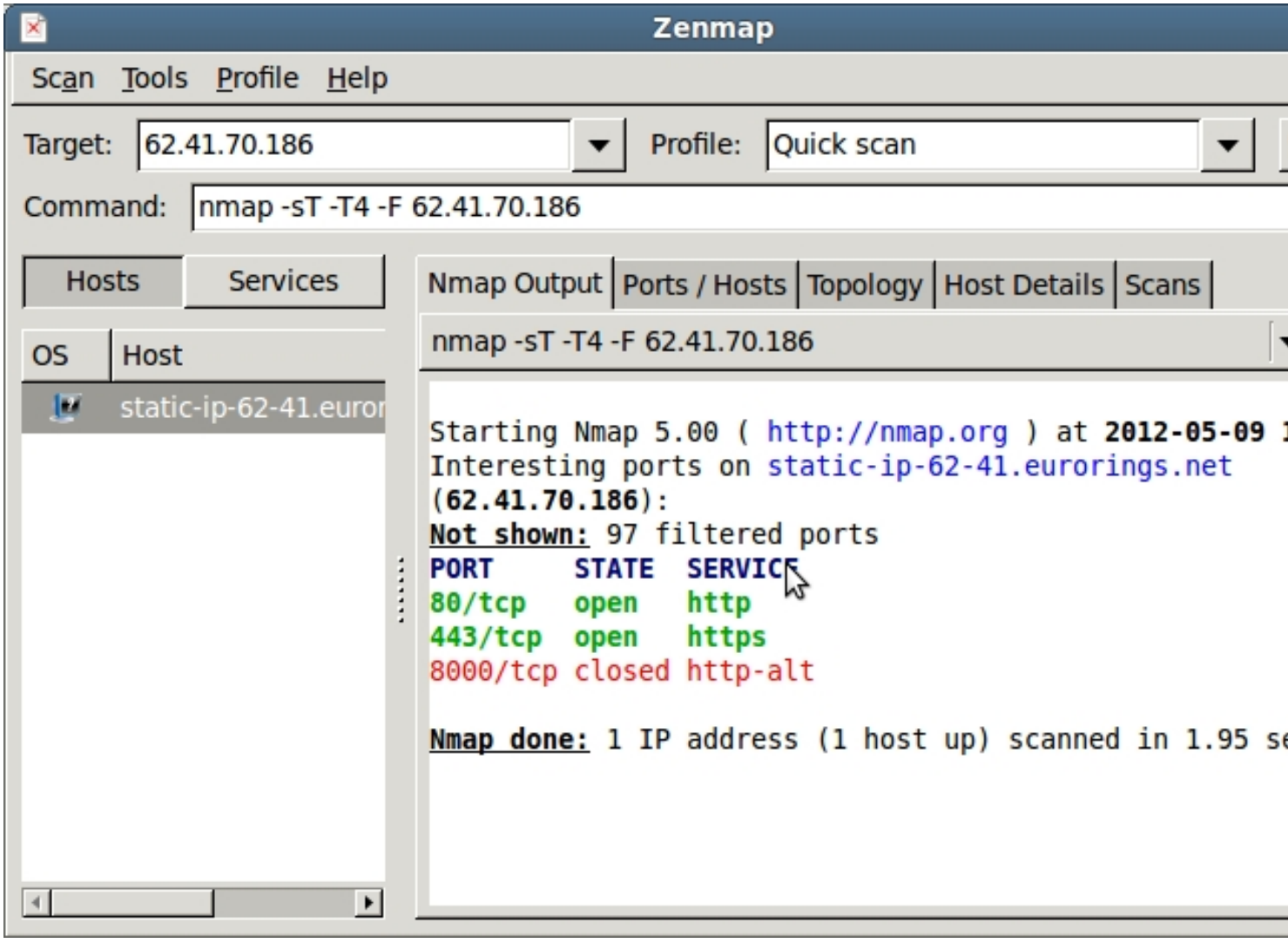
La salida generada con Zenmap en este ejemplo es la siguiente:



## Ejemplo 3. Sondeo básico TCP/UDP

En este caso seleccionamos el perfil Quick Scan y añadimos la IP a explorar. Editamos el perfil y comprobamos que no está activada la opción -sT (TCP connect scan).La activamos y guardamos los cambios.

La salida mostrada es:



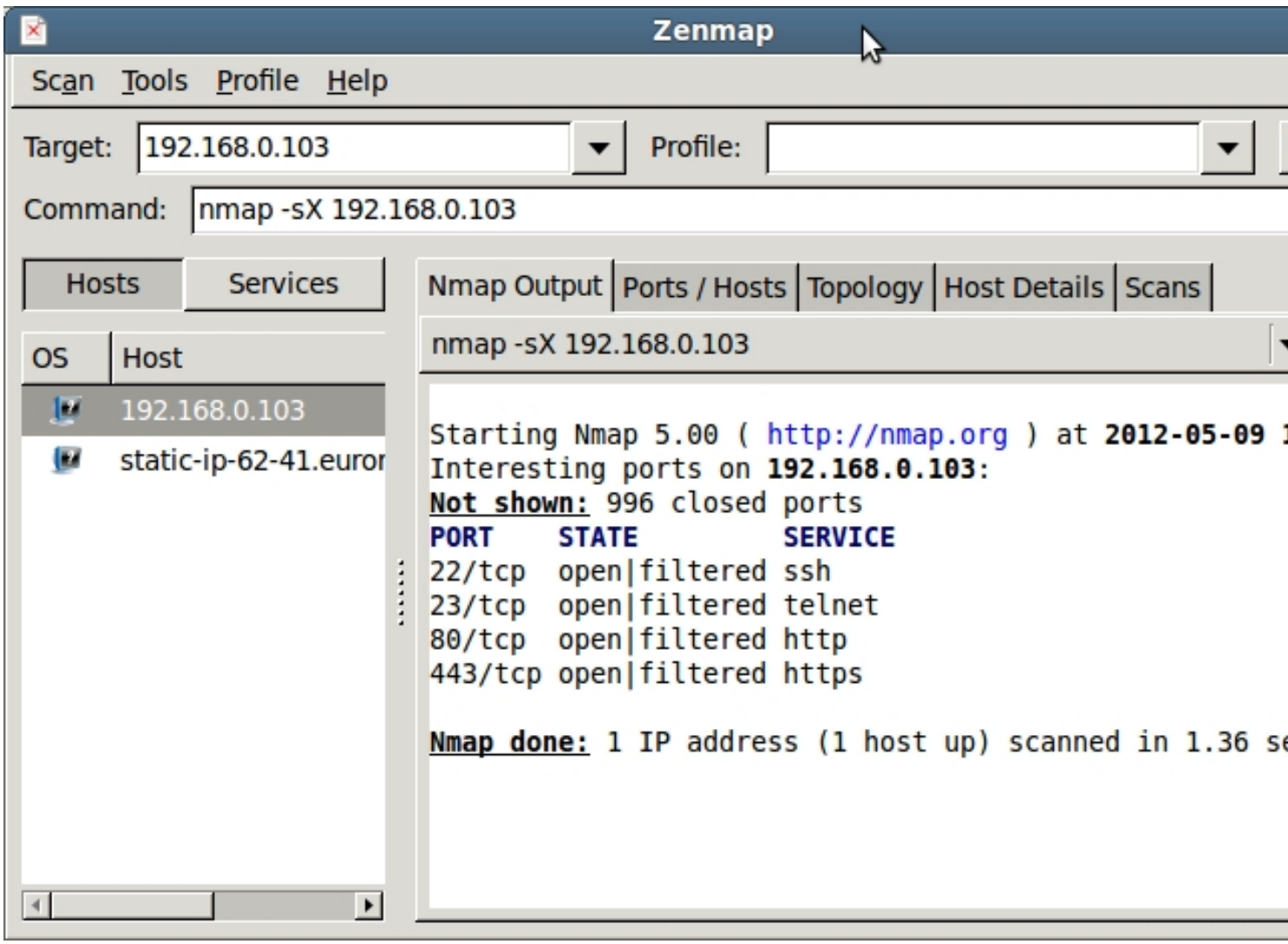

Donde T4 indica que la exploración es agresiva y -F (pestaña Target) indica que es una exploración rápida. Podemos eliminar estas opciones que Zenmap añade por defecto.

## Ejemplo 4. Realizar Stealth Scans (escaneos sigilosos)

Podemos realizar una exploración no asociada a un perfil. En este caso hay que escribir la orden completa que se quiere ejecutar. En nuestro caso será:

**#nmap -sX -O 192.168.0.103**

La orden realiza un stealth scan del tipo Xmas Tree, y además intenta conocer el sistema operativo se está ejecutando en el host destino. La salida generada desde Zenmap es:

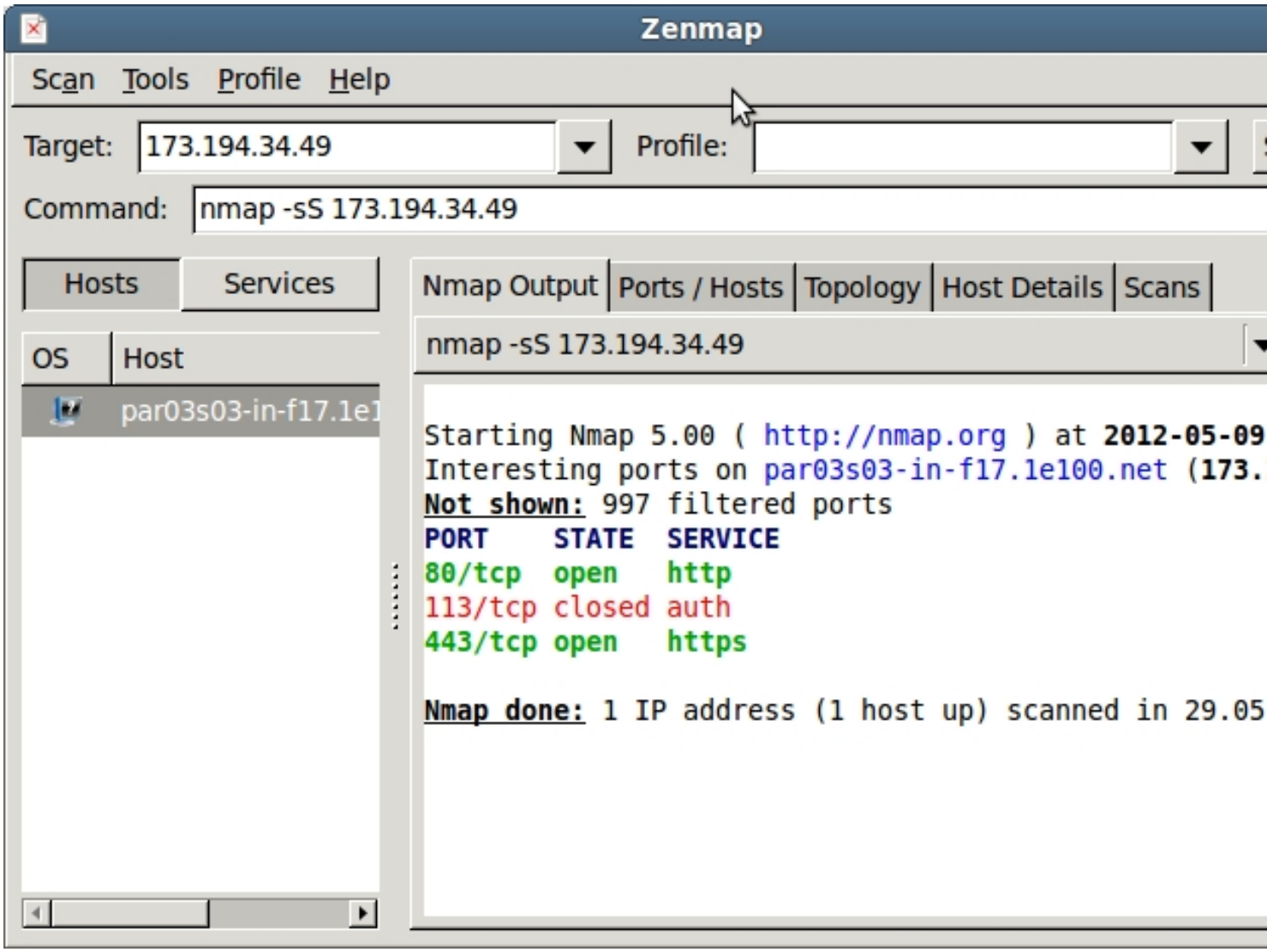


## Ejemplo 5. Sondeo TCP SYN

En este caso tampoco hay un perfil adecuado a esta exploración. Escribimos directamente la orden:

**#nmap -sS 173.194.34.49**

La salida generada es la siguiente:

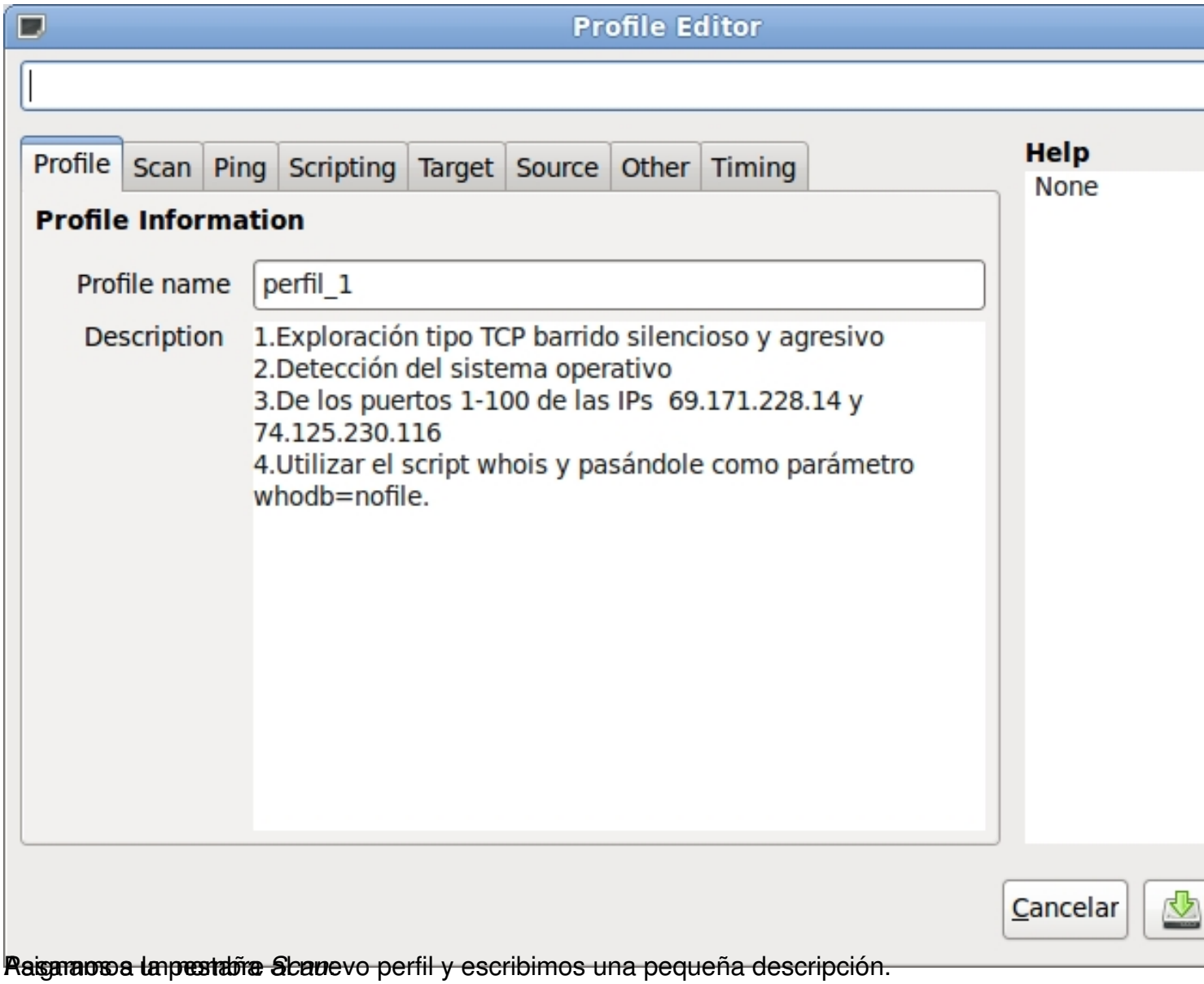


## Ejemplo 6. Creación del perfil_1 personalizado

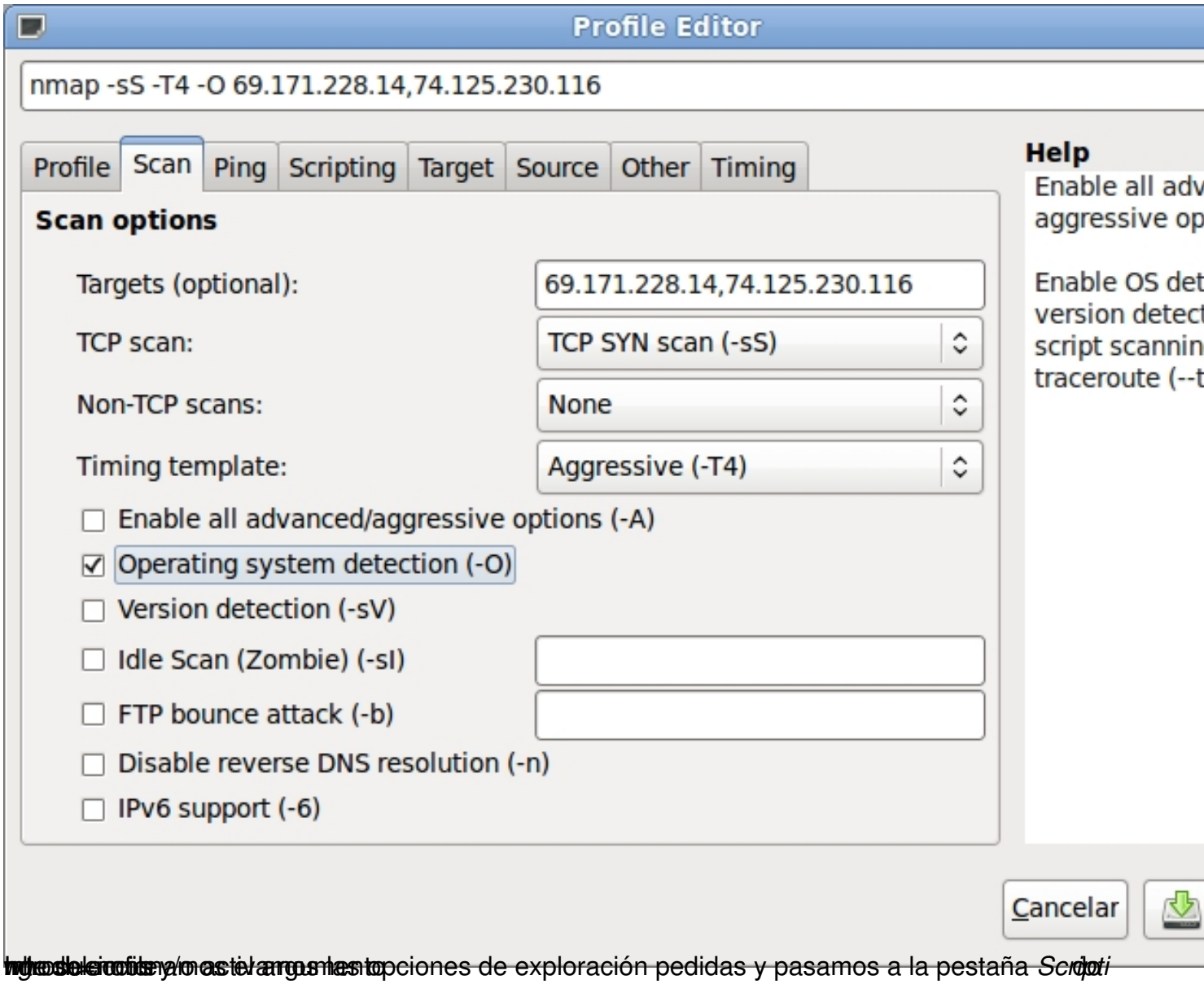
Vamos a crear un perfil personalizado que llamaremos perfil_1 y que haga lo siguiente:

1. Exploración tipo TCP barrido silencioso y agresivo
2. Detección del sistema operativo
3. De los puertos 1-100 de las IPs 69.171.228.14 y 74.125.230.116
4. Utilizar el script whois y pasándole como parámetro whodb=nofile. De esta forma indicará, además de los puertos que tienen abiertos, a qué organización pertenecen. Recordar que el script whois permite hacer una consulta a las bases de datos whois para obtener más información acerca de los hosts explorados.

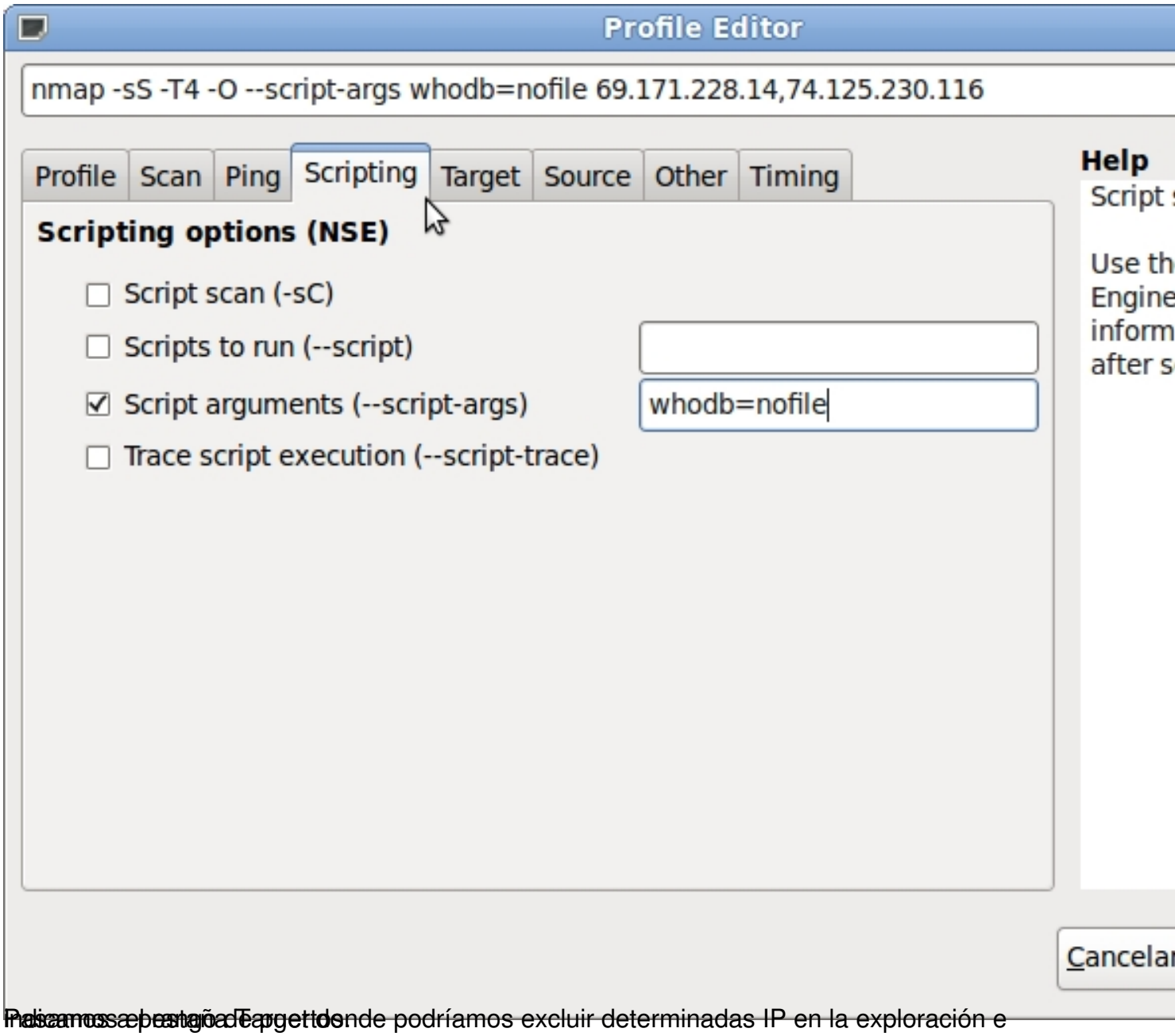
Para ello entramos en el editor de perfiles (*Perfil > Editor de perfiles*) y en la ventana que muestra introducimos los parámetros.



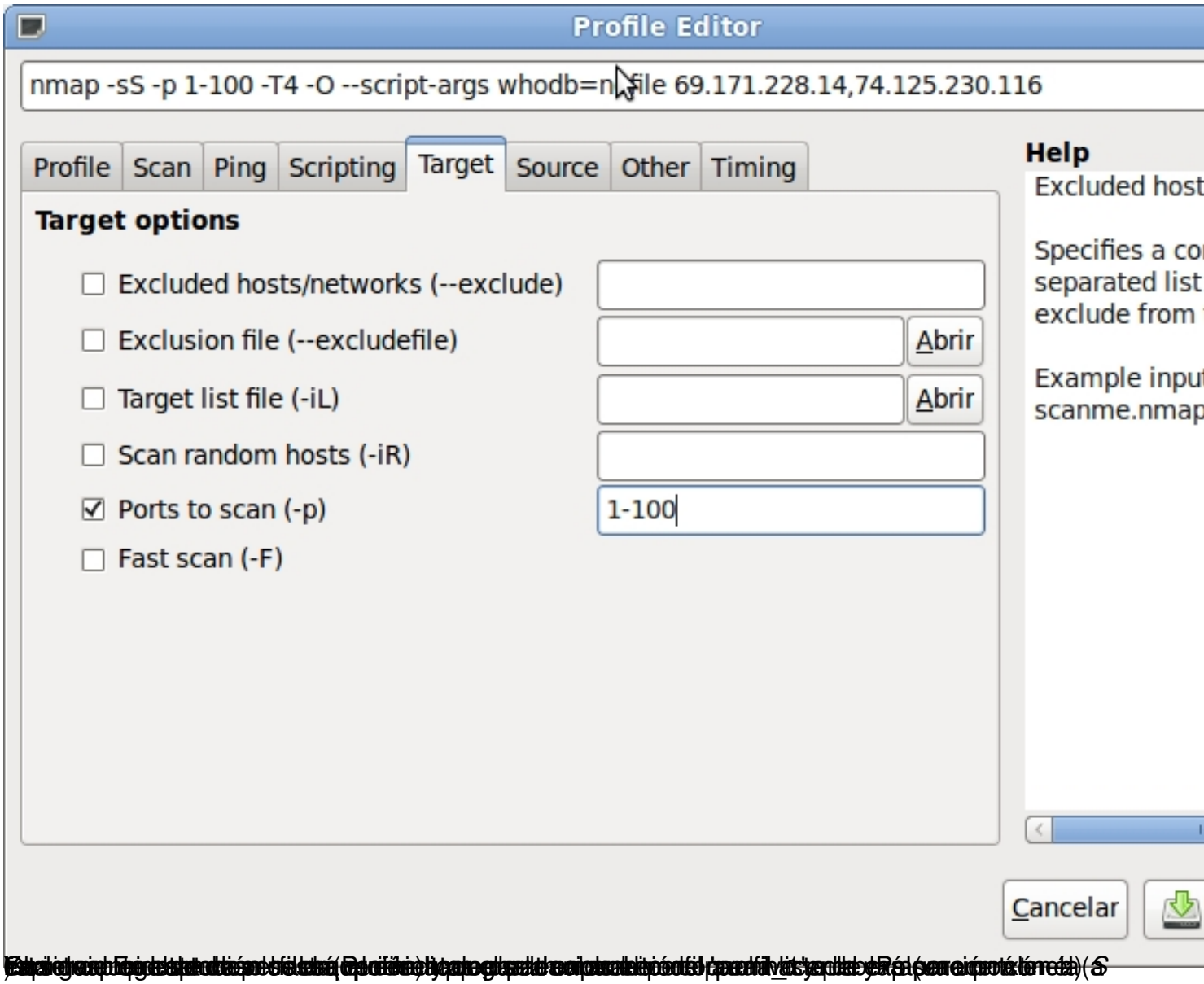

Pasamos a la pestaña Scan nuevo perfil y escribimos una pequeña descripción.

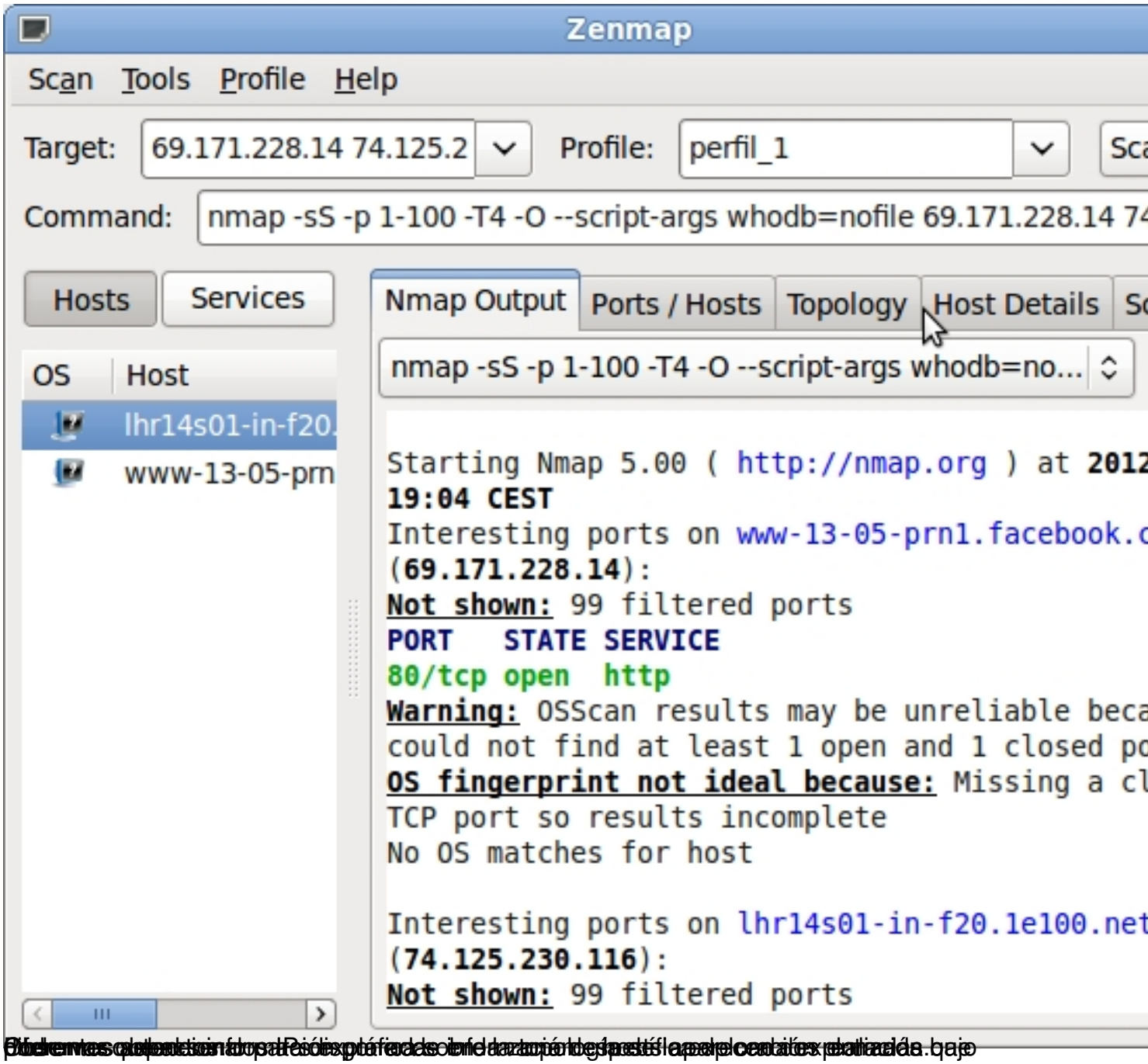


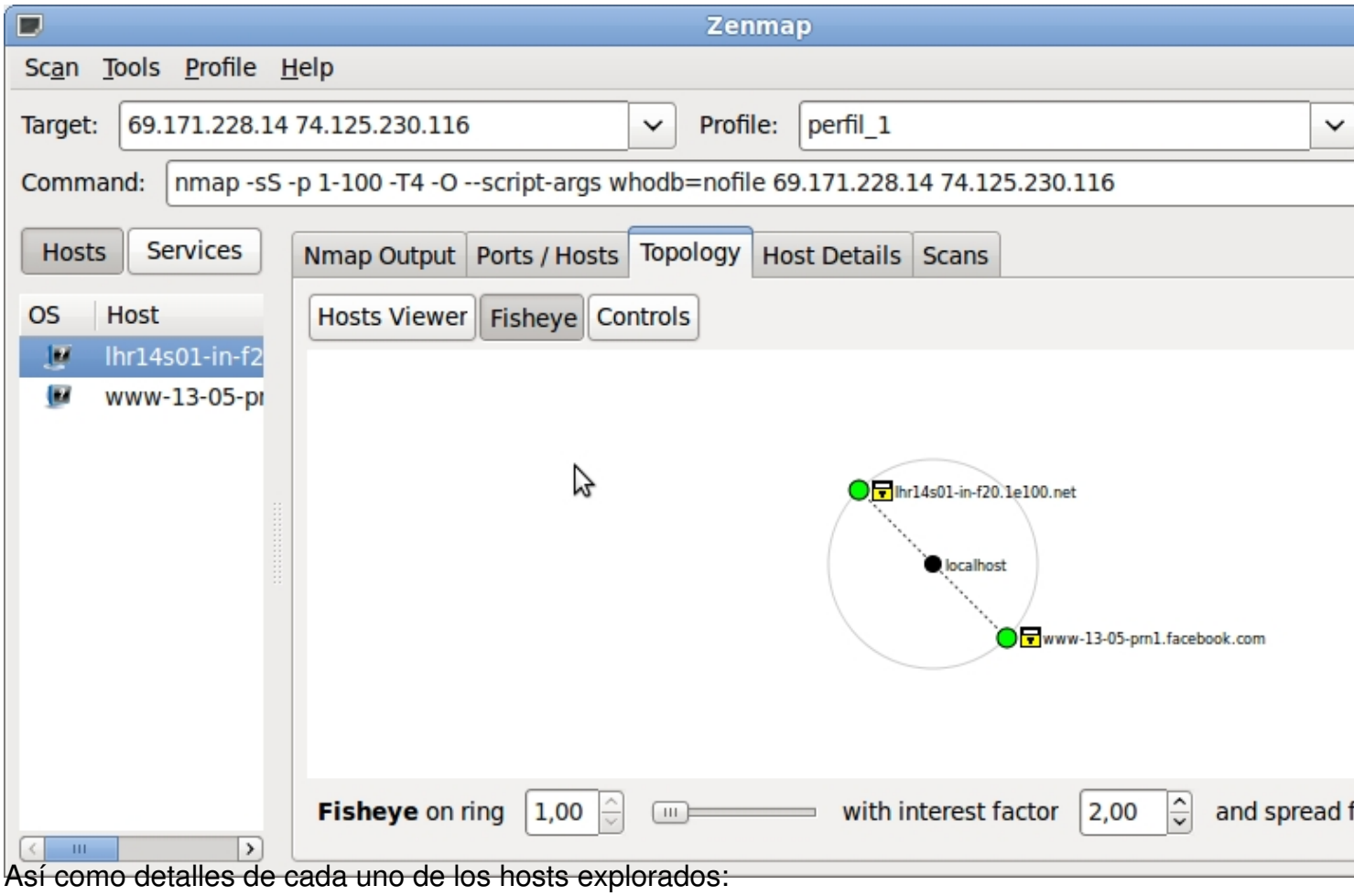

Introducimos y nos llevamos las opciones de exploración pedidas y pasamos a la pestaña *Scripti*



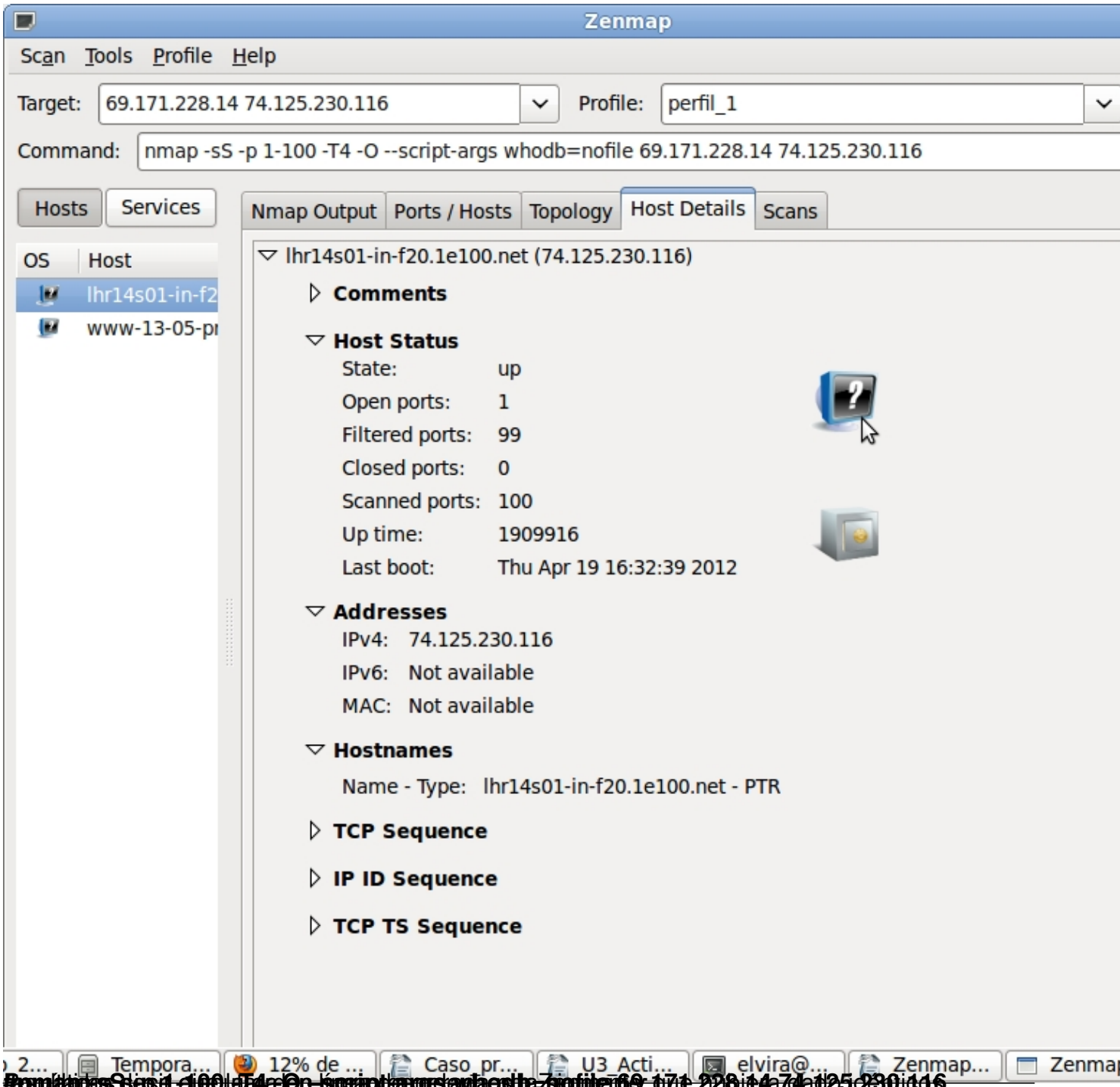

Pasamos a la pestaña Target donde podríamos excluir determinadas IP en la exploración e


Profile Editor
nmap -sS -p 1-100 -T4 -O --script-args whodb=n file 69.171.228.14,74.125.230.116
Profile
Scan
Ping
Scripting
Target
Source
Other
Timing
Target options
Excluded hosts/networks (--exclude)
Exclusion file (--excludefile)
Abrir
Target list file (-iL)
Abrir
Scan random hosts (-iR)
Ports to scan (-p)
1-100
Fast scan (-F)
Help
Excluded host
Specifies a co
separated list
exclude from
Example input
scanme.nmap
Cancelar


Zenmap
Scan Tools Profile Help
Target: 69.171.228.14 74.125.2
Profile: perfil_1
Command: nmap -sS -p 1-100 -T4 -O --script-args whodb=nofile 69.171.228.14 74
Hosts
Services
OS
Host
lhr14s01-in-f20.
www-13-05-prn
Nmap Output
Ports / Hosts
Topology
Host Details
nmap -sS -p 1-100 -T4 -O --script-args whodb=no...
Starting Nmap 5.00 ( http://nmap.org ) at 2012
19:04 CEST
Interesting ports on www-13-05-prn1.facebook.c
(69.171.228.14):
Not shown: 99 filtered ports
PORT STATE SERVICE
80/tcp open http
Warning: OSScan results may be unreliable beca
could not find at least 1 open and 1 closed po
OS fingerprint not ideal because: Missing a cl
TCP port so results incomplete
No OS matches for host
Interesting ports on lhr14s01-in-f20.1e100.net
(74.125.230.116):
Not shown: 99 filtered ports




Así como detalles de cada uno de los hosts explorados:




## Conclusión

Tanto nmap como su interfaz gráfica Zenmap son herramientas muy útiles para los administradores de sistemas. Permiten hacer, de forma rápida, intuitiva y sencilla, una auditoría del sistema en el ámbito de su competencia, que es la exploración de puertos.  Y no hace falta ser responsable de un gran sistema para verle la utilidad a nmap. Cualquiera de nosotros, al fin y al cabo, somos administradores de nuestro propio sistema y debemos vigilar la integridad, disponibilidad y confidencialidad de nuestros datos. En definitiva, la seguridad.