

Escaneo de Computadores y Redes

Práctica 10B

1. Objetivo

En esta práctica el alumno debe aprender a utilizar herramientas para evaluar la seguridad de una red y/o un computador. Existen muchas herramientas. Las más comunes son los escáneres de puertos como Nmap y Nessus. En esta práctica se utilizará Nmap, que debe instalarse y usarse en la **Máquina Virtual (MV)** utilizada en las prácticas. El adaptador de red de la MV debe estar configurado en puente y en la opción Modo promiscuo se debe Permitir todo.

2. La herramienta Nmap: visión general

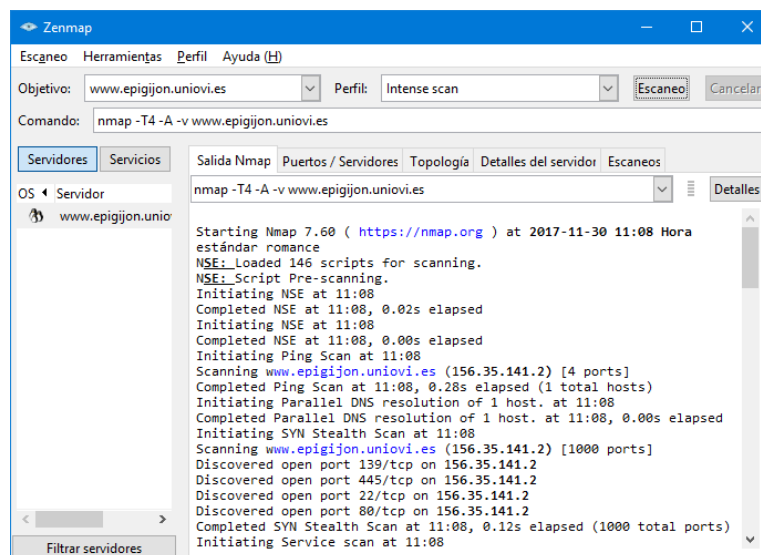
Acceder a la página web de Nmap para descargar el instalador de la herramienta:

<https://nmap.org/download.html>

Instala la herramienta y su interfaz gráfica, Zenmap, en la máquina virtual usada para prácticas.

Para una ayuda online detallada usar: <https://nmap.org/book/zenmap.html>

Al arrancar Zenmap, aparece la ventana siguiente, en la que se ha seleccionado un nombre de host en el campo "Objetivo" (Target) y se ha pulsado el botón "Escaneo" (Scan) para comprobar el correcto funcionamiento.



La **elección del objetivo** (target) a escanear incluye nombres de hosts, que debe resolver el DNS y también, direcciones IP específicas como 156.35.33.105. También se puede escanear una subred completa, como 156.35.141.0/24. Observar cómo se utiliza el sufijo /24 para indicar la máscara de subred. Esta notación se denomina CIDR (*Classless Inter-Domain Routing*). También se pueden usar direcciones como 156.35.141-145.*. El * se usa como un comodín que representa todo el rango válido que va de 0 a 255.

Zenmap recuerda los objetivos escaneados recientemente. Para volver a realizar un escaneo previo, despliega los escaneos recientes pulsando el botón flecha abajo del campo "Objetivo" (Target) y selecciona al escaneo previo deseado.

Nmap es una herramienta diseñada para utilizarse en modo comando. Zenmap es tan solo una interfaz gráfica de Nmap y existen otras interfaces alternativas.

Zenmap siempre muestra el comando Nmap que se genera en base a las opciones seleccionadas en la interfaz gráfica. En la figura anterior el comando es: `nmap -T4 -A -v www.epigijon.uniovi.es`

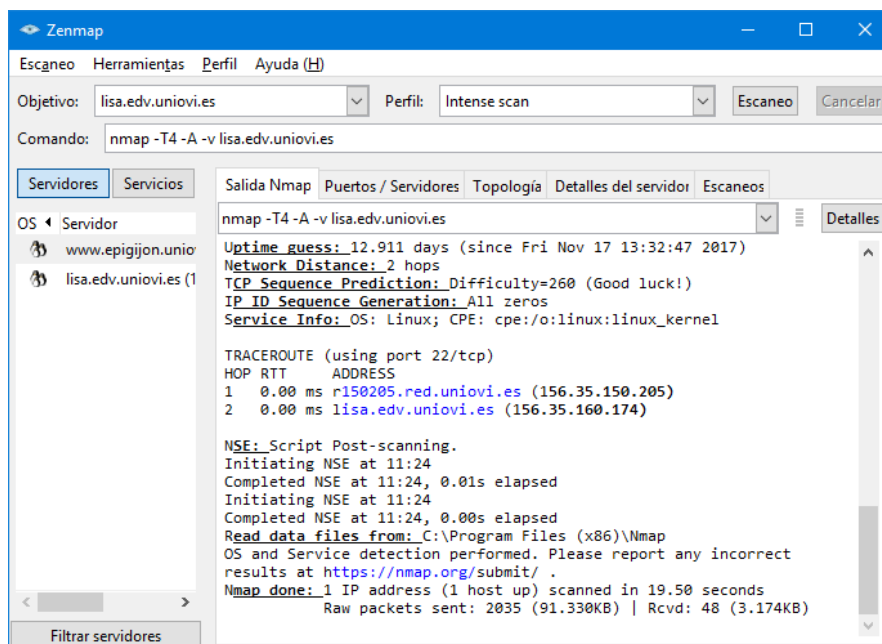
Observar que mientras el comando está ejecutándose, el icono compuesto por 5 barritas horizontales que está a la derecha del comando, y a la izquierda del botón "Detalles" (Details), está fluctuando.

La **elección del perfil** de escaneo también es importante. Por defecto Zenmap ofrece el perfil "Intense scan", que se traduce a la opción `-A` en el comando Nmap. Este perfil realiza un análisis intensivo para descubrir los equipos que hay en una red y analizarlos. Si hay muchos equipos empleará mucho tiempo.

Si tan solo se desea saber que equipos hay en una red se puede usar un perfil más simple, por ejemplo "Ping scan".

Es posible editar perfiles y almacenarlos para realizar un escaneo adaptado a unas determinadas necesidades. También es posible editar directamente el comando Nmap para realizar un escaneo específico. En este caso el campo "Perfil" (Profile) se pone en blanco, para indicar que no se está utilizando ningún perfil predeterminado.

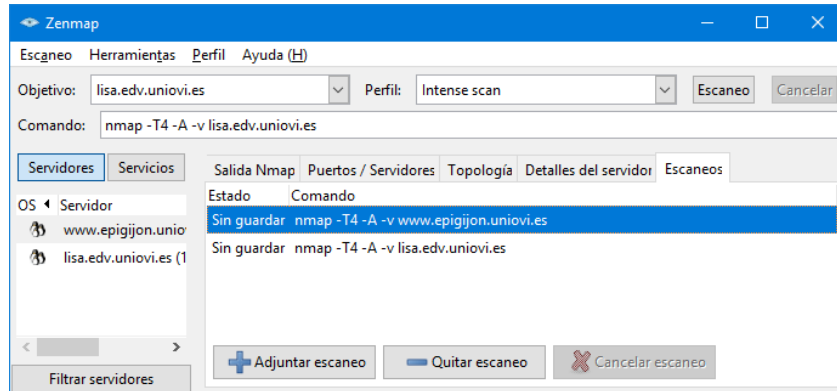
El concepto de **inventario de red** es una característica importante de Zenmap. Cuando ha terminado un escaneo, se puede iniciar otro en la misma ventana de Zenmap. Los resultados del segundo escaneo se añaden a los del primero. Como ejemplo escanear un nuevo host:



Observar que en el panel izquierdo aparece el nuevo host escaneado. Observar también que Nmap ha identificado sus sistemas operativos, cuyos iconos aparecen a la izquierda de sus nombres.

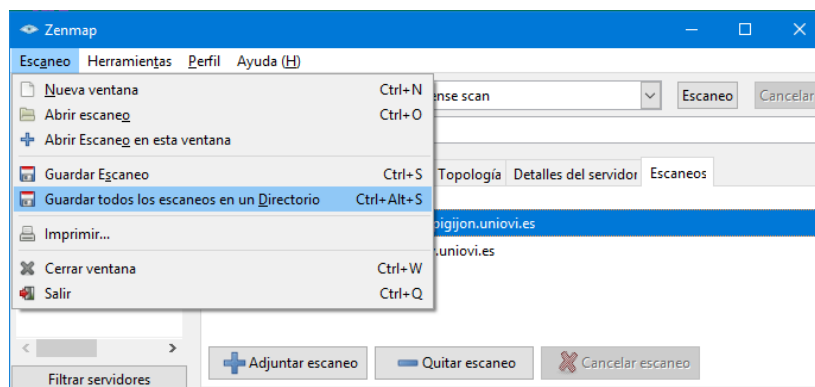
En el panel derecho está seleccionada la ficha "Salida Nmap" (Nmap output). Debajo de la ficha hay un campo para la selección del comando de escaneo. Hay que seleccionar específicamente cada escaneo para ver sus resultados.

La ficha "Escaneos" (Scans) contiene un listado de los escaneos realizados, tal como muestra la figura siguiente. Observar que su estado es "Sin guardar" (Unsaved), pues aun no se han guardado en disco.

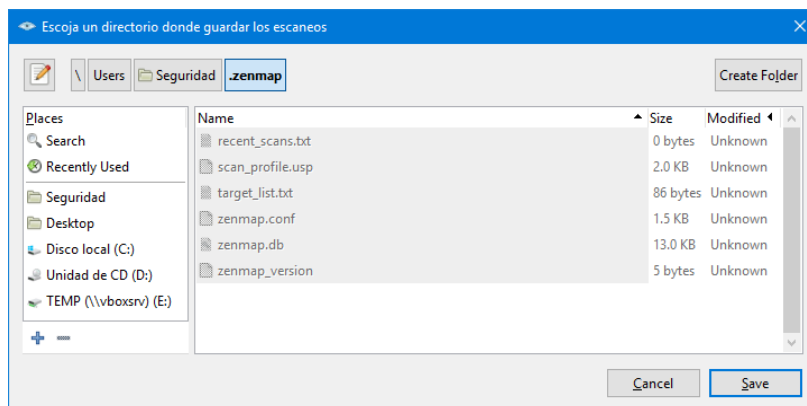


La colección de escaneos que se agregan en una misma vista o ventana de Zenmap, se denomina un inventario de red.

Para **guardar un inventario en disco** hay que seleccionar el menú "Escaneo" (Scan) de la barra de menús de Zenmap, y seleccionar la opción "Guardar todos los escaneos en un Directorio" (Save All Scans to Directory), tal como muestra la figura siguiente:

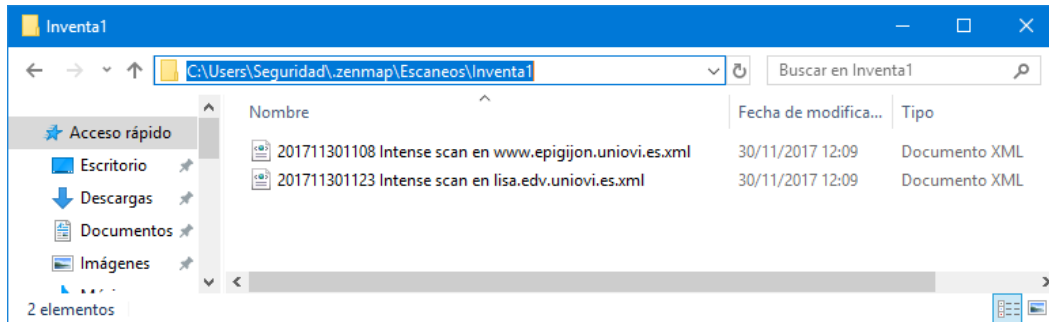


Se recomienda guardarlos dentro del mismo directorio que contiene la configuración de Zenmap. En la ventana siguiente pulsa del botón "Create Folder" para crear el directorio Escaneos.

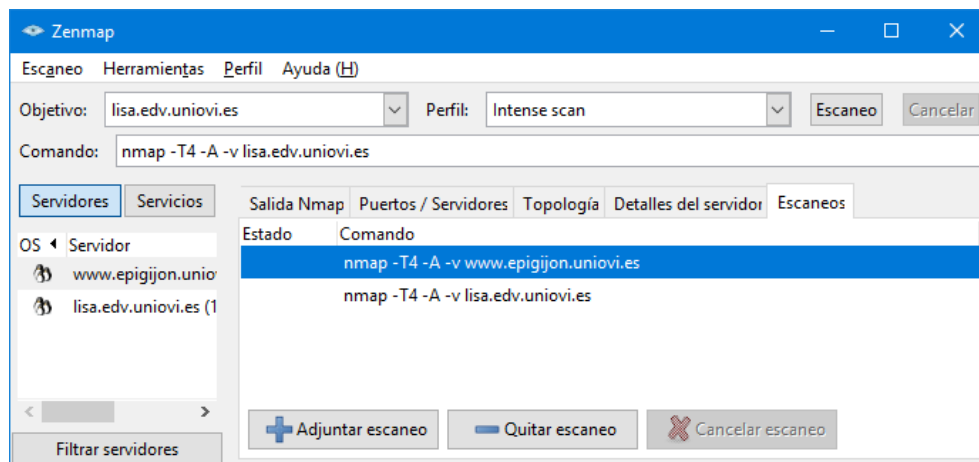


Vuelve a pulsarlo para crear el directorio Inventa1 y luego pulsa "Save".

Finalmente tenemos los dos escaneos en formato XML almacenados en el directorio seleccionado:



Observa la nomenclatura de los ficheros de escaneo: AñoMesDiaHoraMinuto Perfil Objetivo. Comprueba que después de guardar en disco el inventario, el estado de los escaneos ya no es "Sin guardar" (Unsaved) sino que está vacío:



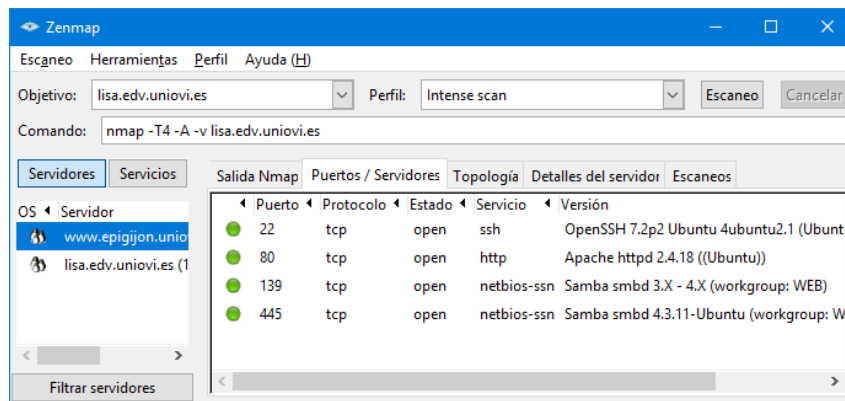
Zenmap usa la convención de que una ventana representa un inventario de red. Si se desea abrir un nuevo inventario sin cerrar el actual, seleccionar el menú "Escaneo" (Scan) de la barra de menús de Zenmap, y seleccionar la opción "Nueva ventana" (New Window).

Para **cargar un inventario almacenado en disco** hay dos posibilidades. Seleccionar el menú "Escaneo" (Scan) de la barra de menús de Zenmap, y seleccionar la opción "Abrir escaneo" (Open Scan). Se crea una nueva ventana y por tanto un nuevo inventario a partir del contenido del directorio seleccionado. Para usar la otra posibilidad selecciona la opción "Abrir Escaneo en esta ventana" (Open Scan in This Window). En este caso no se crea una nueva ventana, sino que los escaneos del directorio seleccionado se añaden a los de la ventana actual.

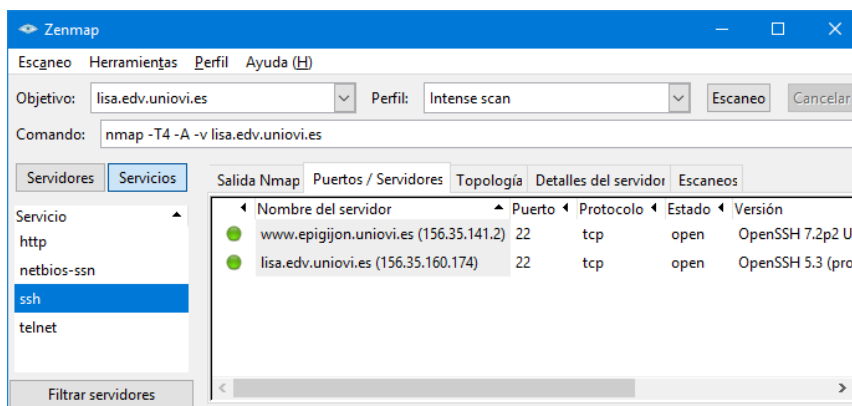
El **análisis de los resultados** se puede realizar usando varias fichas.

La ficha "Salida Nmap" (Nmap Output) muestra la secuencia de operaciones que realiza Nmap y los resultados que obtiene.

La ficha "Puertos / Servidores" (Ports / Hosts) muestra los puertos de interés del host que está seleccionado en el panel izquierdo. Cuando el puerto está abierto, se muestra un punto (semáforo) verde a su izquierda y cuando está cerrado se muestra un punto (semáforo) rojo.

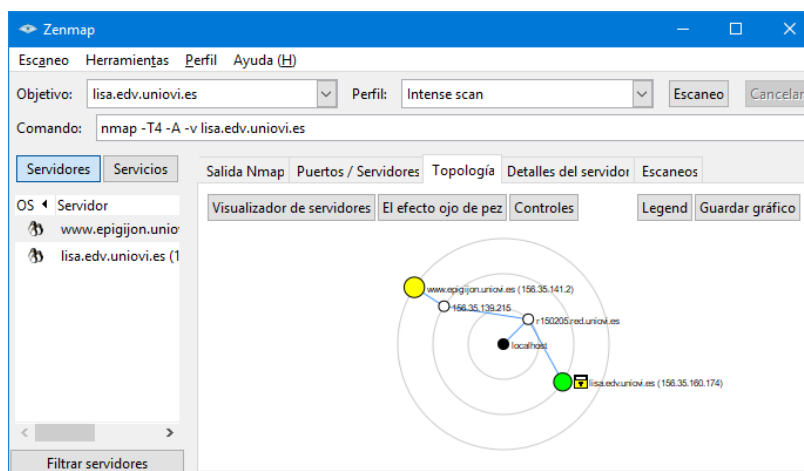


Selecciona "Servicios" (Services) en el panel izquierdo en vez de "Servidores" (Hosts). Selecciona progresivamente un servicio tras otro en el panel izquierdo y comprueba que en la ficha "Puertos / Servidores" (Ports / Hosts) se muestran todos los servidores (hosts) de nuestro inventario de red que proporcionan el servicio seleccionado.



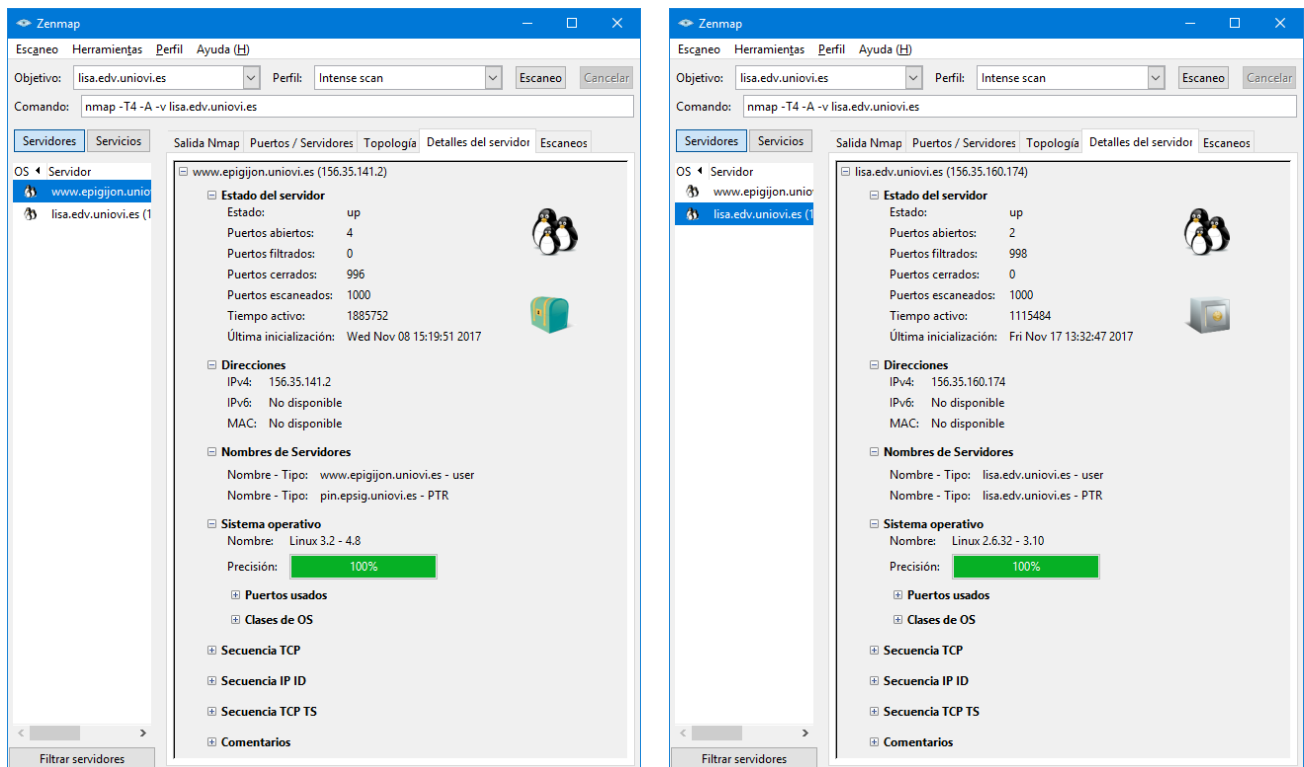
Este puede ser un buen método para responder a una pregunta cómo ¿qué computadores de la red están ejecutando http?

La ficha "Topología" (Topology) muestra la topología de la red en un formato determinado. Los servidores (hosts) se ubican en anillos concéntricos. Cada anillo representa un salto de red adicional desde el nodo central. El gráfico es interactivo. Selecciona un host y comprueba que pasa a ser el centro de la red.



Comprueba la funcionalidad que proporcionan los botones "Visualizador de servidores" (Hosts Viewer), "El efecto ojo de pez" (Fisheye) y "Controles" (Controls).

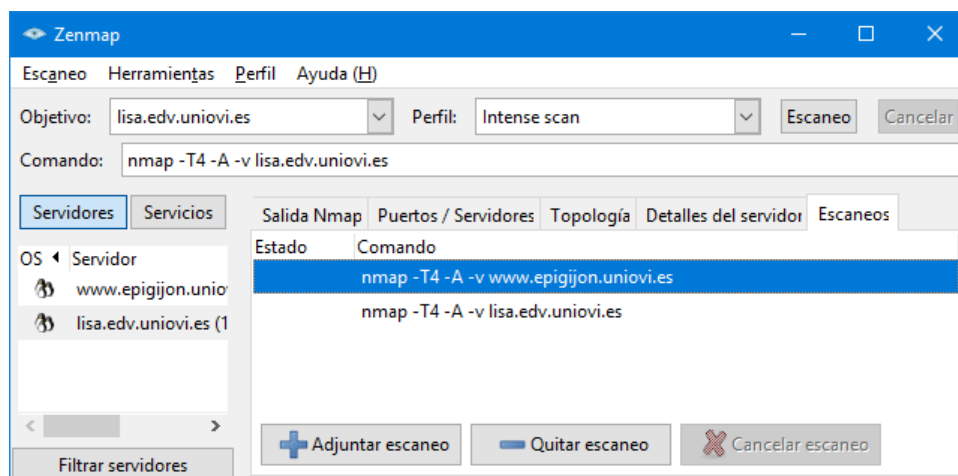
La ficha "Detalles del servidor" (Host Details) muestra la información del host seleccionado en el panel izquierdo.



Zenmap asocia un icono a cada host que indica de forma gráfica su vulnerabilidad en función de número de puertos abiertos del modo siguiente:

| Puertos abiertos | 0-2 | 3-4 | 5-6 | 7-8 | 9 o más |
|------------------|-----|-----|-----|-----|---------|
| Icono | | | | | |

La ficha "Escaneos" (Scans) muestra los escaneos realizados que constituyen el inventario de red actual.



Comprobar la funcionalidad de los botones "Adjuntar escaneo" (Append Scan) y "Quitar escaneo" (Remove Scan).

3. Escaneo de una red con Nmap (descubrimiento de hosts)

Aunque Zenmap construye de modo automático el comando a ejecutar con Nmap, es necesario conocer como se construyen los comandos para particularizar las búsquedas y los escaneos.

El comando inicial, `nmap -T4 -A -v www.epigijon.uniovi.es` se interpreta del modo siguiente:

-T4 indica que se utilice el "Timing Template 4". Un Timing Template es una preselección de varias opciones de temporización. Hay seis plantillas de temporización, T0 a T5, que se pueden usar para acelerar el escaneo (para obtener resultados rápido) o para ralentizar el escaneo (evadir los cortafuegos). Las plantillas disponibles y su comportamiento se resumen en la tabla siguiente:

| Plantilla | Nombre | Comportamiento |
|-----------|------------|---|
| -T0 | Paranoid | Extremadamente lenta |
| -T1 | Sneaky | Útil para evitar a los sistemas de detección de intrusiones |
| -T2 | Polite | Es improbable que interfiera con el sistema objetivo |
| -T3 | Normal | Esta es la plantilla de temporización por defecto |
| -T4 | Aggressive | Produce resultados más rápidamente en redes locales |
| -T5 | Insane | Escaneo muy rápido y agresivo |

-A indica que se realice un "Aggressive scan" y es una preselección de varias opciones avanzadas. como `-o -sV -sC --traceroute`, para evitar el teclear una larga línea de comandos.

-v indica que se realice una salida detallada "Verbose output" para que Nmap muestre todos los detalles de las operaciones que va realizando.

La **exploración de una red** con Nmap suele organizarse en **dos fases**: 1ª) Descubrimiento de los hosts de la red realizando escaneos denominados generalmente "Ping scans" y 2ª) Análisis de cada uno de los host realizando escaneos denominados generalmente "Port scans".

Para la **fase de descubrimiento** de los hosts de una red se puede utilizar el perfil de Zenmap denominado "Ping scan", que simplemente utiliza la opción `-sn` de Nmap. Prueba el comando siguiente:

```
nmap -v -sn 156.35.141.0/24
```

La opción `-sn` (**no port scan**) le indica a Nmap que no escanee los puertos de los hosts descubiertos. Además, para la fase de descubrimiento Nmap envía a cada objetivo seleccionado:

Solicitud de echo ICMP

+Paquete TCP SYN al puerto 443

+Paquete TCP ACK al puerto 80

+Solicitud de tiempo ICMP

Observar que el descubrimiento no consiste solo en enviar un paquete de eco ICMP, el clásico ping, sino que el concepto de ping es genérico y se refiere a toda la fase de descubrimiento.

En versiones previas de Nmap la opción `-sn` se conocía como `-sP`.

Esta búsqueda descubre unos pocos hosts rápidamente (en segundos), pero en la subred hay muchos más hosts no descubiertos.

Para descubrir los hosts de una red también es posible prescindir de lo que Nmap denomina la fase de descubrimiento, que aunque parezca un contrasentido, se explica a continuación.

Normalmente, Nmap realiza unas operaciones para descubrir los hosts de una red y luego solo en los hosts descubiertos realiza las operaciones de escaneo de puertos, descubrimiento del sistema operativo, etc.

La opción **-Pn** (**no ping**) indica a Nmap que prescinda de la fase de descubrimiento. Entonces Nmap aplica todas las operaciones de escaneo especificadas (o las que utiliza por defecto si no se han especificado algunas) sobre cada objetivo indicado. Prueba el comando siguiente:

```
nmap -v -Pn 156.35.141.0/24
```

Esta opción es útil cuando los hosts a escanear están protegidos por un cortafuegos que bloquea los paquetes enviados para descubrirlos. Con esta opción Nmap puede generar una lista de puertos abiertos en hosts que no responden a los comandos ping.

Esta búsqueda descubre muchos más hosts UP, pero necesita mucho tiempo para escanear todos los posibles objetivos (más de 3 horas). Cancela este escaneo.

Para particularizar la fase de descubrimiento se puede utilizar diversas opciones:

-PE = ICMP Echo Ping. Es la opción por defecto si no se especifican otras. Muchos hosts están configurados para no responder a paquetes ICMP por razones de seguridad.

-PP = ICMP Timestamp Ping. Es otra opción basada en ICMP para intentar recibir una respuesta que no sea bloqueada por los cortafuegos.

-PS = TCP SYN Ping. Envía un paquete SYN al objetivo y espera la respuesta. Este método puede ser útil para los sistemas que bloquean los pings estándar ICMP.

-PA = TCP ACK Ping. Envía un paquete TCP ACK al objetivo, aunque no existe una conexión, y espera algún tipo de respuesta. Este método puede ser útil para los sistemas que bloquean los pings estándar ICMP.

Prueba las cuatro opciones separadamente y luego combínalas entre ellas progresivamente hasta terminar así:

```
nmap -v -PE -PP -PS -PA 156.35.141.0/24
```

Si no se obtienen buenos resultados se puede emplear la opción **-sS** (Sondeo TCP SYN). Consulta este concepto de sondeo en la ayuda de Nmap:

<https://nmap.org/man/es/man-port-scanning-techniques.html>

4. Escaneo de un computador con Nmap (determinar el estado de los puertos)

Esta es la **segunda fase** en la que se analiza el estado (abierto, cerrado, indeterminado, ...) de los puertos de cada host encontrado en la primera fase. A veces, es necesario empezar directamente en esta fase, utilizando un escaneo detallado de todos los puertos para descubrir el host.

Una vez que Nmap escanea los puertos, les asigna un estado. Muchos escáneres le asignan a un puerto uno de dos estados posibles: abierto o cerrado. Nmap utiliza 6 estados para los puertos. Los estados no son propiedades intrínsecas de los puertos, sino una indicación de como los ve Nmap. Los 6 estados son: open, closed, filtered, unfiltered, open|filtered, closed|filtered.

open: puerto que responde activamente a una conexión entrante.

closed: puerto que responde a un sondeo pero no hay ningún servicio escuchando en él.

filtered: puerto que está protegido, típicamente por un cortafuegos, lo que impide a Nmap determinar si el puerto está abierto o cerrado.

unfiltered: puerto que está desprotegido y accesible a Nmap, pero Nmap no puede determinar si el puerto está abierto o cerrado.

open|filtered: puerto que Nmap estima que está abierto O filtrado, pero no puede determinar el estado exacto.

closed|filtered: puerto que Nmap estima que está cerrado O filtrado, pero no puede determinar el estado exacto.

Hay un total de 65535 puertos TCP y 65335 puertos UDP. Por defecto, Nmap solo escanea los 1000 puertos más comúnmente usados, para ahorrar tiempo cuando escanea múltiples objetivos. Pero se pueden usar opciones para particularizar el escaneo.

Prueba las siguientes opciones progresivamente y observa las diferencias de tiempos:

-F = Escanea solo los 100 puertos más comúnmente usados.

-p puertos = Escanea solo los puertos especificados.

```
nmap -p 25,53,80-200 156.35.141.2
```

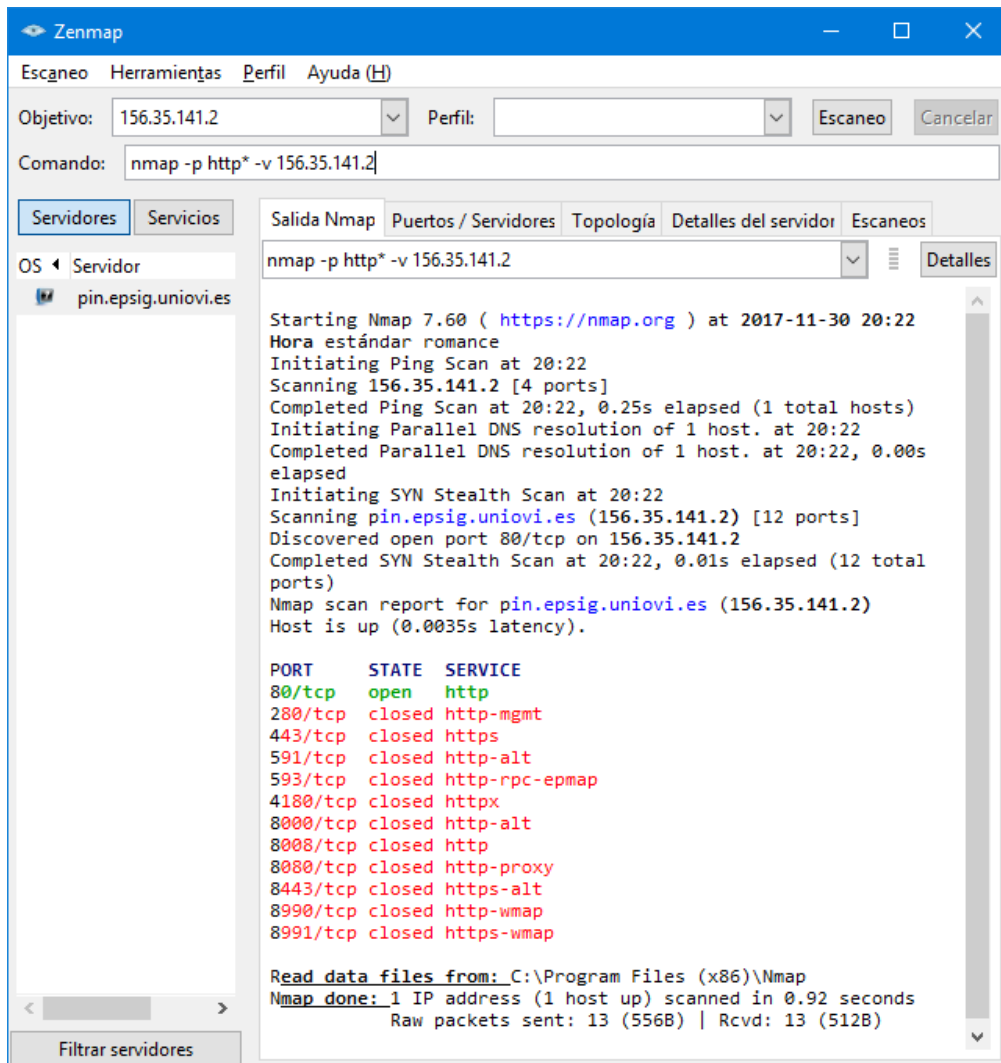
También se pueden especificar los puertos por sus nombres. Pero los nombres especificados deben coincidir con algún nombre de servicio incluido en el fichero nmap-services que está ubicado en el directorio C:\Program Files\Nmap\

```
nmap -p smtp,http 156.35.141.2
```

Además, se pueden usar comodines. El comando siguiente escanea todos los puertos cuyo nombre comienza con http, incluyendo los puertos para el protocolo http y el https.

```
nmap -p "http*" 156.35.141.2
```

La figura siguiente muestra un ejemplo del uso de la opción anterior:



Usar las siguientes opciones para realizar un escaneo de puertos específicos:

-sU -sT -p U:[udp ports], T:[tcp ports]

La opción -sU indica que se realice un escaneo de puertos UDP

La opción -sT indica que se realice un escaneo de puertos TCP intentando conexiones

La opción -p permite indicar junto con U: y T: los puertos específicos a escanear.

```
nmap -p U:53,T:25 156.35.141.2
```

-p "*" permite escanear todos los 65535 puertos TCP

--top-ports [numero] permite indicar el número de puertos más comúnmente usados a escanear.

```
nmap --top-ports 300 156.35.141.2
```

Se usa para escanear un número intermedio de puertos entre 100 (opción -F) y 1000 (defecto).

5. Detección del SO y los servicios

El proceso de identificación del SO del objetivo y su versión, se denomina "TCP/IP fingerprinting". El valor de algunos parámetros del protocolo TCP es definido en cada implementación del protocolo, esto es, en cada sistema operativo. Recopilando y almacenando esos valores se puede detectar el sistema operativo que se ejecuta en un host.

La **opción -O** habilita la detección del SO de los hosts escaneados.

Para que funcione correctamente es necesario que Nmap encuentre al menos un puerto abierto y un puerto cerrado en el host. Si Nmap no es capaz de detectar el SO se puede forzar a Nmap a generar una estimación usando la opción `--osscan-guess`.

También se puede indicar a Nmap que identifique los vendedores y las versiones del software que proporciona el servicio en cada puerto abierto detectado.

La **opción -sV** habilita la identificación de los servicios.

6. Evasión de cortafuegos

Nmap incluye algunos mecanismos que pueden ayudar a evadir los cortafuegos y los sistemas de detección de intrusiones.

La **opción -f** indica a Nmap que envíe paquetes de 8 bytes, fragmentando entonces una prueba en muchos paquetes muy pequeños. No obstante, los sistemas de defensa actuales, si están bien configurados, suelen detectar esta situación, y esta opción no sería útil.

La **opción -D** se usa para enmascarar un escaneo utilizando señuelos (*decoys*) del modo siguiente:

```
nmap -sn -D 156.35.6.5,156.35.6.7 156.35.141.0/24
```

Con este comando Nmap utiliza dos direcciones adicionales de origen falsas, además de la suya propia, para enviar paquetes. El objetivo es aparentar que se está realizando un escaneo distribuido desde múltiples máquinas y complica el rastreo del origen del escaneo.

Otra posibilidad es indicar a Nmap que genere aleatoriamente un determinado número de direcciones de origen falsas. Por ejemplo para indicar que utilice 10 señuelos aleatorios:

```
nmap -sn -D RND:10 156.35.141.0/24
```

La **opción --source-port** permite especificar el número de puerto origen en los paquetes enviados por Nmap en cada prueba. Por defecto Nmap utiliza un número de puerto aleatorio para cada prueba. La idea es que hay cortafuegos que aceptan directamente el tráfico que proviene de determinados puertos: 20 (FTP), 53 (DNS), 67 (DHCP). Para indicar esta opción se suele usar la abreviación `-g` tal como se muestra en el ejemplo siguiente:

```
nmap -sn -g 20 156.35.141.0/24
```

Hay muchas más opciones que se pueden consultar en los libros especializados.