CURSO NMAP

[Subtítulo del documento]

Contenido

Introducción 2

Objetivos del curso 2

Índice de contenidos 3

Instalación 4

Funcionamiento del Nmap 6

Especificación de objetivos 7

Descubrimiento de hosts 9

Técnicas de escaneo de Nmap 11

Especificación de puertos 16

Detección de la versión de los servicios 18

Detección del sistema operativo 20

Salida 22

Miscelánea 23

Nmap Scripting Engine (NSE) 30

Interfaz gráfica de Nmap: Zenmap 32

Cuestionario 34

Introducción

La herramienta Nmap es una aplicación de código abierto (y gratuita), creada por Gordon "Fyodor" Lyon en el año 1997. Fyodor se ha encargado del mantenimiento y mejora de Nmap desde entonces, además de mantener los sitios Web **Insecure.Org**, **Nmap.Org**, **SecLists.Org** y **SecTools.Org**, todos ellos dedicados a la Seguridad. Estos sitios Web son de visita obligada, ya que son un referente y albergan contenidos de calidad.

Nmap se puede definir como una herramienta de exploración de red y auditoría de seguridad.

Resulta útil para los administradores de sistemas y de comunicaciones, para la realización de tareas como inventario de red o monitorización de sistemas y servicios. La herramienta puede averiguar los hosts que están levantados, los servicios que ofrecen y el sistema operativo de los mismos.

La herramienta está soportada por múltiples sistemas operativos: Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS y Amiga.

Objetivos del curso

En el presente curso se explicarán los fundamentos básicos de la herramienta Nmap.

El curso está dirigido a profesionales de las TIC (administradores de sistemas, ingenieros de comunicaciones y auditores de seguridad o penetration testers), estudiantes o aficionados interesados en la informática, las redes y la seguridad.

Es importante destacar que toda la funcionalidad, comandos y ejemplos que se van a mostrar pueden emplearse tanto desde la versión en "línea de comandos" de Nmap como desde la "versión gráfica" llamada Zenmap. Cada uno que decida cual usar según sus gustos personales.

Quizá la curva de aprendizaje sea más leve con el Zenmap para los más nuevos, ya que además de una interfaz más amigable, ofrece varios perfiles de escaneo preconfigurados para los que muestra los parámetros que habría que utilizar con el Nmap en la línea de comandos. Por lo tanto, puede ser muy interesante como herramienta didáctica.

El curso tiene una duración aproximada de 45 minutos.

Índice de contenidos

índice de los contenidos del curso:

1.- Instalación

2.- Funcionamiento del Nmap

3.- Especificación de objetivos

4.- Descubrimiento de hosts

5.- Técnicas de escaneo del Nmap

6.- Especificación de puertos

7.- Detección de la versión de los servicios

8.- Detección del sistema operativo

9.- Salida

10.- Miscelánea

11.- Escaneo mediante el uso de scripts: Nmap Scripting Engine (NSE)

12.- Interfaz gráfica de Nmap: Zenmap

Instalación

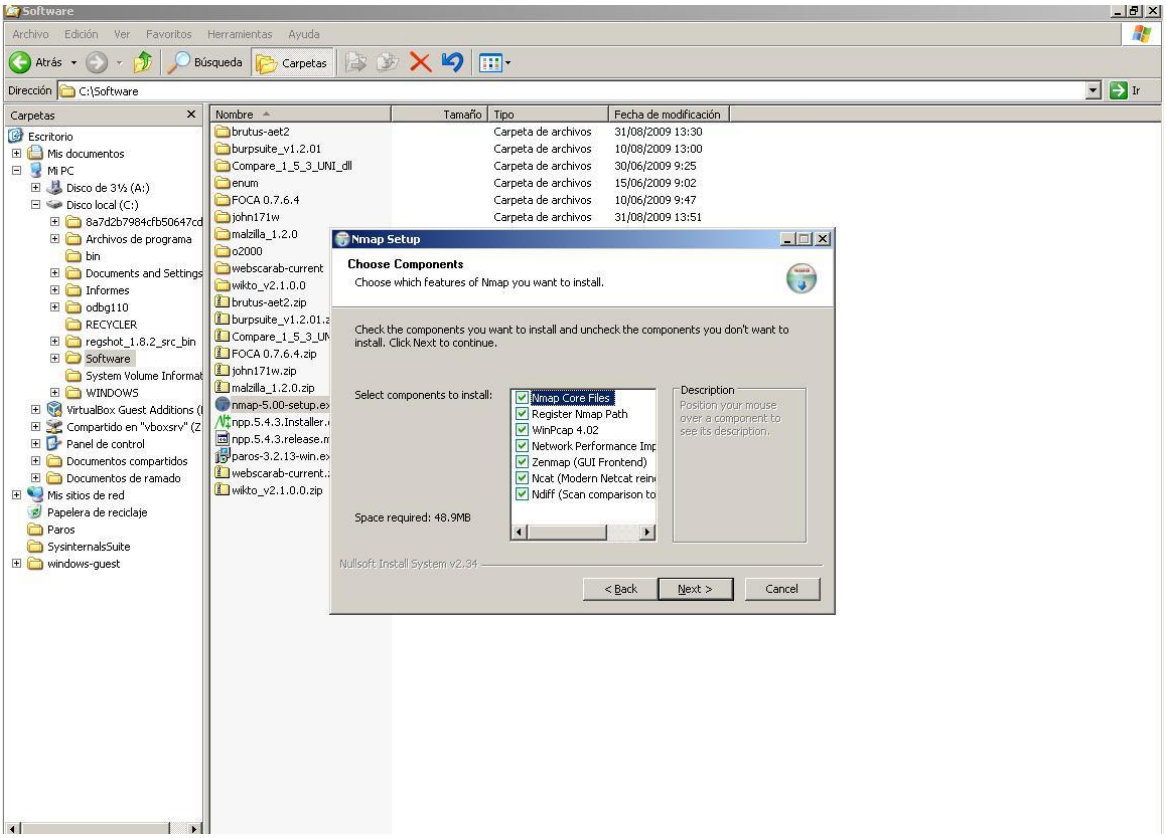
Se distribuyen versiones binarias de Nmap para Linux, Mac OS X y Windows.

En el caso de Windows se incluye una versión con un ejecutable que instala la aplicación. El port realizado de Nmap a Windows, aunque es bueno es menos estable y ofrece un menor rendimiento que su versión para Linux.

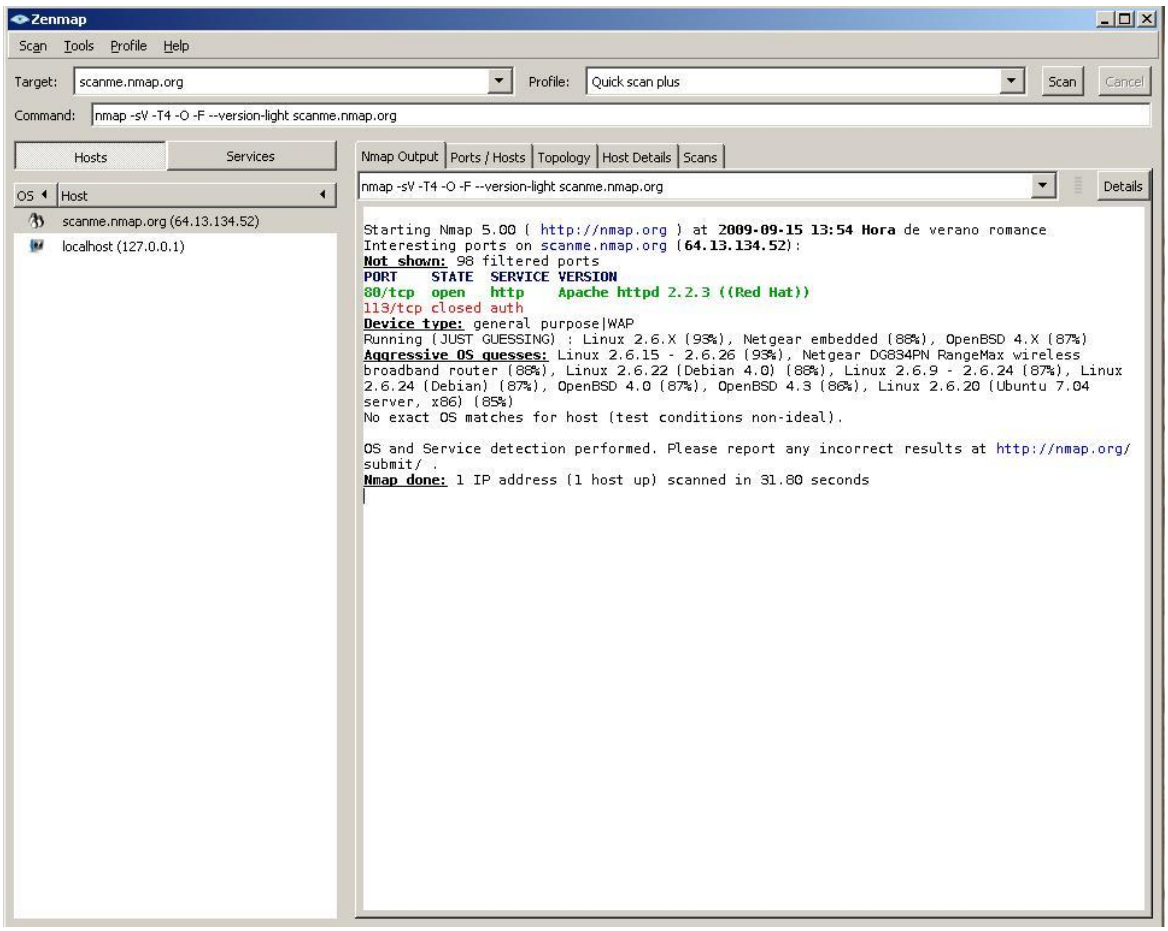
Para la instalación bajo Windows debemos descargar el instalador en **http://nmap.org/download.html**

En estos momentos está disponible la versión 5.00. A continuación se procede a instalarlo con las opciones por defecto.

Así:



Después de una sencilla instalación ya podemos empezar a usar el Zenmap GUI:



En el caso de Linux Nmap está disponible en los respositorios de paquetes de la mayoría de las distribuciones, aunque si queremos estar a la última, entonces necesitaremos compilar el código fuente.

Para más información consultar las guías de instalación disponibles en la dirección: **http://nmap.org/download.html**

Funcionamiento del Nmap

En primer lugar, vamos a mostrar las fases de un escaneo completo, luego nos centraremos en detallar cada una de las mismas:

- **Enumeración**: se especifican unos objetivos, a través de nonbres DNS, direcciones IP, notación CIDR, etc. Por ejemplo, en notación CIDR se especifican rangos de Ips como 192.168.1.0/24. Nmap resuelve estos objetivos para Ipv4. En el caso de IPv6 solo permite especificar la dirección completa o el nombre DNS.

- **Descubrimiento**: los escaneos de red suelen comenzar descubriendo cuales de los objetivos están online. Nmap ofrece múltiples métodos para realizarlo, desde una simple petición ARP hasta elaborados métodos TCP, ICMP, etc. En algunos casos, debido a restricciones del tráfico ICMP, es necesario asumir que todos los hosts están online, mediante la opción -PN.

- **Resolución inversa DNS**: Nmap trata de resolver la dirección dada por el nombre DNS (Reverse-DNS) para todos los hosts que están online.

- **Escaneo de puertos**: Esta es la función fundamental del Nmap. Este envía paquetes a los distintos puertos y según las respuestas (o la falta de las mismas) clasifica los puertos como open, closed o filtered.

- **Detección de versiones**: si se encuentran puertos a la escucha, entonces procede analizar las respuestas recibidas comparándolas con una base de datos de firmas, para poder averiguar el nombre del servicio y su versión.

- **Detección sistema operativo**: Nmap basándose en las respuestas y en el comportamiento del sistema puede averiguar el sistema operativo con un grado de acierto variable.

- **Traceroute**: mediante diversos paquetes ICMP trata de reconstruir la ruta que siguen para llegar hasta el objetivo.

- **Scripts (NSE)**: Nmap incluye un motor para la ejecución de scripts y varios scripts que ofrecen distintas posibilidades.

- **Salida**: Nmap permite configurar el formato del fichero de salida que sea necesario.

Especificación de objetivos

Veamos el aspecto que tiene un escaneo por defecto de Nmap:

```
nmap 172.16.35.90

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-03 13:50 CEST

All 1000 scanned ports on 172.16.35.90 are filtered

MAC Address: 08:00:27:XX:XX:XX (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 27.71 seconds
```

Ahora pasemos a analizar la información que nos ofrece.

La **dirección IP** especificada 172.16.35.90 es la que fijamos como objetivo. La salida que nos muestra indica que la versión del Nmap es la 5.00, que se han escaneado 1000 puertos y que todos están filtrados. Luego muestra la **dirección MAC** de nuestra tarjeta de red, la cual ha sido fabricada por Cadmus Computer Systems. Como comentario, quiero advertirles que no confíen demasiado en que la dirección MAC sea la correcta, ya que se puede **modificar** muy fácilmente. Por último, nos muestra el tiempo que ha tardado en realizar el proceso.

Veamos a continuación un resultado que ofrezca más información:

```
nmap 192.168.1.3

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-03 14:26 CEST

Interesting ports on 192.168.1.3:

Not shown: 996 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

111/tcp open rpcbind

113/tcp open auth

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 6.84 seconds
```

En este caso la máquina tiene cuatro puertos abiertos, es decir, ofrece los servicios ftp, ssh, rpcbind y auth. Nótese, que en este caso la MAC Address indica que es una tarjeta fabricada por HP.

Se pueden especificar objetivos con la notación CIDR, por ejemplo:

```
nmap -sS 172.16.28.1/25
```

La instrucción anterior escaneará con un SYN Scan el rango de direcciones 172.16.28.1-172.16.28.128.

Se pueden especificar objetivos mediante un fichero de texto:

```
nmap -iL hosts.txt
```

El contenido de hosts.txt debe incluir una dirección o un nombre de dichos objetivos en cada línea.

Descubrimiento de hosts

La opción -sL nos permite listar los objetivos posibles. Se encarga de efectuar una resolución inversa del DNS, pero no interactúa con ninguna de las máquinas.

Así, para listar los hosts disponibles en nuestra red, para el caso en que tengamos una **máscara de red**255.255.255.0 (/24) sería:

```
nmap 172.16.20.0/24 -sL

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-03 14:43 CEST

Host csirtcv1.cap.gva.es (172.16.20.11) not scanned

Host csirtcv2.cap.gva.es (172.16.20.65) not scanned

Host csirtcv3.cap.gva.es (172.16.20.71) not scanned

Host csirtcv4.cap.gva.es (172.16.20.72) not scanned

Host csirtcv5.cap.gva.es (172.16.20.74) not scanned

Host csirtcv6.cap.gva.es (172.16.20.81) not scanned

Host csirtcv7.cap.gva.es (172.16.20.82) not scanned

Host csirtcv8.cap.gva.es (172.16.20.83) not scanned

Nmap done: 256 IP addresses (0 hosts up) scanned in 2.16 seconds
```

La salida está truncada, por simplicidad (256 IP son muchas). En ella podemos ver el nombre relacionado con la IP de las máquinas para las que el DNS ha respondido.

La opción -sP realiza un ping a las máquinas y nos devuelve un listado de las que responden con un mensaje **ICMP echo reply**. De esta forma:

```
nmap 172.16.20.0/24 -sP

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-03 16:51 CEST

Host 172.16.20.1 is up (0.00015s latency).

MAC Address: 00:00:5E:XX:XX:XX (USC Information Sciences Inst)

Host 172.16.20.11 is up (0.00011s latency).

MAC Address: 00:0D:88:XX:XX:XX (D-Link)

Host csirtcv4.gva.es (172.16.28.13) is up (0.00014s latency).

MAC Address: 00:0D:88:XX:XX:XX (D-Link)

Host 172.16.20.65 is up (0.00013s latency).
```

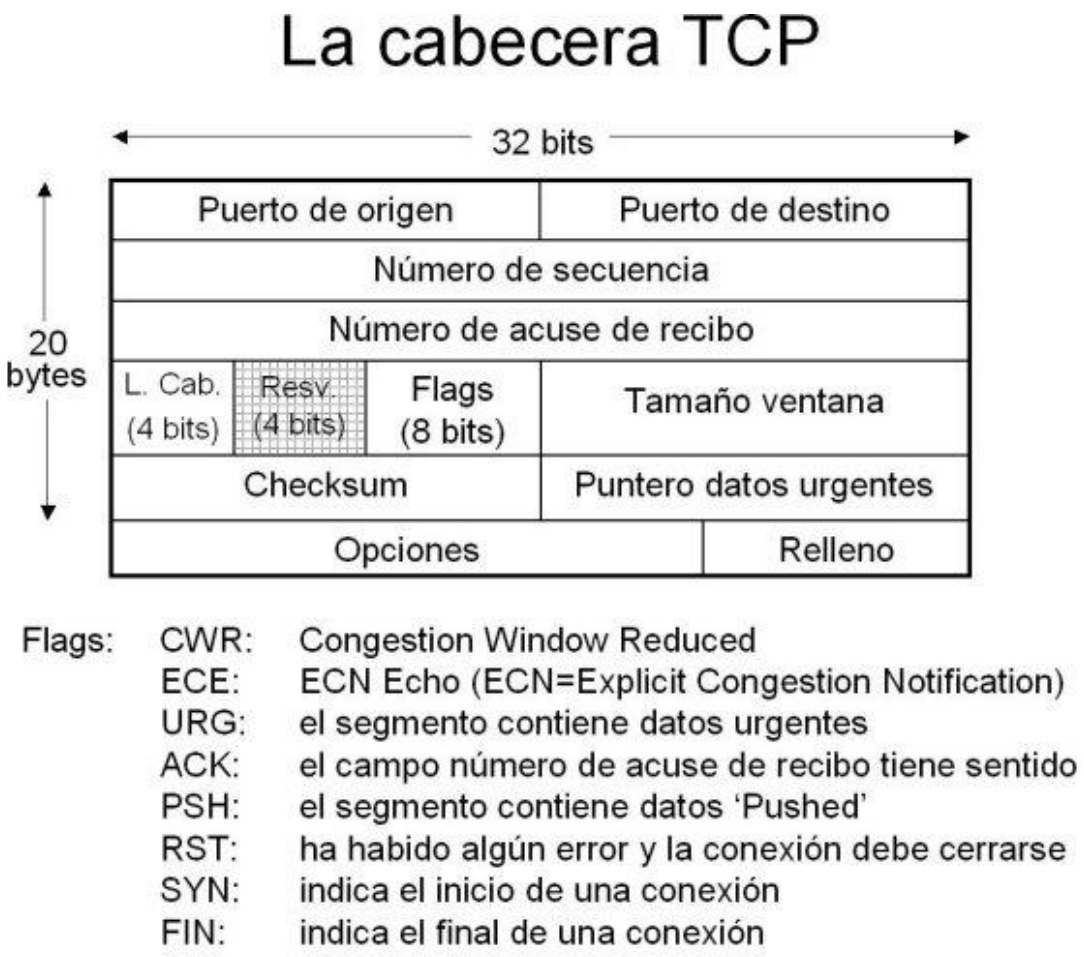
```
MAC Address: 00:19:BB:XX:XX:XX (Hewlett Packard)

Host csirtcv3.gva.es (192.168.1.2) is up.

Host 172.16.20.82 is up (0.00017s latency).

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

Host 172.16.20.90 is up (0.00036s latency).

MAC Address: 08:00:27:XX:XX:XX (Cadmus Computer Systems)

Host 172.16.20.125 is up (0.00072s latency).

MAC Address: 00:18:FE:XX:XX:XX (Hewlett Packard)

Nmap done: 256 IP addresses (8 hosts up) scanned in 2.15 seconds
```

La opción -PN evita la realización del ping a la máquina y resulta muy útil en los entornos donde se ha deshabilitado el tráfico ICMP. Que una máquina no conteste al ping no significa que no esté ahí.

Técnicas de escaneo de Nmap

Para poder comprender los diversos tipos de escaneo es preciso realizar un breve recordatorio del funcionamiento del protocolo TCP, en concreto del saludo a tres vías (three-way handshake) empleado para el establecimiento de la conexión.

Veamos la siguiente imagen:



Las fases del saludo 'a tres vías' son:

a. El host emisor envía un paquete con el bit de SYN activado, indicando al receptor que desea establecer una conexión TCP.

b. El host receptor recibe el paquete y envía un paquete con el bit de SYN y ACK activados (SYN/ACK).

c. El host emisor contesta al paquete recibido enviándole un paquete con el bit ACK activado. A partir de entonces ya pueden comenzar la comunicación entre ellos.

- **SYN scan**

El escaneo SYN del Nmap envía un paquete con el bit de SYN activado a cada puerto que se va a escanear y espera contestación.

- Si se recibe un paquete SYN/ACK por parte del receptor, entonces Nmap anota que el puerto está abierto, envía un paquete con el bit RST (reset) activado y pasa a escanear el siguiente puerto.
- Si se recibe un paquete con el bit de reset activado (RST/ACK) el puerto está filtrado por un firewall o cerrado.

La operación se repite para todos los puertos a escanear.

Este tipo de escaneo se invoca mediante la opción -sS y tiene la ventaja de que suele ser más sigiloso, desde el punto de vista de los sistemas de detección de intrusos (**IDS**).

A continuación veamos el siguiente ejemplo:

nmap -sS 192.168.1.3

Starting Nmap 5.00 (http://nmap.org) at 2009-09-03 17:18 CEST

Interesting ports on 192.168.1.3:

Not shown: 996 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

111/tcp open rpcbind

113/tcp open auth

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds

El escaneo nos indica que hay 4 puertos abiertos.

Para mostrar con exactitud cuales son los paquetes que circulan por la red, veamos una captura tcpdump del siguiente escaneo:

nmap -sS 192.168.1.3 -p 22

Starting Nmap 5.00 (http://nmap.org) at 2009-09-08 08:45 CEST

Interesting ports on 192.168.1.3:

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

A continuación veamos la traza de red correspondiente:

```
08:45:47.888489 IP 192.168.1.1.40429 > 192.168.2.2: S 3905293039:3905293039(0) win
4096 <mss 1460>

08:45:47.888857 IP 192.168.2.2.22 >
192.168.1.1.40429: S 3565060489:3565060489(0) ack 3905293040 win 5840 <mss 1460>

08:45:47.888878 IP 192.168.1.1.40429 > 192.168.2.2.22: R 3905293040:3905293040(0)
win 0
```

En la captura anterior se puede ver como la máquina origen 192.168.1.1 (la que lanza el Nmap) envía un paquete SYN a la máquina 192.168.2.2. La máquina destino le contesta con un paquete con el bit de SYN y ACK activados. Por último, la máquina origen contesta con el bit de RST activado. Según puede apreciarse en la captura se intercambian tres paquetes.

- TCP Connect

El escaneo TCP Connect del Nmap establece una conexión TCP completando los tres pasos que especifica el protocolo. Una vez que ésta ha sido establecida, Nmap corta la conexión enviando un paquete con el bit de RST activado.

Veamos un ejemplo:

```
nmap -sT -p1-27556 csirtcv1

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-04 09:08 CEST

Interesting ports on 172.16.20.1:

Not shown: 27551 filtered ports

PORT STATE SERVICE

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1723/tcp closed pptp

3389/tcp open ms-term-serv

19226/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 751.78 seconds
```

Aparecen los puertos 139, 445, 1723, 3389 y 19226 como abiertos.

De forma análoga a como hicimos con la técnica SYN scan, procederemos a mostrar la captura tcpdump del siguiente escaneo:

nmap -sT 172.16.22.1 -p 445 -PN

Starting Nmap 5.00 (http://nmap.org) at 2009-12-14 13:20 CET

Interesting ports on 172.16.22.1:

PORT STATE SERVICE

445/tcp open microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

La traza de red correspondiente es:

13:20:37.923403 IP 172.16.28.71.60597 >
172.16.28.196.445: **S** 1306037756:1306037756(0) win 5840

13:20:37.923717 IP 172.16.28.196.445 >
172.16.28.71.60597: **S** 2490814414:2490814414(0) **ack** 1306037757 win 16384

13:20:37.923742 IP 172.16.28.71.60597 > 172.16.28.196.445: . **ack** 1 win 46

13:20:37.923820 IP 172.16.28.71.60597 > 172.16.28.196.445: **R** 1:1(0) ack 1 win 46

- UDP Scan

El escaneo UDP se encarga de verificar los puertos que admiten tráfico UDP. Se envían paquetes UDP de 0 bytes a cada puerto del host destino. Si recibimos respuesta entonces el puerto está abierto. Si recibimos un ICMP Port Unreachable significa que el puerto está cerrado. Este método es menos fiable que los basados en el protocolo TCP, y puede producir falsos positivos.

Para realizar un escaneo UDP se emplea el parámetro -sU:

nmap -sU 172.16.20.1

Starting Nmap 5.00 (http://nmap.org) at 2009-09-04 14:10 CEST

Interesting ports on 172.16.20.1:

Not shown: 997 closed ports

PORT STATE SERVICE

111/udp open|filtered rpcbind

631/udp open|filtered ipp

```
5353/udp open|filtered zeroconf

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 1076.38 seconds
```

En el escaneo anterior nos indica que tiene tres posibles servicios a la escucha, pero es incapaz de distinguir si están abiertos o filtrados.

Especificación de puertos

Los escaneos por defecto (en TCP y en UDP) solo incluyen unos 1000 puertos. En algunos casos este escaneo puede ser insuficiente, por ello Nmap incluye la opción -p para indicarle los puertos que queremos que explore. Se pueden indicar puertos separados por comas o rangos de los mismos.

Veamos un par de ejemplos:

```
nmap -sS csirtcv1 -p 80,25

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-07 10:48 CEST

Interesting ports on csirtcv1.cap.gva.es (192.168.1.2):

PORT STATE SERVICE

25/tcp open smtp

80/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

En la captura anterior se especifica que se analicen los puertos 80 y 25, mediante la separación por comas.

A continuación veamos un escaneo de un rango amplio de puertos:

```
nmap -sS csirtcv1 -p 1-15000

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-07 11:14 CEST

Interesting ports on csirtcv1.cap.gva.es (192.168.1.2):

Not shown: 14991 closed ports

PORT STATE SERVICE

22/tcp open ssh

25/tcp open smtp

80/tcp filtered http

111/tcp open rpcbind

113/tcp open auth

139/tcp open netbios-ssn

389/tcp open ldap

445/tcp open microsoft-ds
```

```
10050/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

En la captura anterior se han escaneado los puertos entre el 1 y el 15000. Esto se indica separándolos por un guión.

Detección de la versión de los servicios

Nmap es capaz de determinar, con bastante precisión, la versión de los servicios del objetivo. Para ello Nmap consulta una base de datos de firmas basadas en los servicios y puertos conocidos definidos por el IANA en la página Web
http://www.iana.org/assignments/port-numbers

Esta funcionalidad resulta muy útil a la hora de hacer una auditoría, ya que podemos averiguar si las versiones de las aplicaciones son vulnerables, incluso si existen exploits públicos para las mismas.

La opción que se usa para invocarla es -sV:

```
nmap -sV -p 1-15000 csirtcv3

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-07 11:36 CEST

Interesting ports on csirtcv3.cap.gva.es:

Not shown: 14995 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp ProFTPD 1.3.1

22/tcp open ssh OpenSSH 5.1p1 Debian 5 (protocol 2.0)

111/tcp open rpcbind

113/tcp open ident

10050/tcp open tcpwrapped

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

Service Info: OSs: Unix, Linux

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

Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

En el escaneo anterior se pueden apreciar las versiones de los servicios que escuchan en los puertos:

- 21: servicio ftp. La aplicación que ofrece este servicio es ProFTPD versión 1.3.1
- 22: servicio ssh. La aplicación que ofrece el servicio es OpenSSH 5.1p1 Debian 5 (protocol 2.0)
- 111: servicio rpcbind. En este caso no se ha detectado ni la aplicación ni la versión.
- 113: servicio ident. En este caso no se ha detectado ni la aplicación ni la versión.

Hay que destacar que, como nmap confía en el listado de puertos conocidos para mapear los números de puerto con los servicios, es posible que encontremos errores, ya que es posible que algún servicio no esté escuchando en el puerto predeterminado. Por ejemplo, si tenemos un servidor FTP escuchando en el puerto 80 (por defecto debería escuchar en el 21) puede creer que es un Servidor Web como Apache.

En algunos casos, como el anterior, la versión de un servicio nos ofrece pistas sobre el sistema operativo (y la versión del mismo) sin necesidad de especificar una detección del sistema operativo (OS detection) de manera explícita. El servicio ssh indica "Debian 5" en la columna VERSION, lo que significa que el sistema operativo de la máquina tiene muchas probabilidades de ser Debian Lenny (se puede configurar para que los servicios no den pistas, incluso para que aparenten ser servicios distintos, pero no es lo más común).

Veamos la detección de servicios en otro host:

```
nmap -sV csirtcv4

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-07 12:51 CEST

Interesting ports on csirtcv4:

Not shown: 995 filtered ports

PORT STATE SERVICE VERSION

139/tcp open netbios-ssn

445/tcp open microsoft-ds Microsoft Windows 2003 microsoft-ds

1024/tcp open http Microsoft IIS webserver 6.0

1723/tcp closed pptp

3389/tcp open microsoft-rdp Microsoft Terminal Service

Service Info: OS: Windows

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

Nmap done: 1 IP address (1 host up) scanned in 21.78 seconds
```

Asimismo, en este caso, los puertos abiertos nos proporcionan pistas sobre el sistema operativo. El puerto 445 y 139 son puertos que suelen estar a la escucha en sistemas Windows. Es más, en el campo VERSION se indica "Microsoft Windows 2003".

Para finalizar, es necesario avisar de que es posible que Nmap sea incapaz de reconocer un servicio en concreto. En este caso nos mostrará una huella digital y una URL donde podremos contribuir a la mejora de la base de datos de Nmap indicando la versión del servicio para esa huella dada (si la conocemos). Desde este curso queremos sugerir que, por favor, colaboréis activamente en la mejora de las bases de datos de firmas de Nmap, ya que todos saldremos beneficiados.

Detección del sistema operativo

La detección remota del sistema operativo es una característica interesante de Nmap que averigüa con una gran probabilidad el sistema y la versión del host objetivo. Con dicho propósito, Nmap envía paquetes TCP y UDP y examina cuidadosamente las respuestas. Presta atención a las respuestas y al comportamiento de los siguientes parámetros:

- TCP **ISN**: número de secuencia inicial que se emplea por el protocolo TCP para identificar los segmentos de datos duplicados.
- IP ID (identification): campo de identificación que sirve para saber como reconstruir un paquete fragmentado.
- **TTL** Inicial.
- Tamaño de la ventana inicial.

La detección se invoca con la opción -O. Veamos un ejemplo del uso:

```
nmap  192.168.1.3 -O

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-08 13:04 CEST

Interesting ports on 192.168.1.3:

Not shown: 996 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

111/tcp open rpcbind

113/tcp open auth

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

Device type: general purpose

Running: Linux 2.6.X

OS details: Linux 2.6.13 - 2.6.27

Network Distance: 1 hop

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

Nmap done: 1 IP address (1 host up) scanned in 8.86 seconds
```

En el ejemplo anterior se identifica el sistema operativo como un Linux, con el Kernel de la rama 2.6.x.

Veamos otro ejemplo, esta vez sobre un sistema operativo Windows:

nmap -O csirtcv1.gva.es

Starting Nmap 5.00 (http://nmap.org) at 2009-10-06 13:25 CEST

Interesting ports on 172.16.20.4:

Not shown: 995 filtered ports

PORT STATE SERVICE

139/tcp open netbios-ssn

445/tcp open microsoft-ds

1024/tcp open kdm

1723/tcp closed pptp

3389/tcp open ms-term-serv

Device type: general purpose

Running (JUST GUESSING): Microsoft Windows XP|2003 (92%) Aggressive OS guesses: Microsoft Windows XP SP3 (92%), Microsoft Windows Server 2003 SP2 (92%), Microsoft Windows Server 2003 SP1 or SP2 (90%), Microsoft Windows XP SP2 or Server 2003 SP2 (89%), Microsoft Windows XP Home SP1 (French) (86%)

No exact OS matches for host (test conditions non-ideal). OS detection performed. Please report any incorrect results at http://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 9.10 seconds

En este caso nos avisa de que las condiciones no son ideales para detectar de forma fiable cual es el sistema operativo, pero estima que es un Windows XP.

Salida

Las opciones de salida nos permiten especificar el formato de la misma. Algunas opciones permiten crear ficheros en XML o texto plano, entre otros. Son interesantes las opciones:

- oN: texto normal
- oX: XML

Formato texto:

```
nmap -sS 172.16.24.2 -O -oN prueba.txt
```

Formato XML:

```
nmap -sS 172.16.24.2 -O -oX prueba_xml.txt
```

Miscelánea

Otras opciones interesantes que pueden resultar útiles si se desea aprender como funciona y que es lo que hace realmente Nmap son:

- '--packet-trace': muestra todos los paquetes enviados y recibidos.
- '-v (o vv)': muestra información adicional.
- -A: Esta opción es muy cómoda ya que activa las opciones de detección del sistema operativo, detección de versiones, escaneo de scripts y traceroute.
- '--script-trace': muestra lo que realiza el script NSE.

Veamos algunas capturas de ejemplo, donde se puedan apreciar las diferencias. Con la opción -v al aplicarlo sobre un escaneo realizado con anterioridad nos aparece:

nmap -sS 192.168.1.3 -p 22 -v

Starting Nmap 5.00 (http://nmap.org) at 2009-09-08 13:57 CEST

NSE: Loaded 0 scripts for scanning.

Initiating ARP Ping Scan at 13:57

Scanning 192.168.1.3 [1 port]

Completed ARP Ping Scan at 13:57, 0.01s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 13:57

Completed Parallel DNS resolution of 1 host. at 13:57, 5.50s elapsed

Initiating SYN Stealth Scan at 13:57

Scanning 192.168.1.3 [1 port]

Discovered open port 22/tcp on 192.168.1.3

Completed SYN Stealth Scan at 13:57, 0.01s elapsed (1 total ports)

Host 192.168.1.3 is up (0.00075s latency).

Interesting ports on 192.168.1.3:

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

Read data files from: /usr/local/share/nmap

Nmap done: 1 IP address (1 host up) scanned in 5.72 seconds

Raw packets sent: 2 (86B) | Rcvd: 2 (86B)

La opción --packet-trace también resulta interesante, ya que podemos ver a nivel de red que es lo que está sucediendo. Veamos el resultado para el mismo escaneado:

nmap -sS 192.168.1.3 -p 22 --packet-trace

Starting Nmap 5.00 (http://nmap.org) at 2009-09-08 14:05 CEST

SENT (0.0710s) ARP who-has 192.168.1.3 tell 192.168.1.2

RCVD (0.0710s) ARP reply 192.168.1.3 is-at 00:21:5A:12:01:6F

NSOCK (0.0820s) UDP connection requested to 192.168.1.24:53 (IOD #1) EID 8

NSOCK (0.0820s) Read request from IOD #1 [192.168.1.24:53] (timeout: -1ms) EID 18

NSOCK (0.0820s) UDP connection requested to 192.168.255.2:53 (IOD #2) EID 24

NSOCK (0.0820s) Read request from IOD #2 [192.168.255.2:53] (timeout: -1ms) EID 34

NSOCK (0.0820s) UDP connection requested to 192.168.255.3:53 (IOD #3) EID 40

NSOCK (0.0820s) Read request from IOD #3 [192.168.255.3:53] (timeout: -1ms) EID 50

NSOCK (0.0820s) Write request for 43 bytes to IOD #1 EID 59 [192.168.1.24:53]:
y.....82.28.16.172.in-addr.arpa.....

NSOCK (0.0830s) nsock_loop() started (timeout=500ms). 7 events pending

NSOCK (0.0830s) Callback: CONNECT SUCCESS for EID 8 [192.168.1.24:53]

NSOCK (0.0830s) Callback: CONNECT SUCCESS for EID 24 [192.168.255.2:53]

NSOCK (0.0830s) Callback: CONNECT SUCCESS for EID 40 [172.16.22.5:53]

NSOCK (0.0830s) Callback: WRITE SUCCESS for EID 59 [192.168.1.24:53]

NSOCK (0.5820s) nsock_loop() started (timeout=500ms). 3 events pending

NSOCK (1.0820s) nsock_loop() started (timeout=500ms). 3 events pending

NSOCK (1.5820s) nsock_loop() started (timeout=500ms). 3 events pending

NSOCK (2.0820s) nsock_loop() started (timeout=500ms). 3 events pending

NSOCK (2.5820s) Write request for 43 bytes to IOD #1 EID 67 [192.168.1.24:53]:
y.....82.28.16.172.in-addr.arpa.....

NSOCK (2.5820s) nsock_loop() started (timeout=500ms). 4 events pending

NSOCK (2.5820s) Callback: WRITE SUCCESS for EID 67 [192.168.1.24:53]

NSOCK (3.0820s) nsock_loop() started (timeout=500ms). 3 events pending

NSOCK (3.5820s) nsock_loop() started (timeout=500ms). 3 events pending

```
NSOCK (4.0820s) nsock_loop() started (timeout=500ms). 3 events pending

NSOCK (4.5820s) nsock_loop() started (timeout=500ms). 3 events pending

NSOCK (5.0820s) nsock_loop() started (timeout=500ms). 3 events pending

NSOCK (5.5820s) Write request for 43 bytes to IOD #2 EID 75 [192.168.255.2:53]:
y.....82.28.16.172.in-addr.arpa.....

NSOCK (5.5820s) nsock_loop() started (timeout=500ms). 4 events pending

NSOCK (5.5820s) Callback: WRITE SUCCESS for EID 75 [192.168.255.2:53]

NSOCK (5.5840s) Callback: READ SUCCESS for EID 34 [192.168.255.2:53] (120 bytes)

NSOCK (5.5840s) Read request from IOD #2 [192.168.255.2:53] (timeout: -1ms) EID 82

SENT (5.5940s) TCP 192.168.1.2:61809 > 192.168.1.3:22 S ttl=59 id=2980 iplen=44
seq=2089176135 win=4096 <mss 1460>

RCVD (5.5940s) TCP 192.168.1.3:22 > 192.168.1.2:61809 SA ttl=64 id=0 iplen=44
seq=3900035888 win=5840 ack=2089176136 <mss 1460>

Interesting ports on 192.168.1.3:

PORT STATE SERVICE

22/tcp open ssh

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

Nmap done: 1 IP address (1 host up) scanned in 5.70 seconds
```

Tal y como se puede observar en la captura anterior, la información que muestra es muy a bajo nivel, por lo que resulta muy didáctico.

Con la opción -A:

```
nmap -A 192.168.1.3

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-08 14:22 CEST

Interesting ports on 192.168.1.3:

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp ProFTPD 1.3.1

22/tcp open ssh OpenSSH 5.1p1 Debian 5 (protocol 2.0)

| ssh-hostkey: 1024 46:e7:8a:cb:23:13:19:XX:XX:XX:XX:XX:XX:XX:XX:XX (DSA)
```

```
|_ 2048 93:ad:c4:75:97:06:c9:f7:20:XX:XX:XX:XX:XX:XX:XX (RSA)

111/tcp open rpcbind

| rpcinfo:

| 100000 2 111/udp rpcbind

| 100024 1 42434/udp status

| 100000 2 111/tcp rpcbind

|_ 100024 1 34541/tcp status

113/tcp open ident

MAC Address: 00:21:5A:XX:XX:XX: (Hewlett Packard)

Device type: general purpose

Running: Linux 2.6.X

OS details: Linux 2.6.13 - 2.6.27

Network Distance: 1 hop

Service Info: OSs: Unix, Linux

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

Nmap done: 1 IP address (1 host up) scanned in 19.72 seconds
```

En la captura se puede apreciar que al encontrar servicios para los que Nmap tiene algún script del **Nmap Scripting Engine**, éste ejecuta los scripts asociados al mismo para extraer más información. Véase, que al encontrar un servicio **RPC** ha ejecutado un script asociado al rpcbind.

Para ver todo lo que realizan los scripts se puede incluir la opción '--script-trace' con el siguiente comando:

```
nmap -A 192.168.1.3 --script-trace -p 22

Starting Nmap 5.00 ( http://nmap.org ) at 2009-09-09 12:35 CEST

NSOCK (2.9020s) nsock_loop() started (timeout=50ms). 0 events pending

NSOCK (2.9020s) TCP connection requested to 192.168.1.3:22 (IOD #1) EID 8

NSOCK (2.9020s) TCP connection requested to 192.168.1.3:22 (IOD #2) EID 16

NSOCK (2.9040s) nsock_loop() started (timeout=50ms). 2 events pending

NSOCK (2.9040s) Callback: CONNECT SUCCESS for EID 8 [192.168.1.3:22]
```

NSE: TCP 192.168.1.2:59680 > 192.168.1.3:22 | CONNECT

[...]

NSOCK (2.9330s) Write request for 20 bytes to IOD #1 EID 43 [192.168.1.3:22]: SSH-1.5-NmapNSE_1.0.

NSE: TCP 192.168.1.2:59681 > 192.168.1.3:22 | 00000000: 53 53 48 2d 31 2e 35 2d 4e 6d 61 70 2d 53 53 48 SSH-1.5-Nmap-SSH

00000010: 31 2d 48 6f 73 74 6b 65 79 0d 0a 1-Hostkey

NSOCK (2.9330s) Write request for 27 bytes to IOD #2 EID 51 [192.168.1.3:22]: SSH-1.5-Nmap-SSH1-Hostkey..

NSOCK (2.9330s) nsock_loop() started (timeout=50ms). 2 events pending

NSOCK (2.9340s) Callback: WRITE SUCCESS for EID 43 [192.168.1.3:22]

NSOCK (2.9340s) Callback: WRITE SUCCESS for EID 51 [192.168.1.3:22]

NSOCK (2.9350s) nsock_loop() started (timeout=50ms). 0 events pending

NSOCK (2.9350s) Read request for 13 bytes from IOD #1 [192.168.1.3:22] EID 58

NSOCK (2.9350s) Read request from IOD #2 [192.168.1.3:22] (timeout: 30000ms) EID 66

NSOCK (2.9370s) nsock_loop() started (timeout=50ms). 2 events pending

NSOCK (2.9370s) Callback: READ SUCCESS for EID 58 [192.168.1.3:22] (32 bytes): Protocol major versions differ..

NSE: TCP 192.168.1.2:59680 < 192.168.1.3:22 | Protocol major versions differ.

[...]

NSE: TCP 192.168.1.2:59682 > 192.168.1.3:22 | 00000000: 00 00 01 5c 04 14 69 7c 66 66 fa e4 95 c7 ef 93 \ i|ff

00000010: ea b5 93 ba b3 fe 00 00 00 1a 64 69 66 66 69 65 diffie

00000020: 2d 68 65 6c 6c 6d 61 6e 2d 67 72 6f 75 70 31 2d -hellman-group1-

00000030: 73 68 61 31 00 00 00 07 73 73 68 2d 64 73 73 00 sha1 ssh-dss

00000040: 00 00 57 61 65 73 31 32 38 2d 63 62 63 2c 33 64 Waes128-cbc,3d

00000050: 65 73 2d 63 62 63 2c 62 6c 6f 77 66 69 73 68 2d es-cbc,blowfish-

00000060: 63 62 63 2c 61 65 73 31 39 32 2d 63 62 63 2c 61 cbc,aes192-cbc,a

00000070: 65 73 32 35 36 2d 63 62 63 2c 61 65 73 31 32 38 es256-cbc,aes128

00000080: 2d 63 74 72 2c 61 65 73 31 39 32 2d 63 74 72 2c -ctr,aes192-ctr,

```
00000090: 61 65 73 32 35 36 2d 63 74 72 00 00 00 57 61 65 aes256-ctr Wae

000000a0: 73 31 32 38 2d 63 62 63 2c 33 64 65 73 2d 63 62 s128-cbc,3des-cb

000000b0: 63 2c 62 6c 6f 77 66 69 73 68 2d 63 62 63 2c 61 c,blowfish-cbc,a

000000c0: 65 73 31 39 32 2d 63 62 63 2c 61 65 73 32 35 36 es192-cbc,aes256

000000d0: 2d 63 62 63 2c 61 65 73 31 32 38 2d 63 74 72 2c -cbc,aes128-ctr,

000000e0: 61 65 73 31 39 32 2d 63 74 72 2c 61 65 73 32 35 aes192-ctr,aes25

000000f0: 36 2d 63 74 72 00 00 00 21 68 6d 61 63 2d 6d 64 6-ctr !hmac-md

00000100: 35 2c 68 6d 61 63 2d 73 68 61 31 2c 68 6d 61 63 5,hmac-sha1,hmac

00000110: 2d 72 69 70 65 6d 64 31 36 30 00 00 00 21 68 6d -ripemd160 !hm

00000120: 61 63 2d 6d 64 35 2c 68 6d 61 63 2d 73 68 61 31 ac-md5,hmac-sha1

00000130: 2c 68 6d 61 63 2d 72 69 70 65 6d 64 31 36 30 00 ,hmac-ripemd160

00000140: 00 00 04 6e 6f 6e 65 00 00 00 04 6e 6f 6e 65 00 none none

00000150: 00 00 00 00 00 00 00 00 00 00 00 00 05 b5 1d 6d m

[...]

Interesting ports on 192.168.1.3:

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 5.1p1 Debian 5 (protocol 2.0)

| ssh-hostkey: 1024 XX:XX:... (DSA)

|_ 2048 XX:XX:... (RSA)

MAC Address: 00:21:5A:XX:XX:XX (Hewlett Packard)

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 2.6.13 - 2.6.27

Network Distance: 1 hop

Service Info: OS: Linux

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

La captura está truncada porque es demasiado grande, pero en ella podemos ver incluso el contenido de las tramas enviadas en hexadecimal.

Nmap Scripting Engine (NSE)

El Nmap Scripting Engine (NSE) es una potente funcionalidad del Nmap que permite la ejecución de scripts, que además permite que los usuarios puedan escribir y compartir scripts para realizar multitud de tareas. El propio Nmap en sus últimas versiones incorpora varios scripts, algunos de los cuales pueden resultar muy útiles. Las tareas que se pueden realizar con el NSE se agrupan en:

- Descubrimiento de red.
- Detección de versiones de servicios mejorada.
- Detección de vulnerabilidades.
- Detección de gusanos y backdoors.
- Explotación de vulnerabilidades.

Estos scripts nos permiten de una forma muy cómoda, tanto prepararnos para prevenir una posible intrusión como identificar si la hemos sufrido, y tenemos **Malware**, **Backdoors** o **Troyanos** en nuestros sistemas.

A continuación veremos un par de ejemplos prácticos de detección.

Gusano Conficker

El script smb-check-vulns.nse, comprueba si el **RPC** de un sistema Windows es vulnerable (descrita en el boletín**MS08-067**). Esta vulnerabilidad no sólo permite realizar un **DoS** a regsvc, sino que además es utilizada por Conficker para ejecutar código, lo que vamos a intentar prevenir detectando si es o no vulnerable. Al respecto de esto, se debe tener mucho cuidado al utilizarlo porque podría tumbar el servicio en caso de ser vulnerable. Se recomienda avisar a los responsables y obtener su aprobación antes de efectuar las pruebas.

La presencia o no de esta vulnerabilidad la comprobaremos así:

```
nmap -sV -sC --script=smb-check-vulns.nse  172.16.22.1

Starting Nmap 5.00 ( http://nmap.org ) at 2009-12-14 12:12 CET

Interesting ports on 172.16.22.1 :

Not shown: 995 filtered ports

PORT STATE SERVICE VERSION

139/tcp open netbios-ssn

445/tcp open microsoft-ds Microsoft Windows 2003 microsoft-ds

1024/tcp open http Microsoft IIS webserver 6.0

1723/tcp closed pptp

3389/tcp open microsoft-rdp Microsoft Terminal Service

Service Info: OS: Windows

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

Nmap done: 1 IP address (1 host up) scanned in 21.94 seconds
```

Si por el contrario, hemos sufrido una intrusión o sospechamos que podemos tener algunos sistemas infectados podemos utilizar el script p2p-conficker.nse, que examina las comunicaciones P2P y detecta en función de las mismas si la máquina está infectada con Conficker.C (o superior).

De esta forma:

nmap -sV -sC --script=p2p-conficker.nse 172.16.22.1

Starting Nmap 5.00 (http://nmap.org) at 2009-12-14 11:29 CET

Interesting ports on 172.16.22.1: Not shown: 995 filtered ports

PORT STATE SERVICE VERSION

139/tcp open netbios-ssn

445/tcp open microsoft-ds Microsoft Windows 2003 microsoft-ds

1024/tcp open http Microsoft IIS webserver 6.0 1723/tcp closed pptp

3389/tcp open microsoft-rdp Microsoft Terminal Service

Service Info: OS: Windows

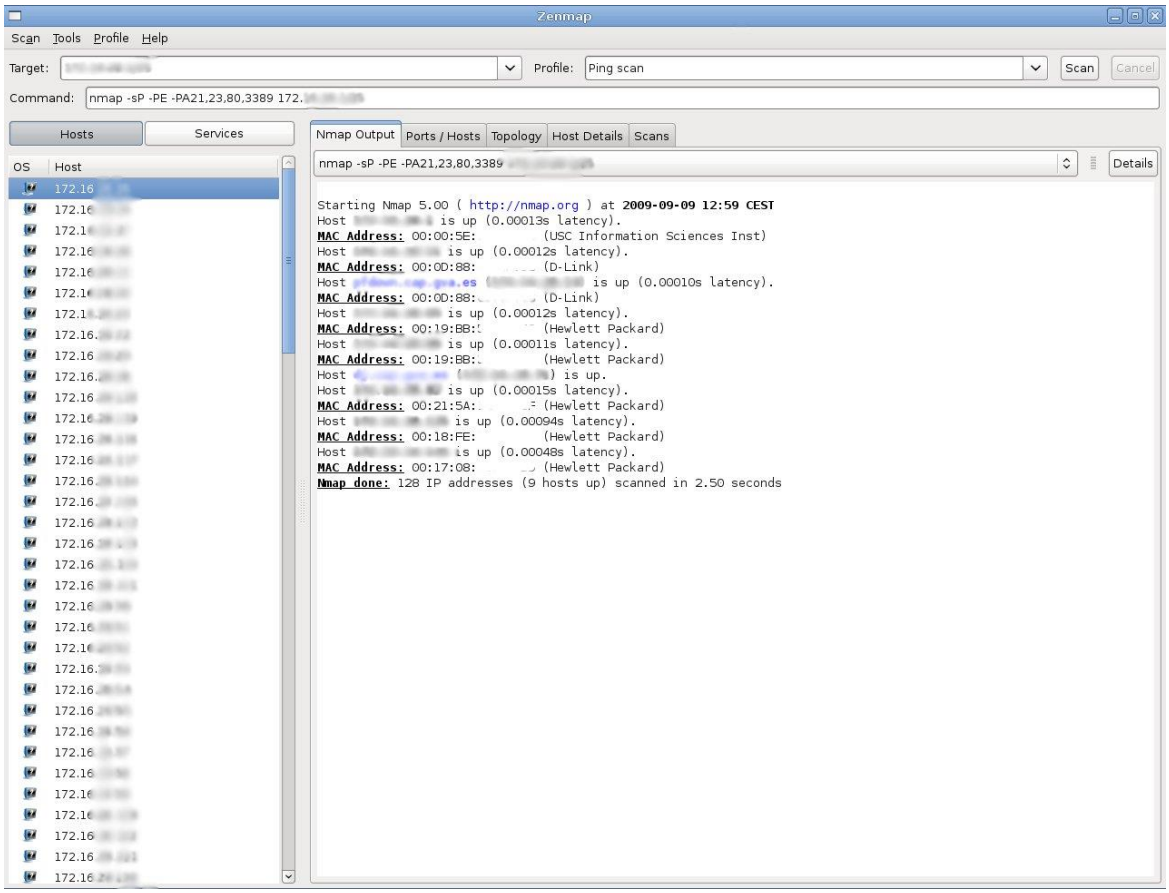
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 61.74 seconds

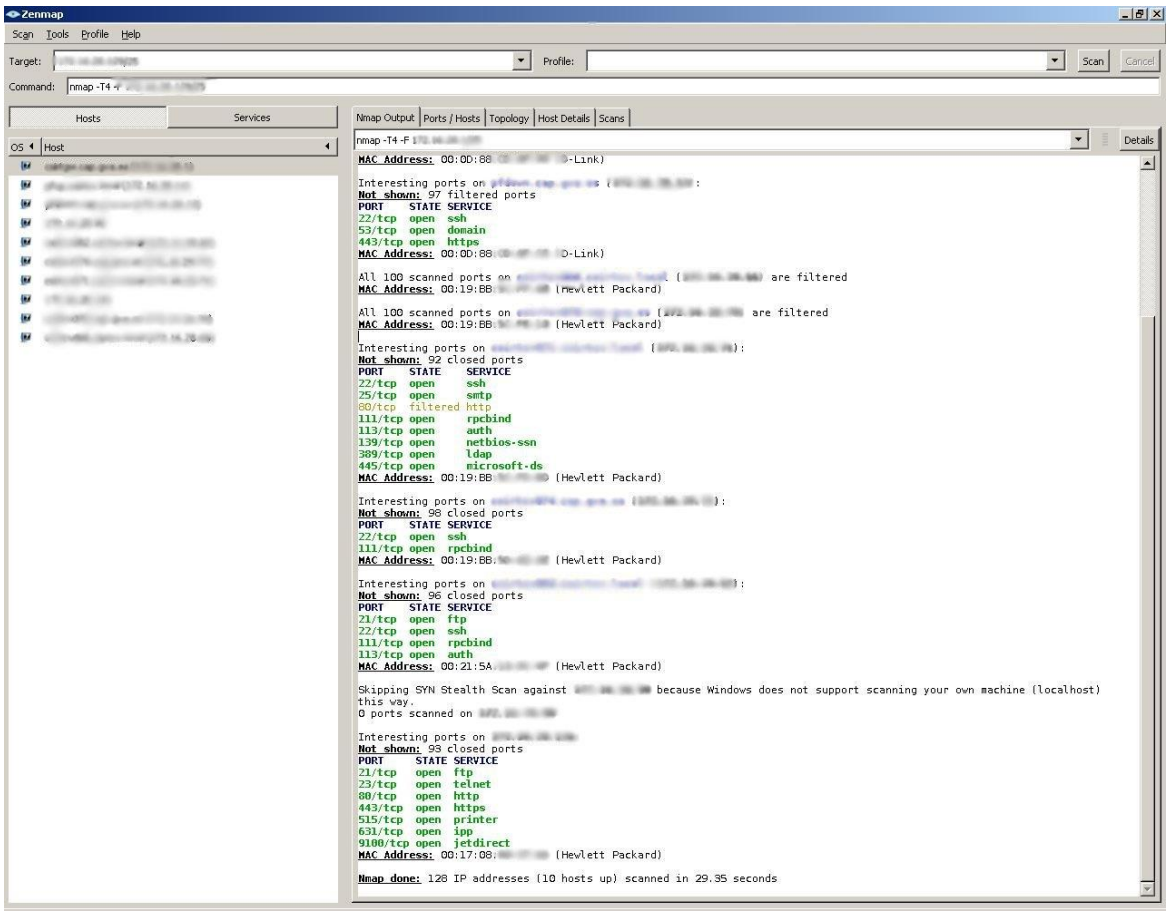
Interfaz gráfica de Nmap: Zenmap

La interfaz gráfica es muy sencilla e intuitiva de manejar.

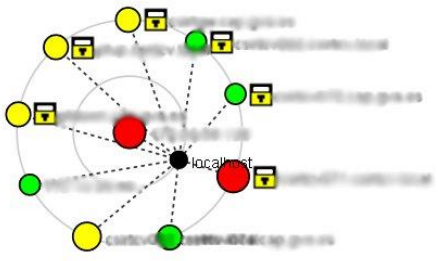
En la siguiente captura podemos ver un escaneo ping (ping scan):



En la parte superior se definen los objetivos, el perfil y el comando a ejecutar. Si desplegamos varios perfiles podremos ver como cambia el comando que se va a utilizar. Como ya dije anteriormente esto resulta muy útil para aprender como se invocan las distintas opciones del Nmap. En la parte inferior, a la izquierda se muestra un listado con los hosts o servicios encontrados y en la parte derecha se muestran los resultados obtenidos con el comando, pero con colores, al contrario que en la terminal.



El Zenmap tiene la funcionalidad de generar un mapa con la topología de red correspondiente al escaneo realizado. Veamos el mapa generado a raíz del escaneo anterior:



Cuestionario

Para superar el curso se debe obtener una puntuación de al menos 6 puntos sobre 12 en el cuestionario del curso.

La prueba es un examen tipo test con cuatro opciones en el que solo hay una respuesta válida y donde las preguntas erróneas no restan.

Pregunta 1 / 12

Puntuación: 1

Nmap es...

- Un escáner de vulnerabilidades.
- Un escáner de puertos.
- Aplicación para la edición de vídeo.
- Entorno de ejecución de exploits.

Pregunta 2 / 12

Puntuación: 1

La herramienta Nmap es:

- Comercial.
- Software libre de pago.
- Software libre gratuito.
- Freeware.

Pregunta 3 / 12

Puntuación: 1

La herramienta ha sido creada por:

- Bruce Schneier.
- Antonio Banderas.
- Fyodor.
- Dan Kaminsky.

Pregunta 4 / 12

Puntuación: 1

¿Con qué comando puedo realizar un Ping Scan de Nmap?

- Con el comando Ping.
- Con el comando traceroute en Linux y tracert en Windows.
- Con el comando Telnet.
- Con el navegador Web.

Pregunta 5 / 12

Puntuación: 1

¿Para qué sirve la opción -O de Nmap?

- Para saltarse las comprobaciones de conectividad mediante Ping.
- Para detectar cual es el sistema operativo de la máquina objetivo.
- Para detectar la versión de los programas instalados.
- Es una opción incorrecta, la correcta es -PO.

Pregunta 6 / 12

Puntuación: 1

¿Cuántos paquetes se intercambian al realizar un SYN Scan para determinar que un puerto TCP está abierto?

- 2
- 3
- 4
- 5

Pregunta 7 / 12

Puntuación: 1

¿Y si está cerrado?

- 1
- 2
- 3
- 4

Pregunta 8 / 12

Puntuación: 1

¿Cuántos paquetes se intercambian al realizar un TCP Connect Scan para determinar si un puerto TCP está abierto?

- 2
- 3
- 4
- 5

Pregunta 9 / 12

Puntuación: 1

¿Para qué plataformas no está disponible el Nmap?

- Microsoft Windows.
- Solaris.
- PS3.
- Mac OS X.

Pregunta 10 / 12

Puntuación: 1

¿Cuál de las siguientes órdenes realiza un escaneo por toda la red 192.168.1.0-255?

- nmap 192.168.1.1
- nmap 192.168.1.1, 255
- nmap 192.168.1.0 netmask 255.255.255.0
- nmap 192.168.1.0/24

Pregunta 11 / 12

Puntuación: 1

El motor de scripting de Nmap NSE contiene una serie de scripts que permiten realizar una serie de acciones, ¿cuáles son?

A. Descubrimiento de red.
B. Realización de cambios en la configuración del objetivo.
C. Detección de vulnerabilidades.
D. Explotación de vulnerabilidades.

- A, B y C.
- A, B. C y D.
- A, C y D.
- Ninguna.

Pregunta 12 / 12

Puntuación: 1

¿Cómo se llama la interfaz gráfica para Nmap?

- Gmap.
- GTKMap.
- Zenmap.
- Amap.