2. Pasos de un Ataque a la Ciberseguridad

2. Escaneo de Redes

2.1 Introducción

El escaneo en redes es un procedimiento para identificar hosts activos en una red, ya sea con el propósito de atacarlos o para la evaluación de la seguridad de la red. Los procedimientos de escaneo, tales como barridos de ping y escaneo de puertos, devuelven información acerca de las direcciones IP que se asignan a los hosts activos en Internet o en una red local y cuáles son los servicios que ofrecen. Otro método de escaneo, como el mapeo inverso, devuelve información acerca de las direcciones IP que no se han asignado a hosts, lo que permite a un atacante hacer suposiciones acerca de direcciones viables para otras actividades.

El escaneo es uno de los tres componentes de la recopilación de inteligencia para un atacante. En la fase de footprinting, el atacante crea un perfil de la organización de destino, con información como su sistema de nombres de dominio (DNS) y servidores de correo electrónico, o su rango de direcciones IP. La mayor parte de esta información está disponible en línea. En la fase de escaneo, el atacante encuentra información sobre las direcciones IP específicas que se pueden acceder a través de Internet, de sus sistemas operativos, la arquitectura del sistema y los servicios que se ejecutan en cada equipo. En la fase de enumeración, el atacante recopila información como el usuario de la red y los nombres de grupos, tablas de enrutamiento, y datos del protocolo simple de administración de redes (SNMP).

2.2 Herramientas de Escaneo de Redes

Una herramienta de escaneo de puertos es una necesidad para cualquier red, incluso si la red es pequeña. Estas herramientas nos pueden proporcionar información crucial, incluyendo qué servicios se están ejecutando en los puertos, el nombre y versión, sistema operativo de la aplicación, etc.

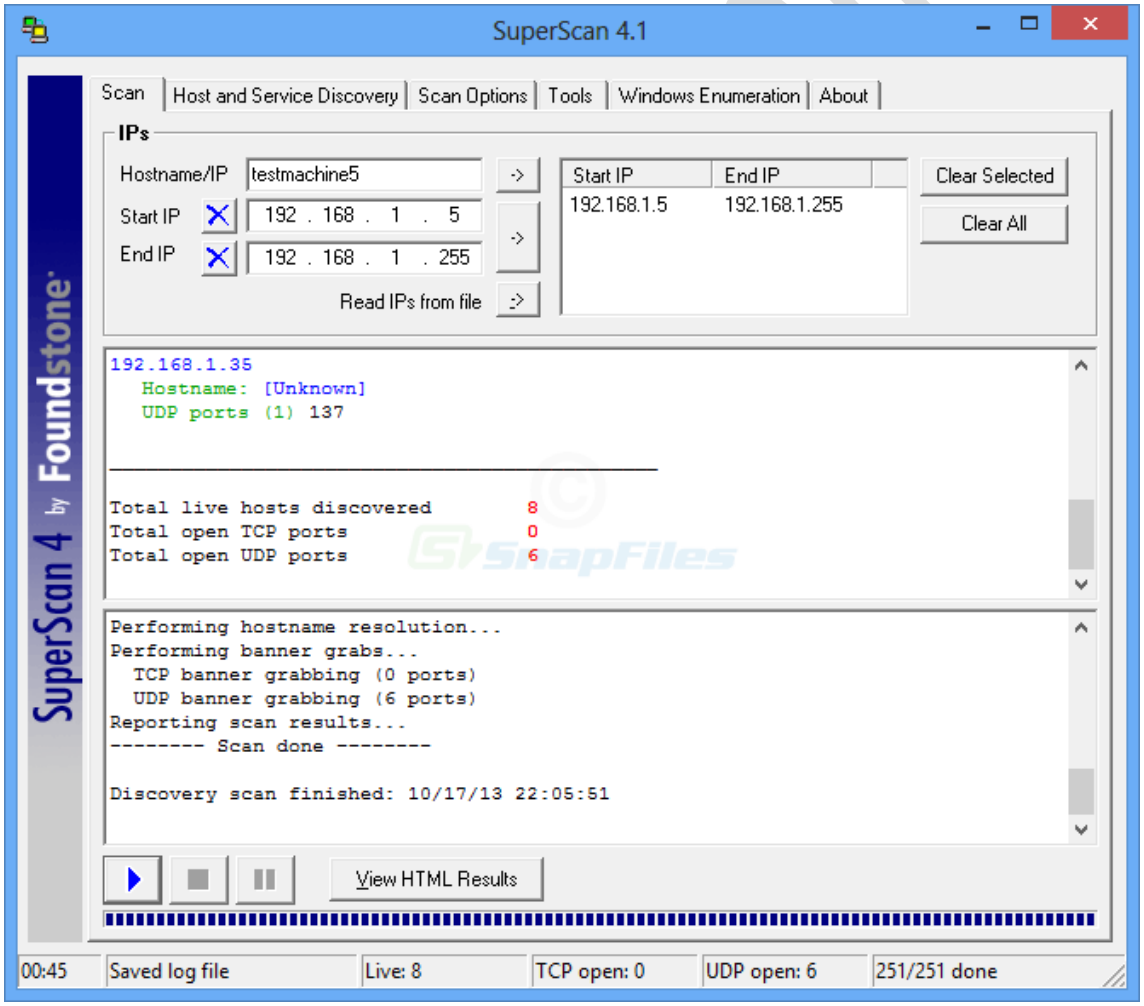
Podemos encontrar multitud de herramientas de escaneo de red en Internet que son gratuitos, entre ellas: SuperScan, Nmap y Fping. Estas herramientas de escaneo de red tienen características valiosas que podemos utilizar para gestionar nuestra red.

También debemos tener en cuenta que estas herramientas son las favoritas para los atacantes. Así que para estar siempre un paso por delante querremos utilizarlas para proteger nuestra red.

2.2.1 SuperScan

Una de las primeras aplicaciones de escaneo de puertos que debemos tener en cuenta es SuperScan.

http://www.snapfiles.com/get/superscan.html



Si elegimos esta herramienta estamos en buena compañía, porque muchos administradores de sistemas utilizan esta herramienta para analizar la seguridad de su red. Por desgracia, esta es una de las herramientas que también son ampliamente utilizadas por los piratas informáticos. Usarán SuperScan para explorar puertos abiertos. Después, intentarán infiltrarse en nuestra red. Los atacantes pueden iniciar un ataque de denegación de servicio o recopilar información sobre el host remoto.

SuperScan, cuyo objetivo es identificar puertos TCP y UDP abiertos en un equipo de destino, está repleto de características que encontraremos muy útiles para nuestra red. Por un lado, no sólo puede realizar escaneos de puertos, sino también de ping. Se puede usar un rango de IPs o crear un archivo de texto, una lista de las direcciones IP que queramos escanear. SuperScan luego saca la lista de direcciones IP y empieza a escanearlas.

2.2.2 Nmap

Nmap es una herramienta de escaneo de puertos que utilizan los profesionales de la seguridad de la red. Si administramos una red grande, Nmap está diseñado para escanearla rápidamente.

http://nmap.org/

Nmap realiza diversos análisis de red, tales como exploraciones de ping para ver hosts "vivos" en la red. Nmap también ofrece análisis más sofisticados. Estos análisis se basan en el tipo de paquete y protocolo. Incluso puede ocultar su identidad mediante la difusión de las exploraciones en varios hosts.

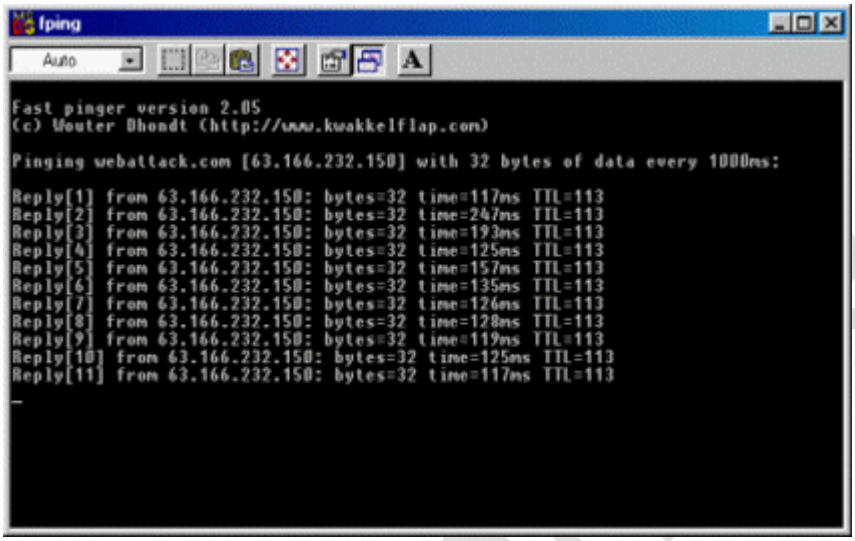
La aplicación, escrita originalmente por Gordon Lyon, crea un "mapa" de la red. Nmap es flexible ya que soporta la mayoría de sistemas operativos, incluyendo Microsoft Windows, FreeBSD, Linux, Solaris, Mac OS X, NetBSD, HP-UX, Amiga, y otros. Nmap viene en dos versiones: la GUI o la consola de comandos.

No debemos pensar que Nmap sólo realiza el escaneo de puertos. Tiene otras funciones de gestión de red. Nmap, siglas de Network Mapper, lleva a cabo tareas, como el inventario de activos de la red, seguimiento de tiempo de actividad de servicios o hosts...

Esta herramienta analiza los paquetes IP en bruto para averiguar información crucial acerca de la red, incluyendo ordenadores disponibles, servicios que los hosts están proporcionando, sistemas operativos y los tipos de cortafuegos/filtros de paquetes que se están ejecutando, así como otros atributos.

2.2.3 Fping

A diferencia de otras herramientas de software de escaneo de puertos, Fping es únicamente una herramienta de consola de comandos. Fping también difiere de las demás en que utiliza el protocolo ICMP (Internet Control Message Protocol). Intenta hacer una conexión TCP a un puerto en particular con el fin de averiguar si el host está activo. Podemos utilizar la línea de comandos para hacer ping a un número determinado de hosts o usar un archivo que consta de los hosts.

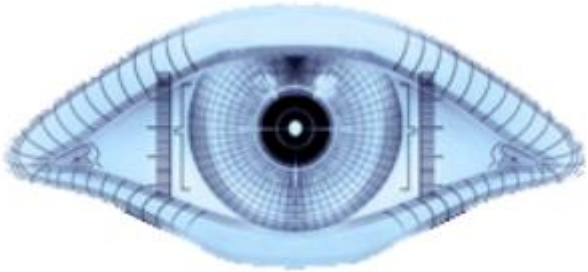


Fping está diseñado para ser integrado en scripts. La herramienta de escaneo de puertos funciona de forma muy parecida al programa ping que se encuentra en Microsoft Windows. Pero Fping tiene características adicionales. Por un lado, se puede ajustar el tiempo entre pings desde 1 milisegundo a 5 segundos. Si deseamos probar el estado de la red en segundo plano, podemos hacer Fping suene cada vez que el ping sea exitoso o cuando el host no responda. Poemos utilizar un comando para hacer ping a varios hosts o abrir un archivo y leer una lista de hosts.

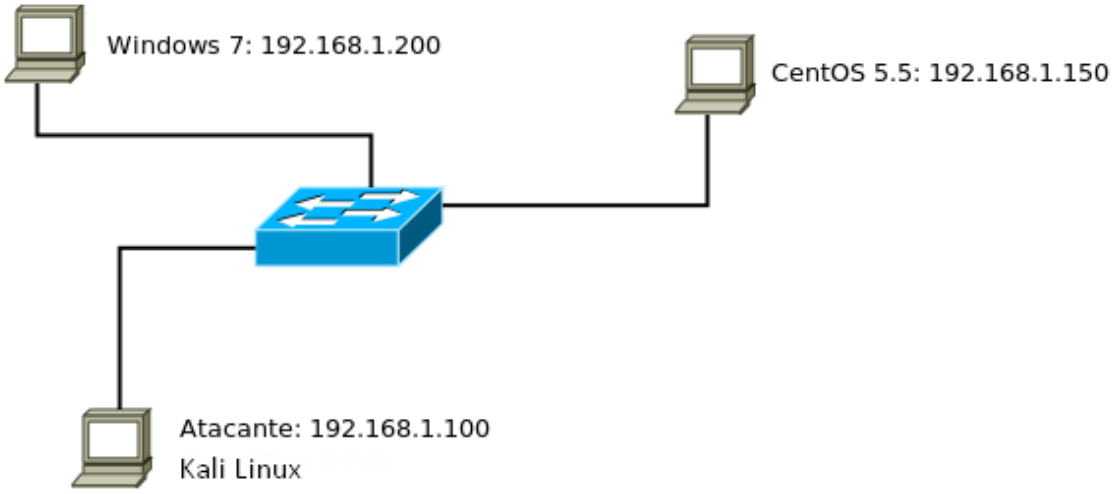
2.3 Escaneo de Puertos con Nmap

Nmap se desarrolló como un escáner para redes básico, pero incluye una gran cantidad de características que podrían usarse en pruebas de penetración y análisis de vulnerabilidades y con cada nueva versión añade aún más funciones:

- Es capaz de determinar el sistema operativo del host que estamos escaneando.
- Puede decirnos los servicios activos y las versiones instaladas de los mismos.
- Incluye facilidades para esquivar cortafuegos y para ocultar la dirección IP de origen del equipo desde el que se lleva a cabo el proceso.
- Puede integrarse con otras herramientas para aumentar su funcionalidad.
- Podemos desarrollar nuestros propios scripts para personalizar la herramienta y añadir nuevas funciones.
- …

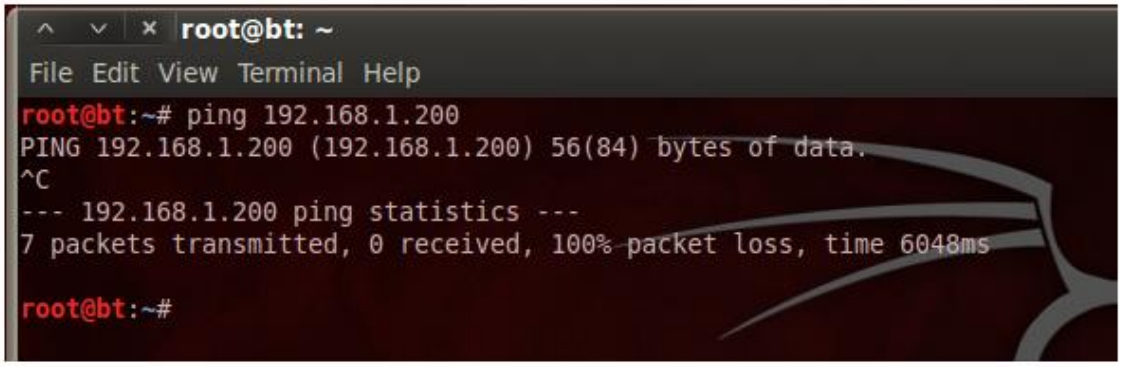


Para realizar demostraciones utilizaremos la siguiente topología creada con máquinas virtuales:



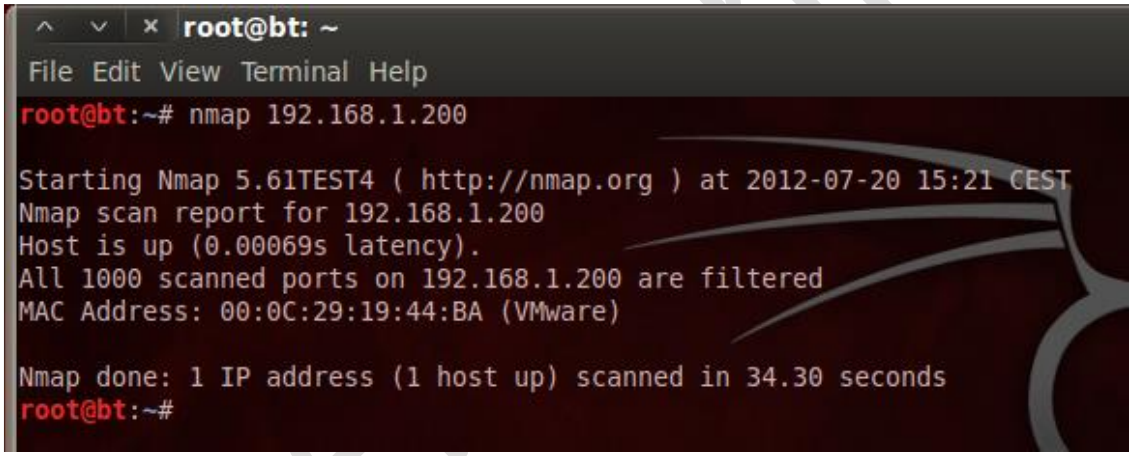
Empezaremos con el escaneo más básico de Nmap, en el que no usaremos ninguna de sus muchas opciones, simplemente indicaremos cuál es la máquina objetivo.

La instalación por defecto de Windows 7 activa el cortafuegos del sistema operativo, por lo que si intentamos hacer un ping veremos que no responde:



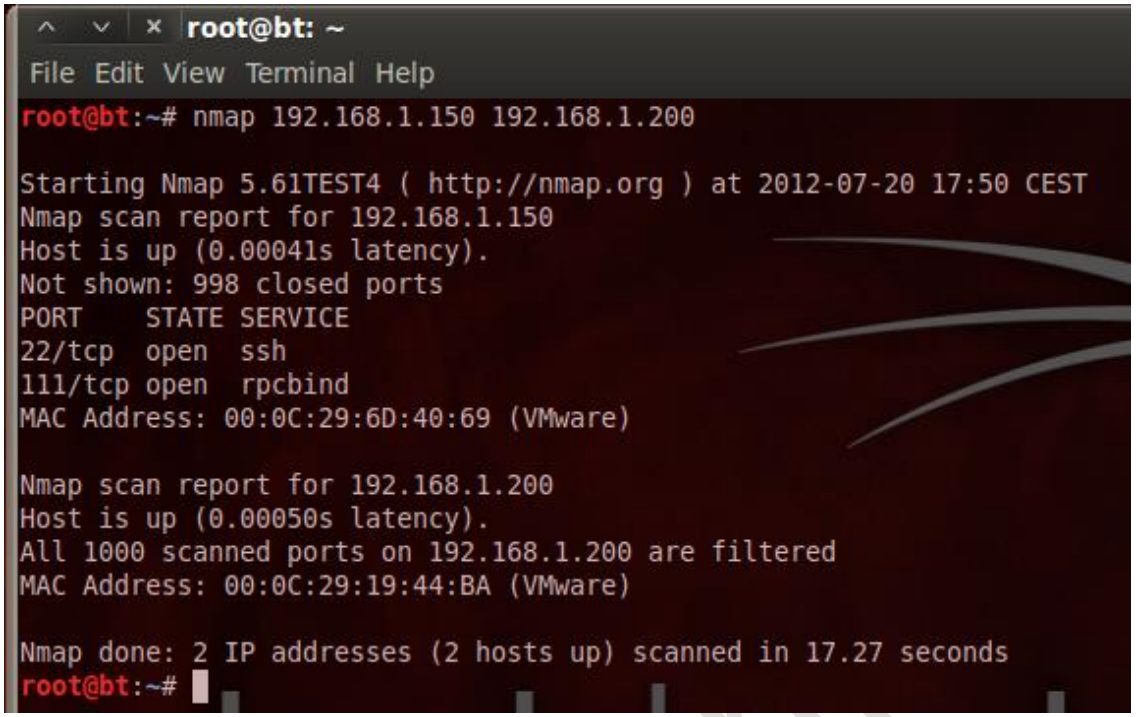
Aunque podemos comprobar que la máquina sí está activa consultando la caché ARP Kali:

Lanzamos Nmap:



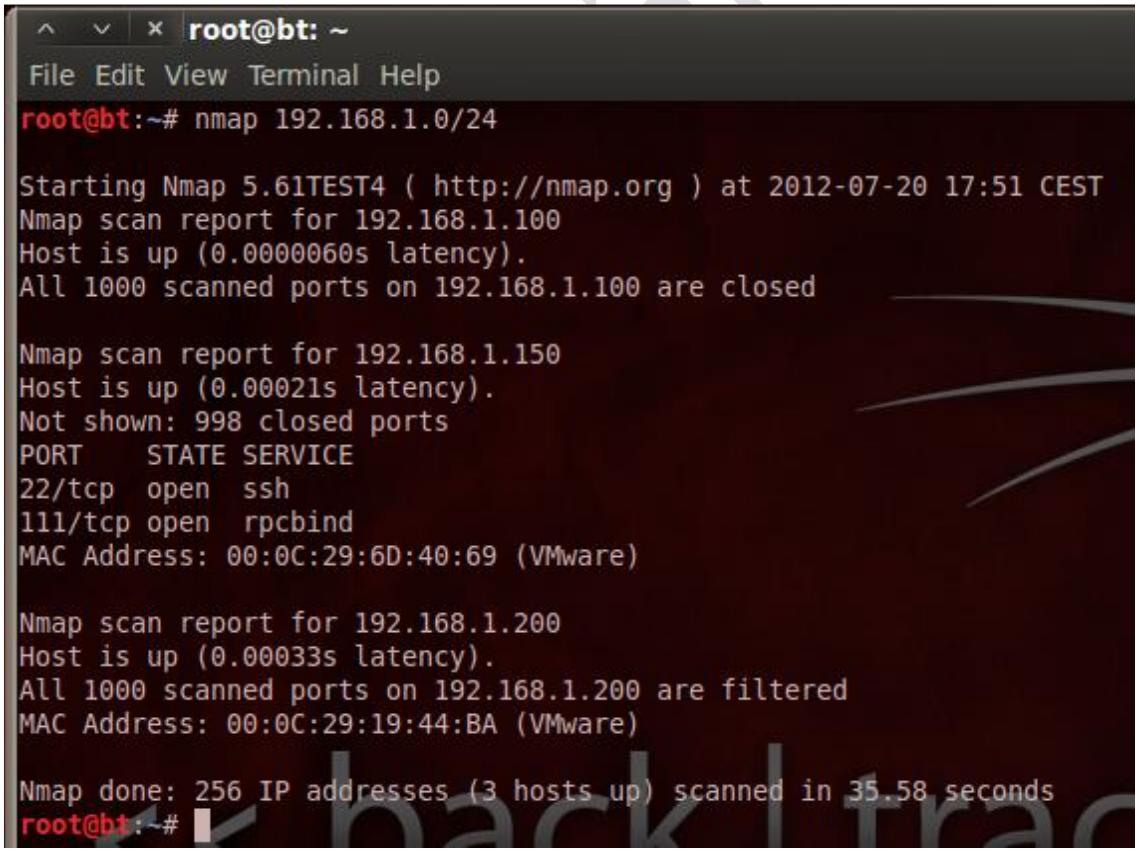
Y vemos que los puertos aparecen filtrados al estar activo el cortafuegos de Windows 7. Más adelante veremos cómo podemos solucionarlo.

También podemos escanear varias máquinas a la vez:



Donde vemos que CentOS tiene abiertos los puertos 22 y 111.

O una red o subred completa:

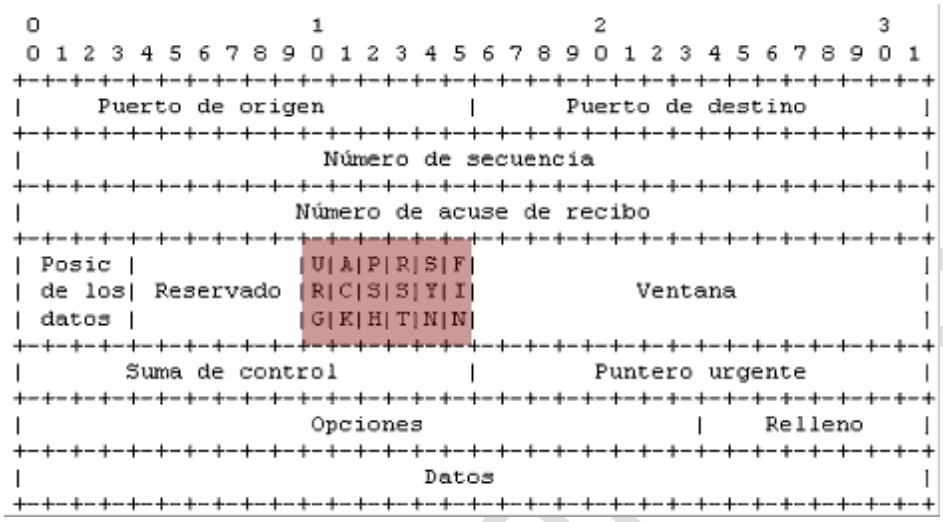


Como vemos es muy fácil lanzar un escaneo básico, pero también es muy sencillo para un firewall pararlo y evitar que consigamos la información que estamos buscando. A partir de aquí tenemos que utilizar las múltiples características que nos ofrece Nmap para saltarnos esas

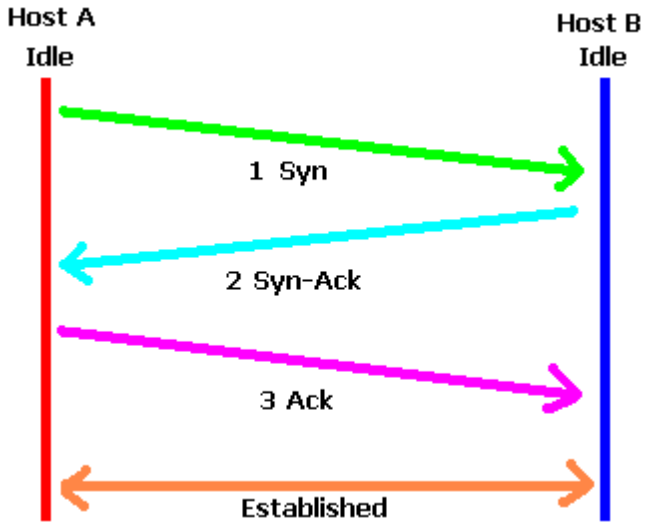
medidas de seguridad y hacer un análisis más profundo y más realista de la seguridad de nuestra red.

2.3.1 Escaneo Basado en TCP

Muchas de las técnicas de escaneo que incluye Nmap están basadas en el protocolo TCP. Como sabemos, este es un protocolo orientado a conexión que se usa para ofrecer servicios de red y una buena parte de su funcionalidad se debe a los flags que podemos encontrar en los segmentos TCP.



Los pasos que se siguen en un establecimiento de sesión TCP son los siguientes:



Donde el host que inicia la sesión envía un segmento con el flag SYN activo. El receptor, si está a la escucha, devolverá un segmento con los flags SYN y ACK activos, a lo que el emisor responderá con un segmento con el flag ACK activo. Durante estos pasos, los dos extremos habrán negociado diferentes parámetros de la comunicación, como el tamaño de ventana que van a usar.

Según cómo responda una máquina, Nmap puede usar la información recibida para obtener mucha información sobre el host de destino. Cuando escaneamos un puerto, Nmap no se limita a darnos los dos resultados habituales que nos dan otras herramientas, que son abierto o cerrado, sino que es más detallado y puede darnos hasta 6 resultados diferentes:

- Abierto: La aplicación que está a la escucha en el puerto acepta conexiones que pueden ser TCP o UDP, y en el primer caso devuelve un paquete SYN-ACK. Encontrar un puerto en este estado es el objetivo habitual de un atacante.
- Cerrado: El puerto recibe paquetes de Nmap y responde con un paquete RST, pero no hay ninguna aplicación a la escucha. Detectar un puerto abierto y otro cerrado en una máquina puede ayudar a determinar el sistema operativo que se está ejecutando.
- Filtrado: Los paquetes que envía Nmap no llegan al puerto y por lo tanto no puede decidir si está abierto o cerrado. Este estado nos indica que tenemos delante algún tipo de cortafuegos.
- No filtrado: Nmap sólo marca un puerto en este estado cuando está usando un escaneo ACK, que veremos más adelante. No hay cortafuegos, pero el escaneo no ofrece información suficiente para determinar si el puerto está abierto o cerrado.
- Abierto|filtrado: Los escaneos UDP, IP, FIN, Null y Xmas pueden darnos este resultado al no poder determinar si el puerto está abierto o filtrado.
- Cerrado|filtrado: Nmap sólo nos da este resultado cuando realizamos un escaneo IPID pasivo y se debe a que no puede determinar si el puerto está cerrado o filtrado. Veremos este tipo de escaneo más adelante.

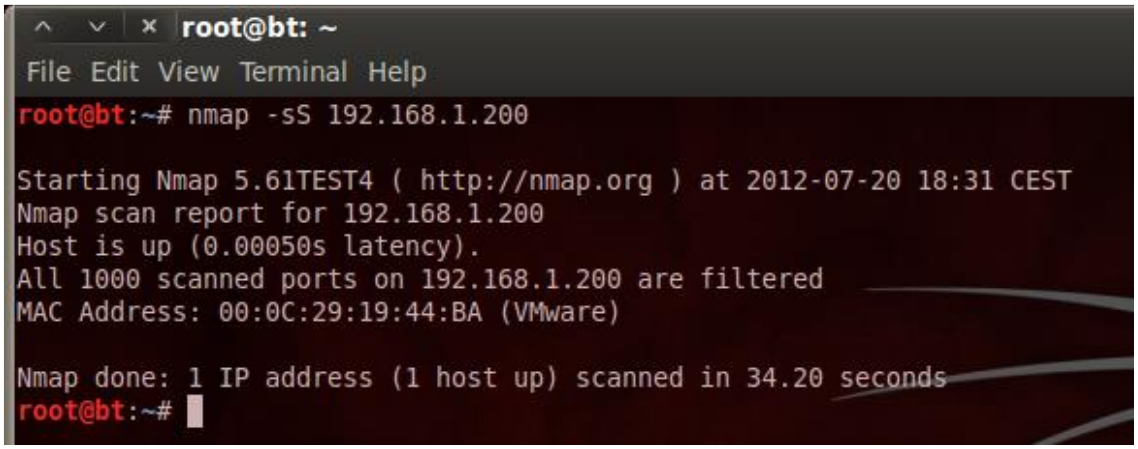
La gran mayoría de los cortafuegos están configurados para bloquear los segmentos SYN salvo para aquellos servicios que sean públicos, lo que hace que el escaneo básico que hemos hecho hasta ahora no haya dado un buen resultado.

Cuando Nmap sigue los mismos pasos que en un establecimiento de conexión TCP (SYN, SYN-ACK, ACK), decimos que el escaneo es del tipo TCP Connect y estamos dando a la máquina objetivo todas las facilidades para que registre nuestra actividad, ya que hemos completado el proceso de inicio de sesión TCP. Un escaneo un poco más elaborado es el escaneo TCP Syn.

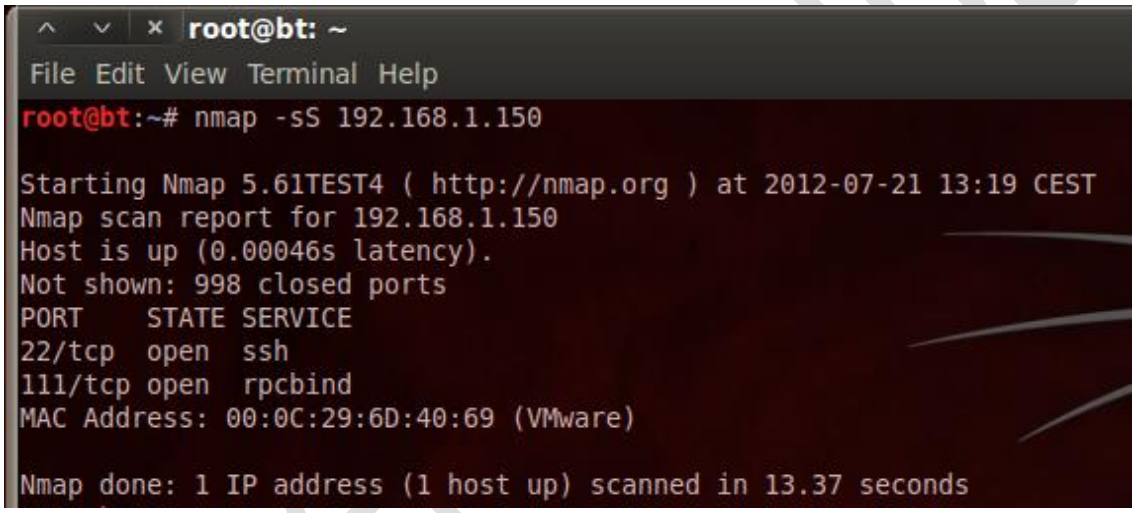
2.3.1.1 Escaneo TCP Syn

No se completa todo el proceso, por lo que también se denomina escaneo semi-abierto. La idea es evitar que quede registrado el escaneo en la máquina objetivo. Para esto, Nmap envía un segmento SYN y queda a la espera de recibir el SYN-ACK, pero aunque lo reciba no devolverá el segmento ACK que cerraría el saludo (handshake). De esta forma no se inicia sesión y es probable que la máquina destino no guarde un registro.

Vamos a probarlo con la máquina Windows:



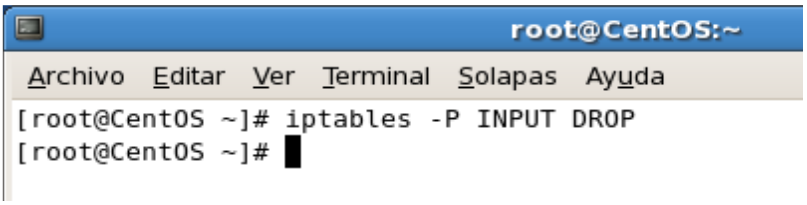
Como vemos, Nmap tampoco nos da mucha información en este caso, ya que el cortafuegos de Windows sigue cortando el paso de los paquetes sonda. Este es el tipo de escaneo que usa Nmap por defecto cuando se ejecuta con permisos de root. Veamos el resultado si lo lanzamos contra CentOS:

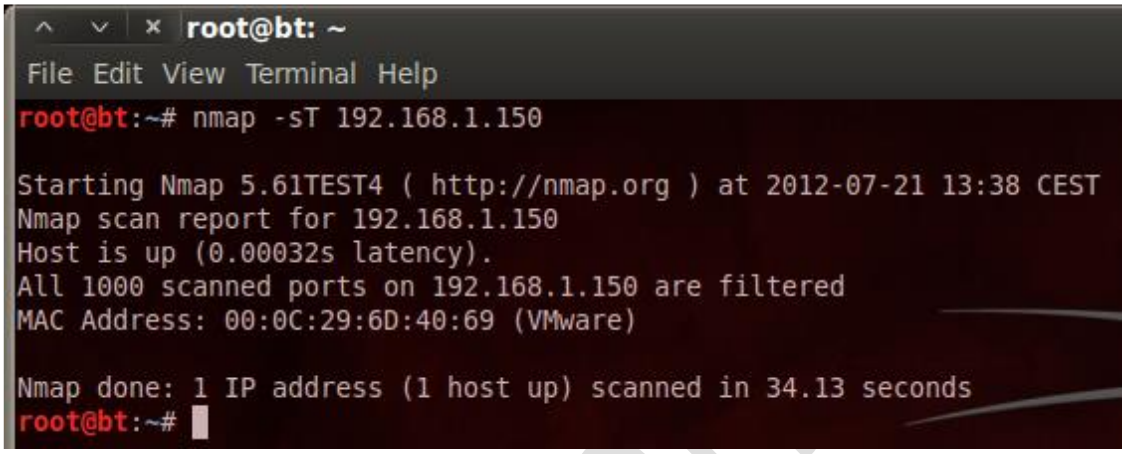


2.3.1.2 Escaneo TCP Connect

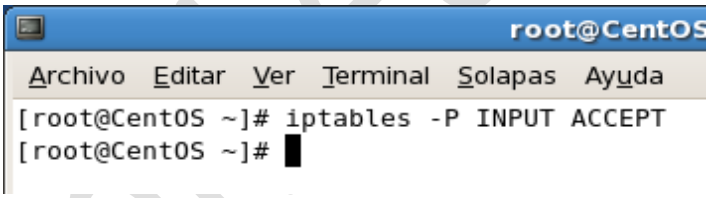
Vamos a ejecutar este tipo de escaneo:

Que nos da la misma información, pero nos arriesgamos mucho más a que nuestra actividad quede registrada. Además, bastaría con cambiar la política de entrada por defecto en CentOS para que dejara de responder:



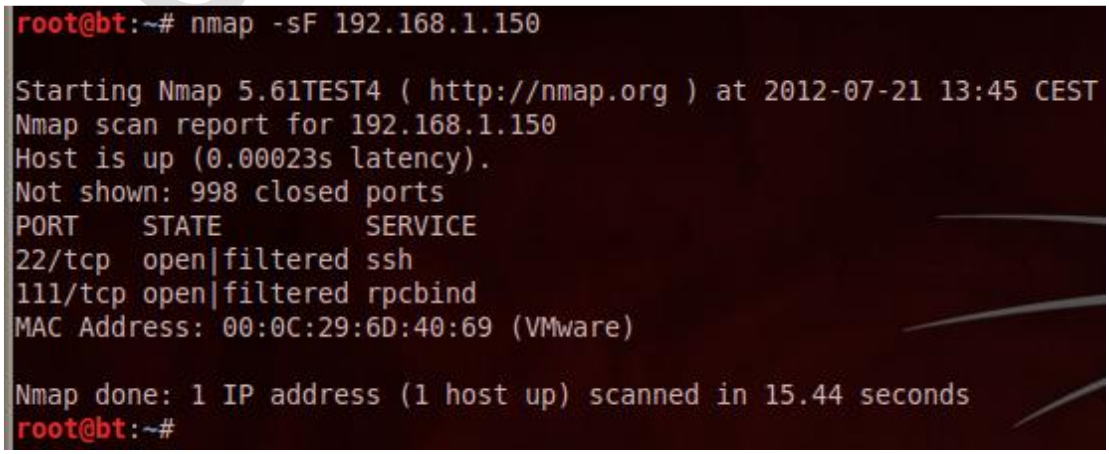


De momento, volvemos a dejar CentOS con la política de entrada por defecto como estaba para ver cómo funcionan el resto de tipos de escaneos:

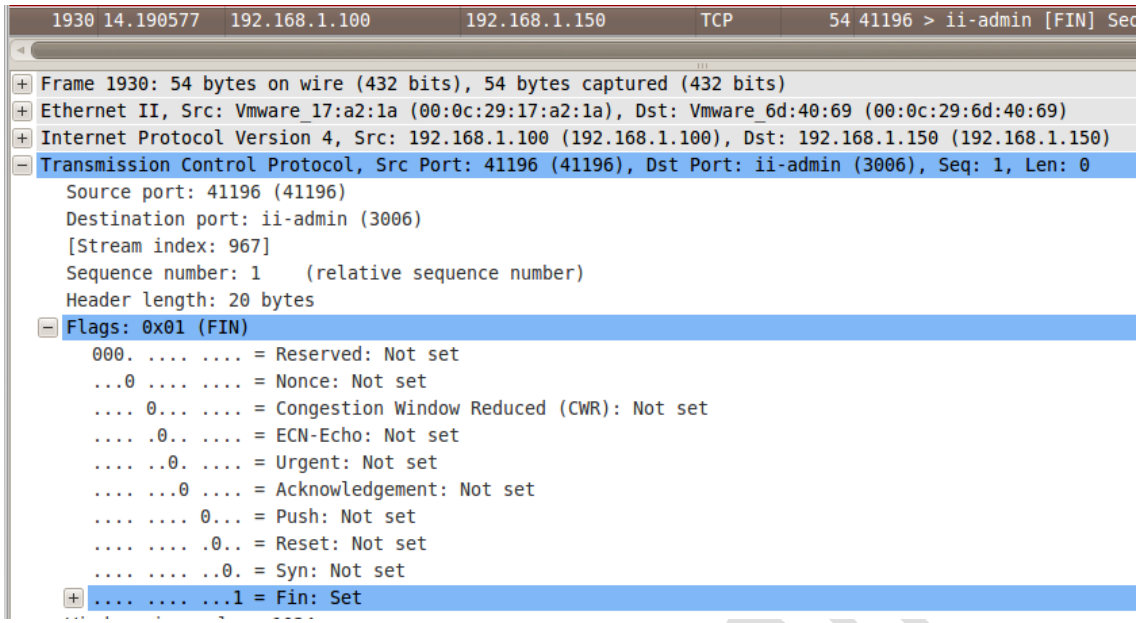


2.3.1.3 Escaneo FIN

Si el cortafuegos está configurado para interceptar los paquetes SYN, bloquearía los dos escaneos que hemos hecho hasta ahora. Una posibilidad de saltar el cortafuegos o un sistema IDS es usar el escaneo FIN, en el que Nmap envía paquetes en los que sólo el flag SYN está activo:



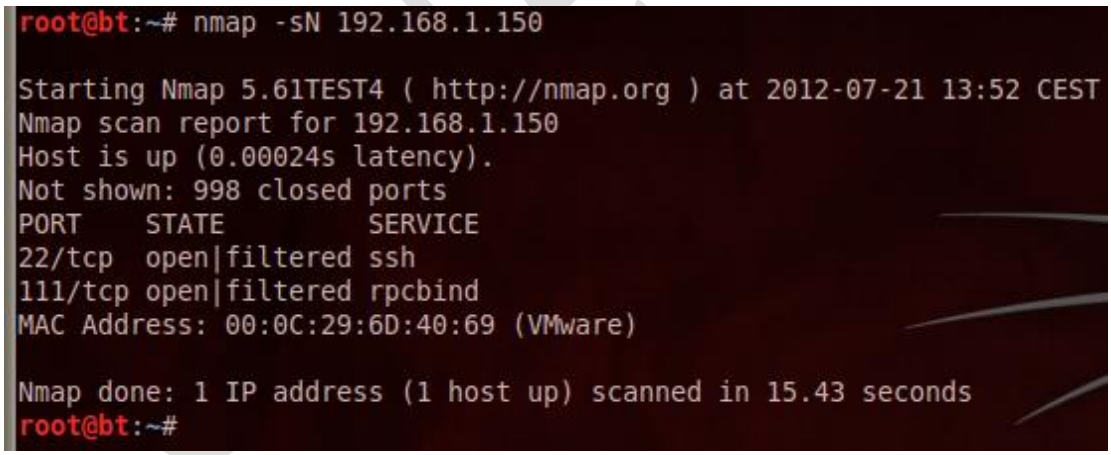
Y si capturamos estos paquetes con Wireshark podemos ver los flags:



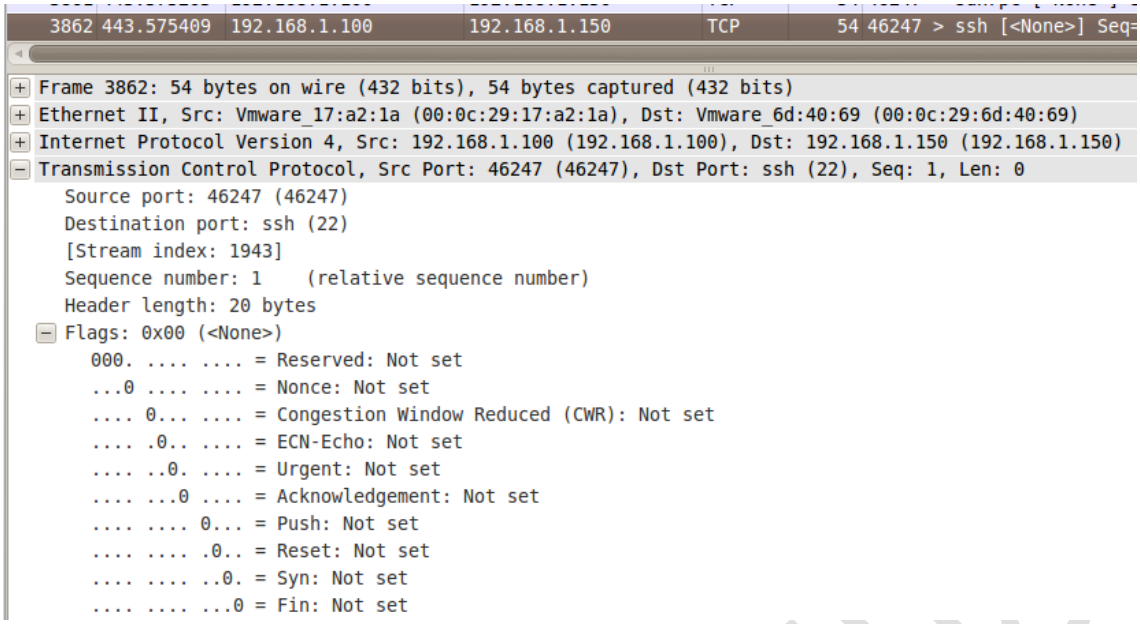
2.3.1.4 Escaneo Null y del Árbol de Navidad

Otras opciones que nos ofrece Nmap son los escaneos Null y Xmas. Vamos a lanzarlos y a capturar uno de los paquetes que enviamos para ver sus características:

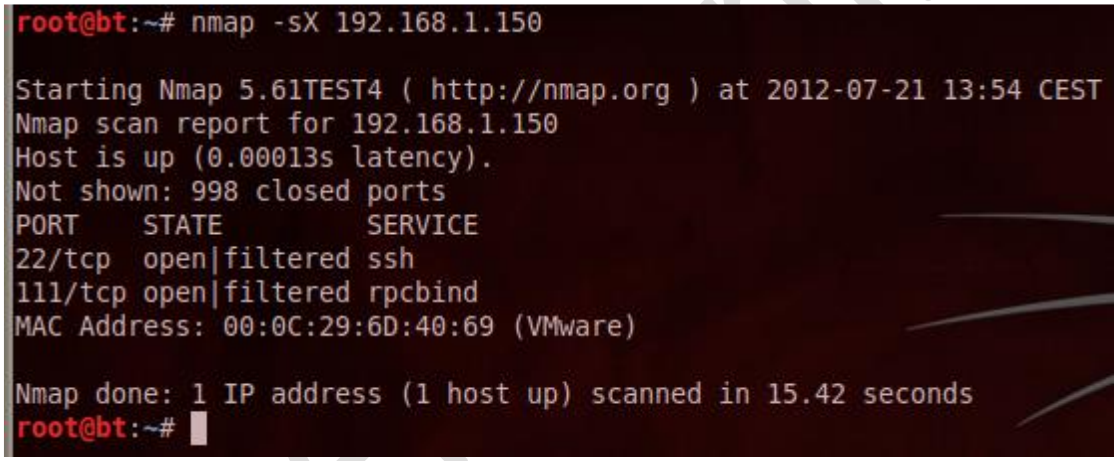
Empezamos con el escaneo Null:



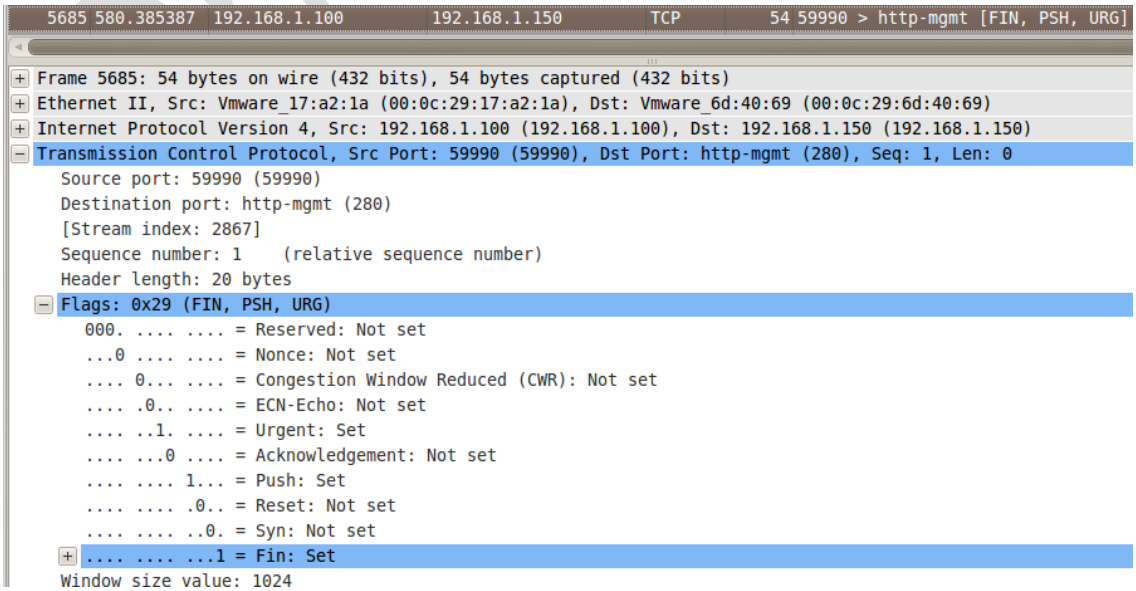
Y vemos que ningún flag está activo:



Y el Xmas:



En el que se activan los flags FIN, PUSH y URG:



2.3.2 Otros Tipos de Escaneo

Los escaneos que hemos visto hasta ahora nos permiten hacer un descubrimiento básico de la red, pero si queremos obtener más detalles sobre las máquinas o si estas están protegidas por cortafuegos, tenemos que avanzar un poco más en el uso de Nmap.

Vamos a ver otros modos de escaneo que, si bien por si solos no nos darán un resultado espectacular, podremos combinar más adelante para llevar a cabo un análisis más profundo.

2.3.2.1 Escaneo UDP

Un tipo de escaneo que suele dar resultado es el escaneo UDP. Cambiamos de protocolo y los cortafuegos no siempre lo bloquean. Cualquiera de los escaneos anteriores falla al lanzarlos contra la máquina Windows 7 con el cortafuegos activo, pero ahora vamos a intentarlo con el UDP:

```
root@bt:~# nmap -sU 192.168.1.200

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-07-21 14:27 CEST
Nmap scan report for 192.168.1.200
Host is up (0.00051s latency).
Not shown: 999 open|filtered ports
PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 00:0C:29:19:44:BA (VMware)
```

Ahora aparece un puerto abierto, el 137 correspondiente al servicio Netbios, que suele ser indicativo de una máquina de Microsoft, aunque no aún no podamos determinarlo con seguridad.

Hay que tener en cuenta que es habitual que los hosts abran y cierren puertos en determinados momentos, por lo que es una buena idea hacer el escaneo en diferentes momentos y podríamos obtener diferentes resultados. Por ejemplo, si repetimos el escaneo anterior en otro momento, obtenemos:

```
root@bt:~# nmap -sU 192.168.1.200

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-07-21 14:31 CEST
Nmap scan report for 192.168.1.200
Host is up (0.00042s latency).
All 1000 scanned ports on 192.168.1.200 are open|filtered
MAC Address: 00:0C:29:19:44:BA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 34.23 seconds
root@bt:~#
```

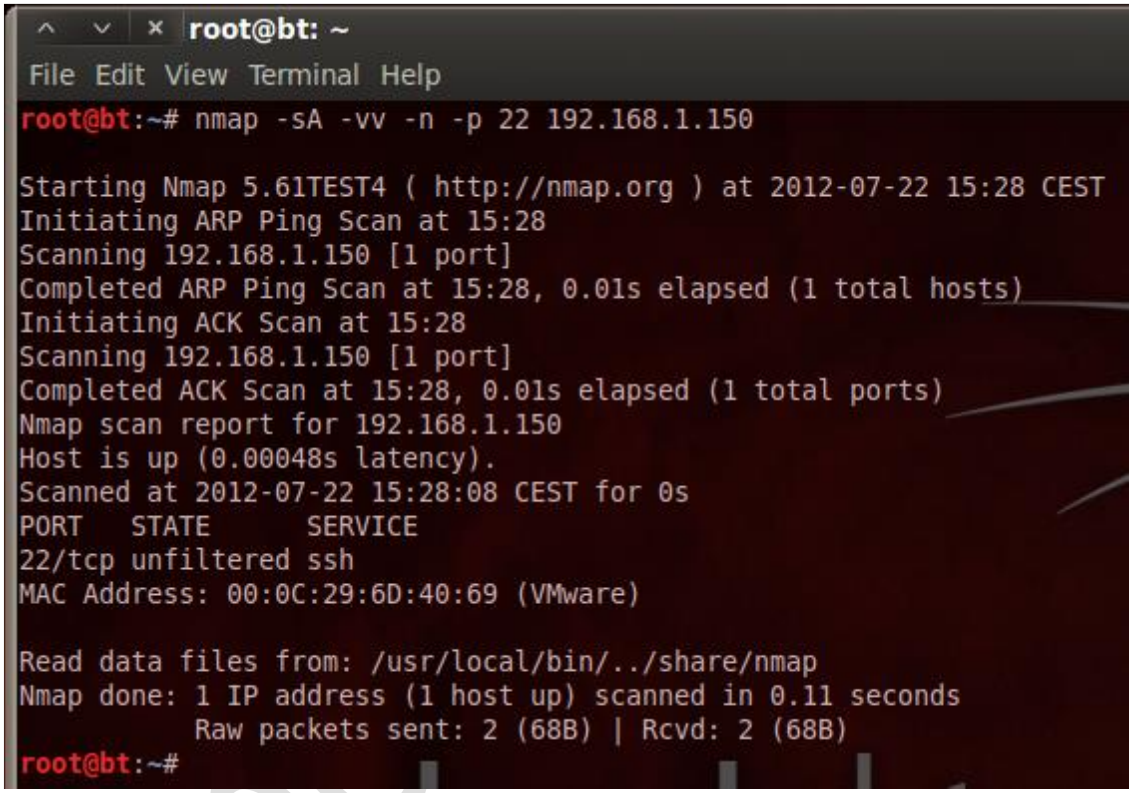
2.3.2.2 Escaneo TCP Ack

Este escaneo no intenta determinar si los puertos están abiertos. De hecho, nunca nos dará como resultado para un puerto “open” ni “open|filtered”. El objetivo de este escaneo es detectar el tipo de cortafuegos que tenemos delante, si es stateful o stateless.

La sonda que se envía sólo tiene el flag ACK activo. Si el puerto no responde o devuelve un paquete ICMP "destination unreachable", se considera que el puerto está filtrado por el cortafuegos. Si el puerto devuelve un paquete RST, se clasificará como "unfiltered", es decir, es alcanzable.

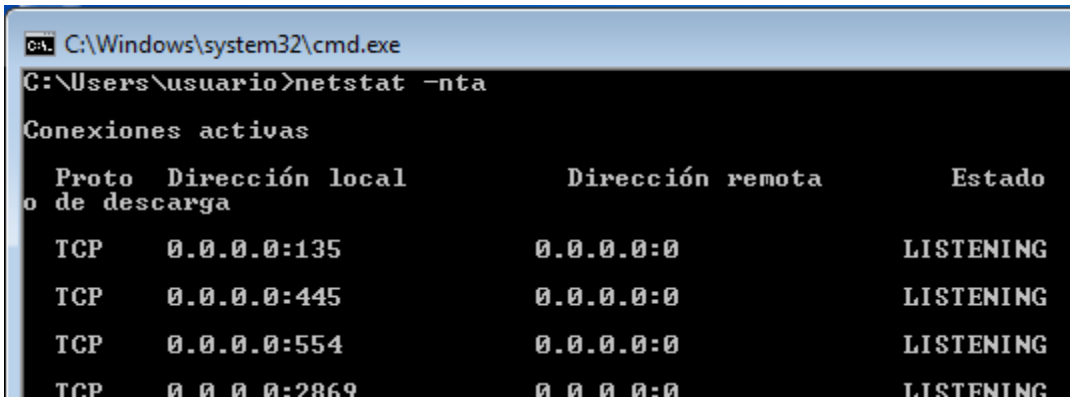
Vamos a lanzar este escaneo y también vamos a introducir la opción "-vv" que aumenta el nivel de detalle de la salida y "-n" que evita el intento de resolución DNS inversa para acelerar el proceso.

En un primer intento usaremos como objetivo nuestra máquina CentOS, que no tiene el cortafuegos habilitado y tiene el puerto 22 a la escucha:

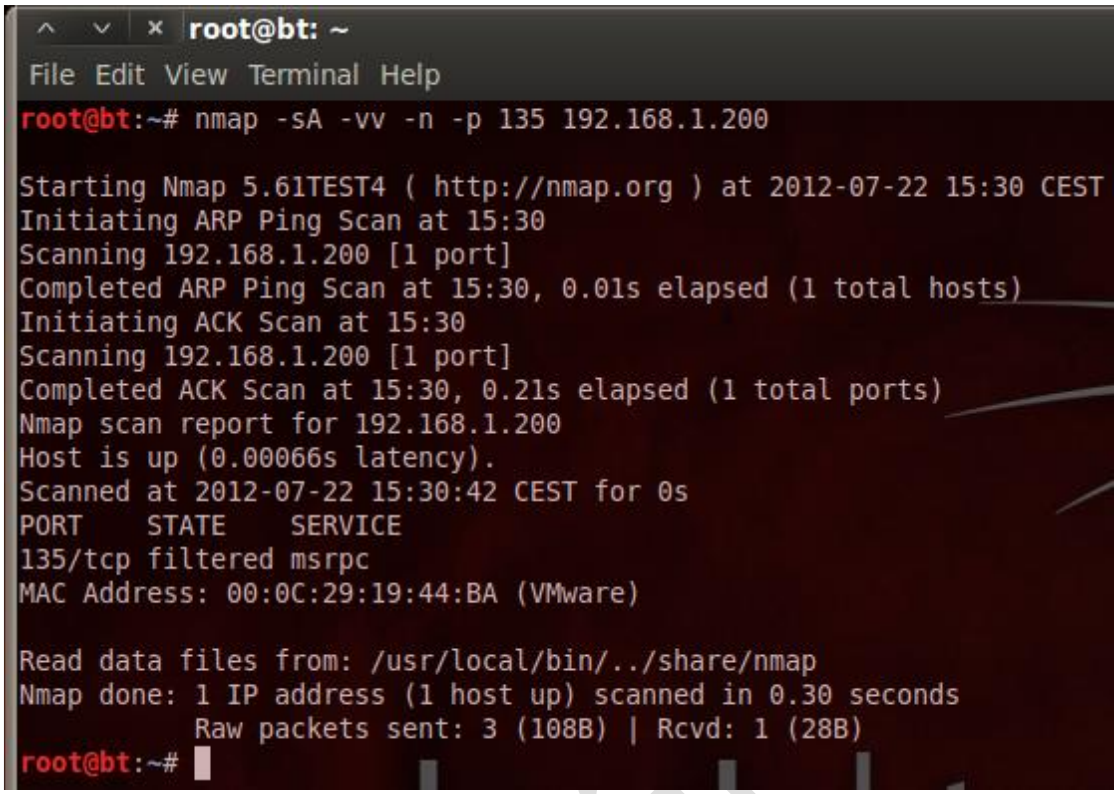


Aparece el puerto como "unfiltered".

Si ahora lo intentamos con Windows 7, que sí tiene el cortafuegos activo, hacia el puerto 135 que está a la escucha. Este puerto es usando por muchos protocolos de nivel superior, como DCOM en el caso de Microsoft e históricamente ha sido uno de los más atacados en Internet. De hecho, el famoso Blaster lo utilizaba para lleva a cabo su ataque:



Obtenemos:



donde el puerto aparece como “filtered”.

2.3.2.3 Escaneo TCP Window

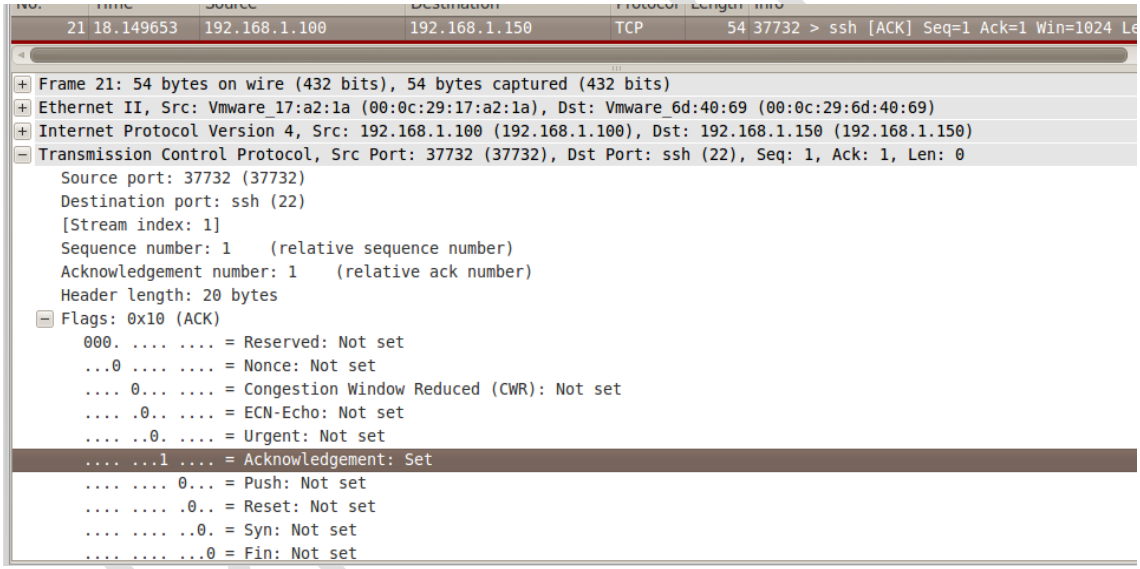
La idea de este escaneo es igual a la del ACK, pero intenta explotar detalles de implementación de determinados sistemas para diferenciar un puerto abierto de otro cerrado (ACK no hace esta diferencia). El flag ACK se envía activo en la sonda y se analiza el campo del tamaño de ventana de la respuesta. En algunos sistemas, este campo tiene un valor positivo si el puerto está abierto y cero si está cerrado.

Como decíamos, este escaneo se basa en un detalle de implementación de una minoría de sistemas, por lo que no siempre podemos confiar en él.

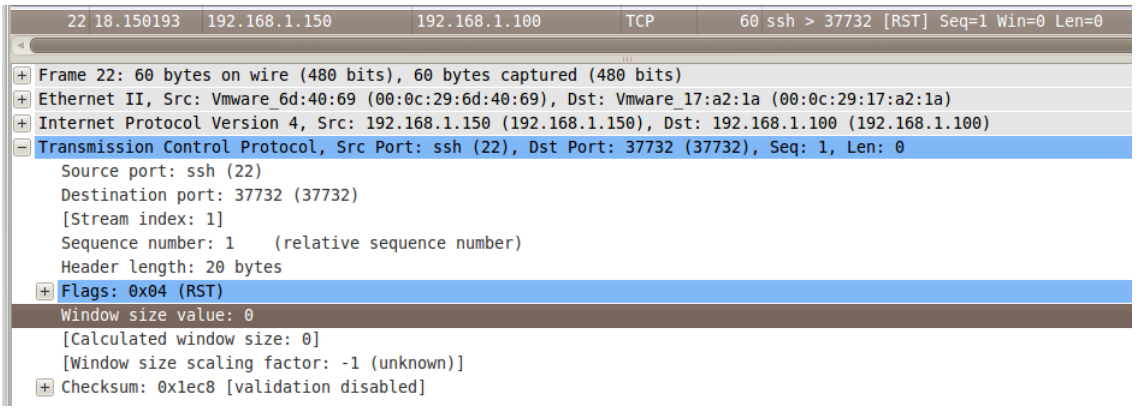
Veamos la respuesta si lo lanzamos contra nuestro CentOS:

```
root@bt:~# nmap -sW -vv -n -p 22 192.168.1.150

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-07-22 15:44 CEST
Initiating ARP Ping Scan at 15:44
Scanning 192.168.1.150 [1 port]
Completed ARP Ping Scan at 15:44, 0.01s elapsed (1 total hosts)
Initiating Window Scan at 15:44
Scanning 192.168.1.150 [1 port]
Completed Window Scan at 15:44, 0.02s elapsed (1 total ports)
Nmap scan report for 192.168.1.150
Host is up (0.00042s latency).
Scanned at 2012-07-22 15:44:30 CEST for 0s
PORT   STATE  SERVICE
22/tcp closed ssh
MAC Address: 00:0C:29:6D:40:69 (VMware)

Read data files from: /usr/local/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
           Raw packets sent: 2 (68B) | Rcvd: 2 (68B)
root@bt:~#
```

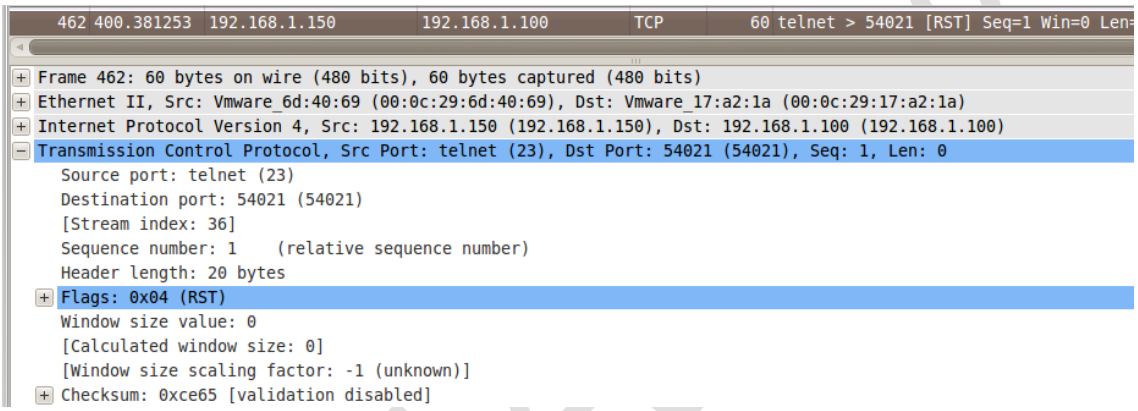
El puerto aparece como cerrado cuando sabemos que en realidad está abierto. En la siguiente imagen tenemos un detalle del paquete enviado:



Donde vemos el flag ACK activo. Y la respuesta desde CentOS cuando el puerto escaneado está abierto:

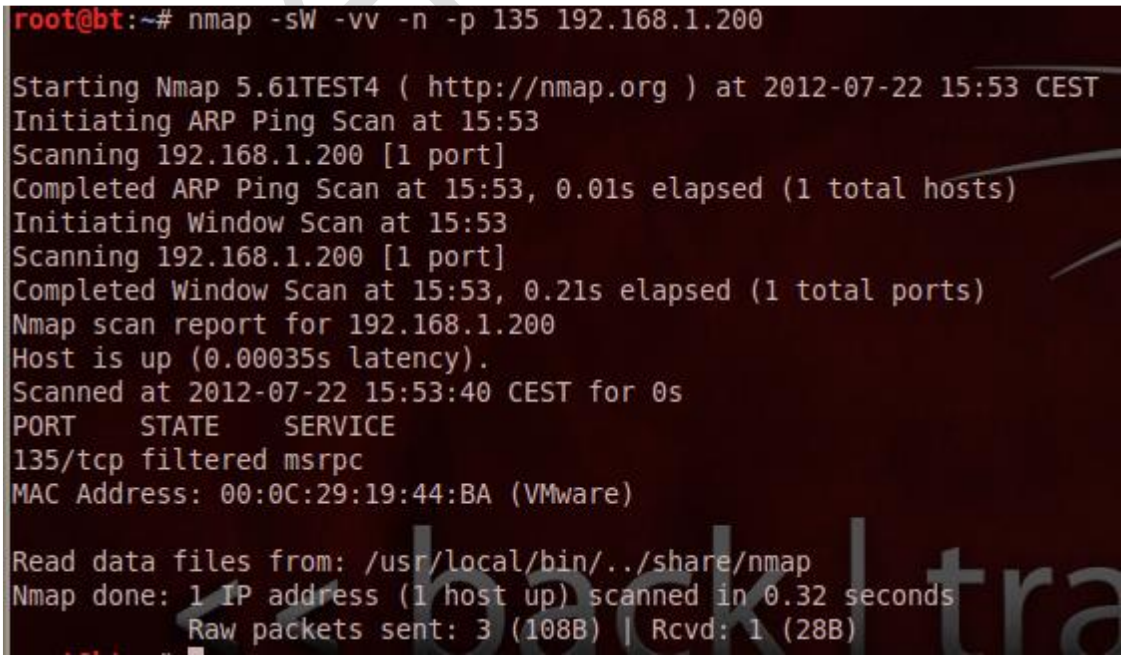


Con un segmento RST y el tamaño de ventana a 0. Si hacemos lo mismo con un puerto que está realmente cerrado en CentOS, como el 23 (Telnet):



Vemos que la respuesta es igual y con esta sonda lanzada contra CentOS, Nmap no puede saber si el puerto está abierto o cerrado.

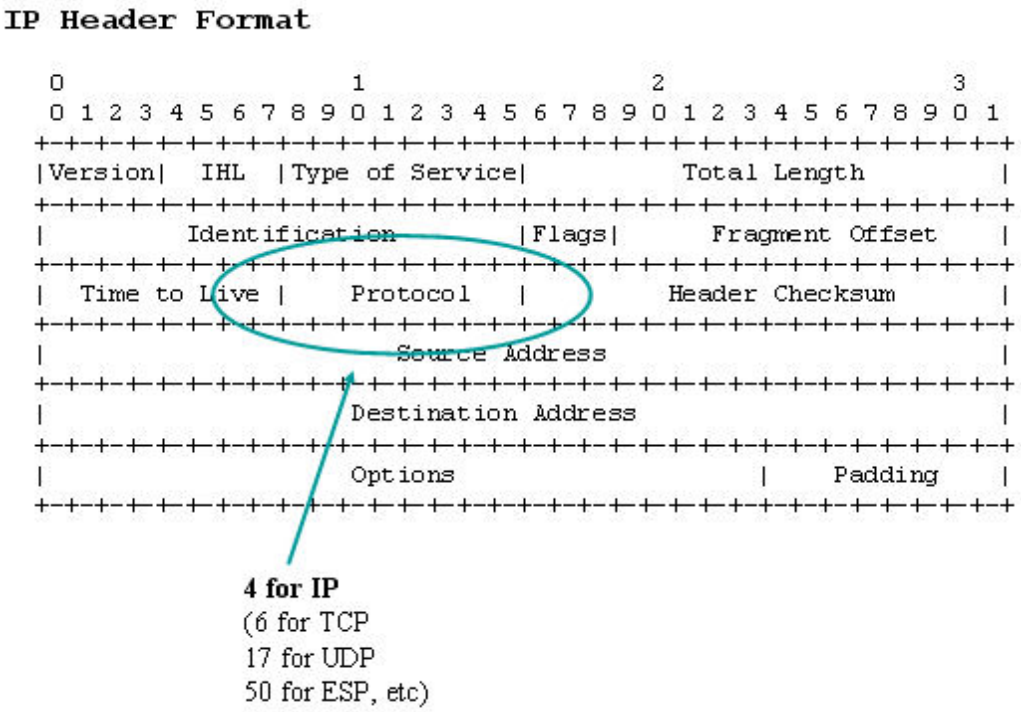
Si se lanza contra la máquina Windows 7, esta no responde y Nmap determina que el puerto está filtrado:



2.3.2.4 Escaneo IP Protocol

Este escaneo está orientado a determinar los protocolos IP (ICMP, TCP, UDP, IGMP, IPv4, IPv6,...) que están soportados por la máquina objetivo, lo que nos puede dar una idea del tipo de máquina que es (Servidor, PC, Router,...).

A diferencia de un escaneo de puertos, lo que hace es utilizar el campo IP Protocol del paquete IP:



Veamos el resultado contra CentOS:

```
root@bt:~# nmap -sO -n 192.168.1.150

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-07-22 18:40 CEST
Warning: 192.168.1.150 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.150
Host is up (0.00052s latency).
Not shown: 251 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
41       open|filtered ipv6
MAC Address: 00:0C:29:6D:40:69 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 268.72 seconds
```

2.4 OS Fingerprinting con Nmap

Un paso fundamental en un análisis de vulnerabilidades es determinar qué sistema operativo y versión está instalado en la máquina objetivo. Conociendo algunos puertos abiertos podríamos hacer suposiciones, pero Nmap pone a nuestro alcance técnicas que nos permiten afinar más y, en algunos casos, obtener con una fiabilidad del 100% la información que buscamos. El proceso de analizar la máquina objetivo para conocer el sistema operativo y la versión que tiene instalada se denomina OS Fingerprinting.

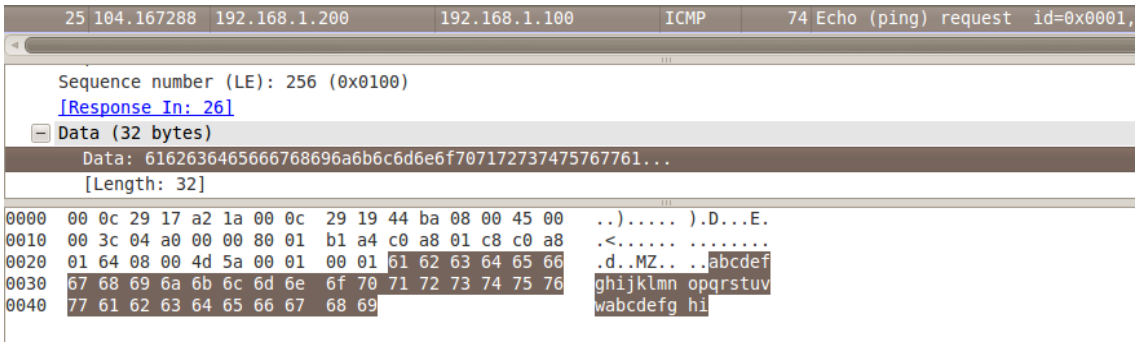
Este proceso se basa en analizar las ambigüedades en la definición de los protocolos estándar que rigen los servicios de red. Cada uno de estos protocolos incluye una serie de reglas de obligado cumplimiento y que podemos encontrar en su RFC correspondiente. Por ejemplo:

- Protocolo SSH: RFC 4251, 4252 y 4253
  - http://www.ietf.org/rfc/rfc4251.txt
  - http://www.ietf.org/rfc/rfc4252.txt
  - http://tools.ietf.org/html/rfc4253
- Protocolo HTTP: RFC 2616 y actualizaciones posteriores
  - http://tools.ietf.org/html/rfc2616

Estos documentos definen las reglas de comportamiento para que un servicio cumpla con el estándar y diferentes máquinas puedan interoperar entre sí. En cualquier caso, es posible que algunos detalles menores no fundamentales para el funcionamiento del protocolo no estén definidos y se dejen a criterio del fabricante. Veamos un ejemplo para un paquete ping. En primer lugar un ping enviado desde nuestra máquina CentOS:

```
    5 1.004603    192.168.1.150         192.168.1.100         ICMP      98 Echo (ping) request  id=0xa210

    Sequence number (LE): 512 (0x0200)
    [Response In: 6]
  - Data (56 bytes)
      Data: 200e11501665010008090a0b0c0d0e0f1011121314151617...
      [Length: 56]

0000  00 0c 29 17 a2 1a 00 0c  29 6d 40 69 08 00 45 00   ..)..... )m@i..E.
0010  00 54 00 00 40 00 40 01  b6 5e c0 a8 01 96 c0 a8   .T..@.@. .^......
0020  01 64 08 00 22 27 a2 10  00 02 20 0e 11 50 16 65   .d.."'.. .. ..P.e
0030  01 00 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ........ ........
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ........ .. !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                             67
```

Y ahora un ping enviado desde Windows 7:



En ambos casos se envía un paquete ping dentro del protocolo ICMP que cumple con el estándar, pero con diferencias. En principio, el contenido del campo de datos de un paquete ping es irrelevante, ya que sólo queremos enviar un paquete al que la máquina destino responderá si está allí. Al no ser útil para el funcionamiento, este campo de datos no está definido en el RFC correspondiente y cada fabricante incluye en él lo que considera conveniente. En CentOS vemos un conjunto de caracteres que terminan con los dígitos del 0 al 7, mientras que en Windows 7 tenemos el abecedario. Este tipo de detalles de implementación serán los que analizará Nmap para determinar el sistema operativo y la versión de la máquina que tenemos enfrente.

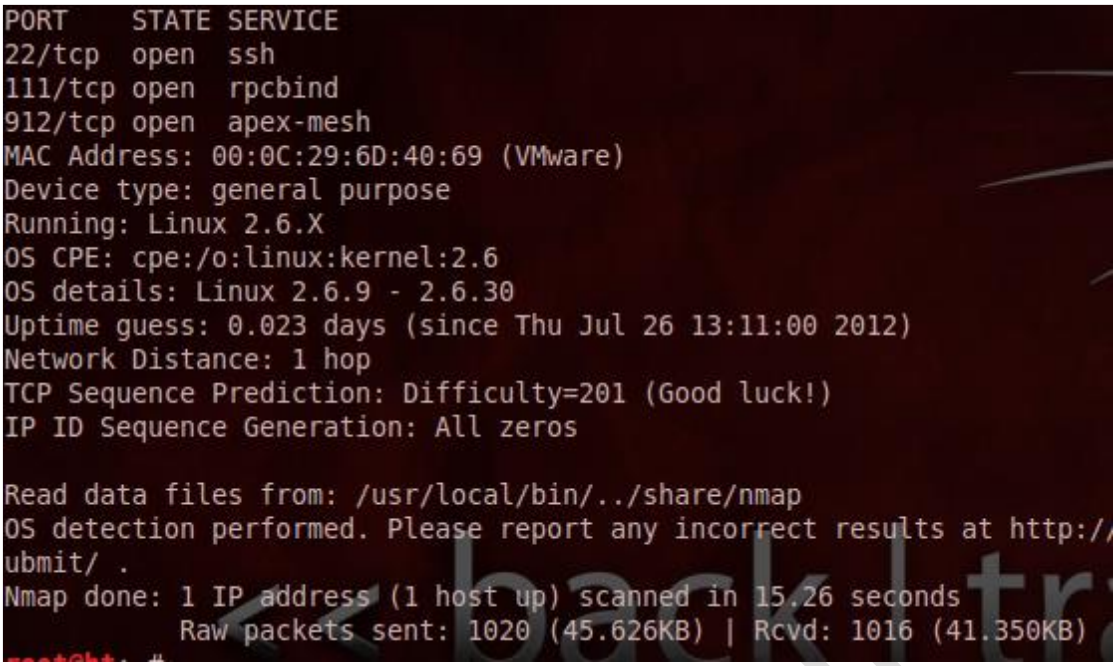
Nmap envía 16 sondas TCP, UDP e ICMP para analizar decenas de parámetros que le permitan "adivinar" cuál es el sistema operativo que está respondiendo. Esto no es una ciencia exacta, ya que depende de diversos factores, y el propio Nmap nos informará de la fiabilidad aproximada con la que ha determinado el sistema operativo. Para obtener más información al respecto podemos visitar el siguiente enlace:

http://nmap.org/book/osdetect-methods.html

La forma básica de iniciar un OS fingerprinting con Nmap es la siguiente:

```
root@bt:~# nmap -O -v 192.168.1.150

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-07-26 13:44 CEST
Initiating ARP Ping Scan at 13:44
Scanning 192.168.1.150 [1 port]
Completed ARP Ping Scan at 13:44, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:44
```

Donde usamos CentOS como objetivo y añadimos la opción "-v" para que nos dé información extra. El resultado es:



donde nos dice que se trata de un sistema Linux basado en la versión 2.6.X del kernel, concretamente entre 2.6.9 y 2.6.30. Si comprobamos esto en CentOS:

```
[root@CentOS ~]# uname -r
2.6.18-194.el5
[root@CentOS ~]#
```

Y vemos que es correcto el resultado que nos ha dado Nmap.