Guía de referencia de Nmap

Recopilación realizada por: **Gerick Toro** <gerickt@gmail.com> (http://grk-t.blogspot.com)

Original: Fyodor <fyodor@insecure.org> (http://www.insecure.org)

Website del manual oficial: http://nmap.org/man/es/

Fecha: 01/04/08

Índice de contenido

Name

nmap — Herramienta de exploración de redes y de sondeo de seguridad / puertos

nmap [*Tipo de sondeo* ...] [*Opciones*] { *especificación de objetivo* }

Descripción

Nmap (“mapeador de redes”) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP "crudos" («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características. Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útil para realizar tareas rutinarias, como puede ser el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas. La información primordial es la “tabla de puertos interesantes”. Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado. El estado puede ser open (abierto), filtered (filtrado), closed (cerrado), o unfiltered (no filtrado). Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Filtrado indica que un cortafuegos, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado. Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como no filtrados son aquellos que responden a los sondeos de Nmap, pero para los que que Nmap no puede determinar si se encuentran abiertos o cerrados. Nmap informa de las combinaciones de estado open|filtered y closed|filtered cuando no puede determinar en cual de los dos estados está un puerto. La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. Nmap ofrece información de los protocolos IP soportados, en vez de puertos abiertos, cuando se solicita un análisis de protocolo IP con la opción (-sO).

Además de la tabla de puertos interesantes, Nmap puede dar información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC.

Puede ver un análisis típico con Nmap en Example 1, “Ejemplo típico de análisis con Nmap”. Los únicos parámetros de Nmap que se utilizan en este ejemplo son la opción -A, que habilita la detección de sistema operativo y versión, y la opción -T4 que acelerar el proceso, y después el nombre de los dos objetivos.

Example 1. Ejemplo típico de análisis con Nmap

```
# nmap -A -T4 scanme.nmap.org saladejuegos

Starting nmap ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
```

```
(The 1663 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33.908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on saladejuegos.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1002/tcp open  windows-icfw?
1025/tcp open  msrpc         Microsoft Windows RPC
1720/tcp open  H.323/Q.931   CompTek AquaGateKeeper
5800/tcp open  vnc-http      RealVNC 4.0 (Resolution 400x250; VNC TCP port:
5900)
5900/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

Puede obtener la versión más reciente de Nmap en http://www.insecure.org/nmap/. La versión más reciente de la página de manual está disponible en http://www.insecure.org/nmap/man/.

Notas de la traducción

Esta edición de la Guía de referencia de Nmap ha sido traducida de la versión 3137 de la versión original en inglés por Arturo Busleiman <buanzo_AT_buanzo.com.ar>, Pablo Fernández <pablo_AT_littleQ.net> y Javier Fernández-Sanguino <jfs_AT_computer.org>. Aunque nuestra intención es hacer Nmap más accesible a los lectores españoles en todo el mundo no podemos garantizar que esta traducción está tan actualizada o completa como la versión oficial en inglés. Este trabajo puede ser modificado y redistribuido bajo los términos de la Licencia Creative Commons Atribución.

Esta traducción ha sido adaptada al español como se habla en España (localización «es_ES») por Javier Fernández-Sanguino. Cualquier comentario o errata sobre esta traducción debe enviarse a Javier Fernández-Sanguino a la dirección arriba indicada. El coordinador de la traducción quiere agradecer el esfuerzo de revisión realizado por Jesús Escoredo.

Glosario de traducción

A continuación se listan las traducciones utilizadas a los términos originales en inglés en este documento, es decir, el glosario utilizado en este documento:

Decoy

Traducido con el término «señuelo».

Fingerprinting

«Identificación por huellas» (se entiende digitales), se utilizado conjuntamente con la detección de sistema operativo por lo que a veces se utiliza éste o se reduce a «identificación».

Host

Traducido habitualmente como «equipo» o «sistema».

Port scan

Barrido de puertos.

(to) Probe

Traducido con el término «sondear» (o «sonda»).

(to) Scan

Traducido como «sondear» (o «sondeo») o «análizar» (o «análisis»), no se utiliza «escanear» (o «escaneo») ya que éste término es, literalmente “pasar por el escáner”.

(To) Spoof

Traducido por «falsificar».

Existen otros términos que puedan aparecer en el documento traducidos pero cuya traducción es ambigua. En este caso las traducciones se introducen en el texto acompañadas de notas de traducción (mostradas como «N. del T.») indicando el término original la primera vez que éste aparezca en el texto.

Nótese que éste glosario difiere en algunos términos del utilizado para otras traducciones, como la traducción realizada por Marbo Babosa del artículo Deteccion Remota de SO via Reconocimiento de Pila TCP/IP (documento traducido al español como se habla en México).

Resumen de opciones

Cuando se ejecuta Nmap sin parámetros se muestra este resumen de opciones. Puede encontrar siempre la última versión en http://www.insecure.org/nmap/data/nmap.usage.txt.

Aunque ayuda a recordar las opciones más habituales no es un sustituto de la documentación en detalle que acompaña al resto de este manual. Algunas de las opciones menos conocidas no se incluyen aquí.

```
Uso: nmap [Tipo(s) de Análisis] [Opciones] {especificación de objetivos}
ESPECIFICACIÓN DE OBJETIVO:
  Se pueden indicar nombres de sistema, direcciones IP, redes, etc.
  Ej: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <archivo_entrada>: Lee una lista de sistemas/redes del archivo.
  -iR <número de sistemas>: Selecciona objetivos al azar
  --exclude <sist1[,sist2][,sist3],...>: Excluye ciertos sistemas o redes
  --excludefile <fichero_exclusión>: Excluye los sistemas indicados en el fichero
DESCUBRIMIENTO DE HOSTS:
  -sL: Sondeo de lista - Simplemente lista los objetivos a analizar
  -sP: Sondeo Ping     - Sólo determina si el objetivo está vivo
  -P0: Asume que todos los objetivos están vivos
  -PS/PA/PU [listadepuertos]: Análisis TCP SYN, ACK o UDP de los puertos indicados
  -PE/PP/PM: Solicita un análisis ICMP del tipo echo, marca de fecha y máscara de red
  -n/-R: No hacer resolución DNS / Siempre resolver [por omisión: a veces]
  --dns-servers <serv1[,serv2],...>: Especificar servidores DNS específicos
  --system-dns: Utilizar la resolución del sistema operativo
TÉCNICAS DE ANÁLISIS:
  -sS/sT/sA/sW/sM: Análisis TCP SYN/Connect()/ACK/Window/Maimon
  -sN/sF/sX: Análisis TCP Null, FIN, y Xmas
  --scanflags <indicador>: Personalizar los indicadores TCP a utilizar
  -sI <sistema zombi[:puerto_sonda]>: Análisis pasivo («Idle», N. del T.)
  -sO: Análisis de protocolo IP
  -b <servidor ftp rebote>: Análisis por rebote FTP
ESPECIFICACIÓN DE PUERTOS Y ORDEN DE ANÁLISIS:
  -p <rango de puertos>: Sólo sondear los puertos indicados
    Ej: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -F: Rápido - Analizar sólo los puertos listados en el archivo nmap-services
  -r: Analizar los puertos secuencialmente, no al azar.
DETECCIÓN DE SERVICIO/VERSIÓN:
  -sV: Sondear puertos abiertos, para obtener información de servicio/versión
  --version-intensity <nivel>: Fijar de 0 (ligero) a 9 (probar todas las sondas)
  --version-light: Limitar a las sondas más probables (intensidad 2)
  --version-all: Utilizar todas las sondas (intensidad 9)
  --version-trace: Presentar actividad detallada del análisis (para depurar)
 DETECCIÓN DE SISTEMA OPERATIVO
  -O: Activar la detección de sistema operativo (SO)
  --osscan-limit: Limitar la detección de SO a objetivos prometedores
  --osscan-guess: Adivinar el SO de la forma más agresiva
TEMPORIZADO Y RENDIMIENTO:
  -T[0-5]: Seleccionar plantilla de temporizado (los números altos son más rápidos)
  --min-hostgroup/max-hostgroup <tamaño>: Paralelizar los sondeos
  --min-parallelism/max-parallelism <msegs>: Paralelización de sondeos
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <msegs>: Indica
    el tiempo de ida y vuelta de la sonda
  --max-retries <reintentos>: Limita el número máximo de retransmisiones de las
    sondas de análisis de puertos
```

```
  --host-timeout <msegs>: Abandonar un objetivo pasado este tiempo
  --scan-delay/--max-scan-delay <msegs>: Ajusta el retraso entre sondas
EVASIÓN Y FALSIFICACIÓN PARA CORTAFUEGOS/IDS:
  -f; --mtu <valor>: fragmentar paquetes (opc. con el MTU indicado)
  -D <señuelo1,señuelo2[,ME],...>: Disimular el análisis con señuelos
     N. del T.: «ME» es «YO» mismo.
  -S <Dirección_IP>: Falsificar la dirección IP origen
  -e <interfaz>: Utilizar la interfaz indicada
  -g/--source-port <numpuerto>: Utilizar el número de puerto dado
  --data-length <num>: Agregar datos al azar a los paquetes enviados
  --ttl <val>: Fijar el valor del campo time-to-live (TTL) de IP
  --spoof-mac <dirección mac/prefijo/nombre de fabricante>: Falsificar la dirección MAC
  --badsum: Enviar paquetes con una suma de comprobación TCP/UDP falsa
SALIDA:
  -oN/-oX/-oS/-oG <file>: Guardar el sondeo en formato normal, XML,
     s|<rIpt kIddi3 (n3n3b4n4n4), y Grepeable (para usar con grep(1), N. del T.),
     respectivamente, al archivo indicado.
  -oA <nombre_base>: Guardar en los tres formatos principales al mismo tiempo
  -v: Aumentar el nivel de mensajes detallados (-vv para aumentar el efecto)
  -d[nivel]: Fijar o incrementar el nivel de depuración (Tiene sentido hasta 9)
  --packet-trace: Mostrar todos los paquetes enviados y recibidos
  --iflist: Mostrar interfaces y rutas (para depurar)
  --append-output: Agregar, en vez de sobreescribir, a los archivos indicados con -o.
  --resume <archivo>: Retomar un análisis abortado/detenido
  --stylesheet <ruta/URL>: Convertir la salida XML a HTML según la hoja de estilo
      XSL indicada
  --webxml: Referenciar a la hoja de estilo de Insecure.Org para tener un XML más portabl
e
  --no_stylesheet: No asociar la salida XML con ninguna hoja de estilos XSL
MISCELÁNEO:
   -6: Habilitar análisis IPv6
   -A: Habilita la detección de SO y de versión
   --datadir <nombreDir>: Indicar la ubicación de los archivos de datos Nmap
     personalizados.
   --send-eth/--send-ip: Enviar paquetes utilizando tramas Ethernet o paquetes IP
     "crudos"
   --privileged: Asumir que el usuario tiene todos los privilegios
   -V: Muestra el número de versión
   -h: Muestra esta página resumen de la ayuda.
EJEMPLOS:
   nmap -v -A scanme.nmap.org
   nmap -v -sP 192.168.0.0/16 10.0.0.0/8
   nmap -v -iR 10000 -P0 -p 80
```

Especificación de objetivos

Todo lo que se escriba en la línea de parámetros de Nmap que no sea una opción se considera una especificación de sistema objetivo. El caso más sencillo es la indicación de sólo una IP, o nombre de sistema, para que sea analizado.

Puede darse la situación en que uno desee analizar una red completa de equipos

adyacentes. Nmap soporta el direccionamiento estilo CIDR para estos casos. Puede añadir /*numBits* a una dirección IP o nombre de sistema para que Nmap sondee toda IP cuyos primeros *numBits* sean los mismos que los de la dirección IP o nombre de sistema indicado. Por ejemplo, 192.168.10.0/24 analizaría los 256 sistemas que existen entre la dirección 192.168.10.0 (que en binario se representa como 11000000 10101000 00001010 00000000) y la dirección 192.168.10.255 (binario: 11000000 10101000 00001010 11111111), ambas inclusives. De hecho, si usa 192.168.10.40/24 obtendría exactamente el mismo resultado. En el caso del sistema scanme.nmap.org que posee una dirección IP 205.217.153.62, la especificación scanme.nmap.org/16 analizaría las 65.536 direcciones IP entre 205.217.0.0 y 205.217.255.255. La máscara mas pequeña permitida es /1, que analizaría media Internet. La más grande, /32, analizaría únicamente la IP o nombre de sistema indicados porque todos los bits estarían fijos.

La notación CDIR es breve pero no siempre es suficiemente flexible. Por ejemplo, puede querer sondear la red 192.168.0.0/16 pero omitir cualquier IP que termine por .0 o por .255 ya que son habitualmente direcciones de difusión. Es posible hacer esto con Nmap mediante el direccionamiento por octetos. En lugar de especificar una dirección IP normal puede especificar una lista separada por comas de números o rangos para cada octeto. Por ejemplo, si utiliza 192.168.0-255.1-254 se omitirán todas las direcciones del rango que terminen en .0 o .255. Los rangos no tienen por qué estar limitados a los últimos octetos. Por ejemplo, si especifica 0-255.0-255.13.37 se realizará un sondeo en todo Internet de las direcciones IP que terminan en 13.37. Este tipo de muestreo amplio puede ser útil para encuestas en Internet y con fines de investigación.

Sólo puede especificar direcciones IPv6 si utiliza su nombre IPv6 totalmente cualificado o su nombre de sistema. No se soporta el uso de CIDR o rangos de octetos para IPv6 porque raramente son útiles.

Con Nmap puede especificar múltiples sistemas en la línea de órdenes y no tienen por qué ser del mismo tipo. Por ejemplo, la orden **nmap scanme.nmap.org 192.168.0.0/16 10.0.0,1,3-7.0-255** hace lo que uno esperaría.

Aunque habitualmente se especifican los objetivos en la línea de órdenes puede utilizar las siguientes opciones para controlar la selección de objetivos:

-iL <archivo_entrada> (Entrada de una lista)

> Toma la especificación de objetivos del archivo *archivo_entrada*. Habitualmente es un tanto molesto especificar una lista de sistemas muy grande en la línea de órdenes, pero es algo que también uno quiere hacer. Por ejemplo, si tu servidor DHCP puede exportar un listado de las 10.000 direcciones entregadas IP que querría analizar. O tal vez quiera analizar todas las direcciones IP *excepto* esas mismas direcciones, para así localizar sistemas que estén utilizando direcciones IP estáticas sin autorización. Para sondear un número elevado de objetivos sólo tiene que generar la lista en un archivo, y entregárselo a Nmap con la opción -iL. Las entradas de ese archivo pueden estar en cualquiera de los formatos aceptados por Nmap en la línea de órdenes (direcciones IP, nombres de sistema, CIDR, IPv6 o rangos de octeto). Cada elemento debe estar separado por uno o más espacios, tabuladores, o por líneas. Si quiere leer el archivo de la entrada estándar puede especificar un guión (-) como nombre de archivo.

-iR <cant. sistemas> (Elegir objetivos al azar)

Cuando se quieren realizar encuestas que cubran toda Internet uno puede querer elegir objetivos al azar. La opción *cant. sistemas* indica a Nmap cuántas direcciones IP debe generar aleatoriamente. Se filtran de forma automática las direcciones no deseables, incluyendo las direcciones privadas, de multicast o direccionamiento no asignado. Si se utiliza el valor 0, Nmap realizará un análisis que no acabará nunca. Hay que tener en cuenta que a algunos administradores de red puede no gustarle que les analicen sus redes, y pueden llegar a quejarse ¡Utilice esta opción bajo su propia responsabilidad! Si está realmente aburrido un día de tarde lluviosa, puede intentar la orden **nmap -sS -PS80 -iR 0 -p 80** para encontrar servidores web al azar para navegar.

--exclude <equipo1[,equipo2][,equipo3],...> (Excluir equipo o redes)

Indica con una lista separada por comas los objetivos que deben excluirse del análisis. Se excluirán aunque se encuentren dentro de un rango especificado en la línea de órdenes. La lista que se indica utiliza la sintaxis normal de Nmap, por lo que puede incluir nombres de equipo, rangos de red CIDR, rangos de octeto, etc. Esto puede ser útil cuando la red a analizar tiene objetivos que no se deben tocar, como puedan ser servidores de misión crítica, que pueden reaccionar adversamente a un análisis de puertos, o si la red incluye subredes administradas por otras personas.

--excludefile <archivo> (Excluir desde una Lista)

Al igual que --exclude, esta función permite excluir objetivos, pero en lugar de utilizar la línea de órdenes toma el listado de un *archivo*, que utiliza la misma sintaxis que la opción -iL.

Descubriendo sistemas

Uno de los primeros pasos en cualquier misión de reconocimiento de red es el de reducir un (muchas veces enorme) conjunto de rangos de direcciones IP en una lista de equipos activos o interesantes. Analizar cada puerto de cada una de las direcciones IP es lento, y usualmente innecesario. Por supuesto, lo que hace a un sistema interesante depende ampliamente del propósito del análisis. Los administradores de red pueden interesarse sólo en equipos que estén ejecutando un cierto servicio, mientras que los auditores de seguridad pueden interesarse en todos y cada uno de los dispositivos que tengan una dirección IP. Un administrador puede sentirse cómodo con obtener un listado de equipos en su red interna mediante un ping ICMP, mientras que un consultor en seguridad realizando un ataque externo puede llegar a utilizar un conjunto de docenas de sondas en su intento de saltarse las restricciones de los cortafuegos.

Siendo tan diversas las necesidades de descubrimiento de sistemas, Nmap ofrece una gran variedad de opciones para personalizar las técnicas utilizadas. Al descubrimiento de sistemas («Host Discovery») se lo suele llamar sondeo ping, pero va más allá de la simple solicitud ICMP echo-request de los paquetes asociados al querido y nunca bien ponderado ping. Los usuarios pueden evitar el paso de ping utilizando un sondeo de lista (-sL) o deshabilitando el ping (-P0), o enviando combinaciones arbitrarias de sondas TCP SYN/ACK, UDP e ICMP a múltiples puertos de la red remota. El propósito de estas sondas es el de solicitar respuestas que demuestren que una dirección IP se encuentra activa (está siendo utilizada por un equipo o dispositivo de red). En varias redes solo un

pequeño porcentaje de direcciones IP se encuentran activos en cierto momento. Esto es particularmente común en las redes basadas en direccionamiento privado RFC1918, como la 10.0.0.0/8. Dicha red tiene más de 16 millones de direcciones IP, pero la he visto siendo utilizada por empresas con menos de mil máquinas. El descubrimiento de sistemas puede encontrar dichas maquinas en un rango tan grande como el indicado.

Si no se proveen opciones de descurbrimiento de sistemas, Nmap envía un paquete TCP ACK al puerto 80 y un ICMP Echo Request a cada máquina objetivo. Una excepción a este comportamiento es cuando se utiliza un análisis ARP, para los objetivos que se encuentren en la red Ethernet local. Para usuarios de shell UNIX que no posean privilegios, un paquete SYN es enviado en vez del ACK, utilizando la llamada al sistema connect(). Estos valores por omisión son el equivalente a las opciones -PA -PE. Este descubrimiento de sistemas es generalmente suficiente cuando se analizan redes locales, pero para auditorías de seguridad se recomienda utilizar un conjunto más completo de sondas de descubrimiento.

Las opciones -P* (que permiten seleccionar los tipos de ping) pueden combinarse. Puede aumentar sus probabilidades de penetrar cortafuegos estrictos enviando muchos tipos de sondas utilizando diferentes puertos o banderas TCP y códigos ICMP. Recuerde que el ARP discovery (-PR) se realiza por omisión contra objetivos de la red Ethernet local incluso si se especifica otra de las opciones -P*, porque es generalmente más rápido y efectivo.

Las siguientes opciones controlan el descubrimiento de sistemas.

-sL (Sondeo de lista)

> El sondeo de lista es un tipo de descubrimiento de sistemas que tan solo lista cada equipo de la/s red/es especificada/s, sin enviar paquetes de ningún tipo a los objetivos. Por omisión, Nmap va a realizar una resolución inversa DNS en los equipos, para obtener sus nombres. Es sorprendente cuanta información útil se puede obtener del nombre de un sistema. Por ejemplo fw.chi.playboy.com es el cortafuegos de la oficina en Chicago de Playboy Enterprises. Adicionalmente, al final, Nmap reporta el número total de direcciones IP. El sondeo de lista es una buena forma de asegurarse de que tenemos las direcciones IP correctas de nuestros objetivos. Si se encontraran nombres de dominio que no reconoces, vale la pena investigar un poco más, para evitar realizar un análisis de la red de la empresa equivocada.
>
> Ya que la idea es simplemente emitir un listado de los sistemas objetivo, las opciones de mayor nivel de funcionalidad como análisis de puertos, detección de sistema operativo, o análisis ping no pueden combinarse con este sondeo. Si desea deshabilitar el análisis ping aún realizando dicha funcionalidad de mayor nivel, compruebe la documentación de la opción -P0.

-sP (Sondeo ping)

> Esta opción le indica a Nmap que *únicamente* realice descubrimiento de sistemas mediante un sondeo ping, y que luego emita un listado de los equipos que respondieron al mismo. No se realizan más sondeos (como un análisis de puertos o detección de sistema operativo). A diferencia del sondeo de lista, el análisis ping es intrusivo, ya que envía paquetes a los objetivos, pero es usualmente utilizado con el

mismo propósito. Permite un reconocimiento liviano de la red objetivo sin llamar mucho la atención. El saber cuántos equipos se encuentran activos es de mayor valor para los atacantes que el listado de cada una de las IP y nombres proporcionado por el sondeo de lista.

De la misma forma, los administradores de sistemas suelen encontrar valiosa esta opción. Puede ser fácilmente utilizada para contabilizar las máquinas disponibles en una red, o monitorizar servidores. A esto se lo suele llamar barrido ping, y es más fiable que hacer ping a la dirección de broadcast, ya que algunos equipos no responden a ese tipo de consultas.

La opción -sP envía una solicitud de eco ICMP y un paquete TCP al puerto 80 por omisión. Cuando un usuario sin privilegios ejecuta Nmap se envía un paquete SYN (utilizando la llamada connect()) al puerto 80 del objetivo. Cuando un usuario privilegiado intenta analizar objetivos en la red Ethernet local se utilizan solicitudes ARP (-PR) a no ser que se especifique la opción --send-ip.

La opción -sP puede combinarse con cualquiera de las opciones de sondas de descubrimiento (las opciones -P*, excepto -P0) para disponer de mayor flexibilidad. Si se utilizan cualquiera de las opciones de sondas de descubrimiento y número de puerto, se ignoran las sondas por omisión (ACK y solicitud de eco ICMP). Se recomienda utilizar estas técnicas si hay un cortafuegos con un filtrado estricto entre el sistema que ejecuta Nmap y la red objetivo. Si no se hace así pueden llegar a pasarse por alto ciertos equipos, ya que el cortafuegos anularía las sondas o las respuestas a las mismas.

-P0 (No realizar ping)

Con esta opción, Nmap no realiza la etapa de descubrimiento. Bajo circunstancias normales, Nmap utiliza dicha etapa para determinar qué máquinas se encuentran activas para hacer un análisis más agresivo. Por omisión, Nmap sólo realiza ese tipo de sondeos, como análisis de puertos, detección de versión o de sistema operativo contra los equipos que se están «vivos». Si se deshabilita el descubrimiento de sistemas con la opción -P0 entonces Nmap utilizará las funciones de análisis solicitadas contra *todas* las direcciones IP especificadas. Por lo tanto, si se especifica una red del tamaño de una clase B cuyo espacio de direccionamiento es de 16 bits, en la línea de órdenes, se analizará cada una de las 65.536 direcciones IP. El segundo carácter en la opción -P0 es un cero, y no la letra O. Al igual que con el sondeo de lista, se evita el descubrimiento apropiado de sistemas, pero, en vez de detenerse y emitir un listado de objetivos, Nmap continúa y realiza las funciones solicitadas como si cada IP objetivo se encontrara activa.

-PS [lista de puertos] (Ping TCP SYN)

Esta opción envía un paquete TCP vacío con la bandera SYN puesta. El puerto destino por omisión es el 80 (se puede configurar en tiempo de compilación cambiando el valor de DEFAULT_TCP_PROBE_PORT en nmap.h), pero se puede añadir un puerto alternativo como parámetro. También se puede especificar una lista de puertos separados por comas (p.ej. -PS22,23,25,80,113,1050,35000). Si hace esto se enviarán sondas en paralelo a cada uno de los puertos.

La bandera SYN indica al sistema remoto que quiere establecer una conexión. Normalmente, si el puerto destino está cerrado se recibirá un paquete RST (de «reset»). Si el puerto está abierto entonces el objetivo responderá con el segundo paso del saludo en tres pasos TCP respondiendo con un paquete TCP SYN/ACK. El sistema donde se ejecuta Nmap romperá la conexión que se está estableciendo enviando un paquete RST en lugar de enviar el paquete ACK que completaría el saludo TCP. Nmap no envía este paquete, sino que lo envía el núcleo del sistema donde se ejecuta Nmap respondiendo al paquete SYN/ACK que no esperaba.

A Nmap no le importa si el puerto está abierto o cerrado. Si, tal y como se acaba de describir, llega una respuesta RST ó SYN/ACK entonces Nmap sabrá que el sistema está disponible y responde.

En sistemas UNIX, generalmente sólo el usuario privilegiado root puede enviar paquetes TCP crudos. Los usuarios no privilegiados tienen una forma de evitar esta restricción utilizando la llamada al sistema «connect()» contra el puerto destino. Esto hace que se envíe el paquete SYN al sistema, para establecer la conexión. Si la llamada «connect()» devuelve un resultado de éxito rápidamente o un fallo ECONNREFUSED entonces se puede deducir que la pila TCP que tiene bajo ésta ha recibido un SYN/ACK o un RST y que puede marcar el sistema como disponible. El sistema se puede marcar como no disponible si el intento de conexión se mantiene parado hasta que vence un temporizador. Esta es también la forma en la que se gestiona esto en conexiones IPv6 ya que Nmap aún no puede crear paquetes IPv6 crudos.

-PA [lista de puertos] (Ping TCP ACK)

El ping TCP ACK es muy parecido al ping SYN que se acaba de tratar. La diferencia es que en este caso se envía un paquete con la bandera ACK en lugar de la SYN. Este paquete indica que se han recibido datos en una conexión TCP establecida, pero se envían sabiendo que la conexión no existe. En este caso los sistemas deberían responder con un paquete RST, lo que sirve para determinar que están vivos.

La opción -PA utiliza el mismo puerto por omisión que la sonda SYN (el puerto 80) y también puede tomar una lista de puertos destino en el mismo formato. Si un usuario sin privilegios intenta hacer esto, o se especifica un objetivo IPv6, se utiliza el procedimiento descrito anteriormente. Aunque en este caso el procedimiento no es perfecto porque la llamada «connect()» enviará un paquete SYN en lugar de un ACK.

Se ofrecen tanto mecanismos de sondeo con ping SYN y ACK para maximizar las posibilidades de atravesar cortafuegos. Muchos administradores configuran los enrutadores y algunos cortafuegos sencillos para que se bloqueen los paquetes SYN salvo para aquellos destinados a los servicios públicos, como pudieran ser el servidor web o el servidor de correo de la organización. Esto evita que se realicen otras conexiones entrantes al mismo tiempo que permite a los usuarios realizar conexiones salientes a Internet. Este acercamiento de filtrado sin estados toma pocos recursos de los cortafuegos/enrutadores y está ampliamente soportado por filtros hardware y software. El programa de cortafuegos Netfilter/iptables de Linux

ofrece la opción --syn para implementar este acercamiento sin estados. Cuando se han implementado reglas de filtrado como éstas es posible que se bloqueen las sondas ping SYN (-PS) cuando éstas se envíen a un puerto cerrado. Sin embargo, en estos casos, las sondas ACK podrían saltarse las reglas y llegar a su destino.

Otros tipos de cortafuegos comunes utilizan reglas con estados que descartan paquetes no esperados. Esta funcionalidad se encontraba antes fundamentalmente en los cortafuegos de gama alta pero se ha hecho cada vez más común. El sistema Netfilter/iptables de Linux soporta esta posibilidad a través de la opción --state, que hace categorías de paquetes en base a su estado de conexión. En estos sistemas es más probable que funcione una sonda SYN, dado que los paquetes ACK no esperados se reconocen como falsos y se descartan. Una solución a este dilema es enviar sondas SYN y ACK especificando tanto la opción -PS como -PA.

-PU [lista de puertos] (Ping UDP)

El ping UDP es otra opción para descubrir sistemas. Esta opción envía un paquete UDP vacío (salvo que se especifique --data-length) a los puertos indicados. La lista de puertos se debe dar en el mismo formato que se ha indicado anteriormente para las opciones -PS y -PA . Si no se especifica ningún puerto se utiliza el puerto 31338 por omisión. Se puede configurar este puerto por omisión en el momento de compilar cambiando DEFAULT_UDP_PROBE_PORT en nmap.h. Se utiliza un puerto alto y poco común por omisión porque no es deseable enviar este sondeo a otro tipo de puertos.

La sonda UDP debería generar un paquete ICMP de puerto no alcanzable si da contra un puerto cerrado en el equipo objetivo. Si llega éste entonces Nmap puede identificar ese sistema como vivo y alcanzable. Otros errores ICMP, como el de sistema o red inalcanzables o TTL excedido indican un sistema que está muerto o que no es alcanzable. Si no llega ninguna respuesta también se entiende que el sistema no está disponible. Si se alcanza un puerto abierto la mayoría de los servicios simplemente descartarán el paquete vacío y no devolverán ninguna respuesta. Ésta es la razón por la que se utiliza el puerto por omisión 31338 ya que es poco probable que esté utilizándose. Algunos servicios, como chargen, responderán con un paquete UDP vacío lo que ayuda a Nmap a determinar que el sistema está disponible.

La principal ventaja de este tipo de sondeos es que atraviesan cortafuegos y filtros que sólo analizan TCP. Yo, por ejemplo, una vez fui propietario de un encaminador de banda ancha inalámbrico BEFW11S4. El interfaz externo de este dispositivo filtraba por omisión todos los puertos TCP, pero las sondas UDP podían generar mensajes de puerto no alcanzable y permitían detectar al dispositivo.

-PE; -PP; -PM (Tipos de ping ICMP)

Nmap puede enviar los paquetes estándar que envía el programa ping además de los tipos de descubrimiento de equipos con TCP y UDP. Nmap envía paquetes ICMP tipo 7 («echo request») a las direcciones IP objetivos y espera recibir un tipo 0 («Echo Reply») de los sistemas que estén disponibles. Lamentablemente para los exploradores de redes, muchos sistemas y cortafuegos ahora bloquean esos

paquetes en lugar de responder como requiere el estándar RFC 1122. Por ésta razón los sondeos que sólo utilizan el protocolo ICMP no son muy fiables para analizar sistemas desconocidos en Internet. Aunque pueda ser una forma eficiente y práctica de hacerlo para administradores que tengan que monitorizar una red interna. Utilice la opción -PE para activar este comportamiento de solicitud de eco.

Nmap no hace sólo ésto, aunque la solicitud eco es la consulta estándar de ping ICMP. El estándar ICMP (RFC 792) también específica solicitudes de huellas de tiempo, de información y de máscara de red, que corresponden con los códigos 13, 15 y 17 respectivamente. Aunque el objetivo de estas solicitudes es obtener la máscara de red o fecha actual de un sistema también pueden utilizarse para descubrir sistemas. Un sistema que responde es por que está vivo y disponible. Nmap no implementa los paquetes de solicitud de información en sí, ya que no están muy soportados. El estándar RFC 1122 insiste en que “un equipo NO DEBE implementar estos mensajes”. Las consultas de huella de tiempo y máscara de red se pueden enviar con las opciones -PP y -PM, respectivamente. Si se recibe una respuesta de huella de tiempo (código ICMP 14) o de máscara de red (código 18) entonces es que el sistema está disponible. Estas dos consultas pueden ser útiles cuando los administradores bloquean los paquetes de consulta eco explícitamente pero se olvidan de que se pueden utilizar otras consultas ICMP con el mismo fin.

-PR (Ping ARP)

Una de las formas de uso más comunes de Nmap es el sondeo de una red de área local Ethernet. En la mayoría de las redes locales hay muchas direcciones IP sin usar en un momento determinado. Esto es así especialmente en las que utilizan rangos de direcciones privadas definidas en el RFC1918. Cuando Nmap intenta enviar un paquete IP crudo, como pudiera ser una solicitud de eco ICMP, el sistema operativo debe determinar primero la dirección (ARP) correspondiente a la IP objetivo para poder dirigirse a ella en la trama Ethernet. Esto es habitualmente un proceso lento y problemático, dado que los sistemas operativos no se escribieron pensando en que tendrían que hacer millones de consultas ARP contra sistemas no disponibles en un corto periodo de tiempo.

El sondeo ARP hace que sea Nmap y su algoritmo optimizado el que se encargue de las solicitudes ARP. Si recibe una respuesta, no se tiene ni que preocupar de los paquetes basados en IP dado que ya sabe que el sistema está vivo. Esto hace que el sondeo ARP sea mucho más rápido y fiable que los sondeos basados en IP. Por ello se utiliza por omisión cuando se analizan sistemas Ethernet si Nmap detecta que están en la red local. Nmap utiliza ARP para objetivos en la misma red local aún cuando se utilicen distintos tipos de ping (como -PE o -PS). Si no quiere hacer un sondeo ARP tiene que especificar la opción --send-ip.

-n (No realizar resolución de nombres)

Le indica a Nmap que *nunca* debe realizar resolución DNS inversa de las direcciones IP activas que encuentre. Ya que DNS es generalmente lento, esto acelera un poco las cosas.

-R (Realizar resolución de nombres con todos los objetivos)

Le indica a Nmap que deberá realizar *siempre* la resolución DNS inversa de las direcciones IP objetivo. Normalmente se realiza esto sólo si se descubre que el objetivo se encuentra vivo.

--system-dns (Utilizar resolución DNS del sistema)

Por omisión, Nmap resuelve direcciones IP por si mismo enviando las consultas directamente a los servidores de nombres configurados en el sistema, y luego espera las respuestas. Varias solicitudes (generalmente docenas) son realizadas en paralelo para mejorar el rendimiento. Especifica esta opción si desea que sí utilice la resolución del sistema (una IP por vez utilizando la llamada getnameinfo()). Este método es más lento y raramente útil, a no ser que hubiera un error en el código DNS de Nmap (por favor, notifíquelo si ese fuera el caso). Éste es el método por omisión para los sondeos IPv6.

--dns-servers <servidor1[,servidor2],...> (Servidores a utilizar para las consultas DNS)

Nmap generalmente determina los servidores DNS de su archivo resolv.conf (UNIX) o del registro (Win32). Puede utilizar esta opción para especificar sus propios servidores. Esta opción no se utiliza si utiliza la opción --system-dns o está realizando un sondeo IPv6. La resolución a través de más de un servidor de DNS es generalmente más rápida que la consulta a uno solo.

Introducción al análisis de puertos

Nmap comenzó como un analizador de puertos eficiente, aunque ha aumentado su funcionalidad a través de los años, aquella sigue siendo su función primaria. La sencilla orden **nmap *objetivo*** analiza más de 1660 puertos TCP del equipo *objetivo*. Aunque muchos analizadores de puertos han agrupado tradicionalmente los puertos en dos estados: abierto o cerrado, Nmap es mucho más descriptivo. Se dividen a los puertos en seis estados distintos: abierto, cerrado, filtrado, no filtrado, abierto|filtrado, o cerrado|filtrado.

Estos estados no son propiedades intrínsecas del puerto en sí, pero describen como los ve Nmap. Por ejemplo, un análisis con Nmap desde la misma red en la que se encuentra el objetivo puede mostrar el puerto 135/tcp como abierto, mientras que un análisis realizado al mismo tiempo y con las mismas opciones, pero desde Internet, puede presentarlo como filtrado.

Los seis estados de un puerto, según Nmap

abierto

Una aplicación acepta conexiones TCP o paquetes UDP en este puerto. El encontrar esta clase de puertos es generalmente el objetivo primario de realizar un sondeo de puertos. Las personas orientadas a la seguridad saben que cada puerto abierto es un vector de ataque. Los atacantes y las personas que realizan pruebas de intrusión intentan aprovechar puertos abiertos, por lo que los administradores intentan cerrarlos, o protegerlos con cortafuegos, pero sin que los usuarios legítimos pierdan acceso al servicio. Los puertos abiertos también son interesantes en sondeos que no están relacionados con la seguridad porque indican qué servicios están disponibles

para ser utilizados en una red.

cerrado

Un puerto cerrado es accesible: recibe y responde a las sondas de Nmap, pero no tiene una aplicación escuchando en él. Pueden ser útiles para determinar si un equipo está activo en cierta dirección IP (mediante descubrimiento de sistemas, o sondeo ping), y es parte del proceso de detección de sistema operativo. Como los puertos cerrados son alcanzables, o sea, no se encuentran filtrados, puede merecer la pena analizarlos pasado un tiempo, en caso de que alguno se abra. Los administradores pueden querer considerar bloquear estos puertos con un cortafuegos. Si se bloquean aparecerían filtrados, como se discute a continuación.

filtrado

Nmap no puede determinar si el puerto se encuentra abierto porque un filtrado de paquetes previene que sus sondas alcancen el puerto. El filtrado puede provenir de un dispositivo de cortafuegos dedicado, de las reglas de un enrutador, o por una aplicación de cortafuegos instalada en el propio equipo. Estos puertos suelen frustrar a los atacantes, porque proporcionan muy poca información. A veces responden con mensajes de error ICMP del tipo 3, código 13 (destino inalcanzable: comunicación prohibida por administradores), pero los filtros que sencillamente descartan las sondas sin responder son mucho más comunes. Esto fuerza a Nmap a reintentar varias veces, considerando que la sonda pueda haberse descartado por congestión en la red en vez de haberse filtrado. Esto ralentiza drásticamente los sondeos.

no filtrado

Este estado indica que el puerto es accesible, pero que Nmap no puede determinar si se encuentra abierto o cerrado. Solamente el sondeo ACK, utilizado para determinar las reglas de un cortafuegos, clasifica a los puertos según este estado. El analizar puertos no filtrados con otros tipos de análisis, como el sondeo Window, SYN o FIN, pueden ayudar a determinar si el puerto se encuentra abierto.

abierto|filtrado

Nmap marca a los puertos en este estado cuando no puede determinar si el puerto se encuentra abierto o filtrado. Esto ocurre para tipos de análisis donde no responden los puertos abiertos. La ausencia de respuesta puede también significar que un filtro de paquetes ha descartado la sonda, o que se elimina cualquier respuesta asociada. De esta forma, Nmap no puede saber con certeza si el puerto se encuentra abierto o filtrado. Los sondeos UDP, protocolo IP, FIN, Null y Xmas clasifican a los puertos de esta manera.

cerrado|filtrado

Este estado se utiliza cuando Nmap no puede determinar si un puerto se encuentra cerrado o filtrado, y puede aparecer aparecer sólo durante un sondeo IPID pasivo.

Técnicas de sondeo de puertos

Cuando intento realizar un arreglo de mi coche, siendo novato, puedo pasarme horas intentando utilizar mis herramientas rudimentarias (martillo, cinta aislante, llave inglesa, etc.). Cuando fallo miserablemente y llevo mi coche antiguo en grúa al taller a un mecánico de verdad siempre pasa lo mismo: busca en su gran cajón de herramientas hasta que saca una herramienta que hace que la tarea se haga sin esfuerzo. El arte de sondear puertos es parecido. Los expertos conocen docenas de técnicas de sondeo y eligen la más apropiada (o una combinación de éstas) para la tarea que están realizando. Los usuarios sin experiencia y los "script kiddies", sin embargo, intentan resolver cada problema con el sondeo SYN por omisión. Dado que Nmap es libre, la única barrera que existe para ser un experto en el sondeo de puertos es el conocimiento. Esto es mucho mejor que el mundo del automóvil, donde puedes llegar a saber que necesitas un compresor de tuerca, pero tendrás que pagar mil dolares por él.

La mayoría de los distintos tipos de sondeo disponibles sólo los puede llevar a cabo un usuario privilegiado. Esto es debido a que envían y reciben paquetes en crudo, lo que hace necesario tener acceso como administrador (root) en la mayoría de los sistemas UNIX. En los entornos Windows es recomendable utilizar una cuenta de administrador, aunque Nmap algunas veces funciona para usuarios no privilegiados en aquellas plataformas donde ya se haya instalado WinPcap. La necesidad de privilegios como usuario administrador era una limitación importante cuando se empezó a distribuir Nmap en 1997, ya que muchos usuarios sólo tenían acceso a cuentas compartidas en sistemas como usuarios normales. Ahora, las cosas son muy distintas. Los ordenadores son más baratos, hay más personas que tienen acceso permanente a Internet, y los sistemas UNIX (incluyendo Linux y MAC OS X) son más comunes. También se dispone de una versión para Windows de Nmap, lo que permite que se ejecute en más escritorios. Por todas estas razones, cada vez es menos necesario ejecutar Nmap utilizando cuentas de sistema compartidas. Esto es bueno, porque las opciones que requieren de más privilegios hacen que Nmap sea más potente y flexible.

Aunque Nmap intenta generar resultados precisos, hay que tener en cuenta que estos resultados se basan en los paquetes que devuelve el sistema objetivo (o los cortafuegos que están delante de éstos). Estos sistemas pueden no ser fiables y envíar respuestas cuyo objetivo sea confundir a Nmap. Son aún más comunes los sistemas que no cumplen con los estándares RFC, que no responden como deberían a las sondas de Nmap. Son especialmente susceptibles a este problema los sondeos FIN, Null y Xmas. Hay algunos problemas específicos a algunos tipos de sondeos que se discuten en las entradas dedicadas a sondeos concretos.

Esta sección documenta las aproximadamente doce técnicas de sondeos de puertos que soporta Nmap. Sólo puede utilizarse un método en un momento concreto, salvo por el sondeo UDP (-sU) que puede combinarse con cualquiera de los sondeos TCP. Para que sea fácil de recordar, las opciones de los sondeos de puertos son del estilo -s*C*, donde *C* es una letra característica del nombre del sondeo, habitualmente la primera. La única excepción a esta regla es la opción obsoleta de sondeo FTP rebotado (-b). Nmap hace un sondeo SYN por omisión, aunque lo cambia a un sondeo Connect() si el usuario no tiene los suficientes privilegios para enviar paquetes en crudo (requiere acceso de administrador en UNIX) o si se especificaron objetivos IPv6. De los sondeos que se listan en esta sección los usuarios sin privilegios sólo pueden ejecutar los sondeos Connect() o de rebote FTP.

-sS (sondeo TCP SYN)

El sondeo SYN es el utilizado por omisión y el más popular por buenas razones. Puede realizarse rápidamente, sondeando miles de puertos por segundo en una red rápida en la que no existan cortafuegos. El sondeo SYN es relativamente sigiloso y poco molesto, ya que no llega a completar las conexiones TCP. También funciona contra cualquier pila TCP en lugar de depender de la idiosincrasia específica de una plataforma concreta, al contrario de lo que pasa con los sondeos de Nmap Fin/Null/Xmas, Maimon o pasivo. También muestra una clara y fiable diferenciación entre los estados abierto, cerrado, y filtrado.

A esta técnica se la conoce habitualmente como sondeo medio abierto, porque no se llega a abrir una conexión TCP completa. Se envía un paquete SYN, como si se fuera a abrir una conexión real y después se espera una respuesta. Si se recibe un paquete SYN/ACK esto indica que el puerto está en escucha (abierto), mientras que si se recibe un RST (reset) indica que no hay nada escuchando en el puerto. Si no se recibe ninguna respuesta después de realizar algunas retransmisiones entonces el puerto se marca como filtrado. También se marca el puerto como filtrado si se recibe un error de tipo ICMP no alcanzable (tipo 3, códigos 1,2, 3, 9, 10, ó 13).

-sT (sondeo TCP connect())

El sondeo TCP Connect() es el sondeo TCP por omisión cuando no se puede utilizar el sondeo SYN. Esto sucede, por ejemplo, cuando el usuario no tiene privilegios para enviar paquetes en crudo o cuando se están sondeando redes IPv6. Nmap le pide al sistema operativo subyacente que establezcan una conexión con el sistema objetivo en el puerto indicado utilizando la llamada del sistema connect(), a diferencia de otros tipos de sondeo, que escriben los paquetes a bajo nivel. Ésta es la misma llamada del sistema de alto nivel que la mayoría de las aplicaciones de red, como los navegadores web o los clientes P2P, utilizan para establecer una conexión. Esta llamada es parte del interfaz de programación conocido como la API de conectores de Berkeley. También, en lugar de leer las respuestas directamente de la línea, Nmap utiliza esta API para obtener la información de estado de cada intento de conexión.

Generalmente es mejor utilizar un sondeo SYN, si éste está disponible. Nmap tiene menos control sobre la llamada de alto nivel Connect() que cuando utiliza paquetes en crudo, lo que hace que sea menos eficiente. La llamada al sistema completa las conexiones para abrir los puertos objetivo, en lugar de realizar el reseteo de la conexión medio abierta como hace el sondeo SYN. Esto significa que se tarda más tiempo y son necesarios más paquetes para obtener la información, pero también significa que los sistemas objetivos van a registrar probablemente la conexión. Un IDS decente detectará cualquiera de los dos, pero la mayoría de los equipos no tienen este tipo de sistemas de alarma. Sin embargo, muchos servicios de los sistemas UNIX habituales añadirán una nota en el syslog, y algunas veces con un mensaje de error extraño, dado que Nmap realiza la conexión y luego la cierra sin enviar ningún dato. Los servicios realmente patéticos morirán cuando ésto pasa, aunque esto no es habitual. Un administrador que vea muchos intentos de conexión en sus registros que provengan de un único sistema debería saber que ha sido sondeado con este método.

-sU (sondeos UDP)

Aunque la mayoría de los servicios más habituales en Internet utilizan el protocolo TCP, los servicios UDP también son muy comunes. Tres de los más comunes son los servicios DNS, SNMP, y DHCP (puertos registrados 53, 161/162, y 67/68 respectivamente). Dado que el sondeo UDP es generalmente más lento y más difícil que TCP, algunos auditores de seguridad ignoran estos puertos. Esto es un error, porque es muy frecuente encontrarse servicios UDP vulnerables y los atacantes no ignoran estos protocolos. Afortunadamente, Nmap puede utilizarse para hacer un inventario de puertos UDP.

El sondeo UDP se activa con la opción -sU. Puede combinarse con un tipo de sondeo TCP como el sondeo SYN (-sS) para comprobar ambos protocolos al mismo tiempo.

Los sondeos UDP funcionan mediante el envío (sin datos) de una cabecera UDP para cada puerto objetivo. Si se obtiene un error ICMP que indica que el puerto no es alcanzable (tipo 3, código 3) entonces se marca el puerto como cerrado. Si se recibe cualquier error ICMP no alcanzable (tipo 3, códigos 1, 2, 9, 10, o 13) se marca el puerto como filtrado. En algunas ocasiones se recibirá una respuesta al paquete UDP, lo que prueba que el puerto está abierto. Si no se ha recibido ninguna respuesta después de algunas retransmisiones entonces se clasifica el puerto como abierto|filtrado. Esto significa que el puerto podría estar abierto o que hay un filtro de paquetes bloqueando la comunicación. Puede utilizarse el sondeo de versión (-sV) para diferenciar de verdad los puertos abiertos de los filtrados.

Uno de las grandes problemas con el sondeo UDP es hacerlo rápidamente. Pocas veces llega una respuesta de un puerto abierto o filtrado, lo que obliga a expirar a Nmap y luego a retransmitir los paquetes en caso de que la sonda o la respuesta se perdieron. Los puertos cerrados son aún más comunes y son un problema mayor. Generalmente envían un error ICMP de puerto no alcanzable. Pero, a diferencia de los paquetes RST que envían los puertos TCP cerrados cuando responden a un sondeo SYN o Connect, muchos sistemas imponen una tasa máxima de mensajes ICMP de puerto inalcanzable por omisión. Linux y Solaris son muy estrictos con esto. Por ejemplo, el núcleo de Linux versión 2.4.20 limita la tasa de envío de mensajes de destino no alcanzable a uno por segundo (en net/ipv4/icmp.c).

Nmap detecta las limitaciones de tasa y se ralentiza para no inundar la red con paquetes inútiles que el equipo destino acabará descartando. Desafortunadamente, un límite como el que hace el núcleo de Linux de un paquete por segundo hace que un sondeo de 65536 puertos tarde más de 18 horas. Puede acelerar sus sondeos UDP incluyendo más de un sistema para sondearlos en paralelo, haciendo un sondeo rápido inicial de los puertos más comunes, sondeando detrás de un cortafuegos, o utilizando la opción --host-timeout para omitir los sistemas que respondan con lentitud.

-sN; -sF; -sX (sondeos TCP Null, FIN, y Xmas)

Estos tres tipos de sondeos (aunque puede hacer muchos más a través de la opción --scanflags que se describe en la próxima sección) aprovechan una indefinición en la

RFC de TCP que diferencia los puertos abiertos y cerrados. La página 65 dice que "si el estado del puerto [destino] es CERRADO .... un segmento entrante que contiene un RST hace que se envíe un RST en la respuesta." Después la página siguiente discute los paquetes que se envían a puertos abiertos sin fijar los bits SYN, RST, o ACK, diciendo: "es improbable que llegue aquí, pero si lo hace, debe descartar el segmento y volver."

Cuando se sondean sistemas que cumplen con el texto de esta RFC, cualquier paquete que no contenga los bits SYN, RST, o ACK resultará en el envío de un RST si el puerto está cerrado. Mientras que no se enviará una respuesta si el puerto está cerrado. Siempre y cuando se incluyan esos tres bits es válida la combinación de cualquiera de los otros tres (FIN, PSH, y URG). Nmap aprovecha esto con tres tipos de sondeo:

Sondeo Null(-sN)

No fija ningún bit (la cabecera de banderas TCP es 0)

sondeo FIN (-sF)

Solo fija el bit TCP FIN.

sondeo Xmas (-sX)

Fija los bits de FIN, PSH, y URG flags, iluminando el paquete como si fuera un árbol de Navidad.

Estos tres tipos de sondeos son exactamente los mismos en comportamiento salvo por las banderas TCP que se fijen en los paquetes sonda. Si se recibe un paquete RST entonces se considera que el puerto está cerrado. Si no se recibe ninguna respuesta el puerto se marca como cerrado|filtrado. El puerto se marca filtrado si se recibe un error ICMP no alcanzable (tipo 3, código 1, 2, 3, 9, 10, o 13).

La ventaja fundamental de este tipo de sondeos es que pueden atravesar algunos cortafuegos que no hagan inspección de estados o encaminadores que hagan filtrado de paquetes. Otra ventaja es que este tipo de sondeos son algo más sigilosos que, incluso, un sondeo SYN. Sin embargo, no cuente con que pase siempre esto ya que la mayoría de los productos IDS pueden configurarse para detectarlos. El problema es que no todos los sistemas siguen el estándar RFC 793 al pie de la letra. Algunos sistemas envían respuestas RST a las sondas independientemente de si el puerto está o no cerrado. Esto hace que la mayoría de los puertos se marquen como cerrados. Algunos sistemas operativos muy utilizados que hacen ésto son Microsoft Windows, muchos dispositivos Cisco, BSDI, e IBM OS/400. Este sondeo no funciona contra sistemas basados en UNIX. Otro problema de estos sondeos es que no se puede distinguir los puertos abiertos de algunos puertos filtrados, lo que resulta en la respuesta abierto|filtrado.

-sA (sondeo TCP ACK)

Este sondeo es distinto de otros que se han discutido hasta ahora en que no puede

determinar puertos abiertos (o incluso abiertos|filtrados). Se utiliza para mapear reglas de cortafuegos, y para determinar si son cortafuegos con inspección de estados y qué puertos están filtrados.

La sonda de un sondeo ACK sólo tiene fijada la bandera ACK (a menos que utilice --scanflags). Cuando se sondean sistemas no filtrados los puertos abiertos y cerrados devolverán un paquete RST. Nmap marca el puerto como no filtrado, lo que significa que son alcanzables por el paquete ACK, pero no se puede determinar si están abiertos o cerrados. Los puertos que no responden o que envían mensajes de error ICMP en respuesta (tipo 3, código 1, 2, 3, 9, 10, o 13), se marcan como filtrados.

-sW (sondeo de ventana TCP)

El sondeo de ventana («window», N. del T.) es exactamente igual al sondeo ACK que se aprovecha de un detalle de implementación de algunos sistemas que permite diferenciar puertos abiertos de los cerrados, en lugar de imprimir no filtrado cuando se devuelve un RST. Hace esto examinando el campo de ventana TCP del paquete RST devuelto. Algunos sistemas fijan un tamaño de ventana positivo para puertos abiertos (incluso para paquetes RST) mientras que se utiliza una ventana de tamaño cero para los cerrados. Así, en lugar de listar el puerto como no filtrado cuando se recibe un RST, el sondeo de ventana permite listar el puerto como abierto o cerrado en función de si el valor de la ventana TCP en ese paquete RST es positivo o cero, respectivamente.

Este sondeo depende de un detalle de implementación de una minoría de sistemas q que existen en Internet, así que no es siempre fiable. Los sistemas que no hacen ésto habitualmente harán que se muestren los puertos como cerrados. Por supuesto, es posible que el sistema no tenga ningún puerto abierto. Si la mayoría de los puertos están cerrados pero alguno de los números de puertos comunes (como pueda ser el 22, 25 ó 53) están filtrados, entonces el sistema es posible que sea susceptible a ésto. Algunas veces hay sistemas que mostrarán el comportamiento justo contrario. Si su sondeo muestra 1000 puertos abiertos y 3 puertos cerrados o filtrados entonces es posible que sean estos últimos los que están abiertos en realidad.

-sM (sondeo TCP Maimon)

El sondeo Maimon debe su nombre a la persona que lo descubrió: Uriel Maimon. Describió la técnica en la revista Phrack número 49 (noviembre de 1996). Nmap, que incluye esta técnica, se publicó dos números más tarde. Esta técnica es exactamente la misma a los sondeos Null, FIN, y Xmas, pero en los que se envía una sonda FIN/ACK. Según el RFC 793 (TCP), se debería generar un paquete RST cuando se responde a dicha sonda independientemente de si el puerto está cerrado o abierto. Uriel se dio cuenta, sin embargo, de que muchos sistemas derivados de BSD simplemente descartan el paquete si el puerto está abierto.

--scanflags (Sondeo TCP a medida)

Los usuarios realmente avanzados de Nmap no tienen por qué limitarse a los tipos de sondeos preparados que se ofrecen. La opción --scanflags le permite diseñar su

propio sondeo mediante la especificación de banderas TCP arbitrarias. Deje volar a su imaginación al tiempo que evita las reglas de los sistemas de detección de intrusos cuyos fabricantes sólo echaron un vistazo a la página de manual de Nmap y añadieron reglas específicas para detectarlo.

La opción --scanflags puede ser un valor numérico como el 9 (PSH y FIN), aunque es más sencillo utilizar nombres simbólicos. Sólo tienes que juntar una combinación de URG, ACK, PSH, RST, SYN, y FIN. Por ejemplo, la configuración --scanflags URGACKPSHRSTSYNFIN fija todas las banderas, aunque no es muy útil para sondear. No importa el orden en que se especifiquen los nombres.

Además de poder especificar las banderas que desee se puede especificar el tipo de sondeo TCP (como -sA o -sF). Ésto le dice a Nmap cómo debe interpretar las respuestas. Por ejemplo, un sondeo SYN considera que si no se recibe respuesta el puerto está filtrado mientras que si no se recibe una respuesta en un sondeo FIN se trata como abierto|filtrado. Nmap se comportará igual que para el sondeo tipo base, con la diferencia de que utilizará las banderas TCP que usted especifique. Se utiliza el sondeo SYN si no se especifica ningún tipo base.

-sI <sistema zombi [:puerto_sonda]> (Sondeo ocioso)

Este es un método de sondeo avanzado que le permite hacer un sondeo de puertos TCP a ciegas de verdad (lo que significa que no se envía ningún paquete al sistema objetivo desde su dirección IP real). En lugar de ésto se utiliza un ataque con un canal alternativo que se aprovecha de la generación de la secuencia de los identificadores de fragmentación IP del sistema zombi para obtener información de los puertos abiertos en el objetivo. Los sistemas IDS mostrarán que el sondeo lo está realizando el sistema zombi que especifique (que debe estar vivo y cumplir algunos requisitos). Este tipo de sondeo tan fascinante es demasiado complejo como para describirlo por completo en esta guía de referencia por lo que escribí y publiqué un documento informal que contiene todos los detalles, el documento está disponible en http://www.insecure.org/nmap/idlescan.html.

Además de ser extraordinariamente sigiloso (debido a su funcionamiento a ciegas), este tipo de sondeo permite determinar las relaciones basadas en IP entre distintos sistemas. El listado de puertos muestra los puertos abiertos *desde la perspectiva del sistema zombi.* Así que puede analizar el mismo objetivo con zombis distintos que cree que podrían ser de confianza para éste (a través de las reglas de filtrados de los paquetes o reglas de filtrados de encaminadores).

Puede añadir un número de puerto separado por dos puntos del sistema zombi si desea analizar un puerto específico del zombi para consultar los cambios IPID. Si no lo hace Nmap utilizará el puerto que utiliza para pings TCP por omisión (el puerto 80).

-sO (sondeo de protocolo IP)

El sondeo de protocolo IP le permite determinar qué protocolos (TCP, ICMP, IGMP, etc.) soportan los sistemas objetivo. Esto no es, técnicamente, un sondeo de puertos, dado que cambia los números de protocolo IP en lugar de los números de

puerto TCP ó UDP. Pero también se puede utilizar la opción -p para seleccionar los números de protocolo a analizar, los resultados se muestran en el formato de tabla utilizado para los puertos e incluso utiliza el mismo motor de sondeo que los métodos de sondeo de puertos reales. Es tan parecido a un sondeo de puertos que debe tratarse aquí.

El sondeo de protocolos, además de ser útil en sí mismo, demuestra el poder del software de fuentes abiertas («opensource», N. del T.). Aunque la idea fundamental era bastante sencilla, no había pensado añadirla ni tampoco había habido personas que solicitaran esta funcionalidad. Entonces, en el verano de 2000, se le ocurrió la idea a Gerhard Rieger y la implementó escribiendo un parche excelente, enviándolo posteriormente a la lista de correo de nmap-hackers. Incorporé ese parche en el árbol de código de Nmap y publiqué una nueva versión ese mismo día. ¡Pocas piezas de programas comerciales tienen usuarios tan entusiastas que diseñan y contribuyen sus propias mejoras!

El sondeo de protocolos utiliza mecanismos parecidos al sondeo UDP. Envía cabeceras de paquetes IP iterando por el campo de 8 bits que indica el protocolo IP, en lugar de iterar por el campo de número de puerto de un paquete UDP. Las cabeceras generalmente están vacías y no contienen datos. De hecho, ni siquiera tienen una cabecera apropiada para el protocolo que se indica. Las tres excepciones son TCP, UDP e ICMP. Se incluye una cabecera de protocolo válida para éstos porque algunos sistemas no los enviarán sin ellas y porque Nmap ya tiene funciones para crearlas. El sondeo de protocolos espera la recepción de mensajes de ICMP *protocolo* no alcanzable en lugar de mensajes ICMP puerto no alcanzable. Nmap marca el protocolo como abierto si recibe una respuesta en cualquier protocolo del sistema objetivo. Se marca como cerrado si se recibe un error ICMP de protocolo no alcanzable (tipo 3, código 2). Si se reciben otros errores ICMP no alcanzable (tipo 3, códigos 1, 3, 9, 10, o 13) se marca el protocolo como filtrado (aunque al mismo tiempo indican que el protocolo ICMP está abierto). El protocolo se marca como abierto|filtrado si no se recibe ninguna respuesta después de las retransmisiones.

-b <sistema de rebote ftp> (sondeo de rebote FTP)

Una funcionalidad interesante en el protocolo FTP (RFC 959) es la posibilidad de utilizar conexiones FTP de pasarela. Esta opción puede abusarse a muchos niveles así que muchos servidores han dejado de soportarla. Una de las formas de abusar de ésta es utilizar el servidor de FTP para hacer un sondeo de puertos a otro sistema. Simplemente hace falta decirle al servidor de FTP que envíe un fichero a cada puerto interesante del servidor objetivo cada vez. El mensaje de error devuelto indicará si el puerto está abierto o no. Esta es una buena manera de atravesar cortafuegos porque, habitualmente, los servidores de FTP de una organización están ubicados en un lugar en el que tienen más acceso a otros sistemas internos que el acceso que tiene un equipo en Internet. Nmap puede hacer sondeos con rebotes de FTP con la opción -b. Esta opción toma un argumento como: *usuario*:*contraseña*@*servidor*:*puerto*. *Servidor* es el nombre de la dirección IP del servidor FTP vulnerable. Al igual que con una URL normal, se puede omitir *usuario*:*contraseña*, en caso de que se deseen utilizar credenciales de acceso anónimo (usuario: anonymous contraseña:wwwuser@) También se puede omitir el número de puerto (y los dos puntos que lo preceden). Si se omiten se utilizará el

puerto FTP estándar (21) en *servidor*.

Esta vulnerabilidad era muy habitual en 1997, el año que se publicó Nmap, pero ya ha sido arreglada en muchos sitios. Aún siguen existiendo servidores vulnerables así que merece la pena probar este sondeo si lo demás falla. Si su objetivo es atravesar un cortafuegos, analice la red objetivo en busca del puerto 21 (o incluso cualquier servicio FTP, si sondea todos los puertos y activa la detección de versiones). Después intente un sondeo de rebote utilizando cada uno. Nmap le indicará si el sistema es o no vulnerable. Si está intentado ocultar sus huellas no tiene que (y de hecho no debería) limitarse a servidores en la red objetivo. En cualquier caso, antes de empezar a sondear Internet al azar para buscar servidores de FTP vulnerables, tenga en cuenta que pocos administradores de sistemas apreciarán el que abuse de sus servidores de esta forma.

Especificación de puertos y orden de sondeo

Nmap ofrece distintas opciones para especificar los puertos que se van a sondear y si el orden de los sondeos es aleatorio o secuencial. Estas opciones se añaden a los métodos de sondeos que se han discutido previamente. Nmap, por omisión, sondea todos los puertos hasta el 1024 además de algunos puertos con números altos listados en el fichero nmap-services para los protocolos que se sondeen.

-p <rango de puertos> (Sólo sondea unos puertos específicos)

Esta opción especifica los puertos que desea sondear y toma precedencia sobre los valores por omisión. Puede especificar tanto números de puerto de forma individual, así como rangos de puertos separados por un guión (p. ej. 1-1023). Puede omitir el valor inicial y/o el valor final del rango. Nmap utilizará 1 ó 65535 respectivamente. De esta forma, puede especificar -p- para sondear todos los puertos desde el 1 al 65535. Se permite sondear el puerto cero siempre que lo especifique explícitamente. Esta opción especifica el número de protocolo que quiere sondear (de 0 a 255) en el caso de que esté sondeando protocolos IP (-sO).

Puede especificar un protocolo específico cuando sondee puertos TCP y UDP si precede el número de puerto con T: o U:. El calificador dura hasta que especifique otro calificador. Por ejemplo, la opción -p U:53,111,137,T:21-25,80,139,8080 sondearía los puertos UDP 53,111, y 137, así como los puertos TCP listados. Tenga en cuenta que para sondear tanto UDP como TCP deberá especificar la opción -sU y al menos un tipo de sondeo TCP (como -sS, -sF, o -sT). Si no se da un calificador de protocolo se añadirán los números de puerto a las listas de todos los protocolos.

-F (Sondeo rápido (puertos limitados))

Indica que sólo quiere sondear los puertos listados en el fichero nmap-services que se incluye con nmap (o el fichero de protocolos si indica -sO). Esto es más rápido que sondear todos los 65535 puertos de un sistema. La diferencia de velocidad con el sondeo TCP por omisión (unos 1650 puertos) no es muy alta dado que esta lista contiene muchos puertos TCP (más de 1200). La diferencia puede ser muy grande si especifica su propio fichero nmap-services más pequeño si utiliza la opción --datadir.

-r (No aleatorizar los puertos)

> Nmap ordena de forma aleatoria los puertos a sondear por omisión (aunque algunos puertos comúnmente accesibles se ponen al principio por razones de eficiencia). Esta aleatorización generalmente es deseable, pero si lo desea puede especificar la opción `-r` para analizar de forma secuencial los puertos.

Detección de servicios y de versiones

Si le indica a Nmap que mire un sistema remoto le podrá decir que tiene abiertos los puertos 25/tcp, 80/tcp y 53/udp. Informará que esos puertos se corresponden habitualmente con un servidor de correo (SMTP), servidor de web (HTTP) o servidor de nombres (DNS), respectivamente, si utilizas su base de datos nmap-services con más de 2.200 puertos conocidos. Generalmente este informe es correo dado que la gran mayoría de demonios que escuchan en el puerto 25 TCP son, en realidad, servidores de correo. ¡Pero no debe confiar su seguridad en este hecho! La gente ejecuta a veces servicios distintos en puertos inesperados

Aún en el caso de que Nmap tenga razón y el servidor de ejemplo indicado arriba está ejecutando servidores de SMTP, HTTP y DNS ésto no dice mucho. Cuando haga un análisis de vulnerabilidades (o tan sólo un inventario de red) en su propia empresa o en su cliente lo que habitualmente también quiere saber es qué versión se está utilizando del servidor de correcto y de DNS. Puede ayudar mucho a la hora de determinar qué ataques pueden afectar a un servidor el saber el número de versión exacto de éste. La detección de versiones le ayuda a obtener esta información.

La detección de versiones pregunta para obtener más información de lo que realmente se está ejecutando una vez se han detectado los puertos TCP y/o UDP con alguno de los métodos de sondeo. La base de datos nmap-service-probes contiene sondas para consultar distintos servicios y reconocer y tratar distintas respuestas en base a una serie de expresiones. Nmap intenta determinar el protocolo del servicio (p. ej. ftp, ssh, telnet ó http), el nombre de la aplicación (p. ej. Bind de ISC, http de Apache, telnetd de Solaris), un número de versión, un tipo de dispositivo (p. ej. impresora o router), la familia de sistema operativo (p. ej. Windows o Linux) y algunas veces algunos detalles misceláneos como, por ejemplo, si un servidor X acepta cualquier conexión externa, la versión de protocolo SSH o el nombre de usuario Kazaa). Por supuesto, la mayoría de los servicios no ofrecen toda esta información. Si se ha compilado Nmap con soporte OpenSSL se conectará también a servidores SSL para determinar qué servicio escucha detrás de la capa de cifrado. Se utiliza la herramienta de pruebas RPC de Nmap (-sR) de forma automática para determinar el programa RPC y el número de versión si se descubren servicios RPC. Algunos puertos UDP se quedan en estado open|filtered (N. del T., 'abierto|filtrado') si un barrido de puertos UDP no puede determinar si el puerto está abierto o filtrado. La detección de versiones intentará obtener una respuesta de estos puertos (igual que hace con puertos abiertos) y cambiará el estado a abierto si lo consigue. Los puertos TCP en estado open|filtered se tratan de forma similar. Tenga en cuenta que la opción -A de Nmap actualiza la detección de versiones entre otras cosas. Puede encontrar un documento describiendo el funcionamiento, modo de uso, y particularización de la detección de versiones en http://www.insecure.org/nmap/vscan/.

Cuando Nmap obtiene una respuesta de un servicio pero no encuentra una definición coincidente en la base de datos se imprimirá una firma especial y un URL para que la

envíe si sabe lo que está ejecutándose detrás de ese puerto. Por favor, tómese unos minutos para enviar esta información para ayudar a todo el mundo. Gracias a estos envíos Nmap tiene ahora alrededor de 3.000 patrones para más de 350 protocolos distintos como smtp, ftp, http, etc.

La detección de versiones se activa y controla con la siguientes opciones:

-sV (Detección de versiones)

Activa la detección de versiones como se ha descrito previamente. Puede utilizar la opción -A en su lugar para activar tanto la detección de versiones como la detección de sistema operativo.

--allports (No excluir ningún puerto de la detección de versiones)

La detección de versiones de Nmap omite el puerto TCP 9100 por omisión porque algunas impresoras imprimen cualquier cosa que reciben en este puerto, lo que da lugar a la impresión de múltiples páginas con solicitudes HTTP get, intentos de conexión de SSL, etc. Este comportamiento puede cambiarse modificando o eliminando la directiva Exclude en nmap-service-probes, o especificando --allports para sondear todos los puertos independientemente de lo definido en la directiva Exclude.

--version-intensity <intensidad> (Fijar la intensidad de la detección de versiones)

Nmap envía una serie de sondas cuando se activa la detección de versiones (-sV) con un nivel de rareza preasignado y variable de 1 a 9. Las sondas con un número bajo son efectivas contra un amplio número de servicios comunes, mientras que las de números más altos se utilizan rara vez. El nivel de intensidad indica que sondas deberían utilizarse. Cuanto más alto sea el número, mayor las probabilidades de identificar el servicio. Sin embargo, los sondeos de alta intensidad tardan más tiempo. El valor de intensidad puede variar de 0 a 9. El valor por omisión es 7. Se probará una sonda independientemente del nivel de intensidad cuando ésta se registra para el puerto objetivo a través de la directiva nmap-service-probes ports. De esta forma se asegura que las sondas de DNS se probarán contra cualquier puerto abierto 53, las sondas SSL contra el puerto 443, etc.

--version-light (Activar modo ligero)

Éste es un alias conveniente para --version-intensity 2. Este modo ligero hace que la detección de versiones sea más rápida pero también hace que sea menos probable identificar algunos servicios.

--version-all (Utilizar todas las sondas)

Éste es un alias para --version-intensity 9, hace que se utilicen todas las sondas contra cada puerto.

--version-trace (Trazar actividad de sondeo de versiones)

Esta opción hace que Nmap imprima información de depuración detallada

explicando lo que está haciendo el sondeo de versiones. Es un conjunto de lo que obtendría si utilizara la opción --packet-trace.

-sR (Sondeo RPC)

Este método funciona conjuntamente con los distintos métodos de sondeo de puertos de Nmap. Toma todos los puertos TCP/UDP que se han encontrado y los inunda con órdenes de programa NULL SunRPC con el objetivo de determinar si son puertos RPC y, si es así, los programas y número de versión que están detrás. Así, puede obtener de una forma efectiva la misma información que **rpcinfo -p** aunque el mapeador de puertos («portmapper», N. del T.) está detrás de un cortafuegos (o protegido por TCP wrappers). Los señuelos no funcionan con el sondeo RPC actualmente. Esta opción se activa automáticamente como parte de la detección de versiones (-sV) si la ha seleccionado. Rara vez se utiliza la opción -sR dado que la detección de versiones lo incluye y es más completa.

Detección de sistema operativo

Uno de los aspectos más conocidos de Nmap es la detección del sistema operativo (SO) en base a la comprobación de huellas TCP/IP. Nmap envía una serie de paquetes TCP y UDP al sistema remoto y analiza prácticamente todos los bits de las respuestas. Nmap compara los resultados de una docena de pruebas como puedan ser el análisis de ISN de TCP, el soporte de opciones TCP y su orden, el análisis de IPID y las comprobaciones de tamaño inicial de ventana, con su base de datos nmap-os-fingerprints. Esta base de datos consta de más de 1500 huellas de sistema operativo y cuando existe una coincidencia se presentan los detalles del sistema operativo. Cada huella contiene una descripción en texto libre del sistema operativo, una clasificación que indica el nombre del proveedor (por ejemplo, Sun), el sistema operativo subyacente (por ejemplo, Solaris), la versión del SO (por ejemplo, 10) y el tipo de dispositivo (propósito general, encaminador, conmutador, consola de videojuegos, etc.).

Nmap le indicará una URL donde puede enviar las huellas si conoce (con seguridad) el sistema operativo que utiliza el equipo si no puede adivinar el sistema operativo de éste y las condiciones son óptimas (encontró al menos un puerto abierto y otro cerrado). Si envía esta información contribuirá al conjunto de sistemas operativos que Nmap conoce y la herramienta será así más exacta para todo el mundo.

La detección de sistema operativo activa, en cualquier caso, una serie de pruebas que hacen uso de la información que ésta recoge. Una de estas pruebas es la medición de tiempo de actividad, que utiliza la opción de marca de tiempo TCP (RFC 1323) para adivinar cuánto hace que un equipo fue reiniciado. Esta prueba sólo funciona en sistemas que ofrecen esta información. Otra prueba que se realiza es la clasificación de predicción de número de secuencia TCP. Esta prueba mide de forma aproximada cuánto de difícil es crear una conexión TCP falsa contra el sistema remoto. Se utiliza cuando se quiere hacer uso de relaciones de confianza basadas en la dirección IP origen (como es el caso de rlogin, filtros de cortafuegos, etc.) para ocultar la fuente de un ataque. Ya no se hace habitualmente este tipo de malversación pero aún existen muchos equipos que son vulnerables a ésta. Generalmente es mejor utilizar la clasificación en inglés como: “worthy challenge” («desafío difícil», N. del T.) o “trivial joke” («broma fácil», N. del T.). Esta información sólo se ofrece en la salida normal en el modo detallado (-v). También se informa de la generación de números de secuencia IPID cuando se activa el modo

detallado conjuntamente con la opción -O. La mayoría de los equipos estarán en la clase “incremental”, lo que significa que incrementan el campo ID en la cabecera IP para cada paquete que envían. Esto hace que sean vulnerables a algunos ataques avanzados de obtención de información y de falseo de dirección.

Puede encontrar un trabajo traducido a una docena de idiomas que detalla el modo de funcionamiento, utilización y ajuste de la detección de versiones en http://www.insecure.org/nmap/osdetect/.

La detección de sistema operativo se activa y controla con las siguientes opciones:

-O (Activa la detección de sistema operativo)

> Tal y como se indica previamente, activa la detección de sistema operativo. También se puede utilizar la opción -A para activar la detección de sistema operativo y de versiones.

--osscan-limit (Limitar la detección de sistema operativo a los objetivos prometedores)

> La detección de sistema operativo funcionará mejor si se dispone de un puerto TCP abierto y otro cerrado. Defina esta opción si no quiere que Nmap intente siquiera la detección de sistema operativo contra sistemas que no cumplan este criterio. Esta opción puede ahorrar mucho tiempo, sobre todo si está realizando sondeos -P0 sobre muchos sistemas. Sólo es de aplicación cuando se ha solicitado la detección de sistema operativo con la opción -O o -A.

--osscan-guess; --fuzzy (Aproximar los resultados de la detección de sistema operativo)

> Cuando Nmap no puede detectar un sistema operativo que encaje perfectamente a veces ofrecerá posibilidades que se aproximen lo suficiente. Las opciones tienen que aproximarse mucho al detectado para que Nmap haga esto por omisión. Cualquiera de estas dos opciones (equivalentes) harán que Nmap intente aproximar los resultados de una forma más agresiva.

Control de tiempo y rendimiento

Una de las prioridades durante el desarrollo de Nmap ha sido siempre el rendimiento. Un sondeo por omisión (**nmap *nombre_de_sistema***) de cualquier sistema en una red local tarda un quinto de segundo. Esto es menos que el tiempo que uno tarda en parpadear, pero se va sumando al tiempo que se tarda cuando se realiza un sondeo sobre decenas o centenares o miles de equipos. Además, ciertas opciones de sondeo como puedan ser el sondeo UDP y la detección de versiones pueden incrementar los tiempos de sondeos de forma sustancial. También puede afectar a este tiempo algunas configuraciones de sistemas cortafuegos, especialmente cuando implementan limitaciones a la tasa de respuestas. Aunque Nmap trabaja en paralelo y tiene muchos algoritmos avanzados para acelerar estos sondeos, el usuario tiene el control en última instancia de cómo funciona éste. Los usuarios con experiencia pueden definir las órdenes a Nmap cuidadosamente para obtener sólo la información que necesitan mientras que, al mismo tiempo, cumplen las limitaciones de tiempo que tengan.

Algunas técnicas que pueden ayudar a mejorar los tiempos de sondeo son el limitar el número de pruebas que no sean críticas y actualizar a la última versión de Nmap (se

hacen mejoras de rendimiento con cierta frecuencia). La optimización de los parámetros de control de tiempo pueden introducir también diferencias significativas. Las opciones aplicables se detallan a continuación.

Algunas opciones aceptan un parámetro tiempo. Este valor se especifica, por omisión, en milisegundos, aunque puede seguirlo de ‘s’, ‘m’, o ‘h’ para indicar segundos, minutos, u horas. Por tanto, el valor 900000, 900s, y 15m hacen exáctamente lo mismo al aplicarse a la opción --host-timeout.

--min-hostgroup <numsists>; --max-hostgroup <numsists> (Ajustar el tamaño del grupo para los sondeos paralelos)

Nmap tiene la capacidad de hacer un sondeo de puertos o versiones sobre múltiples sistemas en paralelo. Hace eso dividiendo el espacio de direcciones IP en grupos y analizando un grupo cada vez. Habitualmente es más eficiente utilizar grupos grandes. La contrapartida es que los resultados por sistema no se pueden dar hasta que se ha terminado de analizar todo el grupo. En este caso, si Nmap empezara con un tamaño de grupo de 50, el usuario no obtendría ningún resultado hasta que termine con los primeros 50 (excepto las actualizaciones que envía el modo detallado)

Nmap tiene una implementación de compromiso por omisión para resolver este conflicto. Empieza los sondeos con un tamaño de grupo inferior a cinco para que los primeros resultados se obtengan con rapidez y después se incrementa el tamaño de grupo hasta, como mucho, 1024. El número exacto por omisión depende de las opciones dadas en la ejecución. Nmap utiliza grupos más grandes para los sondeos UDP y para aquellos sondeos TCP con pocos puertos por razones de eficiencia.

Nmap nunca excede el tamaño indicado cuando éste se especifica con --max-hostgroup. Si se indica un valor mínimo en --min-hostgroup Nmap intentará mantener el tamaño de los grupos por encima de ese nivel. Nmap puede tener que utilizar grupos más pequeños si no hay suficientes sistemas objetivo en una interfaz dada para cumplir el mínimo especificado. Se pueden especificar ambos valores para mantener el tamaño de grupo dentro de un rango específico, aunque ésto es poco habitual.

El uso principal de esta opción es el de especificar el tamaño de grupo mínimo para que los sondeos se ejecuten más rápidamente. 256 es un valor habitual para sondear la red en trozos del tamaño de una clase C. Si se trata de un sondeo con muchos puertos no sirve de mucho incrementar ese número. Si los sondeos son de pocos puertos puede ayudar utilizar un tamaño de grupo de 2048 o más elementos.

--min-parallelism <numsondas>; --max-parallelism <numsondas> (Ajustar el número de sondas enviadas en paralelo)

Esta opción controla el número de sondas activas para un grupo de sistemas. Éstas se utilizan para los sondeos de puertos y el descubrimiento de equipos. Por omisión, Nmap calcula un valor ideal del número de sondas a enviar en paralelo basado en el rendimiento de la red. Si se pierden paquetes Nmap reduce este valor para ir más lento y permitir menos sondas activas. El valor ideal de las sondas se incrementará a medida que la red muestre que puede utilizarse de nuevo. Estas opciones ponen un

valor mínimo o máximo a esa variable. Por omisión, el valor ideal puede ser inferior a 1 si la red no es fiable e incrementarse a varios cientos si ésta funciona correctamente.

Lo más habitual es fijar el valor --min-parallelism a un número mayor que uno para que los sondeos contra sistemas o redes poco eficientes sean rápidos. Esta es una opción que tiene sus riesgos, ya que si se define un valor demasiado elevado se puede reducir la precisión del sondeo. Si se fija también se impide a Nmap controlar el paralelismo de forma dinámica basándose en las condiciones de la red. Un valor razonable puede ser diez, aunque sólo debe ajustarse como último recurso.

A veces se fija la opción --max-parallelism a uno para evitar que Nmap envíe más de una sonda a la vez a los sistemas. Esto puede ser útil conjuntamente con --scan-delay (del que se habla más adelante), aunque habitualmente es suficiente con utilizar este último por sí sólo.

--min-rtt-timeout <tiempo>, --max-rtt-timeout <tiempo>, --initial-rtt-timeout <tiempo> (Ajustar expiración de sondas)

Nmap mantiene un valor de expiración en ejecución para saber cuánto tiempo debe esperar para recibir la respuesta a una sonda o para retransmitir la sonda. Este valor está calculado en base a los tiempos de respuesta de las sondas previamente enviadas. El valor de expiración puede llegar a ser de varios segundos si se demuestra que la latencia de la red es significativa y variable. También empieza en un valor conservador (alto) y puede mantenerse en ese valor durante un tiempo cuando Nmap sondee equipos que no respondan.

Se pueden recortar los tiempos de análisis de forma apreciable si se especifican valores para --max-rtt-timeout y --initial-rtt-timeout por debajo de los de por omisión. Esto es especialmente verdadero en sondeos en los que no se envían paquetes ICMP (-P0) y en aquellos realizados en redes con mucho filtrado. Sin embargo, no se debería establecer a valores muy agresivos. El sondeo puede acabar tardando más de lo esperado si se especifica un valor bajo que hace que las sondas expiren y se retransmitan mientras está llegando la respuesta.

En el caso de que todos los sistemas estén en una red local al equipo que sondea, un valor razonablemente agresivo para --max-rtt-timeout es 100 milisegundos. Si se está rutando, primero envíe un ping a un equipo en la red con la herramienta ICMP ping, o con una herramienta para construir paquetes a medida como hping2 dado que es más probable que atraviese cualquier cortafuegos. Consulte el tiempo máximo de la ronda (tiempo entre solicitud y respuesta) después de haber enviado unos diez paquetes. Una vez obtenido ese valor puede utilizarlo el doble de éste para --initial-rtt-timeout y triplicarlo o cuadruplicarlo para --max-rtt-timeout. Yo no configuro habitualmente el valor máximo rtt por debajo de 100ms, independientemente del valor que den los ping. Ni tampoco lo pongo por encima de 1000ms.

La opción --min-rtt-timeout se utiliza rara vez, aunque puede ser útil cuando la red es tan poco fiable que incluso los valores por omisión son demasiado agresivos. Dado que Nmap sólo reduce el tiempo al mínimo cuando la red parece fiable este valor es

poco habitual y debería reportarse como una errata en la lista de correo nmap-dev.

--max-retries <reintentos> (Especifica el número máximo de sondas de puertos que se retransmiten)

Un puerto podría estar filtrado si Nmap no recibe ninguna respuesta a una sonda de análisis de puertos. O puede que la sonda o la respuesta a ésta se perdiera en la red. También puede darse el caso de que el sistema objetivo tenga una limitación de tasa de tráfico que haga que la respuesta quede bloqueada temporalmente. Así, Nmap lo intenta de nuevo retransmitiendo la sonda inicial. Puede que lo haga más de una vez, si Nmap detecta que hay problemas en el funcionamiento de la red, antes de abandonar los sondeos de un puerto. Cuando el rendimiento es crítico, se pueden acelerar los sondeos limitando el número de retransmisiones permitidas. Puede especificar --max-retries 0 para que no se haga ninguna retransmisión, aunque no se recomienda.

El valor por omisión (cuando no hay una plantilla -T) es permitir las retransmisiones. Nmap generalmente sólo hará una retransmisión si la red parece fiable y el sistema objetivo no tiene una limitación de tasa de tráfico. Es por esto por lo que la mayoría de los sondeos no se verán afectados si reduce el valor de --max-retries a un valor pequeño, como pudiera ser tres. Estos valores pueden hacer que los sondeos a equipos lentos (limitados en tasa) sean más rápidos. Puede que pierda información cuando Nmap dé por finalizado el análisis de un puerto antes de tiempo, aunque eso puede ser mejor que hacer que la expire el --host-timeout y se pierda toda la información del objetivo.

--host-timeout <tiempo> (Abandona equipos objetivo lentos)

Hay algunos equipos en los que simplemente se tarda *demasiado* en sondearlos. Esto puede deberse a hardware de red de bajo rendimiento o poco fiable o bien a software, limitaciones de tasas de paquetes o un cortafuegos demasiado restrictivo. Puede llegar a darse que Nmap dedica la mayor parte del tiempo de análisis en sondear un porcentaje reducido de sistemas. A veces es mejor reducir las bajas y saltarse esos sistemas inicialmente. Esto puede hacerse con la opción --host-timeout, indicando el tiempo máximo que está dispuesto a esperar. Yo especifico habitualmente 30m para asegurarse de que Nmap no gasta más de media hora en un solo sistema. Tenga en cuenta que Nmap puede estar sondeando otros equipos al mismo tiempo durante esa media hora, por lo que no se pierde todo ese tiempo. Cualquier sistema que expire se salta. No se imprimirá la tabla de puertos, la detección de sistema operativo o la detección de versiones para ese sistema.

--scan-delay <tiempo>; --max-scan-delay <tiempo> (Ajusta la demora entre sondas)

Esta opción hace que Nmap espere al menos el tiempo indicado entre cada sonda enviada a un sistema determinado. Esto es muy útil cuando se quiere limitar la tasa de tráfico. Los sistemas Solaris (entre otros) responderán a paquetes de sondeos UDP con sólo un mensaje ICMP por segundo. Enviar más que eso con Nmap sería perder el tiempo. Un valor de 1s para --scan-delay hará que Nmap se mantenga a esa velocidad reducida. Nmap intenta detectar limitaciones de tasa y ajustar la demora del sondeo como considere necesario, pero a veces viene bien especificarlo

de forma explícita si ya sabe qué valor es mejor.

El sondeo se ralentiza de forma drástica cuando Nmap incrementa el valor del tiempo de espera para poder tratar las limitaciones de tasa. Puede utilizar la opción --max_scan-delay para indicar el tiempo máximo de espera que permitirá Nmap. Si especifica un valor muy pequeño tendrá retransmisiones inútiles de paquetes y posiblemente no detecte puertos para los que el objetivo implemente tasas de tráfico estrictas.

También se puede usar --scan-delay para evitar sistemas de detección y prevención de intrusos (IDS/IPS) basados en umbrales.

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> (Fija una plantilla de tiempos)

Algunas personas encuentran confusos los controles de grano fino explicados previamente, aunque éstos sean muy potentes y efectivos. Además, se puede a veces tardar más tiempo en encontrar los valores más apropiados que en hacer el análisis que se quiere optimizar. Nmap ofrece un acercamiento más sencillo, basado en seis plantillas de tiempos. Puede especificar cualquiera de éstas con la opción -T seguido de un número o su nombre. Los nombre de las plantillas son: paranoico (0), sigiloso (1), amable (2), normal (3), agresivo (4) y loco (5) (respectivamente "paranoid", "sneaky", "polite", "normal", "aggressive" e "insane", N. de. T.). Las primeras dos se utilizan para evadir IDS. El modo amable reduce el sondeo para que éste utilice menos ancho de banda y menos recursos de los sistemas analizados. El modo normal es el valor por omisión, así que la opción -T3 no hace nada realmente. El modo agresivo hace que los sondeos sean más rápidos al asumir que está en una red razonablemente más rápida y fiable. En modo loco asume que está en una red extraordinariamente rápida o que está dispuesto a sacrificar fiabilidad por velocidad.

Estas plantillas permiten que el usuario especifique cuan agresivo quiere ser, al mismo tiempo que deja que sea Nmap el que escoja los valores exactos de tiempos. Las plantillas hacen también algunos ajustes menores de velocidad para los cuales no existe aún una opción de control de grano fino. Por ejemplo, -T4 prohíbe que la expiración en sondeos dinámicos exceda los 10ms para puertos TCP y -T5 limita ese valor a 5 milisegundos. Las plantillas pueden utilizarse combinadas con controles de grano fino, siempre que se especifique primero la plantilla. Si no lo hace así los valores especificados por la plantilla modificarán los valores que defina como opción. Le recomiendo utilizar -T4 cuando sondee redes razonablemente modernas y fiables. Mantenga esa opción al principio de la línea de órdenes aún cuando especifique otras opciones de control de grano fino para poder beneficiarse de las optimizaciones menores que activa.

Le recomiendo que empiece siempre con -T4 si está utilizando una conexión de banda ancha o conexión Ethernet decente. Algunas personas adoran la opción -T5 aunque es demasiado agresiva para mi gusto. Otras personas especifican la opción -T2 porque piensan que es menos probable que bloqueen sistemas o porque se consideran a sí mismos amables en general. Muchas veces no se dan cuenta de lo lenta que -T Polite es realmente. Su sondeo puede llegar a tardar diez veces más que un sondeo por omisión. Dado que las caídas de sistemas y problemas de ancho de banda son raros con las opciones de tiempos por omisión (-T3), lo recomiendo

habitualmente para las personas cuidadosas. Para reducir estos problemas es más efectivo omitir la detección de versiones que jugar con los valores de tiempos.

Mientras que puede ser útil evitar alarmas de IDS con -T0 y -T1, éste tardará mucho más tiempo para sondear miles de sistemas o puertos. Para este tipo de sondeos puede que prefiera fijar los valores exactos de tiempos que necesita antes que utilizar los valores predefinidos para -T0 y -T1.

Los efectos principales del uso de T0 es la serialización de los sondeos de forma que sólo se sondea un puerto cada vez, y se espera cinco minutos antes de enviar cada sonda. Las opciones T1 y T2 son similares pero sólo esperan 15 y 0.4 segundos entre sondas, respectivamente. El comportamiento por omisión de Nmap es T3, que incluye sondeos en paralelo. T4 es equivalente a especificar --max-rtt-timeout 1250 --initial-rtt-timeout 500 --max-retries 6 y fija el valor máximo para las demoras de sondeos TCP a 10 milisegundos. T5 hace lo mismo que --max-rtt-timeout 300 --min-rtt-timeout 50 --initial-rtt-timeout 250 --max-retries 2 --host-timeout 15m así como definir el valor máximo para las demoras de sondeos TCP a 5ms.

Evasión de cortafuegos/IDS y falsificación

Muchos pioneros de Internet habían previsto una red global abierta con un espacio de direcciones IP universal que permitiese conexiones virtuales entre dos nodos cualquiera. Esto permitiría a los equipos actuar como verdaderos iguales, sirviendo y recuperando información el uno del otro. La gente podría acceder a todos los sistemas de su casa desde el trabajo, cambiando las propiedades del control del clima o desbloqueando puertas. Esta visión de una conectividad universal fue sofocada por la escasez del espacio de direcciones y los problemas de seguridad. Al comienzo de la década de los años 90, las organizaciones empezaron a replegar cortafuegos con el propósito de reducir la conectividad. Se acordonaron redes enormes para protegerlas de la Internet no filtrada con pasarelas («proxies», N. del T.) de aplicación, sistemas de traducción de direcciones de red y filtros de paquetes. Del flujo sin restricciones de la información se pasó a una regulación estricta de los canales de comunicación aprobados y del contenido que pasa por ellos.

Los filtros de red como los cortafuegos pueden hacer muy difícil el análisis de una red. Esto no va a ser más fácil en el futuro, ya que uno de los objetivos de estos dispositivos es generalmente limitar el reconocimiento casual de la red. En cualquier caso, Nmap ofrece varias funcionalidades para ayudar a entender estas redes complejas, y que también sirven para verificar que los filtros funcionan como se espera de ellos. Incluso tiene mecanismos para saltarse las defensas que no hayan sido implementadas del todo correctamente. Uno de los mejores métodos de entender la posición de la seguridad de su red es intentar comprometerla. Empiece a pensar como un atacante, e intenta utilizar las técnicas de esta sección contra sus propias redes. Lance un sondeo de rebote FTP, un sondeo pasivo, un ataque de fragmentación, o intente realizar un túnel desde una de sus propias pasarelas.

Las compañías, además de restringir la actividad de red, están monitorizando cada vez más el tráfico con sistemas de detección de intrusos (IDS, «Intrusion Detection Systems», N. del T.). Todos los IDS principales vienen preinstalados con reglas diseñadas para detectar sondeos de Nmap porque, a veces, se realizan sondeos previos a un ataque. Muchos de estos productos han mutado recientemente para convertirse en sistemas de

prevención de intrusiones (IPS) que bloquean activamente el tráfico reconocido como maligno. Desafortunadamente para los administradores de redes y para los fabricantes de IDS es muy difícil detectar las malas intenciones analizando los datos de los paquetes. Los atacantes con paciencia, habilidad y con la ayuda de ciertas opciones de Nmap pueden, generalmente, esquivar el análisis de los IDS sin ser detectados. Mientras tanto, los administradores deben lidiar con un alto número de falsos positivos debido a que algunas actividades inocentes se diagnostican erróneamente y generan alarmas o se bloquean.

Algunas personas sugieren que Nmap no debería ofrecer funcionalidades de evasión de cortafuegos o para esquivar los IDS, argumentando que es igual de probable que las funcionalidades las utilicen los atacantes como que las utilicen los administradores para mejorar la seguridad. El problema con esta forma de pensar es que los atacantes van a utilizar estos métodos de todas formas: encontrarían otra herramienta para hacerlo o parchearían a Nmap para añadírsela. Al mismo tiempo, los administradores tendrían muchos más problemas para hacer su trabajo. Es mucho mejor defensa utilizar servidores FTP modernos y parcheados que intentar prevenir la distribución de herramientas que permitan la implementación de ataques de rebote FTP.

No hay ninguna herramienta mágica (u opción de Nmap) que permita detectar y evitar cortafuegos y sistemas IDS. Esto requiere habilidad y experiencia. Un tutorial va más allá del alcance de esta guía de referencia, que sólo lista las opciones relevantes y describe lo que hacen.

-f (fragmentar los paquetes); --mtu (utilizar el MTU especificado)

> La opción -f hace que el sondeo solicitado (incluyendo los sondeos ping) utilicen paquetes IP fragmentados pequeños. La idea es dividir la cabecera del paquete TCP entre varios paquetes para hacer más difícil que los filtros de paquetes, sistemas de detección de intrusos y otras molestias detecten lo que se está haciendo. ¡Tenga cuidado con esta opción! Algunos programas tienen problemas para manejar estos paquetes tan pequeños. El viejo sniffer llamado Sniffit da un fallo de segmentación inmediatamente después de recibir el primero de estos pequeños fragmentos. Especifica esta opción una sola vez y Nmap dividirá los paquetes en ocho bytes o menos después de la cabecera de IP. De esta forma, una cabecera TCP de veinte bytes se dividiría en 3 paquetes. Dos con ocho bytes de cabecera TCP y uno con los últimos ocho. Obviamente, cada fragmento tiene su propia cabecera IP. Especifica la opción -f otra vez para utilizar fragmentos de dieciséis bytes (reduciendo la cantidad de fragmentos). O puedes especificar tu propio tamaño con la opción --mtu. No utilice la opción -f si utiliza --mtu. El tamaño debe ser múltiplo de ocho. Aunque la utilización de paquetes fragmentados no le ayudará a saltar los filtros de paquetes y cortafuegos que encolen todos los fragmentos IP (como cuando se utiliza la opción CONFIG_IP_ALWAYS_DEFRAG del núcleo de Linux), algunas redes no pueden tolerar la pérdida de rendimiento que esto produce y deshabilitan esa opción. Otros no pueden habilitar esta opción porque los fragmentos pueden tomar distintas rutas para entrar en su red. Algunos sistemas defragmentan los paquetes salientes en el núcleo. Un ejemplo de ésto es Linux con el módulo de seguimiento de conexiones de iptables. Realice un sondeo con un programa de captura de tráfico, como Ethereal, para asegurar que los paquetes que se envían están fragmentándose. Intente utilizar la opción --send-eth, si su sistema operativo le está causando problemas, para saltarse la capa IP y enviar tramas directamente a la capa Ethernet en crudo.

-D <señuelo1 [,señuelo2][,ME],...> (Esconde un sondeo con señuelos)

Realiza un sondeo con señuelos. Esto hace creer que el/los equipo/s que utilice como señuelos están también haciendo un sondeo de la red. De esta manera sus IDS pueden llegar a informar de que se están realizando de 5 a 10 sondeos de puertos desde distintas direcciones IP, pero no sabrán qué dirección IP está realizando el análisis y cuáles son señuelos inocentes. Aunque esta técnica puede vencerse mediante el seguimiento del camino de los encaminadores, descarte de respuesta («response-dropping», N. del T.), y otros mecanismos activos, generalmente es una técnica efectiva para esconder su dirección IP.

Se debe separar cada equipo de distracción mediante comas, y puede utilizar ME («YO», N. del T.) como uno de los señuelos para representar la posición de su verdadera dirección IP. Si pone ME en la sexta posición o superior es probable que algunos detectores de sondeos de puertos habituales (como el excelente scanlogd de Solar Designer) ni siquiera muestren su dirección IP. Si no utiliza ME, Nmap le pondrá en una posición aleatoria.

Tenga en cuenta que los equipos que utilice como distracción deberían estar conectados o puede que accidentalmente causes un ataque de inundación SYN a sus objetivos. Además, sería bastante sencillo determinar qué equipo está realmente haciendo el sondeo si sólo uno está disponible en la red. Puede que quiera utilizar direcciones IP en lugar de nombres (de manera que no aparezca en los registros del servidor de nombres de los sistemas utilizados como señuelo).

Se utilizan los señuelos tanto para el sondeo de ping inicial (si se utiliza ICMP, SYN, ACK, o cualquier otro) como durante la fase de sondeo. También se utilizan los señuelos durante la detección de sistema operativo (-O). Los señuelos no funcionarán con la detección de versión o el sondeo TCP connect().

Vale la pena tener en cuenta que utilizar demasiados señuelos puede ralentizar el sondeo y potencialmente hacerlo menos exacto. Además, algunos proveedores de acceso a Internet filtrarán los paquetes falsificados, aunque hay muchos que no lo hacen.

-S <Dirección_IP> (Falsifica la dirección de origen)

Nmap puede que no sea capaz de determinar tu dirección IP en algunas ocasiones (Nmap se lo dirá si pasa). En esta situación, puede utilizar la opción -S con la dirección IP de la interfaz a través de la cual quieres enviar los paquetes.

Otro uso alternativo de esta opción es la de falsificar la dirección para que los objetivos del análisis piensen que *algún otro* los está sondeando. ¡Imagine una compañía a los que les sondea repetidamente la competencia! Generalmente es necesaria la opción -e si lo quiere utilizar así, y también sería recomendable la opción -P0.

-e <interfaz> (Utilizar la interfaz especificada)

Indica a Nmap a través de qué interfaz debe enviar y recibir los paquetes. Nmap

debería detectar esto automáticamente, pero se lo dirá si no.

--source-port <número_de_puerto>; -g <número_de_puerto> (Falsificar el puerto de origen)

Un error de configuración sorprendentemente común es confiar en el tráfico basándose únicamente en el número de puerto origen. Es fácil entender por qué pasa esto. Un administrador que está configurando su nuevo y flamante cortafuegos, recibe de repente quejas de todos sus usuarios desagradecidos que le dicen que sus aplicaciones han dejado de funcionar. En particular, puede romperse el DNS porque las respuestas UDP de DNS de servidores externos ya no pueden entrar en la red. Otro ejemplo habitual es el caso del FTP. En una transferencia activa de FTP, el servidor remoto intenta establecer una conexión de vuelta con el cliente para transferir el archivo solicitado.

Existen soluciones seguras para estos problemas, como las pasarelas en el nivel de aplicación o los módulos de cortafuegos que realizan un análisis del protocolo. Desgraciadamente, también hay soluciones más fáciles y menos seguras. Al darse cuenta que las respuestas de DNS vienen del puerto 53 y que las conexiones activas de FTP vienen del puerto 20, muchos administradores caen en la trampa de configurar su sistema de filtrado para permitir el tráfico entrante desde estos puertos. Generalmente asumen que ningún atacante se dará cuenta de estos agujeros en el cortafuegos ni los aprovechará. En otros casos, los administradores consideran esto una solución a corto plazo hasta que puedan implementar una solución más segura. Y después se olvidan de hacer la mejora de la seguridad.

Los administradores de red con mucho trabajo no son los únicos que caen en esta trampa. Muchos productos se lanzan al mercado con estas reglas inseguras. Hasta Microsoft lo ha hecho. Los filtros de IPsec que se preinstalan con Windows 2000 y Windows XP contienen una regla implícita que permite todo el tráfico TCP o UDP desde el puerto 88 (Kerberos). Otro caso conocido es el de las versiones de Zone Alarm Firewall Personal que, hasta la versión 2.1.25, permitían cualquier paquete entrante UDP desde el puerto 53 (DNS) o 67 (DHCP).

Nmap ofrece las opciones -g y --source-port (son equivalentes) para aprovecharse de estas debilidades. Simplemente indique el número de puerto y Nmap enviará los paquetes desde ese puerto cuando sea posible. Nmap debe utilizar distintos números de puerto para ciertos tipos de prueba en la detección de sistema operativo para que funcionen correctamente, y las solicitudes de DNS ignoran la opción --source-port porque Nmap depende de las librerías del sistema para hacerlas. Esta opción se soporta completamente en muchos sondeos TCP, incluyendo el sondeo SYN, al igual que los sondeos UDP.

--data-length <número> (Añadir datos aleatorios a los paquetes enviados)

Normalmente Nmap envía paquetes mínimos que contienen sólo la cabecera. Así, los paquetes TCP que envía son generalmente de 40 bytes y las solicitudes echo de ICMP son de tan sólo 28. Esta opción le dice a Nmap que añada el número indicado de bytes aleatorios a la mayoría de los paquetes que envía. Esta opción no afecta a los paquetes enviados para la detección de sistema operativo (-O), pero sí a la

mayoría de los paquetes de ping y de sondeo de puertos. Esta opción hace que el sondeo sea un poco más lento, pero también que el sondeo sea un poco más difícil de detectar.

--ttl <valor> (Indica el valor del campo tiempo-de-vida de la cabecera IP)

Establece el campo tiempo-de-vida («time-to-live», N. del T.) en la cabecera de los paquetes IPv4 al valor especificado.

--randomize-hosts (Mezclar aleatoriamente la lista de equipos a sondear)

Indica a Nmap que debe mezclar aleatoriamente cada grupo de hasta 8096 equipos antes de hacer un sondeo. Esto puede hacer que el sondeo sea menos obvio para algunos sistemas de monitorización de la red, especialmente cuando se combina con las opciones que ralentizan el sondeo. Si quiere mezclar aleatoriamente listas más grandes, incremente el valor de la constante PING_GROUP_SZ en nmap.h y recompile el programa. Una solución alternativa es generar la lista de sistemas a sondear con un sondeo de lista (-sL -n -oN *fichero*), ordenarlo aleatoriamente con un script de Perl, y luego darle a Nmap la lista entera con la opción -iL.

--spoof-mac <dirección MAC, prefijo o nombre del fabricante> (Falsifica la dirección MAC)

Solicita a Nmap que utilice la MAC dada para todas las tramas de Ethernet enviadas. Esta opción activa implícitamente la opción --send-eth para asegurar que Nmap envía los paquetes del nivel Ethernet. La MAC dada puede tener varios formatos. Nmap elegirá una MAC completamente aleatoria para la sesión si se utiliza el valor “0”. Nmap utilizará la MAC indicada si el parámetro es un número par de dígitos hexadecimales (separando opcionalmente cada dos dígitos con dos puntos). Nmap rellenará los 6 bytes restantes con valores aleatorios si se dan menos de 12 dígitos hexadecimales. Si el argumento no es ni 0 ni un conjunto de dígitos hexadecimales, Nmap mirará en nmap-mac-prefixes para encontrar un fabricante cuyo nombre coincida con el parámetro utilizado (en esta búsqueda no diferenciará entre mayúsculas y minúsculas). Si se encuentra algún fabricante, Nmap utilizará el OUI del fabricante (prefijo de 3 bytes) y rellenará los otros 3 bytes aleatoriamente. Ejemplos de argumentos --spoof-mac son: Apple, 0, 01:02:03:04:05:06, deadbeefcafe, 0020F2, y Cisco.

--badsum (Envía paquetes con sumas de comprobación TCP/UDP erróneas)

Esta opción le indica a Nmap que debe generar sumas de comprobación inválidas para los paquetes que se envíen a los equipos objetivos. Cualquier respuesta que se reciba vendrá de un cortafuegos o un IDS que no comprobó la suma, dado que la mayoría de las pilas IP descartan estos paquetes. Para obtener más información de esta técnica puede consultar http://www.phrack.org/phrack/60/p60-0x0c.txt

Salida

La utilidad de una herramienta de seguridad está limitada por la salida que genera. De poco sirven pruebas y algoritmos complejos si luego no se presentan de una forma organizada y comprensible. Dada la cantidad de formas en las que puede utilizarse Nmap,

tanto por personas como por otros programas, no es posible complacer a todos con un único formato. Por ello Nmap ofrece varios formatos, incluyendo el modo interactivo para que los humanos lo lean directamente y un formato XML para que sea interpretado por otros programas.

Además de ofrecer distintos formatos de salida, Nmap ofrece opciones adicionales para controlar cuanta información de más se muestra en la salida, así como opciones para controlar los mensajes de depuración que se muestran. Los tipos de salida pueden enviarse a la salida estándar o a algún archivo especificando su nombre. Nmap puede añadir información al archivo o sobreescribirlo. Los formatos de salida pueden utilizarse también para retomar un sondeo que se haya interrumpido.

Nmap puede generar la salida en cinco formatos distintos. El formato por omisión es el llamado salida interactiva, y se envía a la salida estándar («stdout»). También está la salida normal, que es similar a la salida interactiva salvo que muestra menos información de ejecución y menos advertencias, ya que se espera que se analice una vez que el sondeo haya terminado en lugar de ser analizada interactivamente.

La salida XML es uno de los formatos de salida más importantes, ya que puede convertirse a HTML, los programas (como la interfaz de usuario de Nmap) pueden interpretarla fácilmente o puede importarse a una base de datos.

Los dos tipos de salida restantes son la sencilla salida para grep (o «grepeable») que incluye la mayoría de la información de un sistema analizado en una sola línea, y la s4L1d4 sCRiPt KiDDi3 para usuarios que se consideran a sí mismos |<-r4d.

Aunque se utiliza la salida interactiva por omisión y no tiene ninguna opción de la línea de órdenes, los demás formatos utilizan la misma sintaxis. Toman un solo argumento, que es el archivo donde se guardarán los resultados. Pueden especificarse múltiples formatos al mismo tiempo, pero sólo puede especificar el mismo formato una vez. Por ejemplo, puede querer guardar la salida normal para su propia visualización mientras se guarda la información del mismo sondeo en formato XML para realizar un análisis posterior con un programa. Para hacer ésto debe utilizar las opciones -oX misondeo.xml -oN misondeo.nmap. Se recomienda utilizar nombres más descriptivos, si bien este capítulo utiliza nombres sencillos como misondeo.xml por razones de brevedad. Los nombres elegidos son una cuestión de preferencia personal. Yo utilizo nombres largos que incluyen la fecha del análisis y una palabra o dos describiendo el sondeo, dentro de un directorio con el nombre de la empresa que estoy analizando.

Nmap seguirá imprimiendo la salida interactiva en «stdout» como lo hace habitualmente aunque se guarden en archivos la salida con estas opciones. Por ejemplo, la orden **nmap -oX misondeo.xml destino** imprime XML en misondeo.xml y llena la salida estándar con los mismos resultados interactivos que habría impreso si no se hubiese especificado la opción -oX. Puedes cambiar este comportamiento dando un guión como argumento a una de las opciones de salida. Esto hace que Nmap desactive la salida interactiva y que imprima en su lugar los resultados en el formato especificado en la salida estándar. Con lo que la orden **nmap -oX - destino** enviará únicamente la salida XML a la salida estándar («stdout»). Los errores graves seguirán presentándose, posiblemente, en la salida normal de error, «stderr».

A diferencia de algunos argumentos de Nmap, es obligatorio separar con un espacio la opción de salida (como -oX) y el nombre del archivo o el guión. Si los omite y pone el argumento como -oG- o -oXsondeo.xml, una funcionalidad de compatibilidad con versiones anteriores hará que se cree una *salida normal* en los ficheros llamados G- y

Xscan.xml respectivamente.

Nmap también ofrece opciones para controlar la información extra que se ofrece sobre el sondeo y añadirlo a los archivos de salida en lugar de sobreescribirlos. Todas estas opciones se describen a continuación.

Formatos de salida de Nmap

-oN <filespec> (Salida normal)

Solicita que la salida normal sea redirigida al archivo especificado. Como se ha dicho anteriormente, esto difiere un poco de la salida interactiva.

-oX <filespec> (salida XML)

Solicita que la salida en XML se redirigida al archivo especificado. Nmap incluye un DTD que pueden utilizar los intérpretes de XML para validar la salida XML. Aunque está dirigida a que la utilicen programas, también puede ayudar a que una persona interprete la salida de Nmap. El DTD define los elementos legales del formato, y generalmente enumera los atributos y valores que pueden tener. La última versión está siempre disponible en http://www.insecure.org/nmap/data/nmap.dtd.

XML ofrece un formato estable que es fácilmente interpretado por cualquier programa. Hay intérpretes libres de XML para los lenguajes de ordenador más importantes, incluyendo C/C++, Perl, Python, y Java. La gente ha escrito librerías para la mayoría de estos lenguajes que manejan específicamente la salida de Nmap. Por ejemplo Nmap::Scanner y Nmap::Parser en el CPAN de Perl. XML es el formato preferente en la mayoría de los casos en que una aplicación no trivial quiere utilizar Nmap.

La salida de XML hace referencia a la hoja de estilo XSL que puede utilizarse para formatear los resultados en HTML. La forma más fácil de utilizarla es simplemente cargar la salida XML en un navegador web como Firefox o IE. Por omisión, ésto solo funcionará en el equipo en el que ejecutó Nmap (o uno configurado igual que dicho equipo) ya que la ruta de nmap.xsl se incluye directamente dentro del archivo. Puede utilizar la opción --webxml o --stylesheet para crear un XML portable que pueda mostrarse como HTML en cualquier ordenador conectado a la web.

-oS <filespec> (SaLiDa ScRipT KIdd|3)

La salida «script kiddie» es como la salida interactiva, excepto que se post-procesa para que la vean mejor los «l33t HaXXorZ» a los que antes no les gustaba Nmap por su uso consistente de mayúsculas y minúsculas. Aquellos que no tengan sentido del humor deberían tomar nota de que esta opción es una broma sobre los «script kiddies» antes de criticarme por “ayudarlos”.

-oG <filespec> (Salida «grepeable»)

Este formato de salida se trata el último porque está obsoleto. La salida en formato XML es mucho más poderosa, y es igual de conveniente para los usuarios experimentados. XML es un estándar para el que se dispone de docenas de intérpretes, mientras que la salida para grep es un «hack» propio. XML puede

extenderse para soportar nuevas funcionalidades de Nmap tan pronto como se liberen, mientras que en general tengo que omitir estas funcionalidades de la salida para grep por no tener un lugar donde ponerlas.

Sin embargo, la salida para grep es todavía bastante popular. Es simplemente un formato que lista cada sistema en una línea y que puede ser fácilmente tratado con herramientas estándar de UNIX como grep, awk, cut, sed, diff y Perl. Incluso yo la utilizo para pruebas rápidas que hago desde la línea de órdenes. Sólo hace falta un grep para identificar todos los sistemas con el puerto de ssh abierto o que ejecuten Solaris, enviando la salida a través de un conector a awk o cut para mostrar los campos deseados.

La salida para grep consiste en comentarios (líneas que empiezan por una almohadilla, «#») y líneas de objetivo. Una línea de objetivo incluye una combinación de seis campos marcados, separados por tabulaciones y seguidos de dos puntos. Los campos (en inglés) son Host (Sistema), Ports (Puertos), Protocols (Protocolos), Ignored State (Estado omitido), OS (Sistema operativo), Seq Index (índice de secuencia), IPID, y Status (Estado).

El campo más importante de todos habitualmente es Ports, que es el que da los detalles de cada puerto interesante encontrado. Consiste en una lista separada por comas de entradas de puerto. Cada entrada de puerto representa uno de los puertos de interés y se muestra con siete subcampos separados por una barra («/»). Los subcampos son: Port number (Número de puerto), State (Estado), Protocol (Protocolo), Owner (Propietario), Service (Servicio), SunRPC info (Información SunRPC), y Version info (Información de versión).

Esta página de manual, al igual que en el caso de la salida XML, no puede incluir la documentación completa de este formato. Puede encontrar más información detallada de la salida de Nmap para grep en http://www.unspecific.com/nmap-oG-output.

-oA <nombre_base> (Salida en todos los formatos)

Por comodidad, puede especificar la opción -oA *nombre_base* para guardar los resultados de los sondeos en *nombre_base*.nmap, *nombre_base*.xml, y *nombre_base*.gnmap, respectivamente. Al igual que la mayoría de los programas puede poner un prefijo con la ruta del directorio como pudiera ser ~/registros_nmap/empresa_foo/ en UNIX o c:\hacking\sco en Windows.

Opciones de depuración y de detalle

-v (Incrementa el nivel de detalle)

Hace que Nmap imprima más información sobre el sondeo que está realizando incrementando el nivel de detalle. Los puertos abiertos se muestran en cuanto se encuentran y se muestra una estimación del tiempo que Nmap espera que dure la tarea de sondeo si piensa que va a durar más de un par de minutos. Puede utilizarlo dos veces para obtener aún más detalle. No tiene ningún efecto el utilizarlo más de dos veces.

La mayoría de los cambios sólo afectan a la salida interactiva, y algunos también afectan a la salida «script kiddie». Dado que los demás formatos van a ser tratados por programas, Nmap da información detallada en estos formatos por omisión sin fatigar a un usuario humano. Sin embargo, hay algunos cambios en los otros modos que hacen que el tamaño de la salida resultante se reduzca sustancialmente al omitir información detallada. Por ejemplo, sólo se imprime una línea de comentario con todos los puertos sondeados en el formato de salida para grep si se activa el modo de detalle, porque puede ser demasiada información.

-d [level] (Incrementar o fijar el nivel de depuración)

Cuando no obtiene suficientes datos ni siquiera con el modo de detalle, ¡puede utilizar el modo de depuración para inundarse de detalles! Al igual que con la opción de detalle (-v), puede activar la depuración con una opción en la línea de órdenes (-d). Puede incrementar el nivel de depuración si la especifica múltiples veces. También puede fijar directamente el nivel de depuración si da un argumento a la opción -d. Por ejemplo, si utiliza -d9 se fijaría el nivel de depuración en el nueve. Ese es el nivel más alto de depuración y provocará que se impriman miles de líneas a no ser que haga sondeos muy sencillos con pocos puertos y objetivos.

La salida de depuración es útil cuando sospecha que hay un fallo en Nmap o simplemente si está confundido y quiere saber qué hace Nmap y por qué. Las líneas de depuración no son auto-explicativas, dado que esta función está dirigida a los desarrolladores. Puede obtener algo como esto: Timeout vals: srtt: -1 rttvar: -1 to: 1000000 delta 14987 ==> srtt: 14987 rttvar: 14987 to: 100000. Su único recurso si no entiende una línea es ignorarla, buscarla en el código fuente, o solicitar ayuda en la lista de desarrolladores (nmap-dev). Algunas líneas sí son auto-explicativas, pero los mensajes se vuelven más y más extraños a medida que se incrementa el nivel de depuración.

--packet-trace (Trazar paquetes y datos enviados y recibidos)

Esta opción hace que Nmap imprima un resumen de cada paquete que envía o recibe. Esto se utiliza muchas veces para poder depurar el programa, pero también es útil para los usuarios nuevos que quieren entender exactamente que es lo que hace Nmap bajo el capó. Puede especificar un número reducido de puertos para evitar que se impriman miles de líneas, como por ejemplo -p20-30. Si sólo está interesado en el funcionamiento del subsistema de detección de versiones debe utilizar la opción --version-trace.

--iflist (Listar interfaces y rutas)

Imprime la lista de interfaces y las rutas del sistema tal y como las detecta Nmap. Esta opción es útil para depurar problemas de enrutamiento o caracterizaciones equivocadas del tipo de interfaz (como por ejemplo, cuando Nmap trata una conexión PPP como una interfaz Ethernet).

Opciones misceláneas de salida

--append-output (Añadir en lugar de borrar los archivos de salida)

El fichero especificado como salida de un formato como pueda ser -oX or -oN se sobreescribe por omisión. Si prefiere mantener el contenido existente y añadir los nuevos resultados tendrá que especificar la opción --append-output. La información obtenida se añadirá a los ficheros especificados en esa ejecución de Nmap en lugar de sobreescribirlos. Esto no funciona bien para los ficheros de salida XML (-oX) ya que el fichero resultante no se podrá leer correctamente, por regla general, hasta que lo arregle manualmente.

--resume <nombre_archivo> (Continuar un sondeo detenido)

Algunas ejecuciones de Nmap tardan mucho tiempo, del orden de días. Esos sondeos no siempre se ejecutan hasta el final. Es posible que haya restricciones que impidan los sondeos de Nmap durante la jornada laboral, se puede caer la red o el sistema donde se está ejecutando Nmap puede sufrir un reinicio esperado o uno no planificado, o incluso es posible que Nmap aborte. El administrador que está ejecutando Nmap podría cancelarlo también por cualquier otra razón, simplemente pulsando **ctrl-C**. En estos casos puede no desearse empezar el sondeo completo desde el principio. Afortunadamente, si se ha guardado una salida normal (-oN) o para tratarla con grep (-oG), el usuarios puede pedir a Nmap que continúe el sondeo con el objetivo en el que estaba trabajando cuando se detuvo la ejecución. Simplemente se tiene que especificar la opción --resume y dar un archivo de salida normal o «grepeable» como argumento. No se puede dar ningún otro argumento, ya que Nmap trata el archivo para utilizar las mismas opciones que se especificaron entonces. Sólo se debe llamar a Nmap con **nmap --resume *archivo_de_registro***. Nmap añadirá cualquier resultado nuevo a los ficheros de datos especificados en la ejecución previa. No se soporta la capacidad de reanudar un sondeo con el formato de salida XML porque combinar dos salidas en un sólo fichero XML válido sería difícil.

--stylesheet <ruta o URL> (Fija la hoja de estilo XSL para transformar la salida XML)

Nmap se distribuye conjuntamente con una hoja de estilo XSL llamada nmap.xsl para poder ver o traducir la salida XML a HTML. La Salida XML incluye una directiva xml-stylesheet que apunta al punto donde está instalado nmap.xml (o al directorio de trabajo actual en Windows). Para mostrar los resultados basta cargar la salida XML en un navegador de web moderno y éste recogerá y utilizará el archivo nmap.xsl del sistema de ficheros. Si quiere especificar una hoja de estilo diferente, tiene que especificarla como argumento a la opción --stylesheet. Puede dar una ruta completa o un URL. Una forma habitual de llamar a esta opción es la siguiente: --stylesheet http://www.insecure.org/nmap/data/nmap.xsl. Esto le dice al navegador que descargue la última versión de la hoja de estilo de Insecure.Org. La opción --webxml hace lo mismo pero con menos teclas y es más fácil de recordar. Esto facilita la visualización de resultados en un sistema que no tiene Nmap instalado (y que por tanto carece de un archivo nmap.xsl). Así, la URL es lo más útil, pero se utiliza el sistema de ficheros local para el archivo nmap.xsl por omisión por razones de privacidad.

--webxml (Carga la hoja de estilo de Insecure.Org)

Esta opción es simplemente un alias para --stylesheet

http://www.insecure.org/nmap/data/nmap.xsl.

--no_stylesheet (Omite la declaración de hoja de estilo XSL del XML)

Puede utilizar esta opción para evitar que Nmap asocie una hoja de estilo XSL a su salida XML. En este caso, se omite la directiva xml-stylesheet de la salida.

Opciones misceláneas

Esta sección describe algunas opciones importantes (y no tan importantes) que no encajan realmente en ningún otro sitio.

-6 (Activa el sondeo IPv6)

Nmap tiene soporte IPv6 para la mayoría de sus funcionalidades más populares desde 2002. En particular, tiene soporte de: sondeo ping (TCP-only), sondeo connect() y detección de versiones. La sintaxis de las órdenes es igual que las habituales salvo que debe especificar la opción -6 Por supuesto, debe utilizarse la sintaxis IPv6 si se indica una dirección en lugar de un nombre de sistema. Una dirección IPv6 sería parecida a 3ffe:7501:4819:2000:210:f3ff:fe03:14d0, por lo que se recomienda utilizar nombres de equipo. La salida es igual que en los otros casos. Lo único que distingue que esta opción está habilitada es que se muestran las direcciones IPv6 en la línea que indica los “puertos de interés”.

Aunque IPv6 no se está utilizando en todo el mundo, sí que se utiliza mucho en algunos países (generalmente asiáticos) y muchos sistemas operativos modernos lo soportan. Tanto el origen como el objetivo de su sondeo deben estar configurados para utilizar IPv6 si desea utilizar Nmap con IPv6. Si su ISP (como sucede con la mayoría) no le da direcciones IPv6, puede encontrar gestores de túneles gratuitos en muchos sitios y funciona bien con Nmap. Uno de los mejores lo gestiona BT Exact en https://tb.ipv6.btexact.com/. También he utilizado el que Hurricane Electric ofrece en http://ipv6tb.he.net/. Los túneles IPv6 a IPv4 («6to4») son también otro método muy popular y gratuito .

-A (Opciones de sondeos agresivos)

Esta opción activa algunas opciones avanzadas y agresivas. Aún no he decidido qué significa exactamente. Actualmente esto activa la detección de sistema operativo (-O) y el análisis de versiones (-sV). Aunque se añadirán más opciones en el futuro. La idea es que esta opción active un conjunto de opciones para evitar que los usuarios de Nmap tengan que recordar un número de opciones muy elevado. Esta opción sólo activa funcionalidades, no afecta a las opciones de temporización (como -T4) o de depuración (-v) que quizás desee activar también.

--datadir <nombre_directorio> (Indica la ubicación de un archivo de datos de Nmap)

Nmap obtiene algunos datos especiales al ejecutarse de los archivos llamados nmap-service-probes, nmap-services, nmap-protocols, nmap-rpc, nmap-mac-prefixes, y nmap-os-fingerprints. Nmap buscará primero estos ficheros en el directorio que se especifique con la opción --datadir (si se indica alguno). Los

archivos que no se encuentren allí se buscarán en el directorio especificado por la variable de entorno NMAPDIR. A continuación se buscará en ~/.nmap tanto para el identificador (UID) real como el efectivo (sólo en sistemas POSIX) o la ubicación del ejecutable de Nmap (sólo sistemas Win32), y también en una ubicación compilada en la aplicación como pudiera ser /usr/local/share/nmap o /usr/share/nmap. Nmap, por último, buscará en el directorio actual.

--send-eth (Enviar tramas Ethernet en crudo)

Le indica a Nmap que debe enviar paquetes en la capa Ethernet en crudo (enlace de datos) en lugar de en la capa IP (red). Por omisión, Nmap elegirá cuál utilizar en función de lo que sea mejor para la plataforma donde esté ejecutándose. Los sockets crudos (capa IP) son generalmente más eficientes para sistemas UNIX, mientras que las tramas Ethernet son necesarias en sistemas Windows ya que Microsoft deshabilitó el soporte de sockets crudos. Nmap seguirá utilizando paquetes IP crudos en UNIX, aunque se especifique esta opción, cuando no se pueda hacer de otra forma (como es el caso de conexiones no Ethernet).

--send-ip (Enviar al nivel crudo IP)

Indica a Nmap que debe enviar utilizando sockets IP crudos en lugar de enviar tramas Ethernet de bajo nivel. Esta opción es complementaria a la opción --send-eth descrita previamente.

--privileged (Asumir que el usuario tiene todos los privilegios)

Esta opción le dice a Nmap que simplemente asuma que el usuario con el que se ejecuta tiene suficientes privilegios para trabajar con sockets crudos, capturar paquetes y hacer otras operaciones similares que generalmente sólo puede hacerla en sistemas UNIX el usuario root. Por omisión, Nmap aborta si se han solicitado esas operaciones pero el resultado de geteuid() no es cero. La opción --privileged es útil con las capacidades del núcleo Linux y sistemas similares que pueden configurarse para permitir realizar sondeos con paquetes crudos a los usuarios no privilegiados. Asegúrese de indicar esta opción antes de cualquier otra opción que pueda requerir de privilegios específicos (sondeo SYN, detección de SO, etc.). Una forma alternativa a --privileged es fijar la variable de entorno NMAP_PRIVILEGED.

--interactive (Comienza en modo interactivo)

Comienza Nmap en modo interactivo. En este modo, Nmap ofrece un indicador interactivo que facilita el lanzamiento de múltiples sondeos (tanto síncronos como en segundo plano). Es útil para aquellas personas que tienen que sondear desde sistemas multi-usuario, ya que generalmente quieren hacer un análisis de seguridad sin que los demás usuarios sepan exactamente qué sistemas se están analizando. Puede utilizar la opción --interactive para activar este modo y después utilizar **h** para obtener la ayuda. Esta opción se utiliza muy poco porque los intérpretes de línea de órdenes habituales son mucho más cómodos y tienen más funciones. Esta opción incluye un operador de exclamación («!») para ejecutar órdenes de la shell, que es una de las muchas razones por las que Nmap no se debe instalar con el bit «setuid» de root.

-V; --version (Mostrar el número de versión)

Imprime el número de versión de Nmap y aborta.

-h; --help (Mostrar la página resumen de ayuda)

Imprime una pequeña pantalla de ayuda con las opciones de órdenes más habituales. Pasa lo mismo si ejecuta Nmap sin argumentos.

Ejecución interactiva

Todas las pulsaciones de teclado se capturan durante la ejecución de Nmap. Esto le permite interactuar con el programa sin abortarlo ni reiniciarlo. Algunas teclas especiales cambiarán las opciones mientras que otras teclas imprimirán un mensaje de estado informándole del estado del sondeo. La convención es que las *letras en minúsculas incrementan* la cantidad de información que se imprime, mientras que las *letras en mayúsculas reducen* la información impresa. También puede pulsar '*?*' para obtener ayuda.

v / V

Incrementa / Reduce el detalle (más / menos verboso)

d / D

Incrementa / Reduce el nivel de depuración

p / P

Activa / Desactiva la traza de paquetes

?

Imprime la pantalla de ayuda de la ejecución interactiva

Cualquier otra tecla

Imprime un mensaje de estado similar a ésta:

Stats: 0:00:08 elapsed; 111 hosts completed (5 up), 5 undergoing Service Scan

Service scan Timing: About 28.00% done; ETC: 16:18 (0:00:15 remaining)

Ejemplos

A continuación se muestran algunos ejemplos de utilización, desde lo más simple y rutinario hasta algo más complejo y esotérico. Se utilizan algunas direcciones IP y dominios para concretar un poco las cosas. En su lugar deberías poner las direcciones o nombres de *tu propia red.*. Mientras que yo no considero que sondear los puertos de otras redes es o debería ser ilegal, algunos administradores de redes no aprecian un sondeo no solicitado de sus redes y pueden quejarse. Lo mejor es pedir permiso primero.

A modo de prueba, tienes permiso de sondear el servidor scanme.nmap.org. Este permiso sólo incluye sondear mediante Nmap y no para probar "exploits" o ataques de denegación de servicio. Por favor, para conservar el ancho de banda no inicie más de una docena de sondeos contra este servidor el mismo día. Si se abusa de este servicio de sondeo se desconectará y Nmap reportará Failed to resolve given hostname/IP: scanme.nmap.org ("No se pudo resolver la dirección IP o nombre datos: scanme.nmap.org"). Este permiso también se aplica a los servidores analizame2.nmap.org, analizame3.nmap.org, y así sucesivamente, aunque esos servidores actualmente no existen.

nmap -v scanme.nmap.org

Esta opción sondea todos los puertos TCP reservados en el servidor scanme.nmap.org. La opción -v activa el modo detallado (también llamado verboso).

nmap -sS -O scanme.nmap.org/24

Lanza un sondeo de tipo SYN sigiloso contra cada una de las 255 máquinas en la “clase C” de la red donde está el sistema "analizame". También intenta determinar cual es el sistema operativo que se ejecuta en cada máquina que esté encendida. Esto requiere permisos de root por la opción de sondeo SYN y por la de detección de sistema operativo.

nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127

Lanza una enumeración de equipos y un sondeo TCP a cada uno de la primera mitad de las 255 posibles subredes de 8 bit en la red de clase B 198.116. Esto probará si los sistemas están ejecutando sshd, DNS, pop3d, imapd o tienen un servidor en el puerto 4564. Para cualquier puerto que se encuentre abierto, se realizará una detección de versión para determinar qué aplicación se está ejecutando.

nmap -v -iR 100000 -P0 -p 80

Solicita a Nmap que elija 100.000 sistemas aleatoriamente y los sondee buscando servidores web (puerto 80). La enumeración de sistemas se deshabilita con -P0 ya que es un desperdicio enviar un par de pruebas para determinar si el sistema debe ser analizado cuando de todas maneras sólo se va a analizar un puerto.

nmap -P0 -p80 -oX logs/pb-port80scan.xml -oG logs/pb-port80scan.gnmap 216.163.128.20/20

Esto sondea 4096 IPs para buscar cualquier servidor web (sin enviar sondas ICMP) y guarda la salida en formato para grep y en XML.

Fallos

Al igual que su autor, Nmap no es perfecto. Pero tu puedes ayudar a hacerlo mejor enviando informes de fallo o incluso escribiendo parches. Si Nmap no se comporta como tú esperas, primero actualiza a la última versión disponible en

http://www.insecure.org/nmap/. Si el problema persiste, investiga para determinar si la causa ya ha sido descubierta y solucionada. Busca en Google el mensaje de error o navega en los archivos de Nmap-dev en http://seclists.org/. También deberías leer este manual completo. Si esto no te ayuda, envía un informe de error en inglés a <nmap-dev@insecure.org>. Por favor, incluya todo lo que haya visto del problema, así como qué versión de Nmap está utilizando y sobre qué versión del sistema operativo está trabajando. Hay muchas más probabilidades de que un informe de fallo o una pregunta sobre el uso de Nmap se contesten si se envían a nmap-dev@insecure.org que si se envían directamente a Fyodor.

Es mejor enviar parches para arreglar el código que un informe de error. Puedes encontrar las instrucciones básicas para crear parches con sus cambios en http://www.insecure.org/nmap/data/HACKING. Puede enviar los parches a nmap-dev (recomendado) o directamente a Fyodor.

Autor

Fyodor <fyodor@insecure.org> (http://www.insecure.org)

Cientos de personas han realizado valiosas contribuciones a Nmap a lo largo de los años. Sus nombres se detallan en el archivo CHANGELOG que se distribuye conjuntamente con Nmap y que está también disponible en http://www.insecure.org/nmap/changelog.html.

Notas legales

Unofficial Translation Disclaimer / Descargo de traducción no oficial

This is an unnofficial translation of the Nmap license details into Spanish. It was not written by Insecure.Com LLC, and does not legally state the distribution terms for Nmap -- only the original English text does that. However, we hope that this translation helps Spanish speakers understand the Nmap license better.

Esta es una traducción no oficial de los detalles de la licencia de Nmap details al español. Esta traducción no ha sido escrita por Insecure.Com LLC por lo que no refleja legalmente los términos de distribución de Nmap, eso sólo puede hacerlo el texto original en inglés. Esperamos, sin embargo, que esta traducción pueda ayudar a aquellas personas que hablan español a entender mejor la licencia de Nmap.

Licencia y copyright de Nmap

The Nmap Security Scanner is (C) 1996-2005 Insecure.Com LLC. Nmap is also a registered trademark of Insecure.Com LLC. This program is free software; you may redistribute and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; Version 2. This guarantees your right to use, modify, and redistribute this software under certain conditions. If you wish to embed Nmap technology into proprietary software, we may be willing to sell alternative licenses (contact <sales@insecure.com>). Many security scanner vendors already license Nmap technology such as host discovery, port scanning, OS detection, and service/version detection.

Traducción no autorizada: La herramienta de sondeos de seguridad Nmap es (C)

1996-2005 Insecure.Com LLC. Nmap también es una marca registrada por Insecure.Com LLC. Este programa es software libre. Puede redistribuirlo y/o modificarlo bajo los términos de la Licencia Pública General de GNU según es publicada por la Free Software Foundation, versión 2. Esto garantiza su derecho a utilizarla, modificarla y redistribuirla bajo ciertas condiciones. Si desea introducir la tecnología de Nmap en programas propietarios podemos vender licencias alternativas (póngase en contacto con <sales@insecure.com>). Hay muchos fabricantes de herramientas de análisis de seguridad que licencian la tecnología de Nmap como es el descubrimiento de equipos, sondeos de puertos, detección de sistema operativo y detección de servicios y versiones.

Tenga en cuenta que la GPL impone restricciones importantes en los “trabajos derivados”, pero no ofrece una definición precisa de ese término. Para evitar malentendidos, a continuación se definen, para los propósitos de esta licencia, las condiciones bajo las que una aplicación constituye un “trabajo derivado”:

- Integra código fuente de Nmap
- Lee o incluye los ficheros de Nmap que están bajo derechos de copia, eso incluye nmap-os-fingerprints o nmap-service-probes.
- Ejecuta Nmap y analiza los resultados (en contraposición del intérprete de órdenes típico o la ejecución desde un menú, que simplemente muestra la salida de Nmap en crudo y no son, por tanto, trabajos derivados)
- Integra o incluye o agrega Nmap en un instalador ejecutable propietario, como los que produce InstallShield.
- Enlaza a una librería o ejecuta un programa que hace cualquiera de las cosas descritas anteriormente.

Se debe considerar que el término “Nmap” incluye las porciones o trabajos derivados de Nmap. Esta lista no es exclusiva, su único objetivo es clarificar la interpretación de trabajos derivados con algunos ejemplos comunes. Estas restricciones no se aplican cuando redistribuye Nmap. Por ejemplo, nada le impide escribir y vender una interfaz propietaria a Nmap. Sólo debe distribuirla de forma separada e indicar a sus usuarios que vayan a http://www.insecure.org/nmap/ para obtener Nmap.

No consideramos que las restricciones sean añadidos a la GPL, sino simplemente una forma de clarificar cómo interpretamos el término “trabajos derivados” y su aplicación al producto Nmap licenciado GPL. Esto es parecido a la interpretación que Linus Torvalds ha dado a “trabajos derivados” y su aplicación a los módulos del núcleo de Linux. Nuestra interpretación sólo aplica a Nmap, no hablamos en nombre de otros productos GPL.

Estaremos encantados de ayudarle si tiene alguna pregunta de cómo aplican las restricciones de licenciamiento GPL al uso de Nmap en trabajos que no son GPL. Tal y como se menciona más arriba, ofrecemos licencias alternativas para integrar Nmap en aplicaciones propietarias así como en dispositivos hardware. Ya se han vendido este tipo de contratos a fabricantes de dispositivos de seguridad y habitualmente incluye una licencia perpetua, al tiempo que se da soporte prioritario y actualizaciones. Estos contratos financian el desarrollo continuo de la tecnología Nmap. Por favor, contacte con <sales@insecure.com> si desea más información.

Insecure.Com LLC da permiso para enlazar el código de este programa con cualquier librería de OpenSSL que se distribuya bajo una licencia idéntica a la indicada en el fichero Copying.OpenSSL adjunto, así como a la distribución de la combinación enlazada que incluye a ambos. Ésta es una excepción especial a los términos de la GPL. Debe

obedecer los demás términos de la GPL de GNU en cualquier otro aspecto en relación al código que utilice que no sea OpenSSL. Si modifica este fichero puede extender esta excepción a su versión del fichero, aunque no está obligado a hacerlo.

Si recibe estos ficheros con un acuerdo de licencia por escrito o contrato que indique términos distintos de los que se describen arriba entonces dicha licencia alternativa toma precedencia sobre estos comentarios.

Licencia Creative Commons para esta guía Nmap

Esta guía de referencia de Nmap Reference Guide es (C) 2005 Insecure.Com LLC. Se distribuye bajo la versión 2.5 de la Licencia Creative Commons de Reconocimiento. Esta licencia le permite redistribuir y modificar el trabajo como desee siempre que reconozca la fuente original. Puede, si lo desea, tratar este documento con la misma licencia con la que distribuya Nmap (como se ha discutido previamente).

Disponibilidad del código fuente y contribuciones de la comunidad

Se da el código fuente de este programa porque creemos que los usuarios tienen el derecho a saber cómo funciona un programa con exactitud antes de ejecutarlo. También le permite auditar el programa en búsqueda de agujeros de seguridad (no se ha encontrado ninguno aún).

El código fuente le permite migrar Nmap a otras plataformas, arreglar erratas y añadir nuevas funciones. Le pedimos encarecidamente que envíe sus cambios a <fyodor@insecure.org> para que puedan incorporarse en la distribución principal. Al enviar estos cambios a Fyodor o cualquiera de las listas de correo de desarrollo en Insecure.Org se asume que está ofreciendo a Fyodor y a Insecure.Com LLC derechos ilimitados y no exclusivos para reutilizar, modificar y relicenciar el código. Nmap siempre estará disponible como software libre, pero esto es importante porque la incapacidad de relicenciar el código ha dado muchos problemas a otros proyectos de software libre (como es el caso de KDE y NASM). También relicenciamos el código de forma ocasional a terceros, como se ha descrito previamente. Puede especificar condiciones especiales de licencia para sus contribuciones, sólo tiene que indicarlas cuando las envíe.

Sin garantía

Este programa se distribuye con la esperanza de que sea útil, pero SIN NINGUNA GARANTÍA, incluso sin la garantía MERCANTIL implícita o sin garantizar la CONVENIENCIA PARA UN PROPÓSITO PARTICULAR. Véase la Licencia Pública General de GNU para más detalles en http://www.gnu.org/copyleft/gpl.html, o en el fichero COPYING que se incluye con Nmap.

También debería tener en cuenta que se sabe que Nmap ha provocado en algunas ocasiones que alguna aplicación mal escrita se bloquee, como también ha pasado con pilas TCP/IP e incluso sistemas operativos. Esto es muy raro, pero es importante tenerlo en mente. *Nunca debería utilizar Nmap contra sistemas de misión crítica* a no ser que esté preparado para sufrir una caída. Reconocemos que Nmap puede bloquear sus sistemas o redes y hacemos un descargo de responsabilidad frente a cualquier daño o problemas que Nmap pueda causar.

Uso inapropiado

Debido al ligero riesgo de que se produzcan caídas porque un *black hat* (persona que ataca sistemas sin autorización, N. del T.) utilice Nmap para realizar un análisis antes de atacar algún sistema hay administradores que se molestan y se quejan cuando se sondean sus sistemas. Así, por regla general es recomendable pedir permiso para hacer cualquier tipo de sondeo, aún uno ligero, de una red.

Nunca debería instalar Nmap con privilegios especiales (p. ej. suid root) por razones de seguridad.

Programas de terceros

Este producto incluye programas desarrollados por la Fundación Apache Software Foundation. También se distribuye una versión modificada de la librería portable de captura de paquetes Libpcap conjuntamente con nmap. La versión para Windows de Nmap utiliza la librería WinPcap library que es una versión derivada de la libcap. La librería PCRE, software libre escrito por Philip Hazel, da el soporte de expresiones regulares. Algunas de las funciones de acceso a bajo nivel de la red utiliza la librería de red Libdnet, escrita por Dug Song. Se distribuye una versión modificada con Nmap. Nmap puede, opcionalmente, enlazar con las herramientas criptográficas OpenSSL para poder hacer un análisis de versiones SSL. Todos los programas de terceros descritos en este párrafo se distribuyen libremente bajo licencias tipo BSD.

Clasificación de control de exportación de los EEUU

Control de exportación de los EEUU: Insecure.Com LLC cree que Nmap se encuentra dentro del capítulo US ECCN (número de clasificación de control de exportación) 5D992. Esta categoría se denomina “Programas de seguridad de la información no controlados en 5D002”. La única restricción a esta clasificación es AT (anti-terrorismo), que se aplica a casi todos los bienes y deniega la exportación a un número reducido de naciones rebeldes como Irán o Corea del Norte. Así, la exportación de Nmap no requiere de una licencia especial, permiso o cualquier otra autorización del gobierno.