Comandos de NMAP

Sección I – Teoría

Información tomada de: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1050-zenmap

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

- Método para conocer el nivel de seguridad de la configuración de los servicios que se ofrecen.
- Una de las primeras etapas que un posible atacante lleva a cabo, dentro del plan de ataque, para investigar o enumerar qué servicios activos tiene la víctima.

Nmap, cuyo nombre significa mapeador de redes, es software libre y puede redistribuirse y/o modificarse bajo los términos de la Licencia Publica General GNU.

Las opciones disponibles si se desea utilizar nmap son:

- El comando nmap para la consola
- Zenmap como herramienta gráfica.

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

¿Qué permite nmap?

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

Es compatible con un gran número de técnicas de escaneo como:

- UDP,
- TCP connect(),
- TCP SYN (half open),
- ICMP (ping sweep),
- FIN,
- ACK sweep,
- Xmas Tree y Null scan.

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.

Open (abierto),	Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Es decir que hay una aplicación aceptando conexiones TCP, datagramas UDP o asociaciones SCTP en el puerto
Filtered (filtrado),	Filtrado indica que un firewall (cortafuegos), filtro (reglas de router), 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.
Closed (cerrado),	Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento.
Unfiltered (no filtrado).	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. Este estado sólo lo devuelve el tipo de escaneo ACK
open|filtered – closed|filtered	Nmap no es capaz de definir si el puerto está abierto/cerrado o filtrado. Ocurre cuando los puertos abiertos no generan una respuesta.

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.

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

Algunos conceptos de seguridad utilizados:

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

Sintaxis de la herramienta

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).

```
nmap [Tipo de Escaneo] [Opciones] {Especificación del destino "target"}
```

nmap –sS -A -T4 equipo1.destino.com

Sección II – Técnicas de escaneo de puertos

Tomado de: http://nmap.org/man/es/man-port-scanning-techniques.html

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.

Escaneo TCP SYN (-sS)

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).

root@machine:~# nmap -sS (máquina)

Escaneo TCP connect (-sT)

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. 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 esto 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.

user@machine:~$ nmap -sT (máquina)

Escaneos UDP -sU

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 los 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.

root@machine:~# nmap -sU (máquina)

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

La ventaja fundamental de este tipo de sondeos es que pueden atravesar algunos cortafuegos que no hagan inspección de estados o routers 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 esto 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.

root@machine:~# nmap –sN –sF -sX (máquina)

Escaneo TCP ACK (-sA)

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.

Escaneo de ventana TCP (-sW)

El sondeo de ventana 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 que existen en Internet, así que no es siempre fiable. Los sistemas que no hacen esto 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 esto. 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.

Escaneo TCP Maimon (-sM)

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.

Escaneo TCP personalizable (- -scanflags)

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.

Escaneo Zombi (-sI <sistema zombi [:puerto_sonda]>)

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 esto 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://nmap.org/book/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).

Escaneo de protocolo IP (-sO)

El sondeo de protocolo IP le permite determinar qué protocolos (TCP, ICMP, IGMP, etc.) soportan los sistemas objetivos. 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 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.

Escaneo de robote FTP (-b)

Nota: VC = Este escaneo es obsoleto en muchos servidores 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.

Idle Scan (-sI)

Idle scan is one of my favorite techniques, and it is an advance scan that provides complete anonymity while scanning. In idle scan, Nmap doesn't send the packets from your real IP address—instead of generating the packets from the attacker machine, Nmap uses another host from the target network to send the packets. Let's consider an example to understand the concept of idle scan:

nmap -sI zombie_host target_host

```
# nmap -sI 192.168.1.15 192.168.1.123
```

TCP SYN Scan (-sS)

It is a basic scan, and it is also called half-open scanning because this technique allows Nmap to get information from the remote host without the complete TCP handshake process, Nmap sends SYN packets to the destination, but it does not create any sessions, As a result, the target computer can't create any log of the interaction because no session was initiated, making this feature an advantage of the TCP SYN scan.

If there is no scan type mentioned on the command, then avTCP SYN scan is used by default, but it requires the root/administrator privileged.

```
# nmap -sS 192.168.1.1
```

Opciones para evadir Firewall e IDS

Estas opciones están explicadas en la página en español de nmap en la siguiente dirección:
http://nmap.org/man/es/man-bypass-firewalls-ids.html

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

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

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

-e <interfaz> (Utilizar la interfaz especificada)

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

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

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

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

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

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

Sección III – Ejemplos

Tomado de http://unidadlocal.com/Ejemplos-manual-y-opciones-de-el-Nmap-en-Linux consultado 31-10-2013
Tomado de http://nmap.org/man/es/man-examples.html consultado 31-10-2013

Para escanear un equipo
```
nmap 192.168.1.123
nmap equipo1.destino.com
```

Para escanear varios equipos
```
nmap 192.168.1.123  192.168.1.124
nmap equipo1.destino.com  equipo2.destino.com
```

Para escanear las primeras diez direcciones IP
```
nmap 192.168.1.1-10
```

Para obtener el sistema operativo del equipo1
```
nmap -O unidadlocal.com
```

Para obtener el sistema operativo de los equipos de la red
```
nmap -O 192.168.1.0/24
```

Para obtener el sistema operativo y versión de los servicios
```
nmap -A unidadlocal.com
```

Para escanear de forma rápida (-T4) y mostrar versión de servicios y tipo de sistema operativo (-A)
```
nmap -A -T4 192.168.1.123
```

Para escanear todos los puertos TCP reservados (-v activa el modo detallado - verbose).
```
nmap -v equipo1.destino.com
```

Para escanear de forma sigilosa tipo SYN (-sS) cada una de las 255 máquinas en la clase C de la red donde está el sistema "equipo1.destino.com" y que SO de cada equipo encendido. Requiere permisos de root
```
nmap -sS -O equipo1.destino.com/24
```

Para escanear un rango de puertos en este caso del 1 al 65535
```
nmap -sS -A -p 1-65535 192.168.1.123
```

Para escanear los puertos UDP (-sU) bien conocidos (opción por defecto)
```
nmap -sU -A 192.168.1.123
```

Escaneo haciendo ping (-sP) lanzaremos un ping a todas las IP de la red, para saber qué hosts se encuentran activos
```
nmap -sP 192.168.1.0/24
```

Lanzar una enumeración de equipos y un sondeo TCP a cada uno de la primera mitad (1-127) de las 255 posibles subredes de 8 bit (0-255) 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 -sV -p 22,53,110,143,4564 198.116.0-255.1-127
nmap -sV -p 135,139,445,80 10.10.0-255.1-127
```

Usar direcciones IP como señuelo mientras se escanea para no ser detectado (la victima creerá que está siendo escaneada por varias máquinas 192.168.1.15-17)
```
nmap -sS 192.168.1.123 -D 192.168.1.15,192.168.1.16,192.168.1.17
```

Stealth Xmas Tree scan
En el siguiente ejemplo, realizamos un Stealth Xmas Tree scan (-sX) hacia el host 192.168.0.1, en los puertos 25(SMTP), 53(DNS), le indicamos a nmap que no genere pings hacia el host, y tratamos de engañar al host (-D, Decoy), haciéndole creer que los scans se están generando desde los hosts 192.168.1.15, 192.168.1.16 (estas maquinas deben estar activas)

```
nmap -p 25,53 -sX -P0 -D 192.168.1.15,192.168.1.16 192.168.1.123
```

Guardando los resultados de tus scans.
Nmap permite guardar los resultados de un scan, en varios tipos de formato de archivo: Normal, XML, Grepable, All, y en formato "S"

```
nmap -sX -O 192.168.1.123 -oN archivo_reporte.txt
```

Bounce Attack.
Para determinar si la víctima es vulnerable al "bounce attack" (si hay un serviror FTP antiguo)

```
nmap -b 192.168.1.123
```

Bounce Attack.
Ahora si deseo realizar un scan muy suave para no ser detectado por algún firewall se puede utilizar las opciones con la opción -f ya que algunos firewall poseen métodos para detectar este tipo de scan.

```
nmap -sF -f -p 21 23 110 143 192.168.1.123
```

Referencia
http://nmap.org/book/man.html

Maneras interesantes de usar nmap:

Listar servidores con un puerto específico abierto

```
nmap -sT -p 80 -oG – 192.168.1.* | grep open
```

Encontrar IP no usadas en una subnet

```
nmap -T4 -sP 192.168.2.0/24 && egrep "00:00:00:00:00:00" /proc/net/arp
```

Escanear red en busca de AP falsos

```
nmap -A -p1-85,113,443,8080-8100 -T4 –min-hostgroup 50 –max-rtt-timeout 2000 –initial-rtt-timeout 300 –max-retries 3 –host-timeout 20m –max-scan-delay 1000 -oA wapscan 10.0.0.0/8
```

Suplantar una dirección IP durante el escaneo, la IP a suplantar debe estar activa

```
nmap -e <interfaz> -S <IP a suplantar> -PN <IP objetivo>
```

Listar los registros DNS inversos de una subred

```
nmap -R -sL 209.85.229.99/27 | awk '{if($3=="not")print"("$2") no PTR";else print$3" is "$2}' | grep '('
```

Este comando hace un reverse DNS lookup en una subred, se crea una lista con las direcciones IP de los registros PTR en la subred indicada. Se puede insertar la subred en notación CDIR (ejemplo: /24 para la Clase C). Puedes agregar "-dns-servers x.x.x.x" después del parámetro "-sL" si quieres realizar el listado sobre un servidor DNS especifico.

Sección IV – Análisis de datos.

La máquina destino tiene la IP 192.168.20.159, es un XP con XAMPP activo (FTP, Apache y MySQL), el equipo utiliza el firewall de XP.

Hacemos ping y no obtenemos respuesta

```
root@laptopHP2:~# ping 192.168.20.159
PING 192.168.20.159 (192.168.20.159) 56(84) bytes of data.
^C
--- 192.168.20.159 ping statistics ---
188 packets transmitted, 0 received, 100% packet loss, time 188282ms

root@laptopHP2:~# nmap -sP 192.168.20.159

Starting Nmap 5.00 ( http://nmap.org ) at 2013-10-31 18:36 CST
Host 192.168.20.159 is up (0.00049s latency).
MAC Address: 04:21:00:21:AC:4E (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Para obtener la versión de los servicios activos.

```
root@laptopHP2:~# nmap -sV 192.168.20.159

Starting Nmap 5.00 ( http://nmap.org ) at 2013-10-31 18:42 CST
Interesting ports on 192.168.20.159:
Not shown: 996 filtered ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      FileZilla ftpd 0.9.41 beta
80/tcp   open  http     Apache httpd 2.4.3 ((Win32) OpenSSL/1.0.1c PHP/5.4.7)
443/tcp  open  ssl/http Apache httpd 2.4.3 ((Win32) OpenSSL/1.0.1c PHP/5.4.7)
3306/tcp open  mysql    MySQL (unauthorized)
MAC Address: 04:21:00:21:AC:4E (Unknown)
Service Info: OS: Windows

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.35 seconds
```

- Si desea comprobar los servicios activos en un equipo Windows utilice el comando netstat –ano
- Si desea ver los procesos con el PID: tasklist
- Si desea detener un Proceso que utiliza un determinado PID utilice: taskkill /PID Número
- Si desea forzar el cierre de un proceso utilice: taskkill /F /PID Número

Tenga en cuenta que algunos procesos se vuelven a iniciar, revise si un servicio está automático (services.msc), por ejemplo el protocolo SMB se detiene buscando el servicio Servidor. Antes de cerrar un PID (programa o servicio) busque en Internet cuál es la función, ya que, podría reiniciar el sistema operativo Windows, (por ejemplo Iass)

Para los sistemas Linux puede utilizar los siguientes comandos

- Verificar los servicios activos en el equipo: netstat –tapu
- Ver los procesos: ps auxw
- Para eliminar un proceso cuando tiene hijos o conoce el nombre: killall apache2
- Para eliminar un proceso cuando conoce el PID: kill -9 Número

root@laptopHP2:~# nmap -O 192.168.20.159

```
Starting Nmap 5.00 ( http://nmap.org ) at 2013-10-31 16:52 CST
Interesting ports on 192.168.20.159:
Not shown: 997 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
MAC Address: 04:21:00:21:AC:4E (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
Device type: general purpose
Running (JUST GUESSING) : Microsoft Windows 2003|2000|XP (97%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (97%), Microsoft
Windows Server 2003 SP2 (97%), Microsoft Windows 2000 SP0 (96%), Microsoft Windows XP
(96%), Microsoft Windows XP SP2 (95%), Microsoft Windows 2000 SP4 (94%), Microsoft
Windows XP SP2 or SP3 (93%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (93%),
Microsoft Windows XP SP3 (92%), Microsoft Windows 2003 Small Business Server (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 10.03 seconds
```

root@laptopHP2:~# nmap -A 192.168.20.159

```
Starting Nmap 5.00 ( http://nmap.org ) at 2013-10-31 16:53 CST
Interesting ports on 192.168.20.159:
Not shown: 997 filtered ports
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Apache httpd 2.4.3 ((Win32) OpenSSL/1.0.1c PHP/5.4.7)
|  html-title: XAMPP 1.8.1
|_ Requested resource was http://192.168.20.159/xampp/
443/tcp  open  ssl/http Apache httpd 2.4.3 ((Win32) OpenSSL/1.0.1c PHP/5.4.7)
|_ html-title: Did not follow redirect to https://192.168.20.159/xampp/ and no page was
returned.
3306/tcp open  mysql    MySQL (unauthorized)
MAC Address: 04:21:00:21:AC:4E (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
Device type: general purpose
Running (JUST GUESSING) : Microsoft Windows 2003|2000|XP (97%)
Aggressive OS guesses: Microsoft Windows Server 2003 SP1 or SP2 (97%), Microsoft
Windows Server 2003 SP2 (97%), Microsoft Windows 2000 SP0 (96%), Microsoft Windows XP
(96%), Microsoft Windows XP SP2 (95%), Microsoft Windows 2000 SP4 (94%), Microsoft
Windows XP SP2 or SP3 (93%), Microsoft Windows 2000 SP4 or Windows XP SP2 or SP3 (93%),
Microsoft Windows XP SP3 (92%), Microsoft Windows 2003 Small Business Server (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.26 seconds
```

```
root@laptopHP2:~# nmap 192.168.20.6-10

Starting Nmap 5.00 ( http://nmap.org ) at 2013-10-31 17:20 CST
Interesting ports on 192.168.20.6:
Not shown: 999 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:1E:0B:61:20:32 (Hewlett Packard)

Interesting ports on 192.168.20.7:
Not shown: 999 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:1E:0B:26:CC:D0 (Hewlett Packard)

Interesting ports on 192.168.20.8:
Not shown: 999 filtered ports
PORT    STATE SERVICE
135/tcp open  msrpc
MAC Address: 00:19:21:50:27:CA (Elitegroup Computer System Co.)

Interesting ports on 192.168.20.10:
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-term-serv
MAC Address: 00:19:21:3F:F6:03 (Elitegroup Computer System Co.)

Nmap done: 5 IP addresses (4 hosts up) scanned in 23.62 seconds
```

Note que no hay respuesta de la dirección 192.168.20.9 (este escaneo puede ser detectado por un IDS)