Nmap - Introducción

Nmap (http://nmap.org) es un programa de código abierto, multiplataforma, que sirve para efectuar escaneos (también conocidos como "sondeos") de puertos. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red.

Especificación de objetivos

Todo lo que se escribamos 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.

Podemos especificar los objetivos de las siguientes formas:

nmap 8.8.8.8	Host 8.8.8.8
nmap 8.8.8.0/24	Red 8.8.8.0/24
nmap 8.8.8.1-8.8.8.10	Desde 8.8.8.1 a 8.8.8.10
nmap www.google.com	Host www.google.com
nmap 8.8.8.8 4.4.4.4	Hosts 8.8.8.8 y 4.4.4.4

Descubriendo sistemas

Nmap ofrece una gran variedad de opciones para personalizar las técnicas utilizadas. Al descubrimiento de sistemas se lo suele llamar sondeo ping, pero va más allá de la simple solicitud ICMP echo-request asociada al comando ping.

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 muchas veces es utilizada por empresas con menos de mil máquinas. El descubrimiento de sistemas puede encontrar dichas máquinas en un rango tan grande como el indicado.

Las opciones -P* (que permiten seleccionar los tipos de ping) pueden combinarse.

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.

-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.

La opción -sP puede combinarse con cualquiera de las opciones de sondas de descubrimiento (las opciones -P*, excepto -P0) para disponer de mayor flexibilidad.

-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".

(El segundo carácter en la opción -P0 es un cero, y no la letra O)

-n (No resolver 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 (Resolver nombres de 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.

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.

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 cómo 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.

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. Los administradores pueden querer considerar bloquear estos puertos con un cortafuegos. Si se bloquean aparecerán 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 sólo durante un sondeo IPID pasivo.

Técnicas de sondeo de puertos

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.

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 enviar 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 únicamente los sondeos más utilizados (y más útiles). Para obtener una lista y documentación de todos los tipos de sondeos disponibles y su funcionamiento, podemos visitar la documentación oficial de nmap (http://nmap.org)

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) 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().

-sS (sondeo TCP SYN)

El sondeo SYN es el utilizado por omisión y el más popular. 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())

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,

utilizan para establecer una 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. 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.

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.

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. Podemos acelerar los 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.

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> (Sondea puertos específicos)

Esta opción especifica los puertos que desea sondear y toma precedencia sobre los valores por omisión. Podemos especificar tanto números de puerto de forma individual, así como rangos de puertos separados por un guión (p. ej. 1-1023). Podemos omitir el valor inicial y/o el valor final del rango. Nmap utilizará 1 ó 65535 respectivamente. De esta forma, podemos especificar -p- para sondear todos los puertos desde el 1 al 65535. Se permite sondear el puerto cero siempre que se 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).

Podemos especificar un protocolo específico cuando sondeamos puertos TCP y UDP si precedemos el número de puerto con T: o U:. El calificador dura hasta que se 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.

Tengamos en cuenta que para sondear tanto UDP como TCP deberemos 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 queremos sondear una menor cantidad de puertos (100 puertos) que la que es sondeada por defecto (1000 puertos)

Nmap utiliza un archivo llamado “nmap-services”, el cual contiene una lista de puertos que se encuentra ordenada en base a los que son más utilizados. Por defecto, se sondean los mil puertos más utilizados. Con la opción “-F” se sondean los cien puertos más utilizados, haciendo los sondeos mucho más rápidos.

Autor: Fabian Martinez Portantier

Fuentes:

- http://incibe.es
- http://seguridadyredes.wordpress.com
- http://nmap.org