Nmap - Servicios y Sistemas Operativos

Detección de servicios y versiones

Si le indicamos a Nmap que mire un sistema remoto nos 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 utiliza su base de datos nmap-services con más de 2.200 puertos conocidos.

Generalmente este informe es correcto dado que la gran mayoría de demonios que escuchan en el puerto 25 TCP son, en realidad, servidores de correo. Pero no debemos confiar al 100% en este hecho. La gente ejecuta a veces servicios distintos en puertos inesperados.

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, etc).

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 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. Podemos 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 podamos enviar los detalles si sabemos lo que está ejecutándose detrás de ese puerto.

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. Podemos utilizar la opción -A en su lugar para activar tanto la detección de versiones como la detección de sistema

operativo.

--version-intensity <intensidad>

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.

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 muchísimas 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, router, switch, etc.).

Nmap indicará una URL donde podemos enviar las huellas si conocemos (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).

Enviando esta información contribuimos 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 es, 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.

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

-O

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

La detección de sistema operativo funcionará mejor si se dispone de un puerto TCP abierto y otro cerrado. Si definimos esta opción, Nmap no intentará 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.

--fuzzy

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.

Autor: Fabian Martinez Portantier

Fuentes:

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