Tutorial:

Buscar con nmap lagunas de seguridad en la red

Acerca del aislamiento
Acerca de los cortafuegos

Detrás de cada puerto abierto en la red se esconde un programa de servidor que, con mucha probabilidad, contiene errores. Algunos de esos errores son tan graves que pueden ser aprovechados para espiar al sistema afectado, sabotearlo o incluso ejecutar en él un código malicioso. Por ese motivo, el paso más importante para mejorar la seguridad en la red de su empresa es analizar los puertos abiertos y, si es preciso, cerrarlos.

Introducción: análisis de la red con nmap

Los programas de análisis de redes le proporcionan una visión general de posibles puntos débiles en la red de su empresa. Este manual describe tres técnicas de análisis básicas con el escáner de puertos nmap. Esas técnicas sirven para identificar los dispositivos terminales y localizar los servicios que ofrecen. Para finalizar le presentamos dos técnicas para asegurar los puntos débiles encontrados.

Con el programa **nmap** puede analizar la estructura de su red. Este programa está considerado como la "herramienta hacker" por excelencia, porque emplea para ello detalles de implementación de diferentes protocolos de la red. Es capaz de identificar los dispositivos terminales en la red, analizar los programas de servidor activos en ellos y determinar de qué programas se trata. Por lo tanto, nmap le revela muchos detalles sobre la red de su empresa.

Aviso:
¡Por favor, actúe siempre con diligencia y realice únicamente análisis de redes para los que esté autorizado!

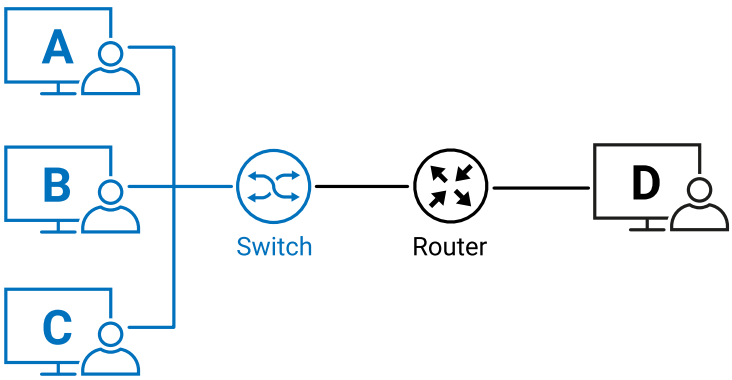
Instalar y utilizar Nmap

En nmap.org puede descargar el programa. nmap es un programa que utiliza exclusivamente líneas de comandos, pero con Zenmap puede disponer de un entorno de usuario gráfico.

En algunas de las técnicas descritas a continuación nmap envía paquetes de datos brutos a través de diferentes capas en la red. Para ello tiene que evadir la pila de red del sistema operativo, por lo que para su ejecución usted necesita disponer de derechos de administración o de root.

Técnica de análisis 1: buscar dispositivos terminales en la red con nmap

Con ayuda de la primera técnica se identifican todos los dispositivos terminales dentro de un mismo dominio de broadcast. Eso significa que todos los ordenadores están conectados entre sí por switches en el mismo Ethernet y no separados entre sí por routers (es decir, a nivel de IP). Otra opción consistiría en enviar un paquete ICMP de solicitud (ping) a la dirección del broadcast del segmento de red, pero, por razones de seguridad, los dispositivos terminales actuales no suelen contestar a estas solicitudes.



Los ordenadores A, B y C están conectados entre sí por un switch y, por lo tanto, se encuentran en el mismo dominio de broadcast. El ordenador A puede encontrar a los ordenadores B y C en la red con ayuda de consultas de ARP. El ordenador D está conectado a la red a través de un router y las consultas de ARP no llegan hasta él.

El envío de un paquete IP a otro ordenador dentro del mismo Ethernet tiene lugar mediante el intercambio de una trama de Ethernet entre dos interfaces de la red. Para ello es necesario conocer la dirección del hardware de destino. El mecanismo que asigna una dirección de IP al hardware perteneciente o a la dirección de MAC lo pone a disposición el Adress Resolution Protocol (ARP).

Con la dirección MAC del broadcast en la red se envía la solicitud a todos los dispositivos terminales dentro de ese dominio de broadcast: "¿Quién tiene la siguiente dirección de IP?". El terminal que recibe el paquete para esa dirección de IP envía, a su vez, su dirección MAC. Ahora la interfaz de la red ya puede enviar datos a exactamente ese usuario.

Durante la inventarización de un segmento de red utilizando ARP se envía esa solicitud a cada dirección de IP dentro del segmento de red especificado. Si un dispositivo está conectado a la red, tiene que responder obligatoriamente a esa solicitud.

El siguiente comando encuentra todos los dispositivos terminales activos con las direcciones de IP desde 192.168.1.1 hasta 192.168.1.254 dentro de un dominio de broadcast conjunto:

```
nmap -PR 192.168.1.0/24
```

Técnica de análisis 2:
buscar los puertos abiertos sin acceso directo al dispositivo

Si usted tiene acceso directo al sistema de destino, puede consultar los puertos abiertos bajo Linux, MacOS y Windows con el comando "netstat". Sin embargo, esto no es posible en muchos casos. Nmap ofrece en esos casos alternativas para localizar los puertos abiertos en el sistema de destino.

Buscar puertos TCP abiertos

Detrás de cada puerto abierto hay un programa de servidor activo que recibe y analiza los datos. En el caso de TCP es fácil determinar los puertos abiertos: puesto que el protocolo trabaja orientado hacia la conexión, solo hay que iniciar el handshake de tres etapas para establecer la conexión (encontrará más información sobre el handshake de tres etapas en nuestro libro gratuito "TCP/IP Ethernet hasta Web-IO"). Para ello se envía al destino un sencillo paquete SYN. En función de su respuesta se puede determinar el estado del puerto.

- **Sin respuesta:**
  el puerto no está abierto o está filtrado
- **Reset:**
  el sistema operativo recibe las solicitudes de conexión para el puerto, pero las rechaza porque no hay ninguna aplicación de servidor activa
- **Aceptar la conexión:**
  el puerto está abierto y, según las circunstancias, puede ser un riesgo para la seguridad

Con el siguiente comando puede escanear un TCP-SYN en el host con la dirección de IP 192.168.1.200:

```
nmap -sS 192.168.1.200
```

Buscar puertos UDP abiertos

Localizar los puertos UDP abiertos es más complicado. Al contrario que TCP, UDP no trabaja orientado a la conexión. Al no haber ningún handshake de tres etapas, la reacción de la otra parte es imprevisible.

El caso más simple consiste en que el sistema operativo de destino responda que el puerto no está accesible. En ese caso se le marca como cerrado. Si no envía ninguna respuesta, no se puede saber si el paquete ha sido aceptado por una aplicación de servidor o si ha sido rechazado en alguna parte por el camino. Por consiguiente, no obtener ninguna respuesta significa que el puerto puede estar abierto o filtrado.

Entonces se envía a los puertos "sospechosos" un paquete específico de servicio. Si el emisor obtiene ahora una respuesta, entonces sabe que el puerto está abierto. Esto funciona, por ejemplo, en la resolución de los nombres de ordenadores con DNS, en la consulta de una configuración de IP a través de DHCP o en las actualizaciones de la hora vía NTP.

Con este comando se ejecuta un escáner simple de UDP:

```
nmap -sU 1 192.168.1.200
```

Como ya se ha mencionado más arriba, este escáner no detecta necesariamente todos los puertos UDP abiertos, pero suele ser suficiente para obtener una primera visión general.

Buscar los puertos TCP y UDP abiertos en una misma operación

Para determinar al mismo tiempo los puertos TCP y UDP abiertos también puede combinar los comandos:

```
nmap -sS -sU 192.168.1.200
```

Técnica de análisis 3:
determinar sistema operativo y programas de servidor

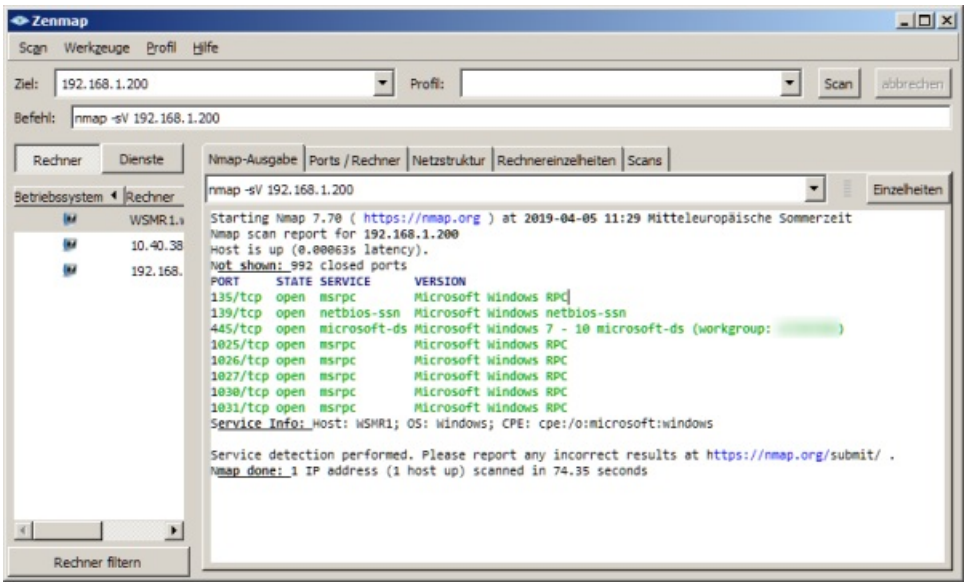
Nmap es capaz de mucho más que identificar terminales y puertos. Al implementar los protocolos de red, los programadores tienen ciertas libertades. Por eso, cada sistema operativo presenta una huella específica con la que puede ser identificado.

La identificación del sistema operativo no funciona siempre. Pero en la mayoría de los casos el resultado es acertado.

```
nmap -0 192.168.1.200
```

Nmap puede analizar las respuestas de los puertos abiertos para identificar los servicios activos en un terminal. Con frecuencia, esos programas comparten por sí mismos bastante información, por ejemplo, su versión actual o los protocolos que soportan. Nmap analiza esa información y la resume.

```
nmap -sV 192.168.1.200
```



Por favor, tenga en cuenta que si usted utiliza sV junto con sU, es decir el escáner de UDP, nmap envía una batería de extensos paquetes de prueba a cada puerto UDP. Eso puede proporcionarle más información sobre los puertos UDP abiertos, pero, según las circunstancias, ¡puede durar mucho tiempo!

Cerrar puertos, aumentar la seguridad

Ahora que conocemos los eventuales riesgos por puertos abiertos, el paso siguiente es minimizar esos riesgos.

Técnica de seguridad 1:
finalizar las aplicaciones de servidor

El primer paso consiste en desactivar todas las aplicaciones de servidor que no sean necesarias. Para conocer qué aplicación abre un puerto puede utilizar también el comando "netstat". En muchos casos no es posible finalizar las aplicaciones de servidor en el dispositivo terminal con el fin de cerrar puertos por carecer de los derechos de acceso, cuando se trata de un software incorporado o cuando el inicio de las aplicaciones de servidor es dinámico según la demanda. En esos casos se puede utilizar la técnica de aislamiento descrita en el capítulo siguiente.

Técnica de seguridad 2:
fácil y eficaz - aislamiento con Microwall

Esta técnica aísla los sistemas potencialmente vulnerables, en los que no sea posible cerrar los puertos abiertos, en un segmento de red propio. La comunicación con ese segmento está supervisada, restringida y protocolizada. Para ello se instala un router cortafuegos, como Microwall VPN de W&T entre los sistemas afectados y la red envolvente. El tráfico de datos por IP conducido a través de ella es filtrado por reglas.

- El filtro de paquetes de Microwall detecta las comunicaciones no deseadas y rechaza los paquetes. Aunque un puerto del dispositivo terminal esté abierto, no se puede llegar a él.
- En el modo NAT se esconden tras Microwall todos los dispositivos terminales aislados. En la red solo está visible Microwall, que reenvía y supervisa la comunicación.
- Los dispositivos terminales aislados se encuentran en otro dominio de broadcast. De ese modo se impiden las consultas de ARP y otros ataques a nivel de red de forma efectiva.

Encontrará información detallada sobre la estrategia de aislamiento en laPágina temática.

¡Lo mejor es probarlo!

Si lo desea, ponemos a su disposición un Microwall gratuitamente durante un periodo de cuatro semanas.

Solicitar dispositivo de prueba

Thomas Clever
t.clever@wut.de

Nuestros técnicos están a su disposición en el teléfono+49 202/2680-110 (lu-vi de 8-17 horas)

Le atendemos personalmente:

Wiesemann & Theis
GmbH
Porschestr. 12
42279 Wuppertal
Tel: +49 202/2680-110 (lu-vi de 8-17
horas)
Fax: +49-202/2680-265
info@wut.de

Protección de datos