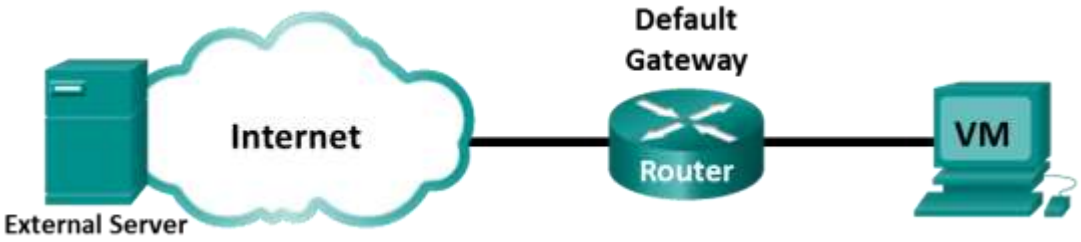
Práctica de laboratorio: Exploración de Nmap
Topología



Objetivos

Parte 1: Explorar Nmap

Parte 2: Escanear para buscar puertos abiertos

Antecedentes / Escenario

El escaneo de puertos suele ser parte de un ataque de reconocimiento. Se pueden utilizar diversos métodos de escaneo de puertos. Estudiaremos cómo se emplea la utilidad Nmap. Nmap es una poderosa utilidad de red que se utiliza para detección de redes y auditorías de seguridad.

Recursos necesarios

- Máquina virtual CyberOps Workstation
- Acceso a Internet

Instrucciones

Parte 1: Explorar Nmap

En esta parte utilizará páginas del manual (o páginas man para abreviar) para saber más sobre Nmap.

El comando **man** [*programa* |*utilidad* | *función*] muestra las páginas del manual asociadas con los argumentos. Las páginas de manuales son los manuales de referencia de los SO Unix y Linux. Estas páginas pueden tener las siguientes secciones, entre otras: Nombre, Sinopsis, Descripciones, Ejemplos y Ver también.

a. Inicie la VM CyberOps Workstation.

b. Abra un terminal.

c. En el cursor del terminal, introduzcan **man nmap**.

```
[analyst@secOps ~]$ man nmap
```

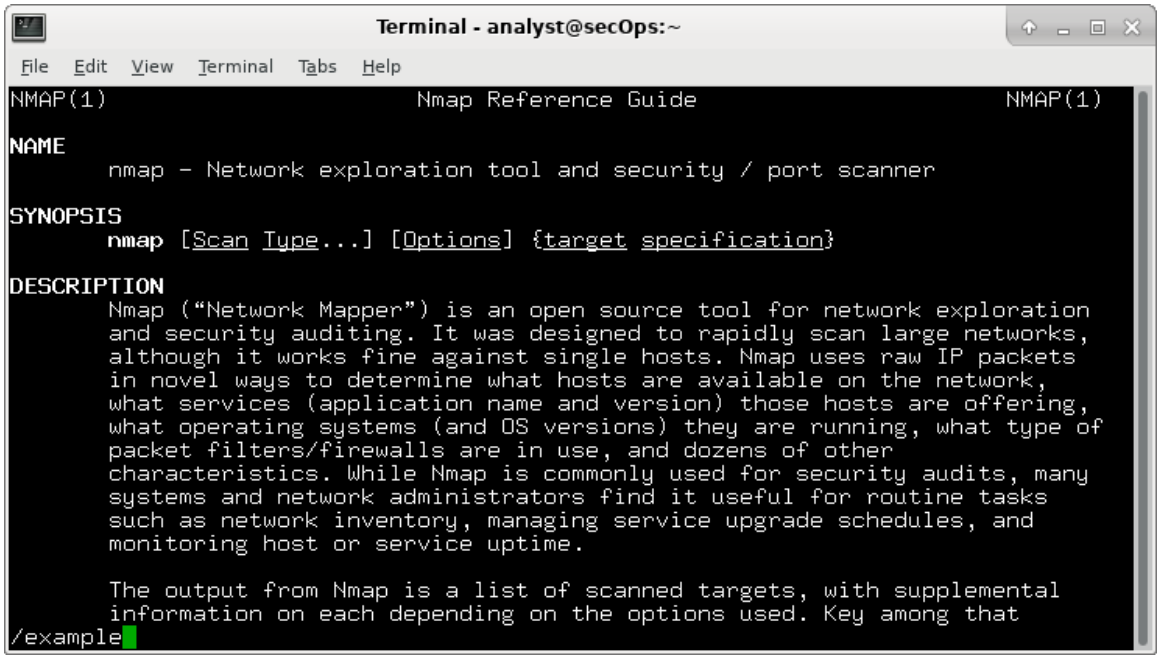
¿Qué es Nmap?

¿Para qué se utiliza Nmap?

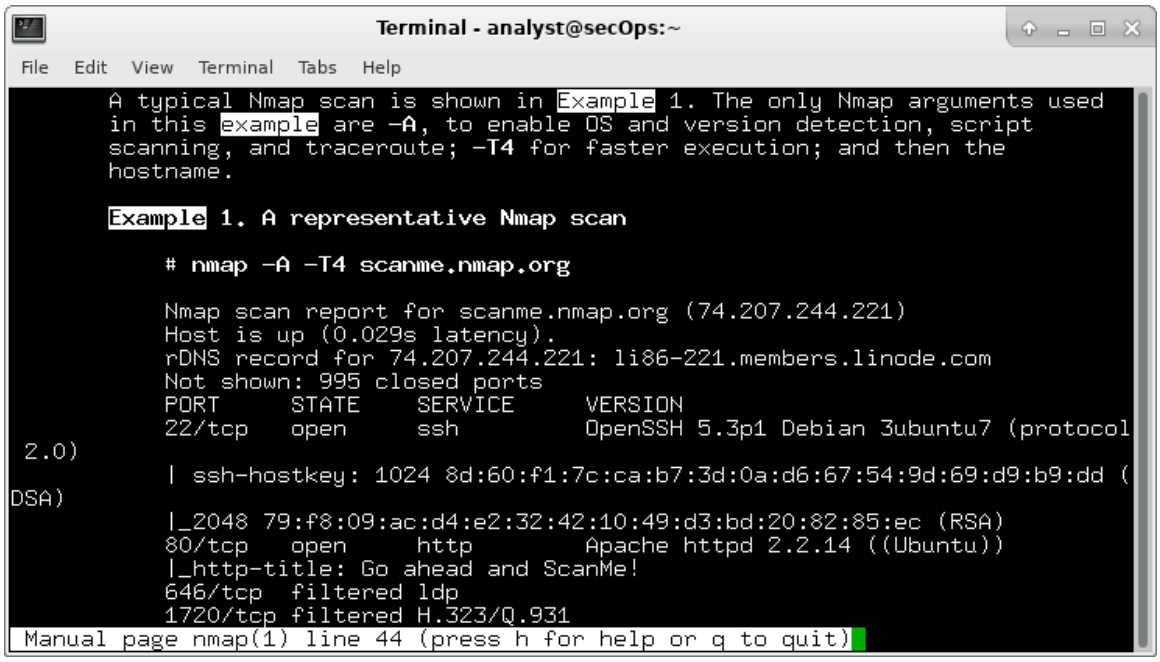
d. Cuando esté en la página man, podrá utilizar las teclas de las flechas hacia arriba y hacia abajo para desplazarse por las páginas. También puede presionar la barra espaciadora para avanzar una página por vez.

Si quiere buscar el uso de un término o una frase específicos, introduzca una barra diagonal (/) o un signo de interrogación (?) seguidos por el término o la frase. La barra diagonal busca hacia adelante en el documento, y el signo de interrogación lo hace hacia atrás. La tecla **n** los lleva a la siguiente coincidencia.

Escriban **/example** y presionen INTRO. Así se buscará la palabra **example** hacia adelante en toda la página man.



e. En la primera instancia de example, vemos tres coincidencias. Presione **n** para pasar a la siguiente coincidencia.



Mire el Ejemplo 1.

¿Cuál es el comando de **nmap** que se utilizó?

Utilice la función de búsqueda para responder las siguientes preguntas.

¿Qué hace el switch -A?

¿Qué hace el switch -T4?

f. Desplácese por la página para obtener más información sobre nmap. Escriba **q** cuando haya terminado.

Parte 2: Escanear para buscar puertos abiertos

En esta parte utilizará los switches del ejemplo en las páginas man de Nmap para escanear sus hosts locales, sus redes locales y un servidor remoto en scanme.nmap.org.

Paso 1: Escanear sus hosts locales

a. Si es necesario, abran un terminal en la VM. Introduzcan **nmap -A -T4 localhost** en el prompt. Dependiendo de la red local y de los dispositivos, el escaneo puede demorar entre unos segundos y algunos minutos.

```
[analyst@secOps ~]$ nmap -A -T4 localhost

iniciar Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:20 EDT
Nmap escanea el reporte para el host local (127.0.0.1)
Host está activo (0.000056s latencia).
Otras direcciones para el host local (not scanned): ::1
```

```
rDNS registro para127.0.0.1: localhost.localdomain
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r-- 1 0 0 0 Apr 19 15:23 ftp_test
<some output omitted>
```

b. Revisen los resultados y respondan las siguientes preguntas.

¿Qué puertos y servicios están abiertos?

Para cada uno de los puertos abiertos, registren el software que está proporcionando los servicios.

Paso 2: Escaneen sus redes.

Advertencia: Antes de utilizar Nmap en cualquier red, obtengan el permiso de sus dueños para continuar.

a. En el command prompt, introduzca **ip address** para determinar cuáles son la dirección IP y la máscara de subred correspondiente a este host. En este ejemplo, la dirección IP correspondiente a esta VM es 10.0.2.15 y la máscara de subred es 255.255.255.0.

```
[analyst@secOps ~]$ ip address
<output omitted>
2: enp0s3: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc fq_codel
estado UP predeterminado grupo qlen 1000
    enlace/éter 08:00:27:ed:af:2c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 alcance global dinámico enp0s3
       valid_lft 85777sec preferred_lft 85777sec
    inet6 fe80¤ a 00:27 ff:feed:af2c/64 enlace de alcance
       valid_lft forever preferred_lft forever
```

Registren la dirección IP y la máscara de subred correspondientes a sus VM.

¿A qué red pertenecen sus VM?

b. Para localizar otros hosts en esta red LAN, introduzca **nmap -A -T4** ***dirección de red/prefijo.*** El último octeto de la dirección IP se debe reemplazar por un cero. Por ejemplo: en la dirección IP 10.0.2.15, el 15 es el último octeto. Por lo tanto, la dirección de red es 10.0.2.0. Al /24 se le llama prefijo y es la abreviatura de la máscara de red 255.255.255.0. Si sus VM tienen otra máscara de red, busquen una “Tabla de conversión CIDR” en Internet para encontrar sus prefijos. Por ejemplo: 255.255.0.0 sería /16. La dirección de red 10.0.2.0/24 se utiliza en este ejemplo

Nota: Esta operación puede demorar, especialmente si tiene muchos dispositivos conectados a la red. En un entorno de prueba el escaneo puede demorar aproximadamente 4 minutos.

```
[analyst@secOps ~]$ nmap -A -T4 10.0.2.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:13 EDT
<output omitted>
Informe de escaneo de Nmap para 10.0.2.15
Host está activo (0.00019s latencia).
```

```
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r—r— 1 0 0 0 Mar 26 2018 ftp_test
| ftp-syst:
| ESTADO
| Estado del servidor FTP
| Conectado a 10.0.2.15
| Se ha iniciado sesión como ftp
| TIPO: ASCII
| Sin límite de ancho de banda de sesión
| Tiempo de espera de sesión en segundos es 300
| Conexión de control es texto sin formato
| Las conexiones de datos serán de texto sin formato
| Al inicio de la sesión, el recuento de clientes era 1
| VSFTpd 3.0.3 - seguro, rápido, estable
|_Fin del estado
22/tcp open ssh OpenSSH 8.2 (protocol 2.0)
23/tcp open telnet Openwall GNU/*/Linux telnetd
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Resultados del guión posterior al escaneo:
| sesgo de reloj:
| 0s:
| 10.0.2.4
| 10.0.2.3
|_ 10.0.2.2
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap hecho: 256 direcciones IP (4 hosts para arriba) escaneadas en 346.89 segundos
```

¿Cuántos hosts están activos?

Desde sus resultados de Nmap, generen una lista de las direcciones IP de los hosts que se encuentran en la misma red LAN que sus VM. Generen una lista de los servicios que están disponibles en los hosts detectados.

Paso 3: Escanear un servidor remoto

a. Abra un navegador web y diríjanse a **scanme.nmap.org**. Lea el mensaje en pantalla.

¿Cuál es el propósito de este sitio?

b. En el cursor del terminal introduzcan **nmap -A -T4 scanme.nmap.org**.

```
[analyst@secOps Desktop]$ nmap -A -T4 scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 16:46 EDT
```

```
Nmap reporte de scaneo para scanme.nmap.org (45.33.32.156)
Host está activo (0.040s latencia).
Otra dirección para scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 992 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp filtered smtp
80/tcp open http Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
593/tcp filtrado http-rpc-epmap
4444/tcp filtro krb524
9929/tcp open nping-echo Nping echo
31337/tcp open tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Desempeño de la detención del servicio Por favor reporte cualquier resultado
incorrecto a  https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.96 seconds
```

c. Revise los resultados y responda las siguientes preguntas.

¿Qué puertos y servicios están abiertos?

¿Qué puertos y servicios están filtrados?

¿Cuál es la dirección IP del servidor?

¿Cuál es el sistema operativo?

Pregunta de reflexión

Nmap es una poderosa herramienta para la exploración y administración de redes. ¿Qué beneficios puede aportar Nmap a la seguridad de la red? ¿De qué manera un atacante puede utilizar Nmap como herramienta maliciosa?