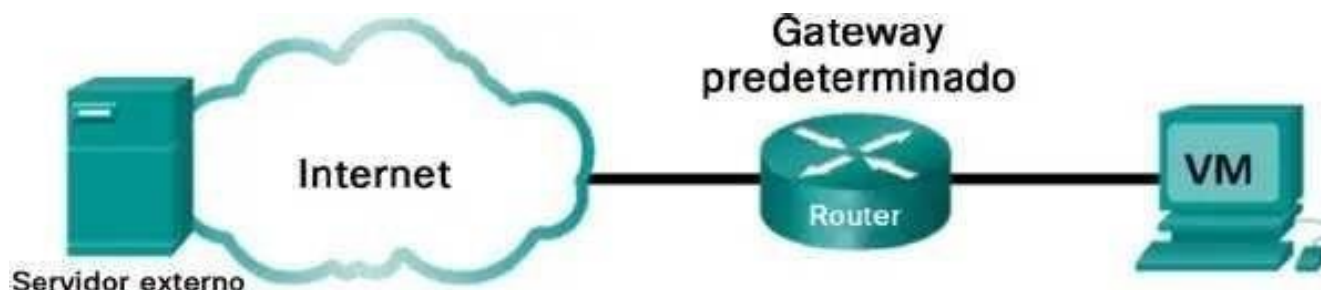


Práctica de laboratorio: Exploración de Nmap

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

Parte 1: Explorar Nmap

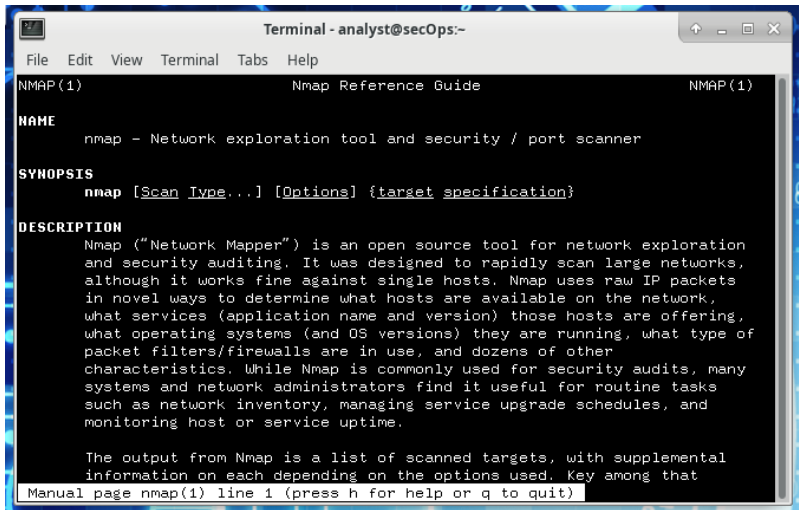
En esta parte utilizarán páginas del manual (o páginas man para abreviar) para saber más sobre Nmap.

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.

1. Inicien la VM CyberOps Workstation.
2. Abran un terminal.
3. En el cursor del terminal, introduzcan `man nmap`.

```
[analyst@sec0ps ~]$ man nmap
```

Práctica de laboratorio: Exploración de Nmap



```
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
NMAP(1) Nmap Reference Guide NMAP(1)

NAME
  nmap - Network exploration tool and security / port scanner

SYNOPSIS
  nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
  Nmap ("Network Mapper") is an open source tool for network exploration
  and security auditing. It was designed to rapidly scan large networks,
  although it works fine against single hosts. Nmap uses raw IP packets
  in novel ways to determine what hosts are available on the network,
  what services (application name and version) those hosts are offering,
  what operating systems (and OS versions) they are running, what type of
  packet filters/firewalls are in use, and dozens of other characteristics.
  While Nmap is commonly used for security audits, many systems and network
  administrators find it useful for routine tasks such as network inventory,
  managing service upgrade schedules, and monitoring host or service uptime.

  The output from Nmap is a list of scanned targets, with supplemental
  information on each depending on the options used. Key among that

Manual page nmap(1) line 1 (press h for help or q to quit)
```

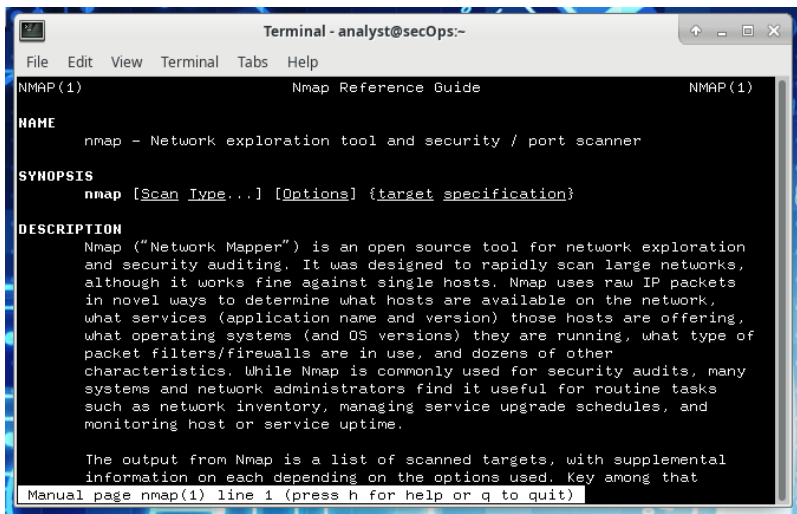
¿Para qué se utiliza nmap?

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

Si quieren buscar el uso de un término o una frase específicos, introduzcan 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.

Escriba /example y presione INTRO. Así se buscará la palabra example hacia adelante en toda la página man.

Práctica de laboratorio: Exploración de Nmap



```
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
NMAP(1) Nmap Reference Guide NMAP(1)

NAME
  nmap - Network exploration tool and security / port scanner

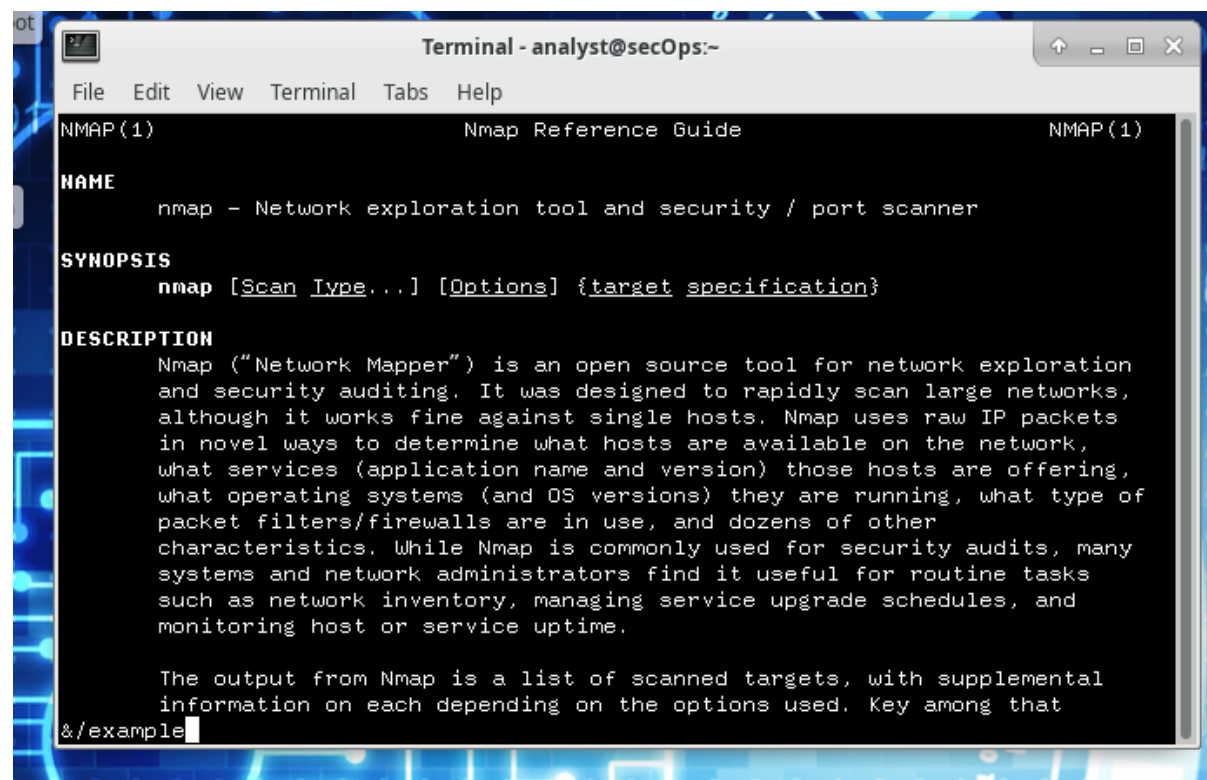
SYNOPSIS
  nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
  Nmap ("Network Mapper") is an open source tool for network exploration
  and security auditing. It was designed to rapidly scan large networks,
  although it works fine against single hosts. Nmap uses raw IP packets
  in novel ways to determine what hosts are available on the network,
  what services (application name and version) those hosts are offering,
  what operating systems (and OS versions) they are running, what type of
  packet filters/firewalls are in use, and dozens of other
  characteristics. While Nmap is commonly used for security audits, many
  systems and network administrators find it useful for routine tasks
  such as network inventory, managing service upgrade schedules, and
  monitoring host or service uptime.

  The output from Nmap is a list of scanned targets, with supplemental
  information on each depending on the options used. Key among that

Manual page nmap(1) line 1 (press h for help or q to quit)
```

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



```
Terminal - analyst@secOps:-
File Edit View Terminal Tabs Help
NMAP(1) Nmap Reference Guide NMAP(1)

NAME
  nmap - Network exploration tool and security / port scanner

SYNOPSIS
  nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
  Nmap ("Network Mapper") is an open source tool for network exploration
  and security auditing. It was designed to rapidly scan large networks,
  although it works fine against single hosts. Nmap uses raw IP packets
  in novel ways to determine what hosts are available on the network,
  what services (application name and version) those hosts are offering,
  what operating systems (and OS versions) they are running, what type of
  packet filters/firewalls are in use, and dozens of other
  characteristics. While Nmap is commonly used for security audits, many
  systems and network administrators find it useful for routine tasks
  such as network inventory, managing service upgrade schedules, and
  monitoring host or service uptime.

  The output from Nmap is a list of scanned targets, with supplemental
  information on each depending on the options used. Key among that

&/example
```

Utilicen la función de búsqueda para responder las siguientes preguntas.

¿Qué hace la opción **nmap -A**?

¿Qué hace la opción **nmap -A T4**?

- f. Desplácese por la página para obtener más información sobre nmap. Escriban q cuando hayan terminado.

Parte 2: Escanear para buscar puertos abiertos

En esta parte utilizarán 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 cursor. Dependiendo de la red local y de los dispositivos, el escaneo puede demorar entre unos segundos y algunos minutos.

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

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:20 EDT
Nmap scan report for localhost (127.0.0.1) Host
is up (0.000056s latency).
Other addresses for localhost (not scanned): ::1 rDNS
record for 127.0.0.1: 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
22/tcp    open  sshOpenSSH 7.4 (protocol 2.0) |
ssh-hostkey:
|  2048 f1:61:50:02:94:ba:f2:bd:be:93:cf:14:58:36:b8:32 (RSA)
|_  256 94:33:25:a5:0e:02:d7:bc:c8:bo:90:8a:a2:16:59:e5 (ECDSA)
23/tcp    open  telnet   Openwall GNU/*/Linux telnetd 80/tcp
open http    nginx 1.12.0
|_http-server-header: nginx/1.12.0 |_http-title:
Welcome to nginx!
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.81 seconds
```

- 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.

¿Cuál es el sistema operativo?

Paso 2: Escaneen sus redes.

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

- a. En el símbolo del sistema del terminal, introduzcan `ifconfig` 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 192.168.1.19 y la máscara de subred es 255.255.255.0.

```
[analyst@secOps ~]$ ifconfig
enpos3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> i mtu 1500 inet
inetnetmask 255.255.255.0 broadcast 192.168.1.255
inet6 fe80::997f:9b16:5aae:1868 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:c9:fa:a1 txqueuelen 1000 (Ethernet)
RX packets 34769 bytes 5025067 (4.7 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10291 bytes 843604 (823.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 19 base 0xd000
```

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 192.168.1.19, el .19 es el último octeto. Por lo tanto, la dirección de red es 192.168.1.0. 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. En este ejemplo se utiliza la siguiente dirección de red: 192.168.1.0/24.

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 192.168 1.0/24
```

Starting Nmap 7.40 (<https://nmap.org>) at 2017-05-01 17:13 EDT

Nmap scan report for 192.168.1.1 Host
is up (0.0097s latency).

Not shown: 996 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

21/tcp	open	ftp	Bftpd 1.6.6
--------	------	-----	-------------

53/tcp	open	domain	dnsmasq 2.15-OpenDNS-1 dns-nsid:
--------	------	--------	---------------------------------------

id.server:

__ bind.version: dnsmasq-2.15-OpenDNS-1

80/tcp	open	tcpwrapped	
--------	------	------------	--

http-auth:

HTTP/1.0 401 Unauthorized\x0D

__ Basic realm=NETGEAR WNR3500Lv2

__http-title: 401 Unauthorized

5000/tcp	opentcpwrapped	Service
----------	----------------	---------

Info: Host: 192.168.1.1

```
Nmap scan report for 192.168.1.19 Host
is up (0.00016s latency).
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
22/tcp    open  sshOpenSSH 7.4 (protocol 2.0) |
ssh-hostkey:
|   2048 f1:61:50:02:94:ba:f2:bd:be:93:cf:14:58:36:b8:32 (RSA)
|_  256 94:33:25:a5:0e:02:d7:bc:c8:bo:90:8a:a2:16:59:e5 (ECDSA)
23/tcp    open  telnet   Openwall GNU/*/Linux telnetd
80/tcp    open  http     nginx 1.12.0
|_http-server-header: nginx/1.12.0 |_http-title:
Welcome to nginx!
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kernel
<some output omitted>
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .
Nmap done: 256 IP addresses (5 hosts up) scanned in 34.21 seconds

¿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. **Abran un navegador web y diríjanse a scanme.nmap.org. Lean 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@sec0ps Desktop]$ nmap -A -T4 scanme.nmap.org
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 16:46 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156) Host
is up (0.040s latency).
Other addresses for 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:bo: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
9929/tcp   open      nping-echo    Nping echo
31337/tcp  open      tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 23.96 seconds

- c. **Revisen los resultados y respondan las siguientes preguntas.**
d.

¿Que puertos y servicios están abiertos?

¿Que puertos y servicios están filtrados?

¿Cuál es la dirección IP del servidor?

¿Cuál es el sistema operativo?

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?