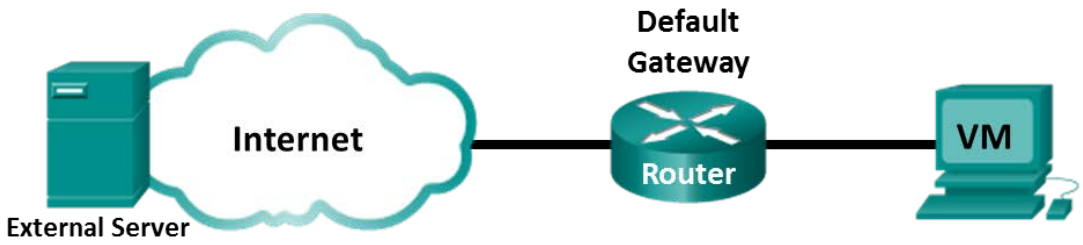
Lab - Exploring Nmap

Topology



Objectives

Part 1: Exploring Nmap

Part 2: Scanning for Open Ports

Background / Scenario

Port scanning is usually part of a reconnaissance attack. There are a variety of port scanning methods that can be used. We will explore how to use the Nmap utility. Nmap is a powerful network utility that is used for network discovery and security auditing.

Required Resources

- CyberOps Workstation Virtual Machine
- Internet access

Part 1: Exploring Nmap

In this part, you will use manual pages (or man pages for short) to learn more about Nmap.

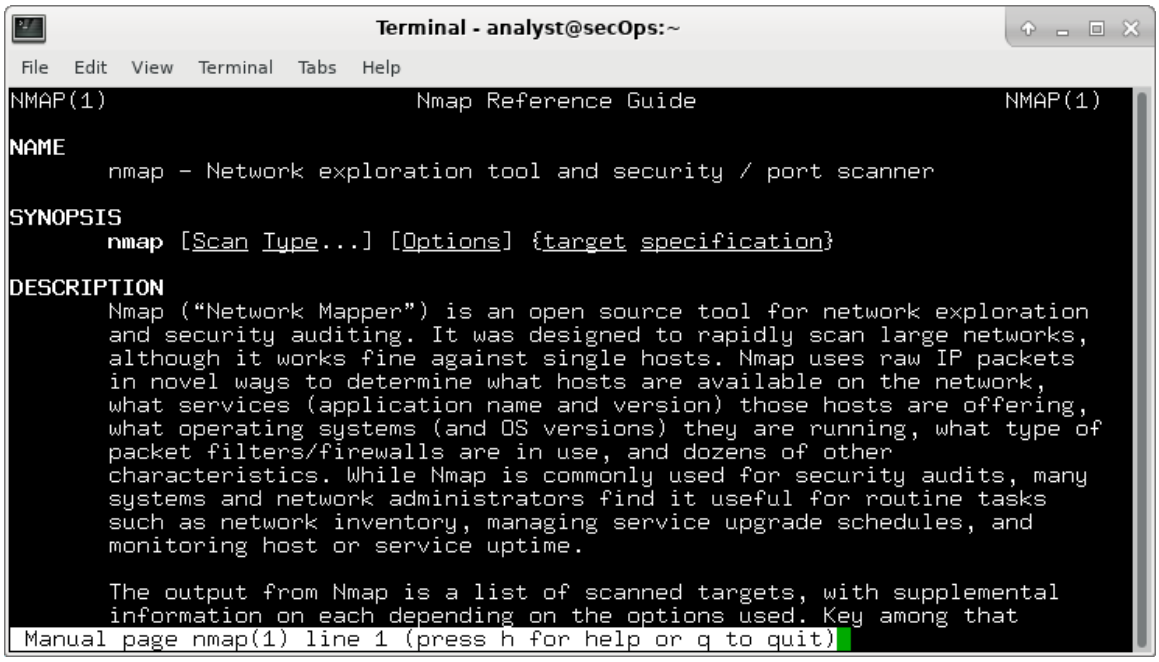
The **man** [*program* |*utility* | *function*] command displays the manual pages associated with the arguments. The manual pages are the reference manuals found on Unix and Linux OSs. These pages can include these sections: Name, Synopsis, Descriptions, Examples, and See Also.

a. Start CyberOps Workstation VM.

b. Open a terminal.

c. At the terminal prompt, enter **man nmap**.

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



What is Nmap?

_____

What is nmap used for?

_____

_____

_____

_____

d. While in the man page, you can use the up and down arrow keys to scroll through the pages. You can also press the space bar to forward one page at a time.

To search for a specific term or phrase use enter a forward slash (/) or question mark (?) followed by the term or phrase. The forward slash searches forward through the document, and the question mark searches backward through the document. The key **n** moves to the next match.

Type **/example** and press ENTER. This will search for the word **example** forward through the man page.

```
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
```

e. In the first instance of example, you see three matches. To move to the next match, press **n**.

```
Terminal - analyst@secOps:~
File  Edit  View  Terminal  Tabs  Help
       A typical Nmap scan is shown in Example 1. The only Nmap arguments used
       in this example are -A, to enable OS and version detection, script
       scanning, and traceroute; -T4 for faster execution; and then the
       hostname.

       Example 1. A representative Nmap scan

           # nmap -A -T4 scanme.nmap.org

           Nmap scan report for scanme.nmap.org (74.207.244.221)
           Host is up (0.029s latency).
           rDNS record for 74.207.244.221: li86-221.members.linode.com
           Not shown: 995 closed ports
           PORT     STATE    SERVICE     VERSION
           22/tcp   open     ssh         OpenSSH 5.3p1 Debian 3ubuntu7 (protocol
 2.0)
           | ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (
DSA)
           |_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
           80/tcp   open     http        Apache httpd 2.2.14 ((Ubuntu))
           |_http-title: Go ahead and ScanMe!
           646/tcp  filtered ldp
           1720/tcp filtered H.323/Q.931
 Manual page nmap(1) line 44 (press h for help or q to quit)
```

Look at Example 1. What is the **nmap** command used?

_____

Use the search function to answer the following questions.

What does the switch -A do?

_____

_____

What does the switch -T4 do?

_____

_____

_____

f. Scroll through the page to learn more about nmap. Type **q** when finished.

Part 2: Scanning for Open Ports

In this part, you will use the switches from the example in the Nmap man pages to scan your localhost, your local network, and a remote server at scanme.nmap.org.

Step 1: Scan your localhost.

a. If necessary, open a terminal on the VM. At the prompt, enter **nmap -A -T4 localhost**. Depending on your local network and devices, the scan will take anywhere from a few seconds to a few minutes.

```
[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  ssh     OpenSSH 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:b0:90:8a: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. Review the results and answer the following questions.

Which ports and services are opened?

_____

For each of the open ports, record the software that is providing the services.

_____

What is the operating system?

_____

Step 2: Scan your network.

Warning: Before using Nmap on any network, please gain the permission of the network owners before proceeding.

a. At the terminal command prompt, enter **ifconfig** to determine the IP address and subnet mask for this host. For this example, the IP address for this VM is 192.168.1.19 and the subnet mask is 255.255.255.0.

```
[analyst@secOps ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.19  netmask 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
```

Record the IP address and subnet mask for your VM. Which network does your VM belong to?

_____

b. To locate other hosts on this LAN, enter **nmap -A -T4** ***network address/prefix***. The last octet of the IP address should be replaced with a zero. For example, in the IP address 192.168.1.19, the .19 is the last octet. Therefore, the network address is 192.168.1.0. The /24 is called the prefix and is a shorthand for the netmask 255.255.255.0. If your VM has a different netmask, search the Internet for a “CIDR conversion table” to find your prefix. For example, 255.255.0.0 would be /16. The network address 192.168.1.0/24 is used in this example

Note: This operation can take some time, especially if you have many devices attached to the network. In one test environment, the scan took about 4 minutes.

```
[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 open  tcpwrapped
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  ssh     OpenSSH 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:b0:90:8a: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
```

How many hosts are up?

_____

From your Nmap results, list the IP addresses of the hosts that are on the same LAN as your VM. List some of the services that are available on the detected hosts.

_____

_____

_____

Step 3: Scan a remote server.

a. Open a web browser and navigate to **scanme.nmap.org**. Please read the message posted. What is the purpose of this site?

_____

b. At the terminal prompt, enter **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 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: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
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. Review the results and answer the following questions.

Which ports and services are opened?

_____

Which ports and services are filtered?

_____

What is the IP address of the server?

_____

What is the operating system?

_____

Reflection

Nmap is a powerful tool for network exploration and management. How can Nmap help with network security? How can Nmap be used by a threat actor as a nefarious tool?

_____

_____

_____

_____