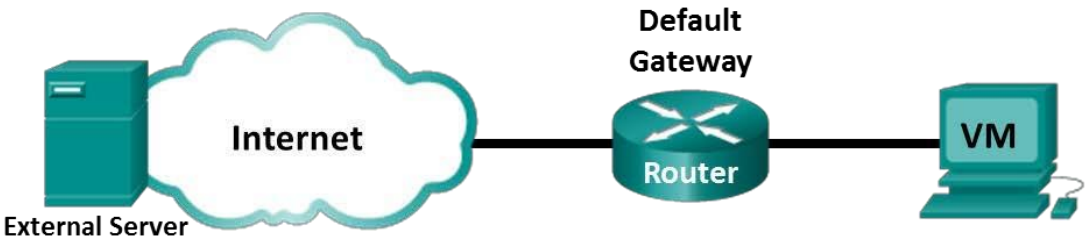
Lab 4.5.2.10 - Exploring Nmap

This lab has been updated for use on NETLAB+.
www.netdevgroup.com

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.

Part 1: Exploring Nmap

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

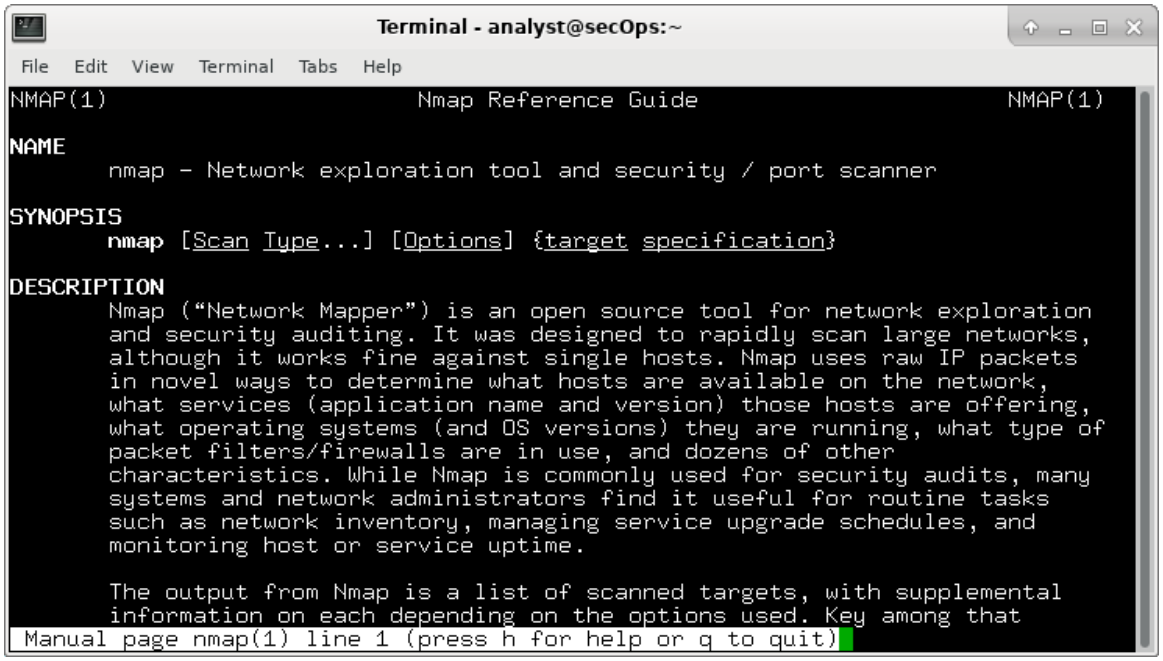
The **man** [*program* |*utility* | *function*] command displays the manual pages associated with the arguments. The manual pages are the reference manuals found on Unix and Linux OSs. These pages can include these sections: Name, Synopsis, Descriptions, Examples, and See Also.

a. Launch the **CyberOps** VM. Log in with username `analyst` and the password `cyberops`.

b. Open a **terminal**.

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

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



What is *Nmap*?

Network Mapper is a Network Exploration tool and security / port scanner. .

What is *Nmap* used for?

Network Mapper is a Exploration tool is used for explores networks and finding hosts and IP addresses, Nmap is a tool for monitoring network activity and detecting topological changes and some Nmap include host discovery and operating systems.

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, 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?

nmap -A -T4 scanme.nmap.org

Use the search function to answer the following questions.

What does the switch *-A* do?

-A: Enable OS detection, version detection, script s scanning, and traceroute.

What does the switch *-T4* do?-

T4 can be used to speed up execution by establish dynamic scan delays do not exceed 10 ms.

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 (*Metasploitable*).

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 ~]$ 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?

21/tcp: ftp, 22/tcp: ssh, 23/tcp: telnet, 80/ tcp : http .

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

ftp:vsftpd, Ssh: Open SSH , Telnet: Openwall , http:nginx.

What is the operating system?

Linux.

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 *192.168.0.11* and the subnet mask is *255.255.255.0*.

```
[analyst@secOps ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.11  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe23:b231  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:23:b2:31  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?

The VM IP is address of 192.168.0.11 and netmask 255.255.255.0.

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 192.168.0.11, the .11 is the last octet. Therefore, the network address is 192.168.0.0. 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 *192.168.0.0/24* 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 192.168.0.0/24
```

```
[analyst@secOps ~]$ nmap -A -T4 192.168.0.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2018-03-30 14:11 EDT
Nmap scan report for 192.168.0.10
Host is up (0.0012s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 5s, deviation: 0s, median: 5s
|_nbstat: NetBIOS name: WIN-8H4SOVG3LCL, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:82:da:48 (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server supports SMBv2 protocol

Nmap scan report for 192.168.0.11
Host is up (0.0012s 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  2017 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?
80/tcp open  http    nginx 1.12.0
|_http-server-header: nginx/1.12.0
|_http-title: Welcome to nginx!
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 253.10 seconds
```

How many hosts are up?

They are 2 hosts 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.

There are service info Oss: Windows, Host : Welcome , service detection performed 256 IP addresses.

Step 3: Scan a remote server.

a. At the terminal prompt, enter **nmap -A -T4 209.165.200.235**.

```
[analyst@secOps ~]$ nmap -A -T4 209.165.200.235
```

```
[analyst@secOps ~]$ nmap -A -T4 209.165.200.235

Starting Nmap 7.40 ( https://nmap.org ) at 2018-03-30 14:23 EDT
Nmap scan report for 209.165.200.235
Host is up (0.0016s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet?
25/tcp   open  smtp?
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODE
S, 8BITMIME, DSN,
|_ssl-date: 2018-03-30T18:36:07+00:00; +9m00s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
53/tcp   open  domain       ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2            111/tcp  rpcbind
|   100000  2            111/udp  rpcbind
|   100003  2,3,4       2049/tcp  nfs
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3      39371/udp  mountd
|   100005  1,2,3      57525/tcp  mountd
|   100021  1,3,4      33215/tcp  nlockmgr
|   100021  1,3,4      56159/udp  nlockmgr
|   100024  1          43862/tcp  status
|_  100024  1          56670/udp  status
139/tcp  open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec?
513/tcp  open  login?
514/tcp  open  shell?
1099/tcp open  java-rmi     Java RMI Registry
1524/tcp open  shell        Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003)
2121/tcp open  ccproxy-ftp?
3306/tcp open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
5432/tcp open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is n
o such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2018-03-30T18:34:46+00:00; +9m00s from scanner time.
5900/tcp open  vnc          VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11          (access denied)
6667/tcp open  irc          UnrealIRCd
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown      Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
Service Info: Hosts: localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 8m59s, deviation: 0s, median: 8m59s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2018-03-30T14:34:46-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 347.61 seconds
```

b. Review the results and answer the following questions.

Which ports and services are opened?

The opened ports and services 22/TCP: Open SSH, 5900/tcp : Open vnc

Which ports and services are filtered?
11/TCP:rpcbind ;139/TCP : netbios-ssn

What is the operating system?
Linux.

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?

Nmap can be used to create a map of the network, including the devices and services on the network, which can help network administrators identify potential vulnerabilities and misconfigurations. Nmap can be used to scan for open ports on a device, which can help network administrators identify and close ports that may be open and insecure.
Nmap can be used to scan a network for open ports, which can be used by an attacker to identify vulnerable services or applications that can be exploited. Nmap can detect the operating system of a target device, which can help an attacker tailor their attacks to the specific vulnerabilities of that system.