Lab - Use a Port Scanner to Detect Open Ports

Objectives

Use Nmap, a port scanner and network mapping, tool to detect open ports.

Background / Scenario

Network Mapper, or Nmap, is an open-source utility used for network discovery and security auditing. A common task is to scan local machines to determine potential vulnerabilities including open and unmanaged ports. All workstations require open ports and services to communicate and perform tasks like printing, sharing a file, or browsing the web. Administrators also use Nmap for monitoring hosts or managing service upgrade schedules. Nmap determines what hosts are available on a network, what services are running, what operating systems are running, and what packet filters or firewalls are running. In this lab, you will use Nmap inside your VM environment to detect open ports.

Introduction to TCP/UDP Ports

All communication that happens over the internet is exchanged using ports. Every IP host can use two types of ports: TCP and UDP. There can be up to 65,535 of each for any given IP address.

Services that connect to the internet (like web browsers, email clients, and file transfer services) use specific ports to receive information. Therefore, each logical connection is assigned a specific number. The port number also identifies which port it must send or receive traffic through when communicating. The Internet Assigned Number Authority (IANA) assigned the official port numbers and divided these ports into three sub-categories:

- Well-Known Ports (0-1023)
- Registered Ports (1024 - 49,151)
- Dynamic / Private Ports (49,152 - 65,535)

The following lists common ports:

20 - File Transfer Protocol - Data (FTP-DATA)

21 - File Transfer Protocol - Control (FTP)

22 - Secure Shell (SSH)

23 - Telnet (TELNET)

25 - Simple Mail Transfer Protocol (SMTP)

53 - Domain Name System (DNS)

67 - Client to server Dynamic Host Configuration Protocol v4 (DHCPv4)

68 - Server to client Dynamic Host Configuration Protocol v4 (DHCPv4)

69 - Trivial File Transfer Protocol (TFTP)

80 - Hypertext Transfer Protocol (HTTP)

Security of Logical Ports

Every logical port is subject to a threat and poses a vulnerability to a system, but some of the commonly used ports receive a lot of attention from attackers. Over 75% of all cyberattacks involve just a few common ports.

Attackers scan systems to identify opened ports on a target system. Here is a list of potential logical ports that are the most common targets of cybercriminals:

20/21 FTP	67/68 BOOTP	123 NTP
22 SSH	69 TFTP	137-139 NetBIOS
23 Telnet	80 HTTP	143 IMAP
25 SMTP	110 POP3	161 SNMP
50/51 IPsec	111 Port Map	389 LDAP
53 DNS	119 NNTP	443 SSL

Required Resources

- PC with the **CSE-LABVM** installed in VirtualBox.

Instructions

Step 1: Open a terminal window in the CSE-LABVM.

a. Launch the **CSE-LABVM**.

b. Double-click the **Terminal** icon to open a terminal.

Step 2: Run Nmap.

At the command prompt, enter the following command to run a basic scan against this system:

```
cisco@labvm:~$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 14:14 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000035s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

The results are a scan of the first 1024 TCP ports.

What TCP ports are open?

Provide a description of the service associated with each open port.

Research the vulnerabilities associated with each of these open ports.

Step 3: Use administrative privileges with Nmap.

a. Type the following command in the terminal to scan the computer's UDP ports (remember, Ubuntu is case sensitive) and enter the password **password** when prompted:

```
cisco@labvm:~$ sudo nmap -sU localhost
[sudo] password for cisco:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 14:18 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed ports
PORT     STATE         SERVICE
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds
```

What UDP ports are open?

Describe the purpose of the UDP services associated with each port.

Research the vulnerabilities associated with each of these open ports.

b. Type the following command in the terminal:

```
cisco@labvm:~$ nmap –sV localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 14:19 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000038s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
23/tcp  open  telnet  Linux telnetd
631/tcp open  ipp     CUPS 2.3
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 6.34 seconds
```

Using the **–sV** switch with the **nmap** command performs a version detection which you can use to research vulnerabilities.

Step 4: Capture SSH keys.

a. Type the following command in the terminal to initiate a script scan:

```
cisco@labvm:~$ nmap –A localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 14:21 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000037s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
```

```
22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 56:68:77:00:41:7f:50:17:5b:73:82:36:47:c4:bc:2d (RSA)
|   256 0e:52:78:ba:08:2a:df:e5:be:1b:07:a7:98:3a:c8:50 (ECDSA)
|_  256 f7:9e:03:10:96:94:cc:f4:4f:2a:f2:7c:6a:37:c1:6f (ED25519)
23/tcp  open  telnet  Linux telnetd
631/tcp open  ipp     CUPS 2.3
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/2.3 IPP/2.1
|_http-title: Home - CUPS 2.3.1
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 13.37 seconds
```

You captured the SSH keys for the host system. The command runs a set of scripts built into Nmap to test specific vulnerabilities.

What are the values of the SSH hostkeys?

How would an attacker use this information?

How could you prevent the cyber attacker from stealing the key information?

b. Enter the **man nmap** command to open the manual pages for the Nmap utility.

```
cisco@labvm:~$ man nmap
NMAP(1)                          Nmap Reference Guide                   NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}
<output omitted>
```

You can use this resource to locate other available options for the Nmap utility. At any time, enter **q** or **quit** to exit the man pages. You can read the manual pages available for any service or command by entering the **man** command followed by the name of the utility or command.

Summary

Highly Vulnerable Ports

Many ports must be open for a host to function in a normal computing and communication environment. However, these common ports should be monitored regularly to ensure they are not compromised and being used to attack a victim, provide unauthorized remote access, or being used to hijack a host to participate in a distributed attack on other victims.

Port 21 of TCP is one of the most popular ports for attackers. This port is designed to transmit and receive files from one host to another. Attackers use this port to perform the following types of malicious activity:

- Unauthorized transfer, deletion, and modification of files
- Unauthorized transfer of malicious code or payloads
- Anonymous authentication to host file systems
- Inject malicious scripts like XSS attack
- Impact the availability of other host services

Another common target is port 23 (Telnet). This port provides authorized remote access to an IP host. This port poses a vulnerability because the data transferred is in plaintext. Attackers use this port to perform the following types of malicious activity:

- Gain unauthorized remote access to a host
- Plant backdoors and other types of malicious code
- View sensitive data and credentials
- Perform man-in-the-middle attacks
- Impact the availability of other host services

Another favorite port for attackers is port 53. This port is used for DNS or looking up domain names when browsing the internet or transferring information. This port is the most common exit route for the attacker after an attack. Because this port is rarely monitored, attackers use this port to exit after clearing their files, logs, and other information to cover their tracks.

The most common port used by attackers is TCP port 80. This port transfers webpages between a web server and the host browser. Attackers use this port to perform the following types of malicious activity:

- Unauthorized transfer, deletion, and modification of data
- Unauthorized transfer of malicious code or payloads
- Injection of malicious scripts (like an XSS attack)
- Impact the availability of other host services

Answer Key

Step 1: Open a terminal window in the CSE-LABVM.

Step 2: Run Nmap.

What TCP ports are open?

Ports 22, 23, and 631

Provide a description of the service associated with each open.

Port 22 - SSH (Secure Shell) is a remote administration protocol used to control and modify a remote server over the internet. SSH authenticates the remote user and uses cryptography to encrypt all communications to and from the remote server.

Port 23 - Telnet provides a command line interface for communication with a remote server and transmits using clear-text (there is no encryption)

Port 631 - CUPS allows a computer to act as a print server. A system running CUPS can accept print jobs from clients and send the print jobs to the appropriate printer. CUPS uses IPP (Internet Printing Protocol).

Research the vulnerabilities associated with each of these open ports.

Answers may vary.

An unauthorized user only needs your username and password to gain access to a server with an open SSH port. You may see many attempts to log in to the server with default or common logins to gain access.

Other common targets are ports 22 and 23 (SSH) and (Telnet). These ports are designed to provide authorized remote access to an IP host. Port 23 is essentially unsafe because the data transferred in plaintext. Port 22 is much more secure and is preferred when connecting to a remote host. These ports can be utilized by cybercriminals to perform the following types of malicious activity.

- **Gain authorized remote access to a host.**
- **Plant backdoors and other types of malicious codes.**
- **View sensitive data and credentials.**
- **Perform man-in-the-middle attacks.**
- **Impact the availability of other host services.**

UDP Port 631 is a popular protocol in TCP/IP networks.

The term CUPS (Common UNIX Printing System) is modular network printing service for Linux host which allows a computer to act as a print server. UPS consists of a print spooler and scheduler, a filter system that converts the print data to a format that the printer will understand, and a backend system that sends this data to the print device.

An unauthorized user may be able to execute arbitrary commands with the privileges of the CUPS daemon. Additionally, a remote DoS may cause the server to be unresponsive.

Step 3: Use administrative privileges with Nmap.

What UDP ports are open?

Ports 68, 631, and 5353

Describe the purpose of the UDP services associated with each port.

Port 67 and 68 provide client-server Dynamic Host Configuration Protocol (DHCP) services. The DHCP is a network management protocol used on Internet Protocol (IP) networks. It dynamically assigns an

IP address and other network configuration parameters to host on the network. This information is required for IP hosts to communicate with other hosts on the IP networks.

UDP Port 631 is used by client applications for CUPS printing services.

Port 5353 is used to discover network peripherals on the local network.

Research the vulnerabilities associated with each of these open ports.

Answers may vary.

An open port 68 provides Dynamic Host Configuration Protocol (DHCP) services.

This port allows hackers to disrupt dynamic network addressing and can be used for network spoofing and remote code execution.

An open port 631 allows cyber attackers to cause a denial of service and possibly execute arbitrary code.

An open port 5353 is used by Multicast Domain Name System (mDNS) which allows hosts to resolve hostnames to IP addresses in small networks that do not include a name server. However, if the mDNS port 5353 is exposed to the internet, attackers can query the service to collect information about the server as well as launch a DoS attack by spoofing a target and flooding the network with mDNS requests.

Step 4: Capture SSH keys.

What are the values of the SSH hostkeys?

| ssh-hostkey:

| 3072 56:68:77:00:41:7f:50:17:5b:73:82:36:47:c4:bc:2d (RSA)

| 256 0e:52:78:ba:08:2a:df:e5:be:1b:07:a7:98:3a:c8:50 (ECDSA)

|_ 256 f7:9e:03:10:96:94:cc:f4:4f:2a:f2:7c:6a:37:c1:6f (ED25519)

How would an attacker use this information?

This information could be used to gain unauthorized remote access to the target host.

How could you prevent the cyber attacker from stealing the key information?

Send the keys by phone, text, or email. This is called out-of-band key exchange.