Lab – Detecting Threats and Vulnerabilities

Objectives

Use Nmap, a port scanner and network mapping tool to detect threats and vulnerabilities on a system.

Background / Scenario

Network Mapper, or Nmap, is an open source utility used for network discovery and security auditing. 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.

Required Resources

- PC with Ubuntu 16.0.4 LTS installed in a virtual machine - you can use the VM from labs completed in chapter 2.

Step 1: Open a terminal window in Ubuntu.

a. Log in to Ubuntu using the following credentials:

User: **cisco**

Password: **password**

b. Click on 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 Ubuntu system:

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

```
cisco@ubuntu:~$ nmap localhost
```

```
cisco@ubuntu:~$ nmap localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:43 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
cisco@ubuntu:~$
```

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

What TCP ports are open?

_____

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@ubuntu:~$ sudo nmap -sU localhost
```

```
cisco@ubuntu:~$ sudo nmap -sU localhost
[sudo] password for cisco:

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:47 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
cisco@ubuntu:~$
```

What UDP ports are open?

_____

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

b. Type the following command in the terminal:

```
cisco@ubuntu:~$ nmap -sV localhost
```

```
cisco@ubuntu:~$ nmap -sV localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:53 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
23/tcp open  telnet  Linux telnetd
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 0.97 seconds
cisco@ubuntu:~$
```

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

Step 4: Capture SSH keys.

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

```
cisco@ubuntu:~$ nmap -A localhost
```

```
cisco@ubuntu:~$ nmap -A localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:56 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000050s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 83:35:a7:81:c7:04:47:d4:6b:b4:87:b3:e3:5b:c7:ab (RSA)
|_  256 78:97:1f:92:cf:38:63:90:c3:7f:d5:ff:85:43:e6:2f (ECDSA)
23/tcp open  telnet  Linux telnetd
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 1.16 seconds
cisco@ubuntu:~$
```

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

References

Nmap: https://nmap.org/

© 2017 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.