PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Networks and Cybersecurity Essentials (ACCA4024)

Lab 7: Tools to check on Threats and Vulnerabilities

Cisco | Networking Academy®
Mind Wide Open™

Objectives

Using Packet Capturing tools and network monitoring tools.

Tasks

1. Use Nmap to scan
2.

Required Resources

- PC with Ubuntu 16.0.4 LTS installed in a VirtualBox or VMware virtual machine. (*Alternatively*, Any Linux Platform)
- Internet Connection to refer the outcomes
- References: https://nmap.org/

Task 1

➔ Login as User Cisco.

➔ Go to Terminal and Type the following commands and examine

- To do that we are using Nmap.
  - 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,
    - What packet filters or firewalls are running?
- So, basically if you could get all the above details using Nmap, you could get few information which could be used later in performing attacks or mitigating attacks.

➔ Commands to execute

- Step 1:
  - **nmap localhost**

(This is a scan performed to get information about the services that are bound to the localhost)

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-11-16 09:35 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00015s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
23/tcp   open  telnet
631/tcp open  ipp
```

- Step 2:
  - **Replace the above command with your IP Address and other hosts (if connected/ else ignore) in your network to check the outcomes.**

Type the command you used to find out your host IP Address

ifconfig

Type the command you used to scan after finding your host IP Address

nmap 10.0.2.15

Record the outcomes of the above command here

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-11-16 09:36 CST
Nmap scan report for 10.0.2.15
Host is up (0.0038s 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 0.09 seconds
```

- Step 3: Analyse the outputs/outcomes from Step 1 and 2 and record your reflections. (Hint: Analyse what is the difference between local host and ip address of the host, If ports displayed are different, Why is it different? etc (not limited to the hints))

The target 'localhost' displays an additional open port: 631/ipp.

All devices on a network can view the status of ports using target '10.0.2.15'
Only the host can view the status of ports with target 'localhost' or '127.0.0.1'

Although both relate to the host machine, they are not interchangeable so port configuration can vary.

- Step 4: Why is the nmap scan only scans the first 1000 ports? What will be the command to scan all the ports?

These are the most commonly used ports.

nmap -p- localhost * Ports 1-65535 *
nmap -p0-65535 localhost * Includes port 0 *

- Step 5: Scan the UDP Ports
  - **nmap –sU localhost**

    (This is a scan performed to get information about the UDP ports and to execute this command you need root privileges. So, try)

  - **sudo nmap –sU localhost**

Record the outcomes of the above command here (Hint: what UDP ports could you find open through your scan)

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-11-16 11:10 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000070s latency).
Not shown: 997 closed ports
PORT      STATE         SERVICE
68/udp    open|filtered dhcpc
631/udp   open|filtered ipp
5353/udp  open|filtered zeroconf
```

- Step 6: From the above outcomes select any ports which is open
  - **sudo nmap –p137 localhost**

    (Change the port number 137 to any port which you found as open in the previous step (5).)

Record the outcomes of the above command here (Hint: Is the port open or closed? Why? Also, record the use of –p command)

```
cisco@ubuntu:~$ sudo nmap -p631 localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2020-11-16 11:13 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
PORT     STATE SERVICE
631/tcp open  ipp
```

Open. It's typically used for communication between client device & printer. The -p command is used to specify a port or a range of ports to scan.

- Step 7: Try other port related commands and record its purpose.
  - **sudo nmap –p***portnumber host_ip*
  - **sudo nmap –p***portnumber_startrange-portnumber_endrange host_ip*
  - **sudo nmap –p***portnumber,portnumber host_ip*

- not limited to the above *(Do a google search, refine your search and find out other port related commands, Hint:nmap.org)*

Record the outcomes of the above commands here

> sudo nmap -p631 10.0.2.15
631/tcp closed ipp

> sudo nmap -p500-699 10.0.2.15
All 200 scanned ports on 10.0.2.15 are closed

> sudo nmap -p68,631 10.0.2.15
68/tcp closed dhcpc
631/tcp closed ipp

- Step 8: Detecting the version is a very important part of information gathering. Try to find out the version.
  - **nmap –sV localhost**

Record the outcomes of the above commands here

```
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000010s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.
0)
23/tcp   open  telnet  Linux telnetd
631/tcp open  ipp     CUPS 2.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Step 9: Try other commands to detect other versions and record its purpose.
  - Command to identify the Operating System version

Record the outcomes of the above commands here

> sudo nmap -O localhost
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.12 - 3.19, Linux 3.8 - 3.19

> sudo nmap -A 10.0.2.15
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 ...

> nmap -oN hostrecord.txt 10.0.2.15
* Standard port scan with output saved as a text file. *

- Command to identify the Service Version

Record the outcomes of the above commands here

```
cisco@ubuntu:~$ nmap -sV 10.0.2.15

Starting Nmap 7.01 ( https://nmap.org ) at 2020-11-16 13:44 CST
Nmap scan report for 10.0.2.15
Host is up (0.000033s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.
0)
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Learnings from tutorials so far:

Part 1 (Packet Tracer, Host Machines)

- ✓ ***Build a home Network***
- ✓ ***Understand and configure IP Address***
- ✓ ***Use Ping/ Trace route Utility to check the connection status***
- ✓ ***Use ipconfig /all command to determine the MAC address of a Windows computer on an Ethernet network.***
- ✓ ***Analyze a MAC address to determine the manufacturer.***
- ✓ ***Analyze the Wired and Wireless Network connection.***
- ✓ ***Analyze Address Resolution Protocol (ARP).***
- ✓ ***Connect to a Wireless Router and configure the basic settings in a wireless router and add security features.***
- ✓ ***Use nslookup command to understand the url to ip conversion.***
- ✓ ***Configure basic connectivity settings in Intermediate devices (Switch/ Router).***
- ✓ ***Work with SBA Packet Tracer Files/ environment***
- ✓ ***Configure ftp, web, email, dns, ntp and aaa Servers***

Part 2

- ✓ ***Set up a virtual lab environment***
- ✓ ***Troubleshooting the virtual lab environment***
- ✓ ***Working with virtual machines***
- ✓ ***Authentication, Authorization and Accounting***
- ✓ ***Threats and Vulnerabilities – Using NMAP***