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)

```
127.0.0.1 : Host is up ( 0.000058s latency)
Not shown: 997 closed ports
PORT   STATE  SERVICE
12/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

ipconfig

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

nmap 192.168.134.140 -Pn

Record the outcomes of the above command here

Host is shown up (0.0045s latency)
not shown: 995 filtered ports
135/tcp open msrpc
139/tcp open microsoft-ds
1947/tcp open sentinelsrm
6646/tcp open unkown

- 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))

Local host is the PCs default name ip address and the dynamic ip address is the address that connects to the network. Localhost is useful for web and software development / testing. The differences between the open ports are that the ports open for the ip address that connects to the web belong to services and software installed on my PC, the localhost is default must have services.

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

  -p- [ip address]

- 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)
  68, 631, 5353.
  dhcpc ipp 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)

  closed

- 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

1. when given a port number and ip address it will report the activity of the port. i checked port 68, its tcp protocol that is filterted runnin the DHCPC service
2. shows the range with n umber of portnumber open

- 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

shows the ssh and telnet service.
aswell as their port number and
version. Also states number of
closed ports

- 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

- Command to identify the Service Version

Record the outcomes of the above commands here

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***