CS 3710 Introduction to Cybersecurity
Term: Spring 2022

Lab Exercise 2 – Reconnaissance and Network Scanning Lab

Due Date: September 9, 2022 11:59pm
Points Possible: 7 points

Name: Jingtao Scott Hong jh4ctf

By submitting this assignment you are digitally signing the honor code, "On my honor, I pledge that I have neither given nor received help on this assignment."

1. Overview

This lab exercise will provide some hands-on experience with reconnaissance, network scanning, and service enumeration.

2. Resources required

This exercise requires a Kali Linux VM running in the Virginia Cyber Range.

3. Initial Setup

From your Virginia Cyber Range course, select the **Cyber Basics** environment. Click "start" to start your environment and "join" to get to your Linux desktop login.

4. Tasks

Task 1: Whois lookups

For this portion of the exercise, you can use a web browser on your laptop or desktop computer, or you can log in to your Cyber Basics environment in the Virginia Cyber Range.

WHOIS is a tool for querying databases containing domain registration data to determine ownership, IP addresses, and other information. A reverse whois lookup can be used to find domains that are registered by a particular individual or organization. ICANN is the authoritative source for WHOIS information, however due to the General Data Protection Regulation (GDPR) a lot of its information is now restricted. Other sources of WHOIS information include https://pk.godaddy.com/whois, and https://whois.domaintools.com/.

Question #1: Do a whois lookup on the domain **jmu.edu**. To whom is the domain registered? What is the administrative contact name, address, email, and phone number? (.5 point)

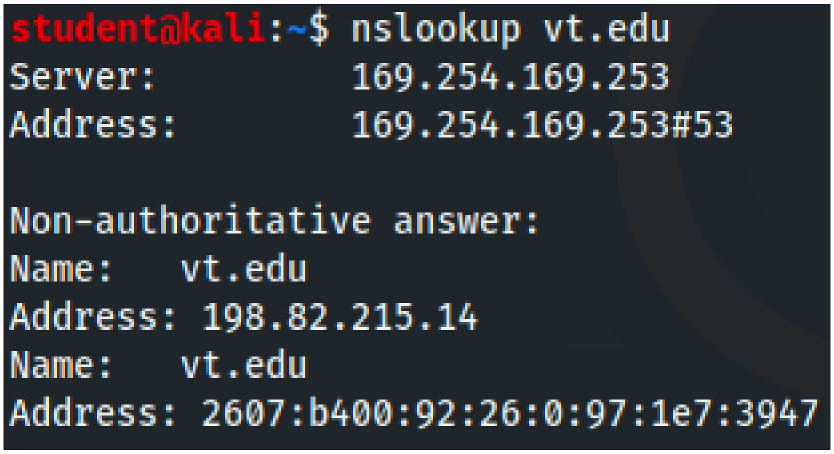
Domain Name: JMU.EDU
Administrative Contact: Dennis Little, James Madison University, Director, Enterprise Infrastructure, Massanutten Hall 265, MSC 5733, Harrisonburg, VA 22807, USA, +1.5405681676, littledr@jmu.edu

Task 2: nslookup and dig

Nslookup is a Linux and Windows tool for querying the distributed database that makes up the domain name system (DNS). This database translates host names (such as www.virginiacyberrange.org) to IP addresses (52.85.144.4). This translation is necessary because your computer must have the IP address of systems, such as web servers, that it communicates with, but humans are not good at remembering strings of numbers so we remember hostnames instead. DNS converts hostnames to the proper IP address so your web browser can find that web page. This DNS lookup usually happens in the background so users don't realize it is happening. You can use the nslookup tool to do this mapping from the command line.

For this exercise, you will log in to your Virginia Cyber Range account and select the Cyber Basics environment, then click "start" to start your environment and "join" to get to your Linux desktop login.

Question #2: Use **nslookup** to find the IP address for vt.edu. What is the IPv4 address? Provide a screen shot and explain where you found the answer. (.5 point)



```
student@kali:~$ nslookup vt.edu
Server:         169.254.169.253
Address:        169.254.169.253#53

Non-authoritative answer:
Name:   vt.edu
Address: 198.82.215.14
Name:   vt.edu
Address: 2607:b400:92:26:0:97:1e7:3947
```

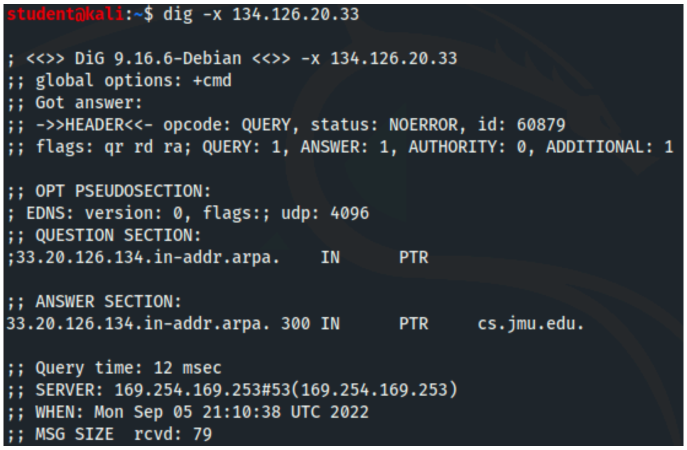
The IPv4 address if 198.82.215.14 which is the first address in the result.

Dig is another, and generally more powerful, tool for DNS database queries. However, dig is only available on Linux and Unix systems.

Question #3: Examine the Linux 'man page' for the dig utility to find more information about dig. What does the '**-x**' command-line option do in dig? (.5 point)

It performs the reverse lookup which maps addresses to names.

Question #4: Use dig to conduct a reverse lookup of the IP address 134.126.20.33. What is the hostname or hostnames correspond with that IP address? (.5 point)



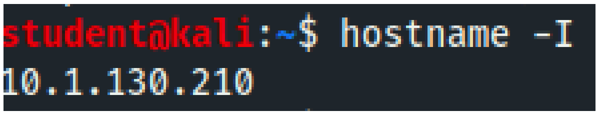
```
student@kali:~$ dig -x 134.126.20.33

; <<>> DiG 9.16.6-Debian <<>> -x 134.126.20.33
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60879
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;33.20.126.134.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
33.20.126.134.in-addr.arpa. 300 IN      PTR     cs.jmu.edu.

;; Query time: 12 msec
;; SERVER: 169.254.169.253#53(169.254.169.253)
;; WHEN: Mon Sep 05 21:10:38 UTC 2022
;; MSG SIZE  rcvd: 79
```

It is cs.jmu.edu.

Task 3: Network scanning using nmap

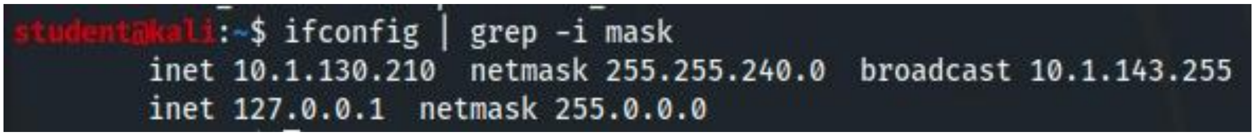
Your Kali Linux virtual machine in the Virginia Cyber Range is connected to a small network subnet with other systems. Your first step in this exercise is to understand your network neighborhood.

Question #5: What is your IPv4 address and netmask? (.5 point)



```
student@kali:~$ hostname -I
10.1.130.210
```

It's 10.1.130.210



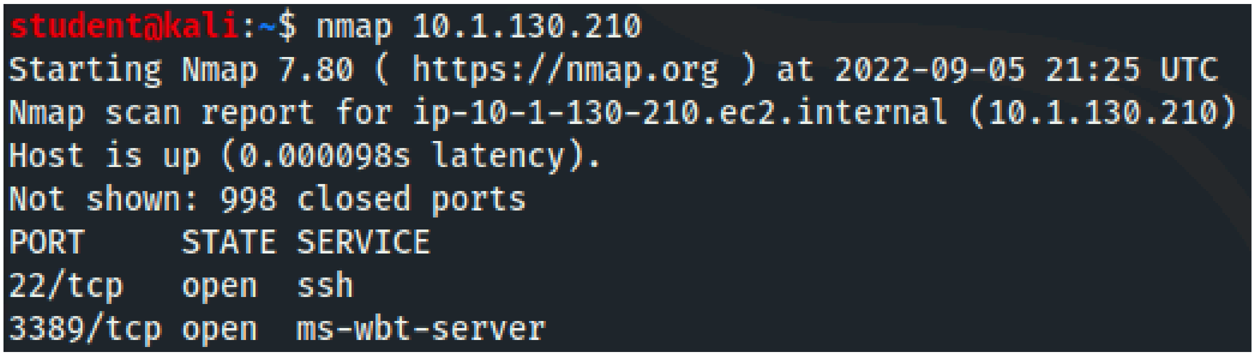
```
student@kali:~$ ifconfig | grep -i mask
        inet 10.1.130.210  netmask 255.255.240.0  broadcast 10.1.143.255
        inet 127.0.0.1  netmask 255.0.0.0
```

It is 255.255.240.0

There are different ways to accomplish host discovery on a network. For this exercise we will use Nmap (https://nmap.org/book/man.html), a widely used tool for network exploration and port scanning. Nmap can be used to scan a single hostname or IP address or range of addresses. You can learn more about Nmap through the man page (**man nmap**) or simply type **nmap** with nothing else and hit enter to see a summary of command options and usage. To scan a single host you would use the following command:

```
$ nmap <options> <hostname or IP address>
```

Question #6: Run an nmap scan against your own IP address. What ports are open? (.5 point)



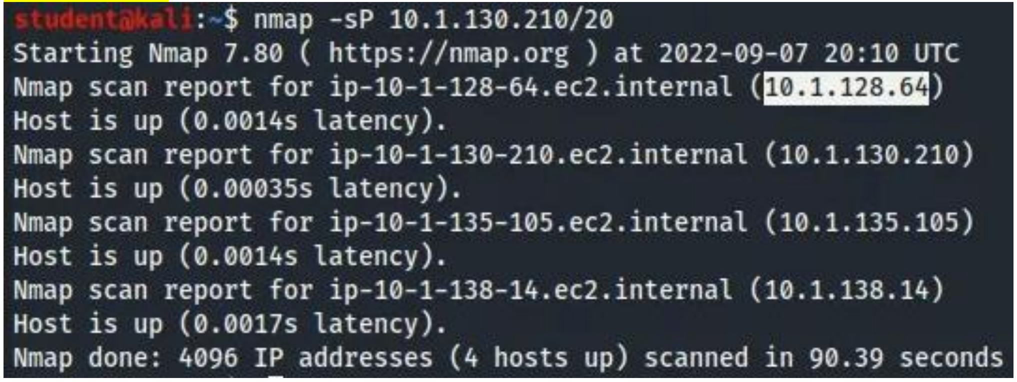
```
student@kali:~$ nmap 10.1.130.210
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-05 21:25 UTC
Nmap scan report for ip-10-1-130-210.ec2.internal (10.1.130.210)
Host is up (0.000098s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
3389/tcp open  ms-wbt-server
```

Port 22 SSH and Port 3389 ms-wbt-server is open.

Ping scan. Let's see what other systems are on the network by using Nmap's ping scan. Nmap has a ping scan option that simply sends a ping packet to each IP address and listens for replies to identify active hosts. For this scan you will scan your network using CIDR notation which looks like the following: **`your_IP_address/CIDR`**

You will replace **`your_IP_address`** with your actual IP that you identified in Question #5. The second part is to replace the **`CIDR`** with the actual CIDR notation for your network. Use your Google skills to find the CIDR notation of your network based on your netmask found in Question #5 and replace the word **`CIDR`** with it to scan the entire network where your system lives. Don't forget to give nmap the **ping scan only** option!

Question #7: Which active IP addresses did you discover on the network? (1 point)



```
student@kali:~$ nmap -sP 10.1.130.210/20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-09-07 20:10 UTC
Nmap scan report for ip-10-1-128-64.ec2.internal (10.1.128.64)
Host is up (0.0014s latency).
Nmap scan report for ip-10-1-130-210.ec2.internal (10.1.130.210)
Host is up (0.00035s latency).
Nmap scan report for ip-10-1-135-105.ec2.internal (10.1.135.105)
Host is up (0.0014s latency).
Nmap scan report for ip-10-1-138-14.ec2.internal (10.1.138.14)
Host is up (0.0017s latency).
Nmap done: 4096 IP addresses (4 hosts up) scanned in 90.39 seconds
```

I found 10.1.128.64, 10.1.130.210, 10.1.135.105, 10.1.138.14

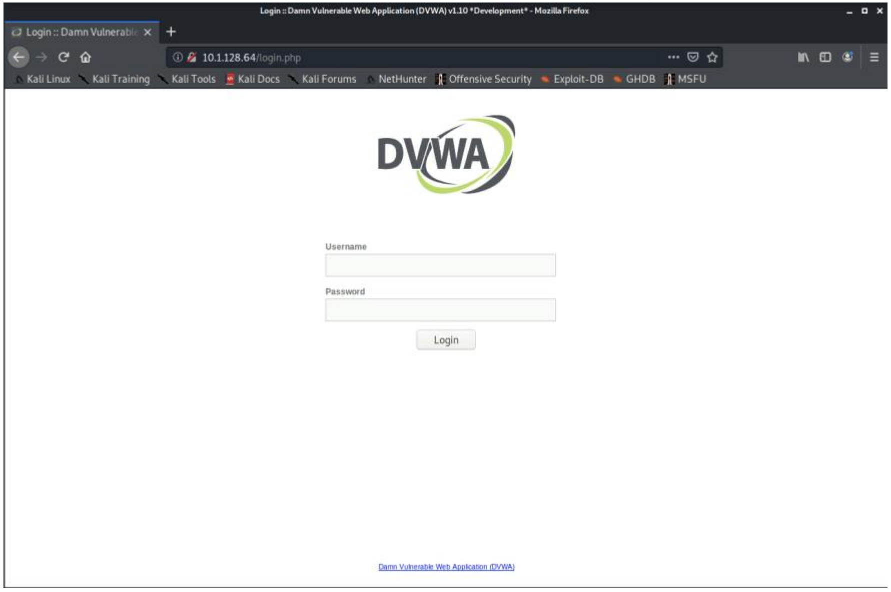
Port scan. By default, **`nmap`** will conduct a port scan of the target address(es), trying to connect to ports 1 – 1000 for each IP address scanned and report which ports it finds open, or "listening". Now that we have identified potential target systems we will scan them to identify open networking ports. Use **`nmap`** with *no options* to scan each host that you discovered in the step above.

Question #8: List each IP address that you scanned and the port numbers and services exposed on each system. (.5 point)

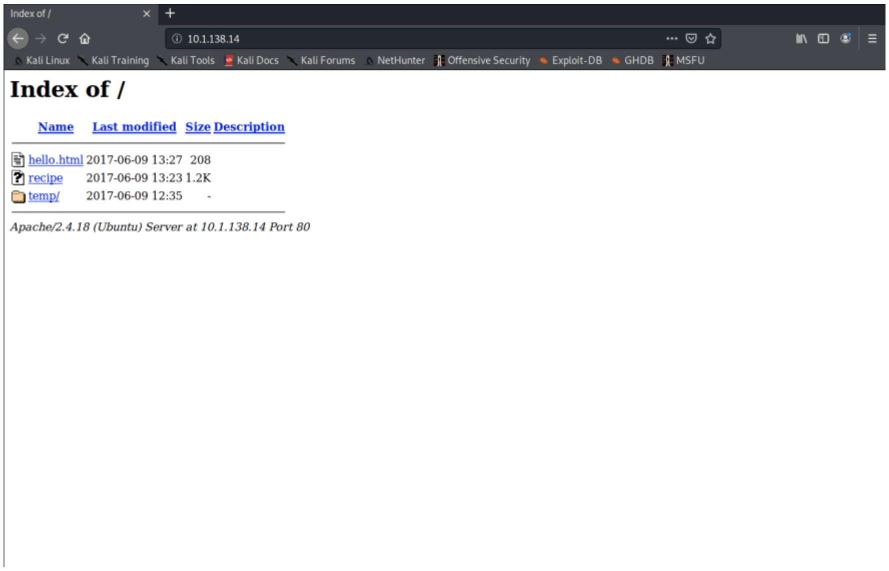
10.1.128.64: 80/tcp open http
10.1.130.210: 22/tcp open ssh | 3389/tcp open ms-wbt-server

10.1.135.105: 21/tcp open ftp
10.1.138.14: 22/tcp open ssh| 80/tcp open http | 139/tcp open netbios-ssn | 445/tcp open microsoft-ds

Question #9: Which systems (IPs) are possibly running a web server? If any of your targets are running a web server, provide a screen shot of the main web page of the server. (.5 point)



10.1.128.64



Index of /

Name	Last modified	Size	Description
hello.html	2017-06-09 13:27	208	
recipe	2017-06-09 13:23	1.2K	
temp/	2017-06-09 12:35	-	

Apache/2.4.18 (Ubuntu) Server at 10.1.138.14 Port 80

10.1.138.14

Question #10: **Version detection**. Now we need to look a little more to find out specifics about the open services you detected. Run an Nmap scan against each target that will perform version detection and show service versions. (there is more than one option that can do this) List all service versions that you find for each IP address. (1 point)

10.1.128.64

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	Apache httpd 2.4.25 ((Debian))

10.1.130.210

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 8.3p1 Debian 1 (protocol 2.0)
3389/tcp	open	ms-wbt-server	xrdp

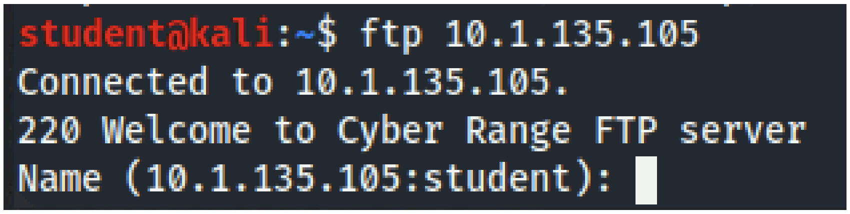
10.1.135.105

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.0.8 or later

10.1.138.14

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.18
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: MYGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: MYGROUP)

Question #11: Taking it one step further. Scanning is the first step to identify active targets, which we did in Question #7 and then to identify open ports and services, which we did in Question #8. By performing version detection like we did in Question #10 we can start to identify potential vulnerabilities. One of the targets you scanned has a File Transfer Protocol (FTP) server running, which is a vulnerable way to transfer files. The **`nmap -A`** scan can give you some really valuable information for logging into that FTP server. Exploit the anonymous FTP login and retrieve a file from the server and paste its contents here. (1 point)



```
student@kali:~$ ftp 10.1.135.105
Connected to 10.1.135.105.
220 Welcome to Cyber Range FTP server
Name (10.1.135.105:student): 
```

Welcome to Cyber Range FTP server

By submitting this assignment you are digitally signing the honor code, "I pledge that I have neither given nor received help on this assignment".

END OF EXERCISE

5. References

- http://viewdns.info/
- https://nmap.org/book/man.html
- https://en.wikipedia.org/wiki/Port_(computer_networking)
- https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing