

Lab Exercise 2 – Reconnaissance and Network Scanning Lab

Due Date: February 4, 2021 11:59pm

Points Possible: 7 points

Name: Joseph Bannon (jb9war)

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 **virginia.edu**. To whom is the domain registered? What is the administrative contact name, address, email, and phone number? (.5 point)

The registrant of virginia.edu is University of Virginia ITC, Carruthers Hall
P.O. Box 400198 Charlottesville, VA 22904-4198 USA

The administrative contact name is Network Systems University of Virginia Information Technology Services. The administrative address is P.O. Box 400324 Charlottesville, VA 22904-4324. The administrative email is networks@virginia.edu and the phone number is +1(434)-924-0621.



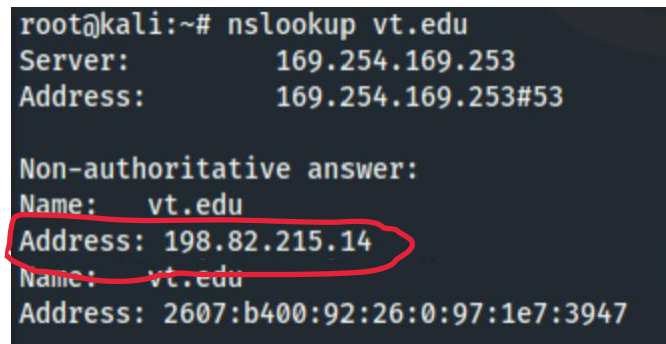
Task 2: nslookup and dig

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)

The IPv4 address is 198.82.215.14. The IPv4 address is found by the looking at the Non-authoritative answer (meaning the dns has the IP relayed from another server) and the IPv4 is the 64-bit dot delimited number. The server: 169.254.169.253 is the server that we used to query the Ip address/



```
root@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
```

Source: <https://www.fasthosts.co.uk/blog/guides/nslookup-explained/#:~:text=nslookup%20is%20an%20abbreviation%20of,of%20your%20chosen%20DNS%20server.>

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)

The -x option is a reverse dns lookup meaning you give an IP address and it tries to find the nameserver, if there is one.

Source: <https://linux.die.net/man/1/dig>



Question #4: Use dig to conduct a reverse lookup of the IP address 134.126.126.30. What is the hostname or hostnames correspond with that IP address? (.5 point)

The hostname that was found was flexecm.jmu.edu.

```
root@kali:~# dig -x 134.126.126.30

; <<>> DiG 9.16.6-Debian <<>> -x 134.126.126.30
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51136
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
30.126.126.134.in-addr.arpa. 300 IN PTR flexecm.jmu.edu.

;; Query time: 32 msec
;; SERVER: 169.254.169.253#53(169.254.169.253)
;; WHEN: Fri Jan 28 21:19:39 UTC 2022
;; MSG SIZE rcvd: 85
```

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)

The IPv4 is 10.1.161.156 and the netmask is 255.255.240.0.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.1.161.156 netmask 255.255.240.0 broadcast 10.1.175.255
    inet6 fe80::10cf:1eff:fe03:bedf prefixlen 64 scopeid 0x20<link>
    ether 12:cf:1e:03:be:df txqueuelen 1000 (Ethernet)
```

Source: <https://yourbusiness.azcentral.com/ip-address-subnet-mask-gateway-computer-14563.html>

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)

```
root@kali:~# nmap 10.1.161.156
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-28 21:28 UTC
Nmap scan report for ip-10-1-161-156.ec2.internal (10.1.161.156)
Host is up (0.0000040s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp   open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

The port 22 and 3389 both tcp ports are open. Port 22 is the secure shell port which allows for secure communication and port 3389 is a Microsoft remote desktop display.

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 Task 3a. 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 Task 3a 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 -sn 10.1.161.156/20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-29 00:49 UTC
Nmap scan report for ip-10-1-161-156.ec2.internal (10.1.161.156)
Host is up (0.00035s latency).
Nmap scan report for ip-10-1-162-108.ec2.internal (10.1.162.108)
Host is up (0.0015s latency).
Nmap scan report for ip-10-1-163-195.ec2.internal (10.1.163.195)
Host is up (0.0013s latency).
Nmap scan report for ip-10-1-174-249.ec2.internal (10.1.174.249)
Host is up (0.0013s latency).
Nmap done: 4096 IP addresses (4 hosts up) scanned in 56.94 seconds
```

Using the CIDR IP address: 10.1.161.156/20, there are four addresses on the network (10.1.161.156, 10.1.162.108, 10.1.163.195, 10.1.174.249).

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)

IP address:

10.1.161.156,

- 22/ tcp ssh - 3389/ tcp ms-wbt-server

10.1.162.108

- 80/tcp http

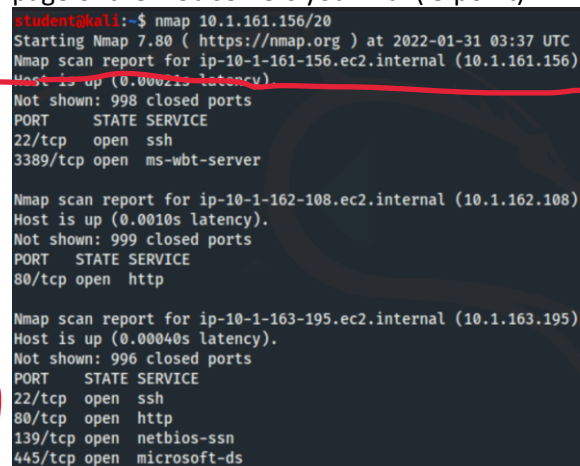
10.1.163.195

- 22/ tcp ssh - 80/ tcp http - 139/ tcp netbios-ssn - 445/tcp microsoft-ds

10.1.174.249

- 21/ tcp ftp

Question #9: Which systems (IPs) are running web server software? Provide a screen shot of the main page of the web servers you find. (.5 point)



```
student@kali:~$ nmap 10.1.161.156/20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-31 03:37 UTC
Nmap scan report for ip-10-1-161-156.ec2.internal (10.1.161.156)
Host is up (0.00021s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
3389/tcp   open  ms-wbt-server

Nmap scan report for ip-10-1-162-108.ec2.internal (10.1.162.108)
Host is up (0.0010s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http

Nmap scan report for ip-10-1-163-195.ec2.internal (10.1.163.195)
Host is up (0.00040s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

According to documentation, the port that runs web servers is port 80. The IP addresses that are running web servers are 10.1.162.108 and 10.1.163.195 and both of them are running http.

Source: <https://nmap.org/book/man-examples.html>

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)




```
student@kali:~$ nmap -sV 10.1.161.156/20
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-31 03:45 UTC
Nmap scan report for ip-10-1-161-156.ec2.internal (10.1.161.156)
Host is up (0.00011s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.3p1 Debian 1 (protocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for ip-10-1-162-108.ec2.internal (10.1.162.108)
Host is up (0.0048s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.25 ((Debian))

Nmap scan report for ip-10-1-163-195.ec2.internal (10.1.163.195)
Host is up (0.0048s latency).
Not shown: 996 closed ports
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)
Service Info: Host: IP-10-1-163-195; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for ip-10-1-174-249.ec2.internal (10.1.174.249)
Host is up (0.0056s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.8 or later
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4096 IP addresses (4 hosts up) scanned in 89.44 seconds
```

The IP address 10.1.161.156 was running ssh (OpenSSH 8.3p1 Debian 1) and ms-wbt-server xrdp. The IP 10.1.162.108 was running http (Apache httpd 2.4.25(Debian)). The IP 10.1.163.195 was running ssh (OpenSSH 7.2p2 Ubuntu 4ubuntu2.1), http (Apache httpd 2.4.18) and netbios-ssn (Samba smbd 3.x-4.x). The IP 10.1.174.249 was running ftp (vsftpd 2.0.8).

Question #11: Taking it one step further. Scanning is the first step to identify active targets, which we did in Task 3c and then to identify open ports and services, which we did in Task 3d. By performing version detection like we did in Task 3e we can start to identify potential vulnerabilities. One of the targets you scanned has an FTP server running, which is often vulnerable. 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)

The nmap -A command identified the FTP server (at ip 10.1.174.249 on port 21) as allowing anonymous logins. I then used the command ftp (ftp 10.1.174.249 21) with the username: anonymous and blank password to login. The online file was welcome.txt which had readable permission. I then copied the file to my file system using get command and the file contained "Welcome to Cyber Range FTP Server".

Source: <https://docs.oracle.com/cd/E19120-01/open.solaris/819-1634/remotehowtoaccess-87541/index.html>

<https://ecrax.github.io/2020/08/13/Anonymous-TryHackMe/>

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/Port_(computer_networking))
- https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

