

## Lab Exercise 2 – Reconnaissance and Network Scanning Lab

Due Date: February 3, 2023 11:59pm

Points Possible: 7 points

**Name:**

*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. org

### 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)

**Performed the whois lookup on "whois.domaintools.com". The domain is registered to the director of enterprise infrastructure at JMU. The administrative contact:**

- **Name:** Dennis Little
- **Address:** Massanutten Hall 265 MSC 5733 Harrisonburg, VA 22807
- **Email:** [littleldr@jmu.edu](mailto:littleldr@jmu.edu)
- **Phone Number:** 5405681676



## 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](http://www.virginiacyberrange.org)) to IP addresses (99.86.229.9). 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)

I believe that the IPv4 address is 169.254.169.253. I chose the authoritative answer for the address because this provides the most up-to-date information and non-authoritative answers come from lower level DNS servers such as local, root, and top-level servers.

```
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
```

Actually, when I performed a reverse lookup on the above address, the reverse lookup failed. But when I tried it on 198.82.215.14, the reverse lookup came up with the "cmsw-prod.hosting.vt.edu" hostname whereas the other address came up with "localhost.nobody.invalid." So, I would have to say that the IPv4 address is 198.82.215.14.

**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' command is a shortcut for reverse lookups. So normal lookups go from domain name to IP address but with the -x command we could go from IP address to domain name.

**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)

When "dig -x" was used on 134.126.20.33 I got the cs.jmu.edu hostname.



### 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)

I believe we can use the `ifconfig` command here for this. I believe we only care about the `eth0` entry as this is the entry exposed to the world.

```
student@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 10.1.85.134 netmask 255.255.240.0 broadcast 10.1.95.255
    inet6 fe80::1075:9eff:fe12:ae21 prefixlen 64 scopeid 0x20<link>
    ether 12:75:9e:12:ae:21 txqueuelen 1000 (Ethernet)
    RX packets 8135 bytes 620675 (606.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16533 bytes 16703724 (15.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 33 bytes 1861 (1.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33 bytes 1861 (1.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

The IPv4 address is **10.1.85.134** and the netmask 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)

We have two ports open. One is port **22/tcp** which is for **ssh** and another **3389/tcp** for “**ms-wbt-server**”.



```
student@kali:~$ nmap 10.1.85.134
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-28 18:37 UTC
Nmap scan report for ip-10-1-85-134.ec2.internal (10.1.85.134)
Host is up (0.000080s 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 0.06 seconds
```

**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)

Using this website: <https://kb.wisc.edu/ns/page.php?id=3493> we can find the CIDR prefix length that his relevant to our netmask. In this case, the CIDR prefix length is **`/20`**.

Using the command **`nmap -sn 10.1.85.134/20`** we can find our relevant IP addresses.

This turned out to be ip addresses **`10.1.82.252`**, **`10.1.83.66`**, **`10.1.85.134`**, **`10.1.87.195`**. I'm pretty sure we shouldn't scan via the internal IP address cause that gives you a lot of internal IP addresses.

**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)

**10.1.82.252:**

- **22/tcp:** ssh
- **80/tcp:** http
- **139/tcp:** netbios-ssn
- **445/tcp:** Microsoft-ds



**10.1.83.66:**

- 80/tcp: http

**10.1.85.134:**

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




**10.1.87.195:**

- 21/tcp: ftp

**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)

I believe that 10.1.85.134 is running a web server as that's what one of the port's service names are. That's wrong. We only care about systems/ips that are running an http service (not the ms-wbt-server service I thought was relevant). Of the two that have an accessible web page, one is essentially just a file server:

## Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">hello.html</a>	2017-06-09 13:27	208	
 <a href="#">recipe</a>	2017-06-09 13:23	1.2K	
 <a href="#">temp/</a>	2017-06-09 12:35	-	

*Apache/2.4.18 (Ubuntu) Server at 10.1.82.252 Port 80*

And the other is an actual website:





Username

Password

Login

@10.1.83.66

**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)

Ran nmap -sV for each IP address noted below (same 4 listed above).

10.1.82.252:

- 22/tcp: ssh – OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)
- 80/tcp: http – Apache httpd 2.4.18
- 139/tcp: netbios-ssn – Samba smbd 3.X – 4.X
- 445/tcp: Microsoft-ds – Samba smbd 3.X – 4.X

10.1.83.66:

- 80/tcp: http – Apache httpd 2.4.25

10.1.85.134:

- 22/tcp: ssh – OpenSSH 8.3p1 Debian 1 (protocol 2.0)
- 3389/tcp: ms-wbt-server xrdp

10.1.87.195:





- 21/tcp: ftp – vsftpd 2.0.8 or later

**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 10.1.87.195
Connected to 10.1.87.195.
220 Welcome to Cyber Range FTP server
Name (10.1.87.195:student): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 21      21              34 Jan 28 18:07 welcome.txt
226 Directory send OK.
ftp> cat welcom.txt
?Invalid command
ftp> cat welcome.txt
?Invalid command
ftp> get welcome.txt
local: welcome.txt remote: welcome.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for welcome.txt (34 bytes).
226 Transfer complete.
34 bytes received in 0.00 secs (721.8071 kB/s)
ftp> quit
221 Goodbye.
student@kali:~$ ls
Desktop  Music  Templates  welcome.txt
Documents Pictures Videos      zenmap-7.80-1.noarch.rpm
Downloads Public  thinclient_drives
student@kali:~$ cat welcome.txt
Welcome to Cyber Range FTP Server
student@kali:~$
```

*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

---

### 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](https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing)

