

Lab Exercise 2 – Reconnaissance and Network Scanning Lab

Due Date: February 4, 2021 11:59pm
Points Possible: 7 points

Name: Hanzhang Zhao (hz9xs)

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 domain is registered for University of Virginia.

Contact name: Network Systems, University of Virginia, Information Technology Services

Address: P.O. Box 400324. Charlottesville, VA 22904-4324, USA

Email: networks@virginia.edu

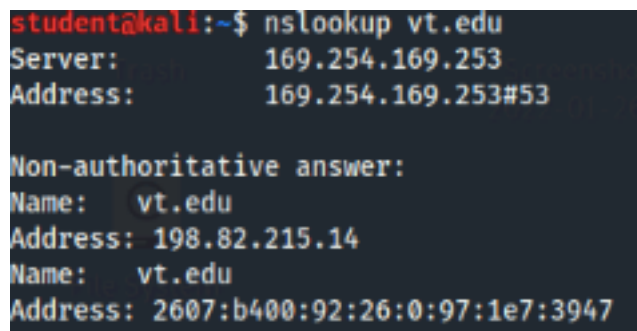
Phone number: +1.4349240621

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
```

IPv4 address is 198.82.215.14

The answer is right below the first "Name: vt.edu", and it is a four byte address which is a IPv4 address.

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)

'-x' option is used to do reverse lookups, which is mapping addresses to names.

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 is flexecm.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)
My IPv4 address is 10.1.47.85, and my 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)
22/tcp open ssh
3389/tcp open ms-wbt-server
Ssh and ms-wbt-server are 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 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)
10.1.42.230
10.1.44.88
10.1.45.94
10.1.47.85

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)
10.1.42.230:
22/tcp open ssh
80/tcp open http
139/tcp open netbios-ssn
445/tcp open microsoft-ds

10.1.44.88:

80/tcp open http

10.1.45.94:

21/tcp open ftp

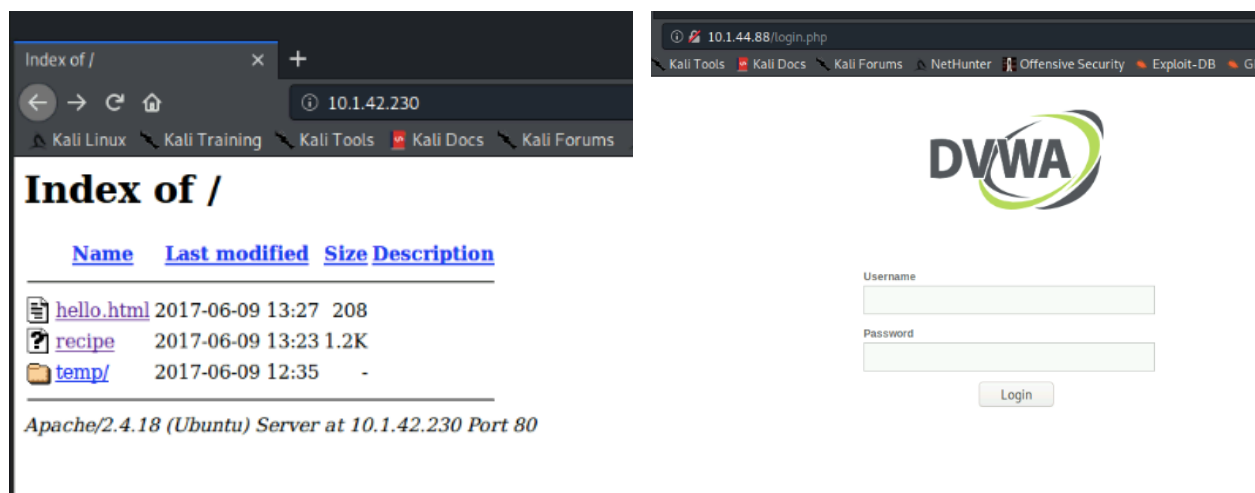
10.1.47.85:

22/tcp open ssh

3389/tcp open ms-wbt-server

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)

10.1.42.230 and 10.1.44.88 are running web server software.



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)

10.1.42.230:

ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol 2.0)

http Apache httpd 2.4.18

netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)

netbios-ssn Samba smbd 3.X - 4.X (workgroup: MYGROUP)

10.1.44.88:

http Apache httpd 2.4.25 ((Debian))

10.1.45.94:

ftp vsftpd 2.0.8 or later

10.1.47.85:

ssh OpenSSH 8.3p1 Debian 1 (protocol 2.0)
ms-wbt-server xrdp

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)

Index of ftp://10.1.45.94/

[↑ Up to higher level directory](#)

Name	Size	Last Modified
File: welcome.txt	1 KB	2/3/22 10:16:00 PM UTC

The contents of the file is “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/Port_(computer_networking))
- https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing