**In-Class Exercise 2 – Reconnaissance Lab Exercise**

Due Date: 09/27/2024

Points Possible: 100

**1. Overview**

This lab will demonstrate the use of the route command to obtain network information and the use of **nmap** and **Zenmap** to map a network.

**2. Resources required**

This lab uses the Cyber Range Cyber Basics (2022.11) environment.

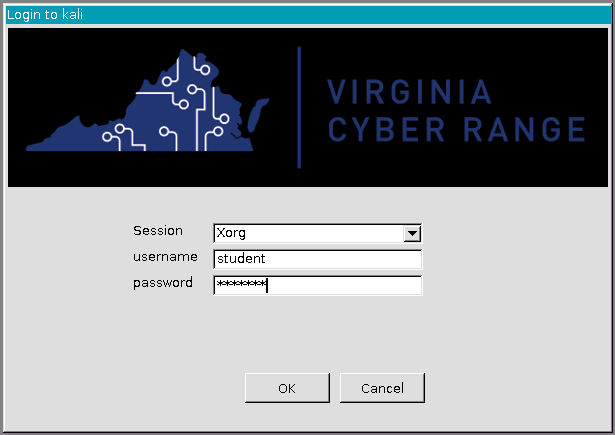
**3. Initial Setup**

Students should already have access to the Cyber Range Cyber Basics (2022.11) environment. They should use the username **student** and the password **student** to access the environment.

**4. Tasks**

**Task 1: Logon to Kali Linux**

Start the Cyber Basics (2022.11) Environment and logon with the username **student** and the password **student**.



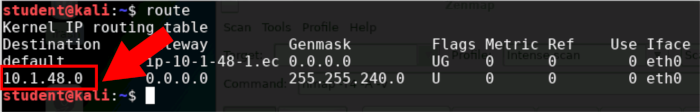
**Task 2: Open a Terminal**

Once Kali Linux starts, click the Terminal icon in the bottom middle of the desktop to open a terminal window.



**Task 3: Run the route command**

In the Terminal window, use the **route** command to locate the network ID of your network. The network ID will be located under the word default as in the example below. Your network ID may be different than the network ID in the example.



屏幕上有字

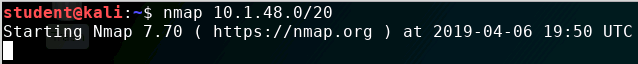
描述已自动生成

Document your network ID \_\_\_\_***10.1.160.0***\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**Task 4: Run the nmap command**

In the Terminal window, use the **nmap** command to scan the network for hosts. This is also known as network reconnaissance. All network use as /20 for the CIDR. CIDR stands for Classes Inter Domain Routing and represents the number of bits in the subnet mask. In the case of /20 the network mask is 255.255.240 which is 20 bits. So, the command to type at the prompt would be as follows where **network\_id** is the IP address you found from Task 3 and **/CIDR** is /20 as we just explained:

**nmap network\_id/CIDR**

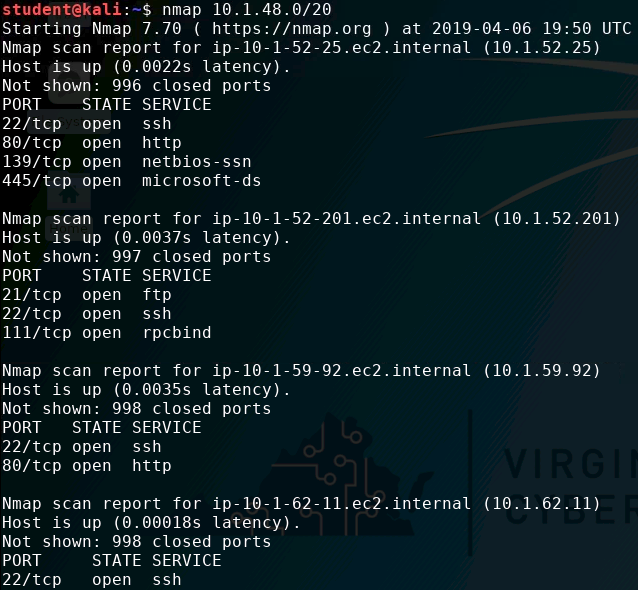


图形用户界面, 文本, 网站

描述已自动生成

**[NOTE: In the sample above, the target network is: 10.1.48.0/20. The target network in your network may be different.]**

The output from the **nmap** will show the IP address of the hosts scanned and any ports that are open on the host. By default, **nmap** scans the 1000 most common ports.

 文本

描述已自动生成

**[NOTE: In the sample above, the target network is: 10.1.48.0/20. The target network in your network may be different.]**

Document each IP address found and all open ports for each host.

Your **nmap** scan should locate at least 4 hosts.

Host 1 Ip address 10.1.160.1

Open Ports: None

Host 1 Ip address 10.1.160.247

Open Ports: None

Host2 Ip address:10.1.160.2

Open Ports:53

Host3 Ip address:10.1.161.56

Open Ports:22/ 80 / 139 / 445

Host 4 Ip address 10.1.161.96

Open Ports: None

Host 5 ip address 10.1.163.92

Ports: None

Host 6 ip address 10.1.163.171

Ports none

Host 7 ip address 10.1.164.16

Porst:80

Host 8 ip address 10.1.164.37

Porst none

Host 9 ip address 10.1.168.234

Ports: 21

Host 10 ip address 10.1.174.165

Ports:22/ 3389

Other None ports ip address

10.1.173.83 10.1.170.245 10.1.169.122

**Task 5: Save the nmap output to a file**

Run the **nmap** command again, but this time dump the output to a file by executing one of the following commands:

**nmap network\_id/CIDR > ~/nmap\_output**

**nmap network\_id/CIDR | tee ~/nmap\_output**

The **~/** in the above commands tells Linux to put the file in the home directory of the current user which is **student**. You can always refer back to the home directory by using **~/**.

In the second command, the **tee** command is used to tell Linux to send the output to the terminal and a file at the same time.

文本

描述已自动生成

You can use the cat command to view the contents of the output file by executing the following command:

**cat ~/nmap\_output**

**Task 6: Scan the network with Zenmap**

**Install Zenmp using the following instructions:**

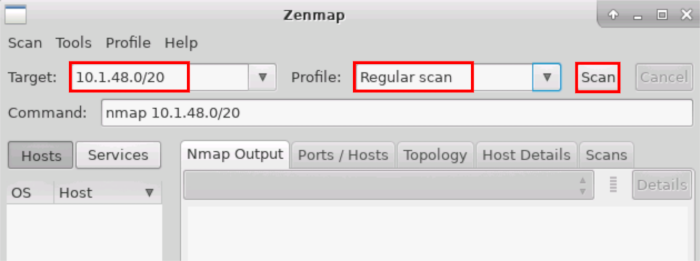
1. **sudo apt-get update**
2. **sudo apt-get install kaboxer -y**
3. **sudo apt-get install zenmap-kbx -y**
4. **sudo adduser $(whoami) kaboxer**
5. **sudo apt install zenmap**
6. **zenmap &**

In a Terminal window, start **Zenmap** with the **sudo** command and the **&** sign executing the following command:

**sudo zenmap &**

The **sudo** command runs **Zenmap** with root privileges and the **&** sign runs it as a background process. This allows you to have access to the terminal again once the program starts.

You will need to provide the **network ID** and **CIDR** for the **Target**, select **Regular scan** for the **Profile**, then click **Scan**.



图形用户界面, 应用程序

描述已自动生成

**[NOTE: In the sample above, the target network is: 10.1.48.0/20. The target network in your network may be different.]**

Compare the results of the **Zenmap** scan to the results of the **nmap** scan. Were the results the same or different?

***These results look very similar, so the results were same.***

图形用户界面, 文本, 聊天或短信

描述已自动生成

电脑屏幕截图

描述已自动生成

图形用户界面, 文本

描述已自动生成

**5. References**

<https://nmap.org/>

[This portion of the lab exercise template is provided for instructors that will be using this lab in a class they are teaching.]

This lab is designed to use the Cyber Range, Cyber Basics (2022.11) Environment. All students will have to register for an account in order to access the Cyber Range. The instructor will have to create a class and add the Cyber Basics (2022.11) Environment for the students to be able to use.

The grading for this lab is based upon the output provided by the students. Each student’s environment will be a little different, so there is no master answer key.

Students should be encouraged to document their work via a Penetration Testing Log which they can turn in for grading. The log can be done in any word processing application and should contain a list of tasks completed, commands run for each task, screenshots of the output from each task, and any issues encountered during the lab. The instructor should review the log to ensure that the students are mastering the appropriate skills.

For this lab, the students should document that they found 4 hosts in the environment, the IP address of each host, and the open ports on each host. Subsequent labs will utilize this information, so it is important students properly document what they found in the lab environment.

For the question in Task 6, students should see that the output of **nmap** and **Zenmap** are very similar as **Zenmap** is just a GUI frontend to **nmap**. Even though students may prefer to use the GUI version of the program, they should be encouraged to use the command line version. In penetration testing, many environments that a penetration tester operates in does not have access to a GUI, so learning how to run the commands from the terminal is very important.

**KSAs from NIST SP 800-181:** <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>

**Knowledge:**

* K0070: Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).
* K0111: Knowledge of common network tools (e.g., ping, traceroute, nslookup) and interpret the information results.
* K0119: Knowledge of hacking methodologies in Windows or Unix/Linux environment.
* K0129: Knowledge of Unix command line (e.g., mkdir, mv, ls, passwd, grep).
* K0307: Knowledge of common network tools (e.g., ping, traceroute, nslookup).
* K0342: Knowledge of penetration testing principles, tools, and techniques.

**Skills:**

* S0051: Skill in the use of penetration testing tools and techniques.

**Abilities:**

* A0055 Ability to operate common network tools (e.g., ping, traceroute, nslookup).

**NSA/DHS CAE Knowledge Units:** https://www.iad.gov/NIETP/documents/Requirements/CAE-CD\_2019\_Knowledge\_Units.pdf

(you may need to accept an invalid iag.gov SSL certificate to reach this PDF)

* Penetration Testing (PTT)