**Laboratory Exercise X – Reconnaissance Lab Exercise**

Name: Afeefah Manzoor

**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 (2018) environment.

**3. Initial Setup**

Students should already have access to the Cyber Range Cyber Basics (2018) 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 (2018) Environment and logon with the username **student** and the password **student**.

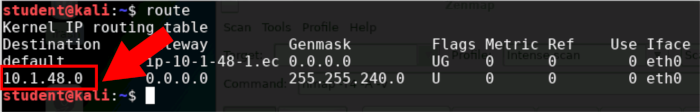
**Task 2: Open a Terminal**

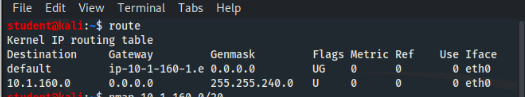
Once Kali Linux starts, click the Terminal icon in the bottom middle of the desktop to open a terminal window.



**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.



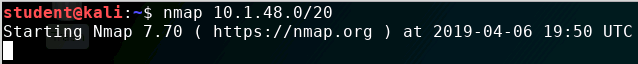


Document your network ID \_\_\_10.1.160.0\_\_\_\_.

**Task 4: Run the nmap command**

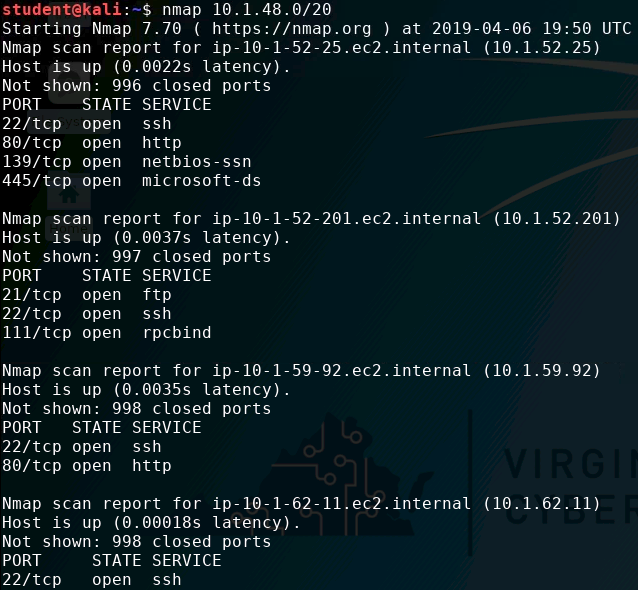
In the Terminal window, use the **nmap** command to scan the network for hosts. This is also known as network reconnaissance. All network use as /20 for the CIDR. CIDR stands for Classes Inter Domain Routing and represents the number of bits in the subnet mask. In the case of /20 the network mask is 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**



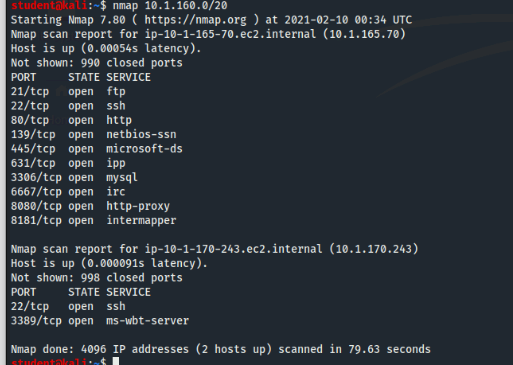
**[NOTE: In the sample above, the target network is: 10.1.48.0/20. The target network in your network may be different.]**

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.



**[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.



|  |  |
| --- | --- |
| IP | Ports Open |
| 10.1.165.70 | 21(ftp) |
|  | 22(ssh) |
|  | 80(http) |
|  | 149 |
|  | 445 |
|  | 631 |
|  | 3306 |
|  | 6667 |
|  | 8080 |
|  | 8181 |
|  |  |
| 10.1.170.243 | 22 |
|  | 3389 |

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

**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.

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

**cat ~/nmap\_output**

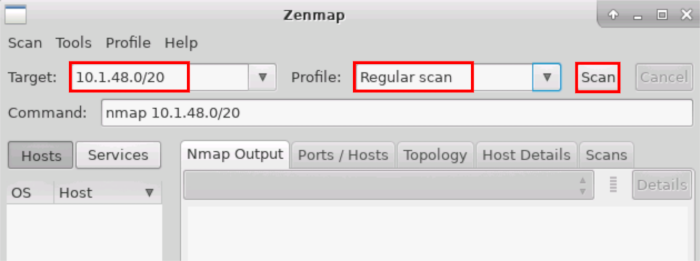
**Task 6: Scan the network with Zenmap**

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

**sudo zenmap &**

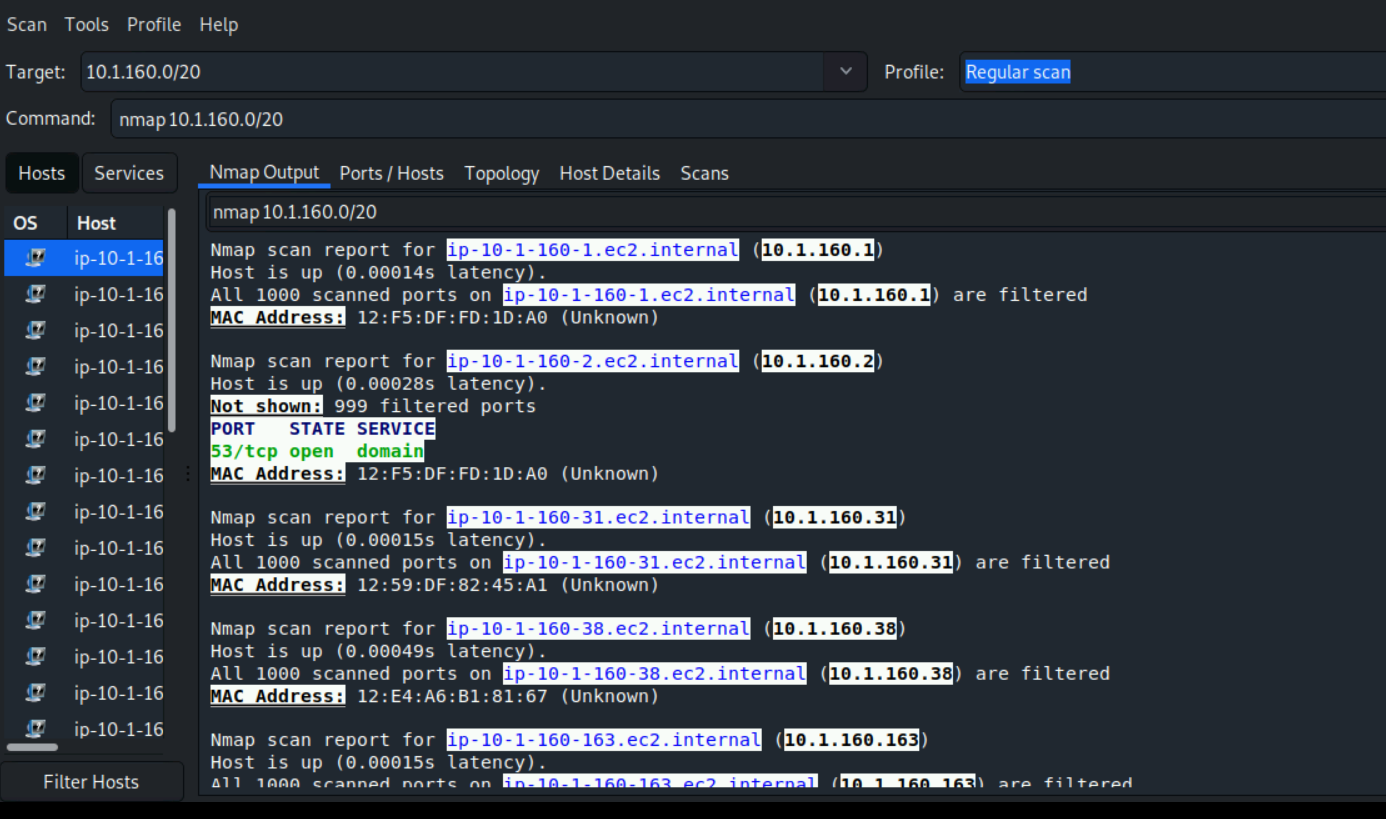
The **sudo** command runs **Zenmap** with root privileges and the **&** sign runs it as a background process. This allows you to have access to the terminal again once the program starts.

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



**[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?



Zenmap has given a lot more information than NMAP gave. Each host has a detailed nmap output, as well as it’s ports, topology, and host details. NMAP just gave the details about the open ports of 2 hosts.