**CYBR430, Penetration Testing and Incident Response  
Week 4 Lab – Scanning and Enumeration**

NAME: \_\_\_\_\_\_\_\_\_\_\_Tylor Underwood\_\_\_\_\_

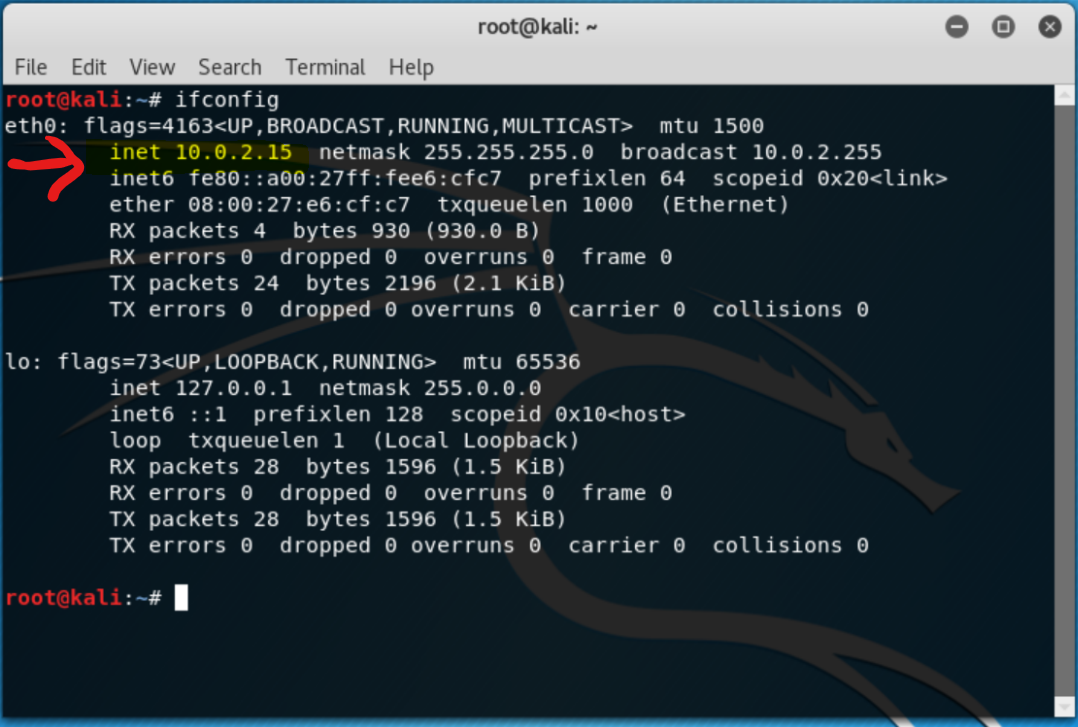
DATE: \_\_\_\_\_\_\_\_April 25, 2022\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Complete the below actions, answering the questions (**in red**). *Rather than just pasting the screen dumps as answers find the information you need in the scan results and provide that as answers*.  
For this exercise, you will use the virtualized systems specified by the professor. See the instructions for access.

Now that you have gained access to the target network the next step in this penetration test is to scan the network and enumerate the present resources. At the completion of this phase you will have developed at least an initial topology of the target network. As you progress through a penetration test you may very often gain access to a network segment or collection of systems not previously available. At that point you may need to return to the scanning and enumeration phase. For this lab we will focus only on your initial scans/enumerations.

At the completion of week three you had gained access to the internal network of Happy Accident Labs through one of their wifi access points. Before you begin scanning you will want to determine your IP address so you can construct an appropriate scanning range. You can easily find out the IP address you have been assigned by opening a terminal window and using the command **ifconfig.**

You can see in the screen shot below where the local machine’s IP address is highlighted after running ifconfig. Your IP address, both the host and subnet portions will be different from that shown.



1. **What is the IP address of the Kali box on the HAL network?**

10.19.99.202

Take a look at your netmask. In this case it is 255.255.255.0. That means that the first three groupings of numbers in your IP address identifies the subnet you are on and the last grouping identifies the host.

Now that you know which subnet you are on you can conduct a ping sweep to see which other hosts are alive on the subnet. For this we will use **nmap**. You are free to use either the command line or Zenmap GUI (under applications/information gathering). I suggest trying both so you become familiar with both tools. You will need to open a terminal window for the command line entries.

Refer to Exercise 6.3 in your textbook. Conduct a ping sweep of the subnet using nmap. The format of the command would be **nmap –sP <target ip address range>**. Note, you shouldn’t type the ‘<>’ characters. For the IP address range you should use the subnet you are on (in this case remember that is the first three groupings of numbers) and the last grouping should be 1-100. So your completed command would have the form **nmap –sP nnn.nnn.nnn.1-100.**  Note that for this class we are going to limit your scans to the 1-100 range as all your student machines have ip addresses with host numbers > 100. Normally you would see your host as well in the scans – and so would an observant system administrator so stealth is necessary.

1. **What are the results of your scan?**

nmap -sP 10.19.99.1-100

Text

Description automatically generated

The scan you just ran is a ping sweep. It will help you find live hosts but it is also noisy on the network. If it’s important to the test you may decide to only scan for a few hosts at a time or otherwise slow down your scanning so as to be less noticeable.

After finding active hosts you will want to determine which ports are open. One way to do this is by conducting what is known as a full open or port scan. You will attempt to make a connection to all, or perhaps just selected ports. The command format to do this is **nmap –v –sT <target ip range>.** (The –v option is for verbose mode and provides more information)

1. **Conduct a full open scan on your live hosts, what have you found?**

This returned a lot of useful information. There were a lot of open ports such as SSH on 10.19.99.5

Nmap -v -sT 10.19.99.1-100

Diagram, text

Description automatically generated with medium confidence

One problem with a full open scan is it is noisy, you are making actual connections to those systems which will show up in logs along with your IP address. Another option is to run what is known as a stealth or half-open scan. With this scan the three-way handshake is not completed, thus no connection, thus less to be noticed by observant sys admins. This scan may sometimes not provide as accurate results but you have less chance of having your activities noticed. You can conduct a stealth or half-open scan with the command **nmap –sS <target ip address range>.**

**4a. Run your previous scan again but as a stealth scan. Are the results the same or different? Explain.**

The results in this case were largely the same as I could not find any differences

Text

Description automatically generated

**4b. Run one additional scan of the types shown in your textbook on pages 141-142. You can learn more about these types of nmap scans at** [**https://nmap.org/book/man-port-scanning-techniques.html**](https://nmap.org/book/man-port-scanning-techniques.html)**. What did you find?**

I ran a UDP scan which looked for open UDP ports specifically

Graphical user interface, text

Description automatically generated

Another piece of valuable information you will want to find out is what operating systems are running on the hosts. Your previous scans may have already given you some indication of that however you can run a specific scan to determine that information. It’s form is **nmap –sS –O <ip address>** (that’s an upper case letter ‘O’).

1. **Run an OS detection scan against the active hosts, report your findings below.**

This command determined that the scanned host was running some version of Windows

Text

Description automatically generated

Your port scans showed that NetBIOS is in use, this is an indication you should check for share and user information. A great tool to do this is enum4linux. See the reference material in your reading this week for a full listing of commands. For this part of the lab you will run enum4linux against the applicable hosts.

**6. Would you run this command against all hosts? If not why not and which ones would you run it against?**

This would only be useful to run against computers running NetBIOS since that is the reason we are running this command in the first place

Run enum4linux against the applicable hosts. We would like to run the command with all the simple enumerations so the format would be **enum4linux –a <host ip>**. The –a is also the default option if you don’t include any other options but specifying your options is a good habit to get into.

**7. What information did you find from your scans?**

I found some useful information from this. I found several known usernames such as guest, root, and krbtgt. For the most part I got a lot of ACCESS\_DENIEDs. It tried many things such as getting domain groups, memberships and finding password policies that if found would be extremely useful.

**Text

Description automatically generated**

You will usually want to run multiple tools to either confirm results or see if a tool shows different results. Another tool with does scanning and enumeration (to include netbios and smb shares) is Sparta. Sparta is located in Kali under Applications and Information Gathering. Start Sparta and click on the host panel on the left. Enter a scan range which is appropriate for the systems on the HAL network. Leave the default options selected. The scan will begin automatically.

**8. Did Sparta return any additional information you did not get from nmap or enum4linux? What?**

The thing that Spart returned that enum4linux didn’t is workgroup names in which it was called WORKGROUP. It returned basically the same information other then that. Enum4linux found some different ports however.

Graphical user interface

Description automatically generated with medium confidence

**9. Submit a system topology (diagram) of what you currently think the network looks like based on what you scans have shown. Include IPs, types of operating system, users, shares, open ports and anything else you think valuable for later testing.**

**IPs: hosts 5, 8, 9, 10 and 202 (10.19.99)**

**Operating Systems: Microsoft Windows of some variation(s)**

**Open Ports:**

**host 8: 135, 137, 139, 445, 500, 4500, 5355,** **49152, 49153, 49154, 49155, 49156, 49157,**

**host 5: 22, 139, 445 9090**

**host 10: 135, 137, 445, 49152, 49153, 49154, 49155, 49156, 49157,**

**Users: Usernames on 10.19.99.8; administrator, guest, domain admins, root, bin, krbtgt**

**Other:**

**Mac of 10.19.99.8: 00:50:56:8D:F1:F0 (vmware)**

**Mac of 10.19.99.5: 00:50:56:8D:69:DF**

**Workgroups: WORKGROUP**