**LAB-03: Reconnaissance and Scanning**

**1. Lab Overview**

The key to successfully exploit or intrude a remote system is about the information you have. The first step for penetration is the scanning and reconnaissance. In this lab, you will learn how to use tools to scan and retrieve information from a targeting system. You will be using *nmap* and *OpenVAS* to scan a vulnerable machine and identify exploits that can be used to attack it. We will use two Linux virtual machines: One is a Kali Linux with *nmap* and *OpenVAS* installed; and the other one is intentionally vulnerable Linux. We will use the *nmap* and *OpenVAS* on Kali Linux to scan the vulnerable Linux machine.

**2. Lab Environment**

* The VirtualBox VM Software

<https://www.virtualbox.org/wiki/Downloads>

* The Kali Linux, Penetration Testing Distribution

<https://www.kali.org/downloads/>

* Metasploitable2: Vulnerable Linux Platform

<http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

* nmap: the Network Mapper - Free Security Scanner

<https://nmap.org/>

* OpenVAS: Open Vulnerability Assessment System

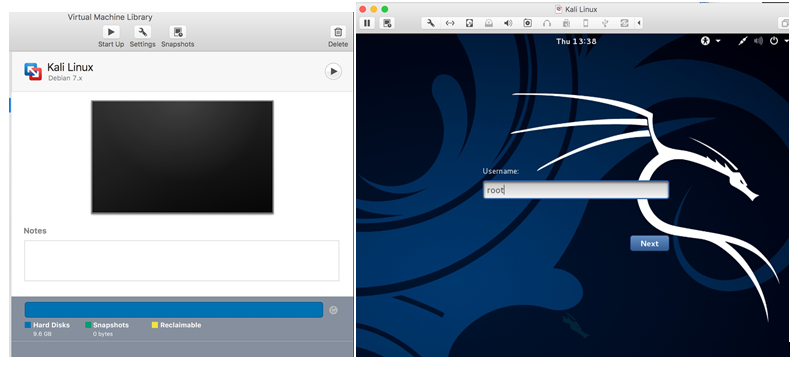
<http://www.openvas.org/index.html>

**3. Lab Task - 1**

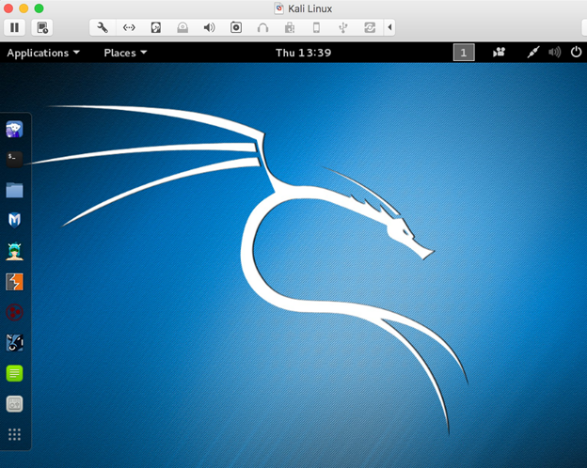
**Part I: Starting Virtual Machines**

We need to use two VMs for this lab: The Kali Linux and the Metasploitable2-Linux.

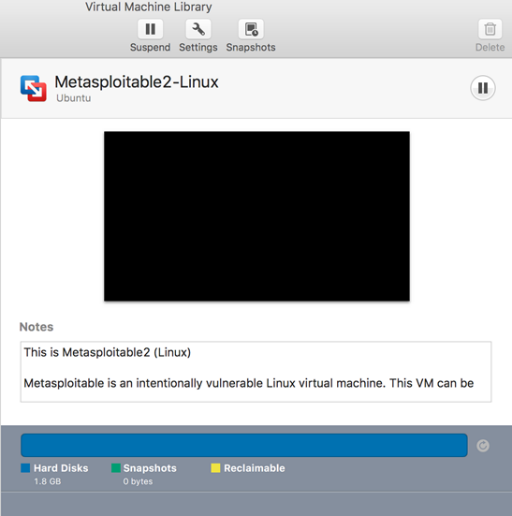
**Step 1:** Start up the Kali Linux.



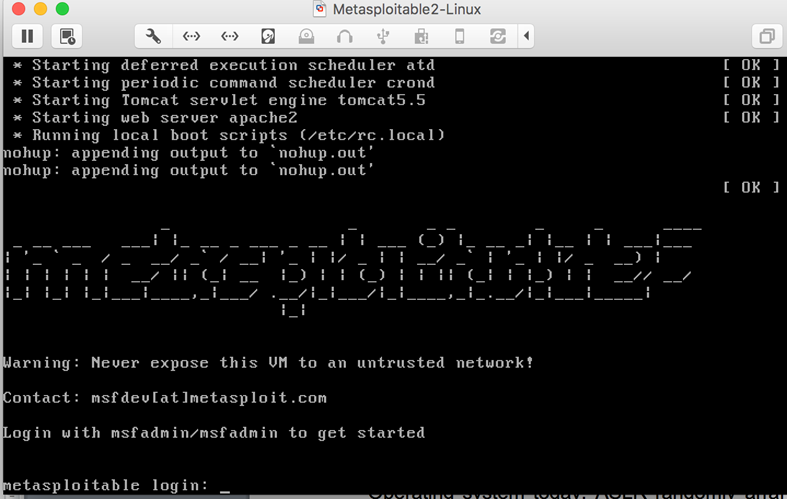
**Step 2:** Login the Kali Linux with username and password. Below is the screen snapshot after login.



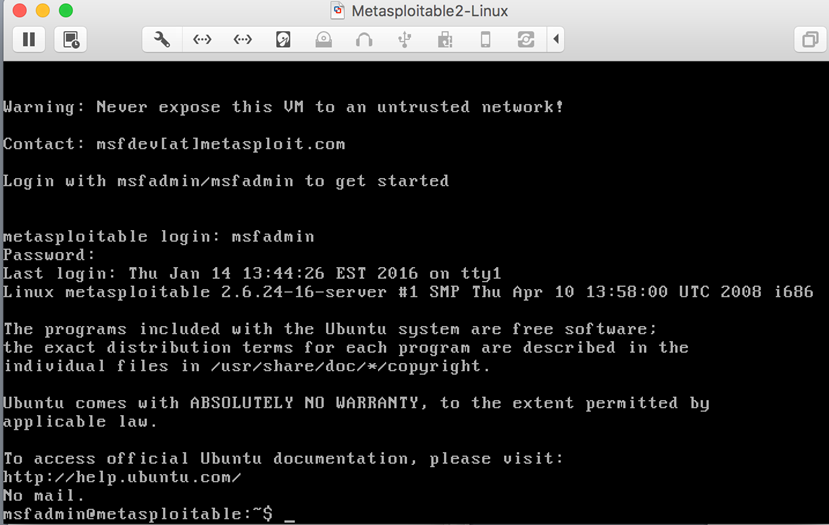
**Step 3:** Then, you select **Metasploitble2-Linux**, and press Start up. This is an intentionally vulnerable Linux VM that you will attack against.



**Step 4:** Log into the virtual machine with username, **msfadmin**, and password **msfadmin**.



**Step 5:** After you log into the VM, you will see the screen below.

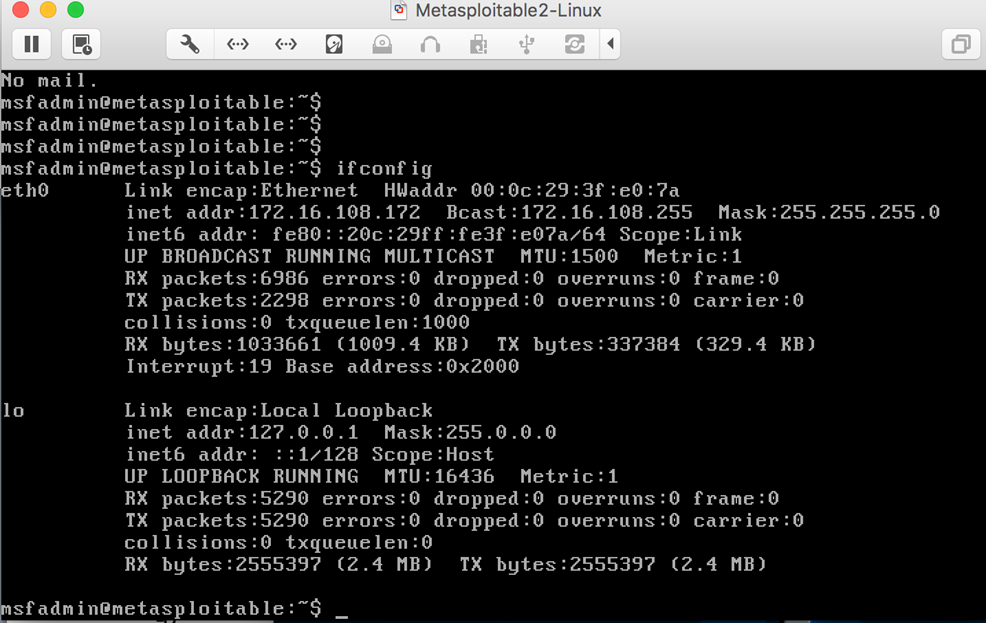


**Part II: Finding the IP Address of the Attacking Target**

For the purpose of this lab, it uses Metasploitable2-Linux as the attacking target. First, we need to find the host IP address of the target to launch a scanning. You can use the command “ifconfig” (ipconfig is the windows equivalent). This command allows you to find all the connected interfaces and network cards.

**Step 1:** Go to the Metasploitable2-Linux VM, and execute the following command

*$ ifconfig*



**Step 2:** From the screenshot above, we can see that the IP address of the network interface, eth0, is **172.16.108.172**. This is the IP address for the target that you will use later in this lab (It may be different for your case).

**Part III: Scanning the Target Using nmap**

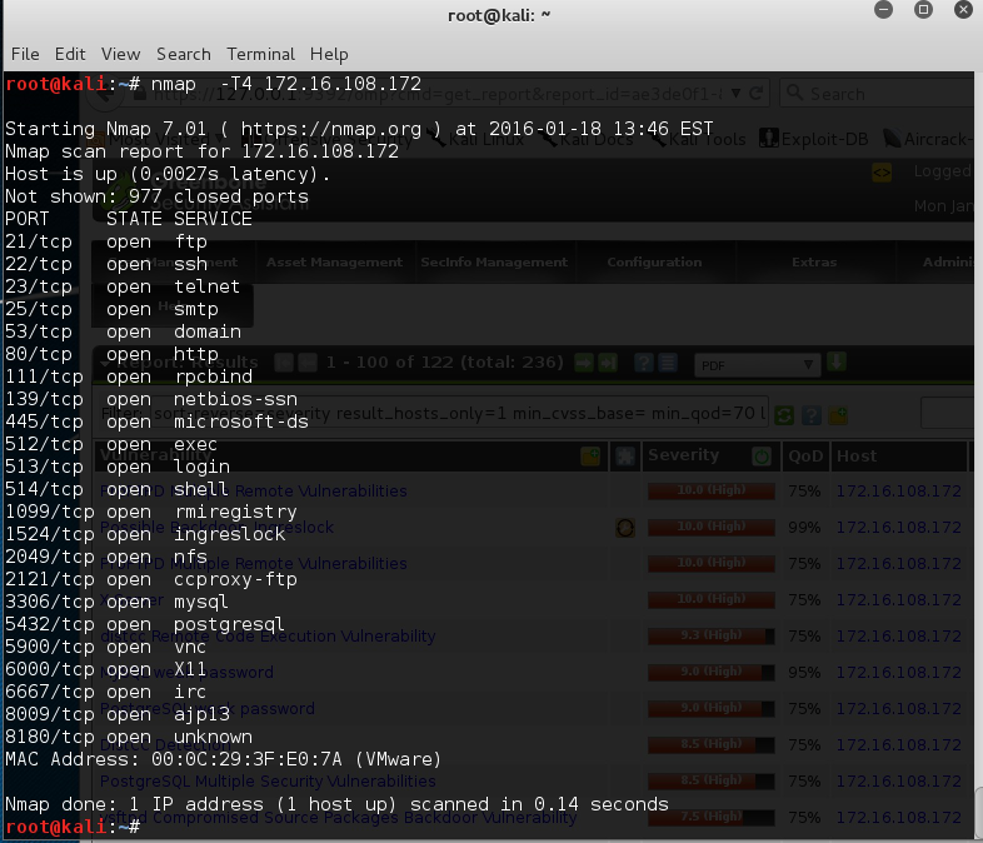
**nmap** ("Network Mapper") is an open-source tool for network exploration and security auditing. Though it was designed to rapidly scan large networks, we use it for scanning the target host in this lab.

**Step 1:** Go to the Kali Linux and open up a terminal by clicking the icon.

**Step 2:** Since nmap has been installed on the Kali Linux, we can just launch the scanning in the terminal by typing the following command:

*$ nmap –T4 172.16.108.172*

**nmap** is the execution command; option **-T4** means faster execution; and **172.16.108.172** is the IP address of the target. As mentioned, you will have a different IP address when working on this with the VMs in the classroom.

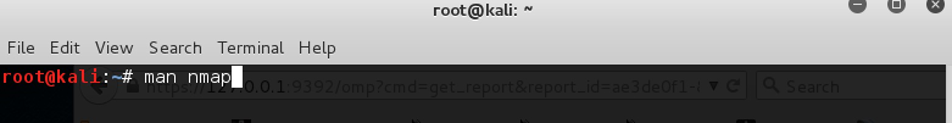


The screenshot above shows a quick scan of the target machine using **nmap**. We can see that there are many open ports and services on the target system including FTP, SSH, HTTP, and MySQL. These services may contain vulnerabilities that you can exploit.

**nmap** provides many useful functions that we can use. You can find more information from the man page of **nmap** from this link: <http://linux.die.net/man/1/nmap>

Or execute the following command in a terminal:

*$ man nmap*



**Part III: Vulnerability Scanning Using OpenVAS**

OpenVAS is an open-source framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. In our Kali Linux image, OpenVAS has been installed and setup for you.

If you want to setup OpenVAS in your own machine, you can follow the steps below.

*root@kali:~# apt-get update*

*root@kali:~# apt-get dist-upgrade*

*root@kali:~# apt-get install openvas*

*root@kali:~# openvas-setup* (OR***gvm-setup***if you use Kali 2020 version*)*

Since the Kali Linux image has everything setup for you, you don’t need to run the setup commands.

**Step 1:** run the following command to check if the OpenVAS manager, scanner, and GSAD services are listening:

*root@kali:~# netstat –antp*

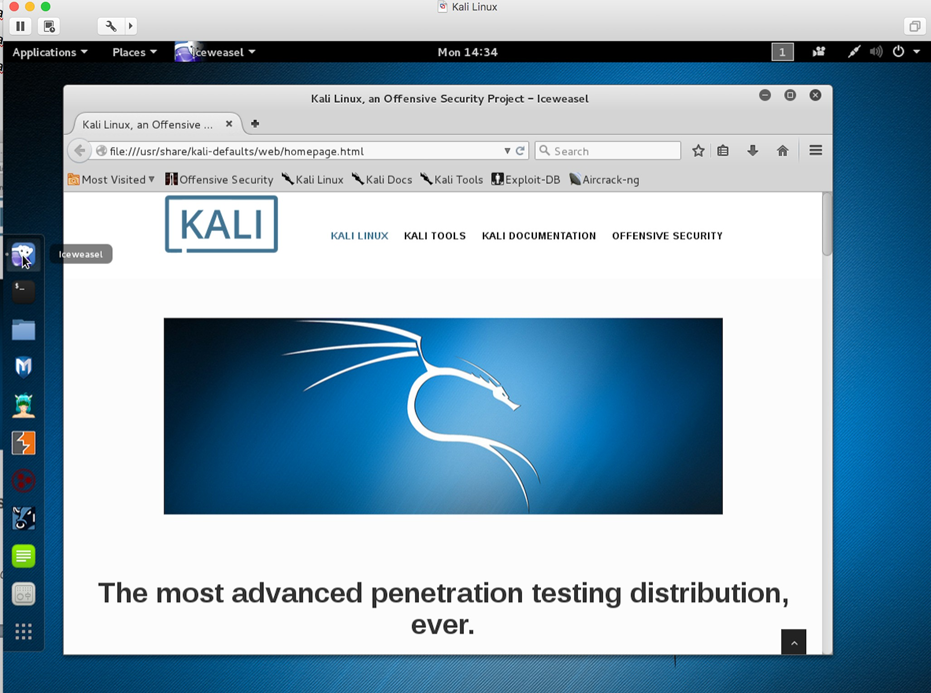
**Step 2:** start the services by executing the following command

*root@kali:~# openvas-start* (OR***gvm-start***if you use Kali 2020 version*)*

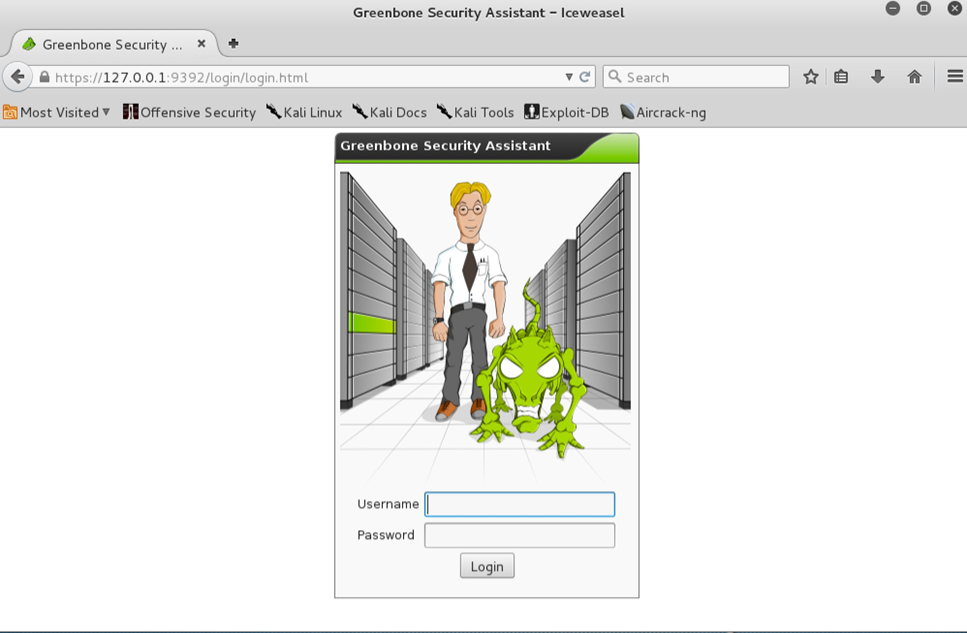


**Part IV: Connecting to the OpenVAS Web Interface**

**Step 1:** Go to the Kali Linux, and open the browser, Iceweasel, by clicking the icon 



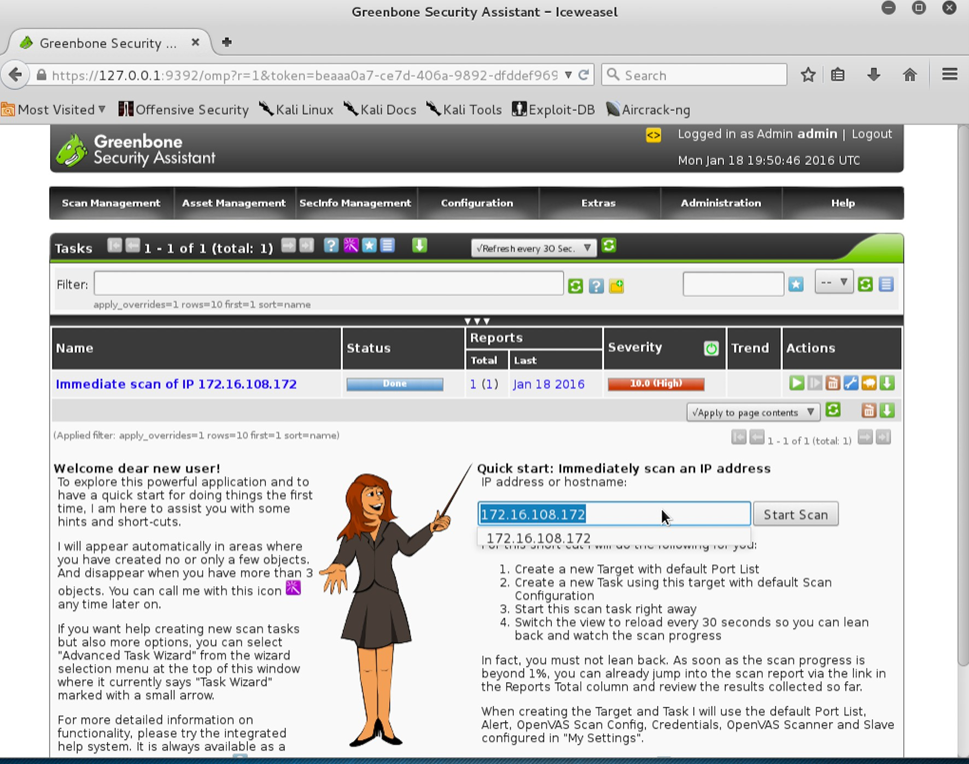
**Step 2:** Then, go to https://127.0.0.1:9392 and accept the self-signed SSL certificate.

****

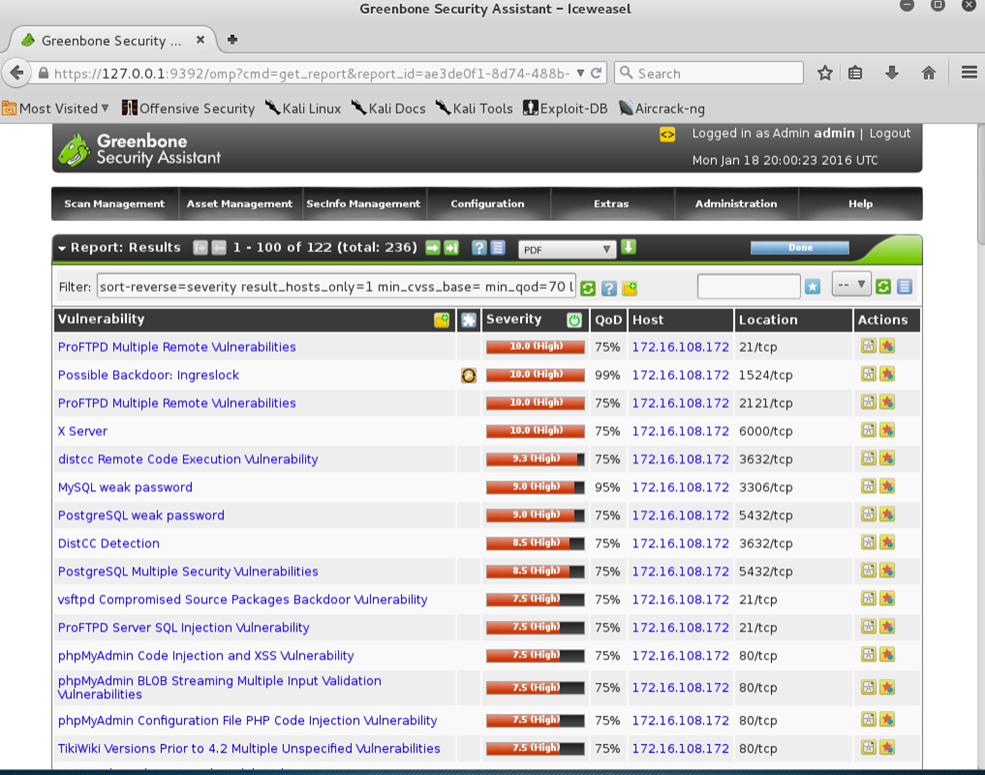
**Step 3:** Input the username as admin, and the password [TAB in the classroom, same password as Kali Linux Login].

The screenshot on next page is the homepage of OpenVAS. Type the IP address of the target in the “Quick start” box, and press “Start Scan”. It will do the following for you:

1. Create a new Target with default Port List.
2. Create a new Task using this target with default Scan Configuration.
3. Start this scan task right away.
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress.



**Step 4:** After finishing the scanning, you can look at the reports as shown in the screenshot below.

****

**4. Lab Task – 2: Anonymous Web Browsing**

It is a common misconception that HTTPS provides anonymous Web browsing. This is not the case. A secured HTTPS connection can ensure confidentiality (what you're sending can't be read by others) and authentication (the website you're visiting is really who they say they are). However, it does not provide anonymity. Eavesdroppers cannot see what you are sending, but they can see that you are sending something to that website.

Onion routing can provide anonymity via an encrypted network of "relay" servers. Computers around the world pass your fully encrypted traffic. The intermediary relay servers do not know the entire path of the onion network. Requests that come from you appear to originate from around the world. You have complete anonymity. It's still a good idea to use a secured end-to-end HTTPS connection, because the connection between the last relay server and the site you are visiting is not encrypted.

1. Open a web browser.

2. Go to www.google.com/.

3. Search for “my IP address.”

4. Press Enter.

5. Click on the first result.

6. Take a screenshot showing your IP address.

7. Go to www.TorProject.org.

8. Click Download Tor Browser.

9. Click on the link for Windows 10 under Tor Browser Bundle.

10. Save the file in your download folder.

11. Browse to your download folder.

12. Right-click the Tor executable and select "run as administrator."

13. Complete the installation process and start the Tor Browser. (If the Tor browser doesn’t automatically start, you can search for “Tor Browser” in the Windows Search menu.)

14. Within the web browser, go to www.Google.com.

15. Search for "my IP address."

16. Click on the first result. (If you get a warning about an "Untrusted" connection, just click on I Understand the Risks, Add Exception, and Confirm Security Exception.)

17. Take a screenshot showing the new IP address. (This is someone else's IP address.)

18. Start Microsoft Edge. (Arrange the windows so that the Tor browser and Microsoft Edge are both visible on your desktop.)

26. Search for "my IP address."

27. Click on the first result.

28. Take a screenshot of your desktop (Ctrl-PrintScreen) showing the IP address results in both web browsers. (Use the results from the same website. Each browser should show a different IP address.)

**5. Lab Task – 3: THOUGHT QUESTIONS**

1. What are wireless network channels? Would one be better than another?
2. Why is WEP considered cryptographically weak?
3. What is the difference between WPA and WPA2?
4. Why do some networks run at 11 Mbps and others at 54 Mbps (Different Network Speeds)?
5. Why would someone want to use a Tor network?
6. What do relay servers do in a Tor network?
7. How do Tor networks provide anonymity?
8. Why is it still important to use an HTTPS connection if you are using a Tor network?

**6. Submission Instructions**

1. **Complete** all the tasks assigned in the project. **Take** screenshots of all major steps involved in this LAB. **Paste** the screenshots into a MS-Word file and if available, **add** the source code of the entire program **(Not all labs have codes)**. **Rename** the MS-Word report file into “LAB-03-Group\_XX” format.
2. You are not always required to follow my steps as it is, you can come up with your own ideas in your own ways to solve the same problem.
3. Try your best to prepare well organized lab report with step by step description for each screenshot.
4. Submit your LAB report to the D2L “LAB-03” drop-box by only one member of each group within one week from the assigned date.

**NOTE-1:** Please add, 1.All group member’s names (LAST\_NAME, FIRST\_NAME) and 2.Page numbers in to the report. If you would, you can create a cover page for each LAB, but not necessary.

**NOTE-2:** Please add all group member’s contributions to complete and submit this lab as a percentage as shown below at the end of the report. (Before submitting to D2L all of the group members must be aware their reported contribution as a percentage in the lab report)

**Example:**

Member-01: 100%

Member-02: 75%

Member-03: 100%

Member-04: 50%