**ISEC 520 – Ethical Obligations in Information Security**

**Lab 2: Remote and Local Exploitation**

The requirements for this lab are to capture the screenshot of the below steps from given sections and submit in the word document. Flag screenshot #1 is shown as an example.

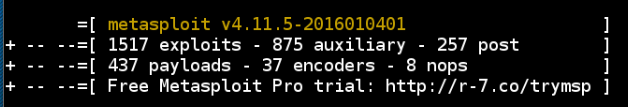
**Part 1**

**challenge #1**

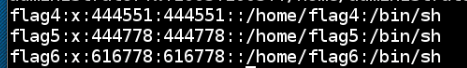
* **Flag screenshot #1**

****

**challenge #2**



**challenge #3 challenge #4 challenge #5**



**PART 2**

If we are using a windows machine, we would have to install nmap on it. But certain linux distros such as kali come with an array of tools for network penetration testing including nmap. This is why we are able to use it right away.

We scan the IP address of 203.0.113.100 and see the state of its ports. If we look at the topology of the system, we can see that this IP address is the public IP address of the local network on the top side of the topology.

Zenmap is the GUI version of nmap. We use it to scan the same IP address. On the ports/hosts tab we were able to see the ports including the postgresql port.

Next we are running the OpenVAS Network Scanning application by typing its directory and its file name on the terminal. This make it seem like it is an executable file at this directory, but I decided to go to this directory to confirm this and was not able see the openvas\_start file. I don’t know if it is a hidden file like we have in windows. In my own computer I have hidden files shown and I have file extensions shown.

We type an IP adress and a port directly (no need for dns) in the URL of our browser to go to Greenbone that is another networking tool. This tool shows us the vulnerabilities.

Now we login to the other kali machine. We use Metasploit tool to search for exploits and especially postgresql expolits. Then we load one up and set the target IP. We set other options and then show the options we set then run it. We were able to login as the posgres user to the machine and execute a command on the target machine but we didn’t have permission to read the file.

Then we used another exploit to gain root access and as we can see with the whoami command we are the root.