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

**Lab 3: Capturing and Analyzing Network Traffic Using a Sniffer**

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**

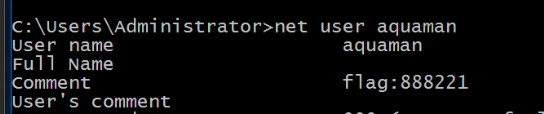
* **Flag screenshot #1**

****

**challenge #2**



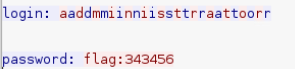
**challenge #3**



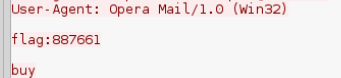
**challenge #4**



**challenge #5**



**challenge #6**



**PART 2**

We log into the kali linux machine and use the bash command ifconfig to get our network information. At first we have an Ipv4 address. But we use another ifconfig command to get rid of our Ipv4 address. Then we launch wireshark and start passively listening to the packets.

We launch the windows 10 machine. If we take a look at the tpoplogy of the network, we can see that ip addresses of all 3 machines start with “192.168.1”. At first I thought these machines were in different local networks but after seeing the Ip addresses, I realized that they are all in a single local network with a subnet mask of “255.255.255.0”. The Ip we use in our ftp connection command is the local ip for the windows server. We were able to get an ftp connection to the server machine, look at the file directory, get a file, and close the connection.

We telnet into the server and create a user and add it to a group.

One of the points of this VL is showing that FTP and Telnet uses plain text, and therefore they are unsafe since people can be listening to the packets and get the information. We were able to use wireshark filter to see the password zombie.