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

**Lab 1: Enumerating Hosts using Wireshark, Windows, and Linux Commands**

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.

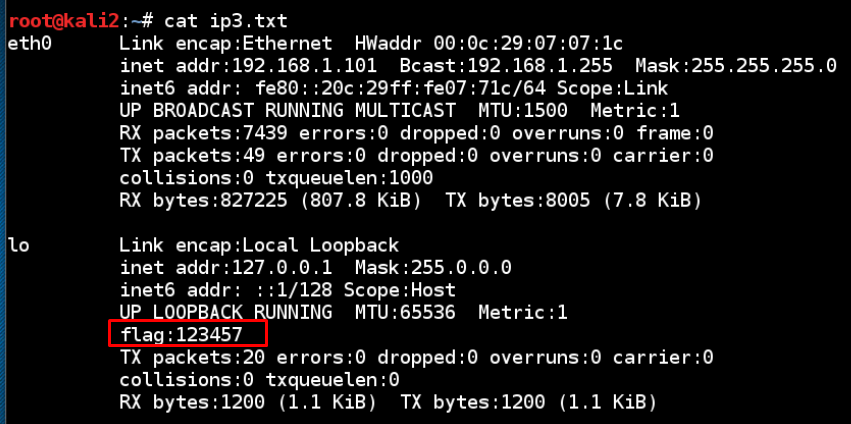
**Part 1**

**challenge #1**

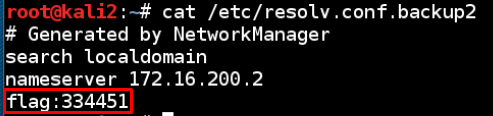
* **Flag screenshot #1**

****

**challenge #2**



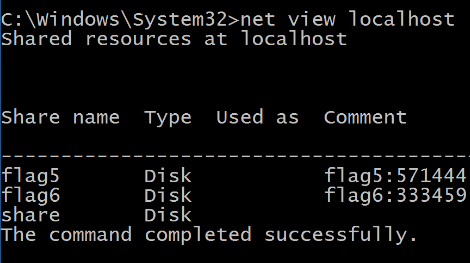
**challenge #3**



**challenge #4**



**challenge #5 challenge #6**



**PART 2**

In windows, we have ipconfig batch command to get the same information returned by ifconfig in Unix based systems (mac and linux). We used ifconfig bash command to get network information. We pipelined the information into a text file. We read text files using the cat command. Using the Lightshot screen capture application made taking screenshots of certain parts of the screen and adding red rectangles on them very easy.

Wireshark is a really good tool to track network packets. We are able to get all this information just by passively listening.

We didn’t have a 32 bit IP address before, so we assigned one. But we have to keep in mind that this is not the public IP address. This is the private IP address.

<https://www.youtube.com/watch?v=FTUV0t6JaDA>

Nmap is an active scan tool unlike wireshark. It can scan what ports are active or not. It can also scan the hosts in a network.