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

**Lab 6: Attacking Webservers from the WAN**

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.

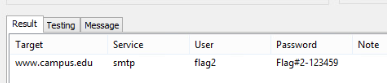
**Part 1**

**challenge #1**

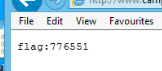
* **Flag screenshot #1**

****

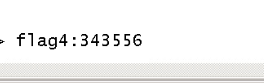
**challenge #2**



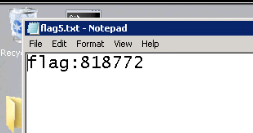
**challenge #3**



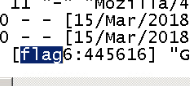
**challenge #4**



**challenge #5**



**challenge #6**



**PART 2**

When we take a look at the network topography, we see that there are two public ip addresses and that one of the public ip addresses includes a local network with two hosts that have local IPs.

We first login to the standalone host at the public ip 175.45.176.200 which is the windows attack machine. We open the cmd and use nmap tool to analyze the [www.campus.edu](http://www.campus.edu) where www is the sub domain, edu is the top domain, and campus is the domain. If we take a look at the network topography, we see that [www.campus.edu](http://www.campus.edu) is the dns for the other public ip. Normally nmap command is an invalid command. Because it is not a windows batch command. But when we install an executible such as nmap.exe, we can add it to enviroment variables, which makes the computer look at that directory when we try to invoke an executible file such as nmap.exe. [www.campus.edu](http://www.campus.edu) is the main method argument we supplied along our call to nmap.exe. It is really interesting to study programming and one day connect all the dots.

Then we launch zenmap.exe to launch the gui zenmap program that is the gui version of nmap. We do the same scan with zenmap.

Then we launch bruter.exe. Which is named appropriately since it is a brute force attack program. And we found out the password for flag2 user.

We use nmap to usee if [www.campus.edu](http://www.campus.edu) has the port 3389 open which is the oprt for rdp. And it is open. We RDP into the server. We go to the xammp htdocs folder of the server. I have used xammp before and the htdocs folder is the default webpage files folder for xammp. We edit the html file and when we go back and refresh the webpage, we see the edit.

We go back to the server and we stop the apache service. We go to the apache log file and delete the logs that contain our ip. Then we restart apache and check our browser to see if it works.