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

**Lab 5: Using Browser Exploitation to Take Over a Host’s Computer**

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.

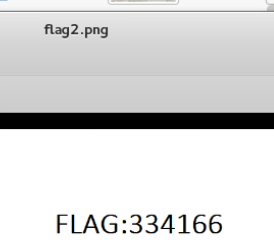
**Part 1**

**challenge #1**

* **Flag screenshot #1**

****

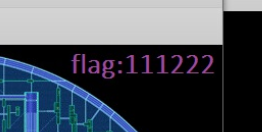
**challenge #2**



**challenge #3**



**challenge #4**



**challenge #5**



**challenge #6**



**PART 2**

If we take a look at the topography of the network we see that we have 3 different public IPs, one of which includes a local network. We first login to the kali attack machine. We start the postgresql that hosts the data and we search through that data using metasploit. We set variables of the exploit and then execute the exploit.

We then login to the prey machine and open the email. If we hover over the link with the title [www.facebook.com](http://www.facebook.com), we see that the address of the link is different than its title. The address is 175.45.176.199 which is the kali attack machine that we just set up with the exploit. And we used that exact ip address while we were setting up the exploit. So whenever an outside machine tries accessing to this ip address, the exploit will execute.

When we click the link we see that we are redirected to 175.45.176.200, which is the windows attack machine if we look at the topography. Though the website looks like the website of facebook. This attack gets the target to give out his username and password. So it is an easy cyber attack since we don’t need to break any security, we literally make the target give us his username and password. But the tricky part is fooling the target with convincing email and website. So there is definitely social engineering involved. When we enter the username and password, the victim realizes that there is a problem. But maybe this attack could be improved by redirecting the target to the real facebook website with url parameters (though I don’t know if facebook supports that).

We go back to the kali attack machine. We were able to see the public ip, port, private ip of the target. We were able to upload a file to the htdocs folder of xampp in order to change what the target server displayed. Htdocs folder of xampp is the folder where the default webpage files are kept.