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

**Lab 7: Exploiting a Vulnerable Web Application**

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.

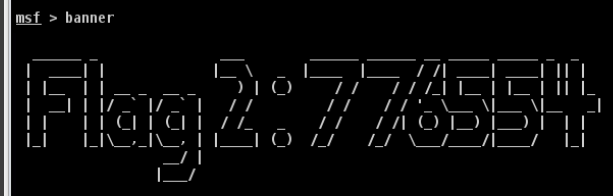
**Part 1**

**challenge #1**

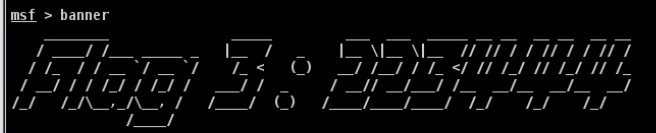
* **Flag screenshot #1**

****

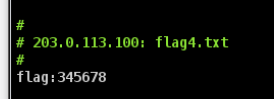
**challenge #2**



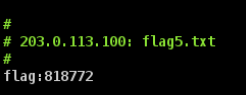
**challenge #3**



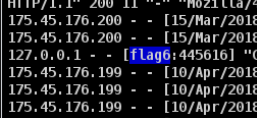
**challenge #4**



**challenge #5**



**challenge #6**



**PART 2**

We first log into kali attack machine and use the preinstalled nmap to scan 203.0.113.100. If we look at the network topology, we can see that this is the public ipv4 of the other local network that contains multiple hosts. We can see that port 8180 is open and its service name is sampleflag:999818.

Then we launch preinstalled zenmap which is the gui version of nmap and we scan the same ip. We can see the service that is provided at port 80 which is apache. When we search the apache version in google with word exploit we can easily find exploits. When it comes to cybersecurity, there is a big database of attacks for all kinds of platforms. But since these attacks are known, newest versions of platforms and developers for these platforms follow certain secure programming practices to defend against these well known attacks.

We launch metasploitable and get the flag2 and flag3 from banner.

We add the target public ip address as the target host. Then we scan it. After the scan begins, we see that the host OS is windows. So we go to windows exploits and select xampp\_webdav\_upload\_php. We can browse the files and download them and view them through this program. We don’t have permission to read the flag4.txt and flag6.txt but we can download them.

Under the public ip, we add another host using the local ip of the windows server.