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

**Lab 8: Performing SQL Injection to Manipulate Tables in a Database Submission**

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**

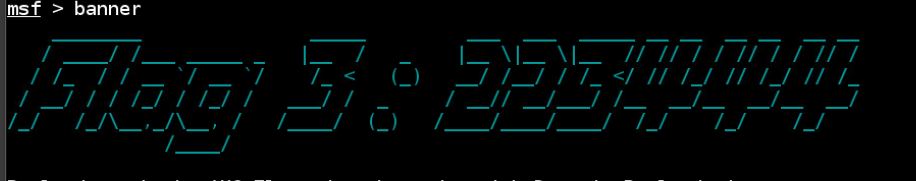
* **Flag screenshot #1**

****

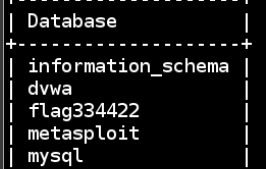
**challenge #2**

****

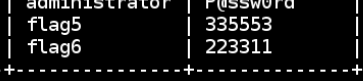
**challenge #3**

****

**challenge #4**



**challenge #5 challenge #6**



**PART 2**

We first connect to the kali attack machine that is in a different public ip that the other local network that has a public ip and multiple hosts. In order to perform banner grabbing on our target, we first scan the ports of the target using nmap. We use a DNS argument with our nmap instead of an IP argument. The DNS corresponds to the public ip of campus.edu (203.0.113.100). We get the output in screenshot1. Then we launch postgresql and metasploitable. We load the exploit, set the parameters, and run it. This allows us to get access to the database and now we can execute sql statements. This allows us to look at the databases and tables.

If we pay attention, we see that at first we logged into the database using the root user. After we got root access to the database, we created a user and gave it all privileges. Then we logged off and logged back in with the new user which is the backdoor.