**Performance Assessment: SQL Injection**

In this Performance Assessment, you will perform the tasks you have been taught in the Guided Practices (iLabs content form EC-Council).  You may use the book, and any notes you have. You may look at your prior labs. You may not give or receive help from other students. You may ask your instructor for assistance, but it is likely to cost points.

*Important*

***Please note the following guidance****: This Assessment should be performed in the VCastle POD using the Parrot Linux or Windows 10 WS virtual machines.*

*All screenshots should reflect your own work and should have the date, time and user information (name, student ID) clearly displayed*

Instructions

***Tasks:***

1. (20 pts) Using any of the tools available on the ParrotOS or Windows 10 WS virtual machines, identify all the servers running on standard web server and SQL server ports in the VCastle environment.
   1. List the command used:
   2. List the web server/SQL server IP addresses:
   3. Provide a screenshot of the command and the beginning of its output here:
2. (5 pts) Question 1: Which of these web servers are web application servers? Explain how you determined this.
3. (5 pts) Question 2: Do the web application servers have open SQL ports? Explain why or why not?
4. (5 pts) Question 3: If the web application does not have SQL ports, how can you use SQL injection attacks against them?
5. (20 pts) Use any of the tools available on the ParrotOS or Windows 10 WS virtual machine to scan for SQL vulnerabilities on one or more of the application servers until you find one that is vulnerable?
   1. List the command used:
   2. Provide a screenshot of the command and the beginning of its output here:
6. (5 pts) Question 4: When scanning for SQL injection vulnerabilities, what is the scanner looking for?
7. (20 pts) Using any of the tools available on the ParrotOS virtual or Windows 10 WS virtual machines or manual methods that you learn, perform an SQL injection attack.
   1. List any commands or techniques used:
   2. Provide a screenshot of the command and the beginning of its output here: