**Performance Assessment: Hacking Web Server & Web Applications**

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. (25 pts) Using any of the tools available on the ParrotOS or Windows 10 WS virtual machines, identify all the web servers running on standard web server ports in the VCastle environment
   1. List the command used:
   2. List the web server IP addresses:
   3. Provide a screenshot of the command and the beginning of its output here:
2. (25 pts) Use any of the tools available on the ParrotOS or Windows 10 WS virtual machine to footprint one of the web servers.
   1. List the command used:
   2. Provide a screenshot of the command and the beginning of its output here:
3. (25 pts) Using any of the tools available on the ParrotOS virtual or Windows 10 WS virtual machines, scan for web vulnerabilities on one of the web servers.
   1. List the command used:
   2. Provide a screenshot of the command and the beginning of its output here:
4. (25 pts) Explain how you could use the information you obtained in the previous steps to gain access to the web server.