# **Final Performance Assessment: Ethical Hacking II**

In this Performance Assessment, you will perform the tasks you have been taught in the Guided Practices (iLabs content from 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.

# Resources Needed

This lab assessment covers all the modules from your EC-council lab content. Thus, all resources you will need will be from your labs, your text, and any research that you might have.

# Level of Difficulty

Moderate

# Important

**Please note the following guidance**: This Assessment should be performed in the Performance Assessment VCastle POD using the Parrot Linux virtual machine.

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

All takeaways/inferences you can make about your target based on the reconnaissance should be clearly expressed (full sentences without excessive use of bullet points) and should be in your own words and result from you doing the work.

# Instructions

***Tasks:***

1. Using any of the tools available on the ParrotOS virtual machine, perform a session hijacking attack using the Windows 10 machine as a target.
   1. Login to the Windows 10 machine open a browser and login to the firewall using the web interface. Use the following credentials: (**Note**: these will not work; they are used so that you can see the authentication attempt in your hijacked session)
      1. fwadmin
      2. Password1
   2. Provide documentation of the following:
      1. Any commands or tools and settings used to hijack the session
      2. A screenshot of any user authentication information captured.
   3. For the exploit above, explain how the exploit worked and what controls could be used to minimize or eliminate this vulnerability.
2. Using the tools available on the ParrotOS virtual machine, use any method available to perform a scan that attempts to evade an IDS or firewall
   1. Provide the following documentation:
      1. A screenshot of the command or tool used and its output
      2. Screenshot showing the command used to perform the FTP bounce scan and its output.
   2. Explain, in your own words, how the previous scan evades the detection of the IDS or circumvents the firewall.
3. Using any of the available tools on the ParrotOS virtual machine, locate a host on the network that is running a web server or web application and enumerate as much information as you can about the web server/application program, the web site, and its configuration.
   1. Provide the following documentation:
      1. A screenshot of the tool(s) used and the output
   2. Explain, in your own words, how the information collected during web scanning and enumeration, in the previous question, can be used to launch an attack against a web server.
4. The Ubuntu machine in your VCASTLE topology is running DVWA. Attempt to perform SQL Injections against DVWA.
   1. Do not log into the Ubuntu machine but rather any other machine that you have access to on the network
   2. Open a web browser and navigate to the website that is running on Ubuntu. Login to the website using admin/password as credentials and select SQL Injection from the menu.
      1. Using any of the tools on the Parrot OS or using any of the techniques you have learned in this course:
         1. Prove that the site is vulnerable to an SQL injection attack
         2. Use any SQL injection technique to expose or manipulate information or run commands on the system.
   3. Provide documentation of the following:
      1. Screenshot showing the system is vulnerable to an SQL injection attack
      2. Screenshot showing the SQL injection vulnerability being exploited.
   4. Explain, in your own words, how the SQL injection attack you performed works and what can be done to mitigate or eliminate this vulnerability.
5. Using any of the tools or techniques mentioned in the text, perform a scan of publicly accessible S3 buckets. If you are unable to access the Internet with these tools, explain how you would use the tool to perform this scan. (**Note**: this step can be performed on any computer that has Internet access)
   1. Provide the following documentation:
      1. A screenshot of the tool(s) used and the output
   2. Explain why an organization might put information in a publicly accessible S3 bucket.
6. Download the Damn Small Linux (DSL) ISO and its associated MD5 hash file. These files are located at this URL <http://distro.ibiblio.org/damnsmall/current/>. Download and install any MD5 hash calculator and verify that the DSL ISO file was not corrupted during the download.

(**Note**: this step can be done on any machine where you have Internet access.)

* 1. Provide the following documentation:
     1. Screenshot of the contents of the DSL MD5 hash file that was downloaded.
     2. Screenshot of the tool used to calculate the MD5 has of the DSL ISO and the resulting MD5 hash.
  2. Explain, in your own words, how the procedure you used above verifies that the file was not corrupted during download.