# **Week Three Lab: Vulnerability Analysis**

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

# How does this practical lab apply in the real world?

During the vulnerability analysis phase of a penetration test, an ethical hacker uses information gathered in previous phases to identify and analyze potential vulnerabilities that may exist on the target systems. This phase will usually include the use of both manual and automated methods to detect these potential vulnerabilities.

In this activity, you will focus on identifying and researching vulnerabilities. Document your findings thoroughly through screenshots and well-written paragraphs describing the purpose of the tools you used, the options you set, and your interpretation of the results.

# Resources Needed

This lab assessment covers Modules 05 from your EC-council lab content. Thus, all resources you need will be from your labs, your text, and any research that you might have.

As a special note: Greenbone is running by default, you will not need to start it. Use your browser and go to the localhost it is on port 443 by default no need to add a port switch.

# Level of Difficulty

Moderate

# Important

**Please note the following guidance**:

* This Assessment should be performed in the 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 the Parrot OS virtual machine, perform a vulnerability scan on one or more targets using one of the built-in vulnerability scanners. Provide a screenshot of the results of the vulnerability scan.
2. Are vulnerability scanners primarily an offensive tool or a defensive tool? Justify your answer.
3. Using any identified vulnerability from the previous scan (or one provided by your instructor), research the vulnerability in an online vulnerability database. Provide a screenshot or screenshots that show the following:
   1. CVSS Rating
   2. CWE
   3. Web locations that provide information on mitigating the vulnerability
4. If you were writing a report for a customer, write a statement for a recommendation for remediation.
5. On a scale from 1 to 10, 1 being low and 10 being high, what is the likelihood of this vulnerability being exploited in an environment? What is your reasoning?
6. Explain in detail how you can use a vulnerability database to both attack and defend an organization's network.
7. Using the identified vulnerability (or one provided by your instructor), search an online exploit database, and provide a screenshot of the code or method (if any) to exploit the vulnerability.
8. What ethical issues must be addressed before posting exploit code in an online exploit database?