**Week 5 Lab: Final Evaluation Chalk and Wire**

In this lab assignment, you will perform the tasks you have been taught in the Guided Practices (iLabs content from EC-Council). You may use the book, online resources, and any notes you have. You may look at your prior labs and use them as a resource.

How does this practical lab apply in the real world?

Evaluating a network through pentesting involves various facets that must be considered. Many insurance companies require organizations to have a penetration test certificate as prerequisite proof that the organization has identified threats and the steps taken to mitigate them. Insurance companies will require all the resources that are within the organization as well as the threats that these assets present to the organization. Insurance companies will require that organizations provide proof of all internal resources and threats to organizational assets. This wholistic approach to security is a continual process that must be taken seriously by the organization.

|  |
| --- |
| This evaluation is based on the labs throughout the entire course. This Chalk and Wire assignment is used for various purposes by the University to measure student progress and determine successful outcomes. This evaluation also indicates how well you met expected learning outcomes. |

Resources Needed

This lab evaluation covers weeks 1-5 and includes content from all labs within this course. You will need to use iLabs for the first section of the evaluation. The second section will be completed in VCastle. Remember that evaluations must be completed on your own. They do not include instructions for direct guidance and are intended to assess your ability to evaluate student understanding of the content and skills throughout the course.

To complete this evaluation, you will use the following:

* iLabs
* VCastle

Various tools that you will select based on your own experience gained through this course.

Please Note:

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

Level of Difficulty

Advanced

**Section One**

***Please note the following guidance****:*

*This section should be performed in iLabs within EC- Council using all the resources available to you.*

\*\*\*Use iLabs for this Section of the evaluation\*\*\*

\*\*\*You are not permitted to use the same company that you did for week one. Choose a different company.

1. Choose an organization and find as much of the following information as possible, list the information below, and provide screenshots (15 points)
   1. IP Address Ranges
   2. Registered Domains
   3. Addresses and names of Name Servers, Web Servers, and mail servers.
   4. Identify any external portal such as O365, Citrix, or a VPN that would log into company resources.
   5. Find at least five email addresses of employees.
   6. Identify the company email format.
   7. Identify the company LinkedIn page, how many employees are there?
2. All takeaways/inferences you can make about your target based on the reconnaissance should be clearly expressed (complete sentences without excessive use of bullet points), in your own words, and result from you doing the work.
3. **Documentation for this section:** Remember documentation is an important detail and is required. Documentation should include a summary paragraph for each section, which must be a complete paragraph including details of steps to receive full credit. (10 points)

**Section Two**

\*\*\*Using VCastle for this section of the evaluation. \*\*\*

1. Step One

Perform a port scan with the following parameters. Remember to complete the IP address to receive full credit for this section.

1. Research what option only displays hosts with identified ports open.
2. Using nmap, only scan once, and include all three subnets in that scan. Use the option only to display hosts with port 445 open. **(Take a screenshot of the command you used and output)**
3. Fill in the chart with the host identified:

|  |  |
| --- | --- |
| IP Address |  |
|  |  |
|  |  |
|  |  |

1. Step Two
2. Using Metasploit and the hosts identified in the previous scan, look for a scanner that identifies systems vulnerable to MS17-010 **(Take a screenshot of your scan and vulnerable host)**
3. Write two complete paragraphs addressing the vulnerability analysis, the CVE, and what needs to be done to mitigate the threat. (10 points)
4. Step Three
5. Perform research for MS17-010/Eternalblue. (10 points)
   * List the following information for one of the identified vulnerabilities: (Eternalblue)
   * CVE Number:
   * CVSS Rating
6. Remember documentation is important and detail is required. Documentation will include summary paragraph must be a complete paragraph and detailed to receive full credit. (10 points) What are they documenting here?
7. Step Four
8. Use Metasploit to exploit a Windows system with MS17-010  (15 points)
   * Using your Parrot machine startup Metasploit and use the proper exploit and payload to exploit a Windows hosts.
   * Configure an exploit and run it with a Meterpreter reverse shell.
   * Attempt to use the built-in Meterpreter features and techniques to escalate privileges.
   * Perform a hashdump **(Take a screenshot)**
   * Drop into a Windows prompt and navigate to the Administrator desktop.
   * Create a text file on the desktop and give it your STUDENTID as a name. **(Take a screenshot)**
9. Remember documentation is important and detail is required. Documentation will include summary paragraph must be a complete paragraph and detailed to receive full credit. (10 points) What are they documenting?
10. Step Five
11. Using SET on the Parrot virtual machine, craft a social engineering attack.  (15 points)
    * Open any email client and start a new message. In this message, craft an email to lure a victim to enter in their username and password.
    * Show what will the embedded link display vs. where it actually points to (Parrot machine). (**Take a screenshot of your crafted email and subject line)**
    * Use the credentials harvesting Google template to capture credentials.
    * Use the Windows 10 machine as the victim host.
    * When the pop-up for Google appears, enter in your **Student ID** followed by a password of your **StudentID+Year (Take a screenshot of the pop-up with the data entered)**
    * On the Parrot machine record the output captured. You should see the data you entered. **(Take a screenshot of the “WE GOT A HIT!”** **output)**
12. Documentation: Remember documentation is important detail is required. Documentation will include summary paragraph must be a complete paragraph and detailed to receive full credit. (10 points) What are they documenting?