# Week 3 Lab: System Hacking (VCastle)

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

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

During the system hacking phase of a penetration test, an ethical hacker attempts to exploit vulnerabilities found to gain access, escalate privileges, maintain access, and cover their tracks in the target systems.

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

|  |
| --- |
| This attack simulates the ability to exploit using standard Windows network traffic and acting as a man in the middle. This also simulates the commonality of the reuse of passwords within many environments and why it is essential to capture both clear text passwords and hashes to attempt to use on other machines. |

# Resources Needed

This lab assignment covers Module 06 from your EC-Council lab content. Thus, all resources you will need are your iLabs, your text, and any research that might help you.

# Level of Difficulty

Moderate

# Important

**Please note the following guidance**:

This Assignment should be performed in the VCastle POD using the Parrot Linux virtual machine and Windows 10 Wireshark Client. (**Note**: This will ONLY work on the Win10 Wireshark machine)

The following images are examples of what will be seen when attempting the lab assignment.

## **Windows 10 Wireshark (Machine AutoLogin to Server)**

A screenshot of a computer

Description automatically generated

This will be the Parrot OS waiting for the intercept. It is important to remember that you must apply the tools and concepts learned from iLabs. This is only a small excerpt demonstrating the two machines you must implement.

A screenshot of a computer

Description automatically generated

Password Cracking Using your tool of choice Please delete the contents of the hash.txt in the perspective folder that is associated with Remina logs. Please see image below for example of what to copy to the hash.txt after it has been cleared.

A computer screen with text

Description automatically generated

\*\*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 (complete sentences without excessive use of bullet points), using your own words. All work should be completed independently by you.

# Instructions

**Tasks:**

1. Step one is to disable the docker server running on the Parrot OS. Otherwise, you will get a port conflict.
   1. docker stop sad\_goldstine
   2. sudo systemctl status docker
   3. Ensure that the docker service is not running
2. Open a terminal window and browse to /usr/share/responder
   1. Start Responder and leave it running **(Take a screenshot of Responder starting with the options you give it)**
3. Leave the Parrot machine and go to the Windows 10 Client machine in the 172.20.242.0/24 subnet.
4. Log into the Windows 10 machine **(This process simulates what a victim would do on the network)**
   1. Browse to CIS403-WIN2019 through the network explorer
5. Leave the Windows Wireshark 10 machine and return to the Parrot machine
   1. You should have a hash within the terminal with Responder running. **(Take a screenshot of the hash)**
   2. Run john-the-ripper to crack the hash **(Take a screenshot of the hash cracking)**
   3. Start Metasploit and use the smb psexec module
   4. Configure the smb/psexec exploit and the meterpreter reverse\_tcp payload
      1. Use the username and password gained from cracking the hash
      2. Use the Windows 2019 IP **(Take a screenshot of the configuration)**
      3. Run
   5. From your meterpreter session, elevate privileges to perform a hash dump.
      1. This can include getsystem or migrate processes
   6. Run hashdump **(Take a screenshot of the output)**
   7. Run john-the-ripper to crack the hashes **(Take a screenshot of the hash cracking)**
   8. Use the gained accounts to log into the XXXXXX machine and screenshot the text file on the desktop.
6. What service(s) is Responder.py targeting?
7. What hash format is the hash that was captured?
8. What is the benefit of dumping hashes and cracking them?
9. Why is it important to understand how a hacker maintains access on a system?
10. Explain at least two actions you would need to take to cover your tracks on your target.

**Deliverables Example for tasks one-X (EXAMPLE ONLY)**

* **Threat:** DNS Dumpster identified a Microsoft server using HTTP API/2.0 with an IP address of 121.171.142.220 in South Korea. The exploits available for this protocol include Banner Disclose vulnerable on WAP servers. (What Threat allowed this attack)
* **Mitigation** The Microsoft-HTTPAPI/2.0 vulnerability can be mitigated by disabling the server Header in the registry key via HKEY\_LOCAL\_MACHINE. (How would this be mitigated in a network?
* **Summary:** This site has various potential vulnerabilities that must be remediated and verified. The use of DNS dumpster provided a DNS snapshot at a moment that indicated potential threats that the United Nations could face. Understanding each threat and making recommendations to prevent such threats is essential. There are more vulnerabilities within this organization that should be mitigated and then reverified as corrected. Please provide a summary of the lab as per the example above.

The following items should be addressed in the above content threat and mitigation.

* ArpSpoof
* Macof

**Deliverables:** Complete this section, using the example above as a template for each answer. If there is more than one task, include as such. If there are less than 6 tasks, only include the tasks needed for the lab, as ***this is a template only.***

Task 1:

Task 2:

Task 3:

Task 4:

Task 5:

Task 6: