# MODULE 09 SOCIAL ENGENERING LAB REPORT

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE
Course Code: T44-17520

## Lab Session Identifiers

1. https://labclient.labondemand.com/LabClient/ac600fa1-4a41-4ece-8ad3-80ae91f819c3

2. https://eccouncil.learnondemand.net/Lab/Launch/55228?AssignmentId=1340522&lang=

## Username on EC-Council System

1. 2110886@uj.edu.sa

# Lab 01

ask 1: Sniff Credentials using the Social-Engineer Toolkit (SET)

1. Begin by switching to the Parrot Security machine and logging in using the provided credentials.
2. Open a terminal window by clicking on the MATE Terminal icon.
3. Gain root access by typing **sudo su** in the terminal and entering the password when prompted.
4. Navigate to the Social-Engineer Toolkit (SET) folder by typing **cd social-engineer-toolkit**.
5. Launch the SET by typing **./setoolkit** in the terminal and agreeing to the terms of service if prompted.
6. In the SET menu, select "Social-Engineering Attacks" by typing **1** and pressing Enter.
7. Choose "Website Attack Vectors" by typing **2** and pressing Enter.
8. Select "Credential Harvester Attack Method" by typing **3** and pressing Enter.
9. Choose "Site Cloner" by typing **2** and pressing Enter.
10. Enter the IP address of the local machine when prompted for the "IP address for the POST back in Harvester/Tabnabbing" and press Enter.
11. Enter the URL you want to clone when prompted and press Enter.
12. Wait for the cloning process to complete and follow the instructions to send the IP address of your Parrot Security machine to the victim.
13. Switch to the Windows 11 machine, log in, and open the email containing the phishing link sent by the attacker.
14. Click on the malicious link in the email, which will lead to a replica of the cloned website.
15. Enter fake credentials into the form fields as instructed, noting the different URLs in the browser address bar.
16. Switch back to the Parrot Security machine and return to the terminal window.
17. Observe the captured credentials displayed in plain text in the terminal, confirming successful credential harvesting.
18. Close all open windows and document the acquired information for analysis and further action.

What I Learned:

- How to use the Social-Engineer Toolkit (SET) for phishing attacks.
- Understanding the different types of social engineering techniques.
- Identifying the steps involved in sniffing credentials using SET.
- Recognizing the importance of user awareness in preventing social engineering attacks.
- The process of using the Social-Engineer Toolkit (SET) to perform a credential harvesting attack.
- How phishing attacks can be executed using SET, targeting users through fake websites and email lures.
- The importance of user awareness and vigilance in recognizing and avoiding phishing attempts to protect sensitive information.

## Lab 02 - Task 01

Task 1: Detect Phishing using Netcraft

1. Begin by installing the Netcraft extension, a powerful tool for identifying and blocking phishing websites.
2. Visit the Netcraft website and download the extension compatible with your browser, such as Firefox.
3. Install the extension, following the prompts provided, and restart your browser if necessary to activate it.
4. Once installed, navigate to a website you wish to check for phishing, like certifiedhacker.com.
5. Click on the Netcraft Extension icon in your browser's toolbar to access site information.
6. Review the summary of information provided by the extension, including the risk rating, site rank, and other relevant details.
7. For more detailed information, click on the "Site Report" link within the dialog box to view a comprehensive report on the site.
8. To test the extension's phishing detection capabilities, visit a known phishing website (e.g., smbc.ctad-co.com/m).
9. Observe how the Netcraft Extension automatically blocks access to suspected phishing sites and alerts you to potential risks.

## Lab 02 - Task 02

Task 2: Detect Phishing using PhishTank

1. Proceed by accessing the PhishTank website, another valuable resource for identifying and reporting phishing attempts.
2. Navigate to the "Recent Submissions" section to view recently reported phishing websites.
3. Click on any phishing website ID to access detailed information about the reported phishing attempt.
4. Check if PhishTank has identified the website as a phishing site and review any available details or reports.
5. Return to the PhishTank homepage and utilize the "Found a phishing site?" search field to manually check a website for phishing.
6. Enter the URL of the website you wish to verify for phishing activity and click the "Is it a phish?" button.
7. Analyze the results provided by PhishTank to determine if the website is indeed a phishing site based on community reports and analysis.

What I Learned:

- The importance of utilizing specialized tools like the Netcraft extension and PhishTank to detect and prevent phishing attacks.
- How these tools leverage community-driven efforts and extensive databases to identify and report phishing attempts.
- The significance of user awareness and vigilance in recognizing and avoiding phishing scams to protect personal and organizational data