Lab 4 – Social Engineering

Introduction

This report details the steps taken to complete Lab 4 - Social Engineering, specifically focusing on a targeted credential harvesting attack. The goal of the lab is to simulate a phishing attack to capture the login credentials of an OU employee's account, within the confines of a controlled educational setting.

Task 1: Email Phishing

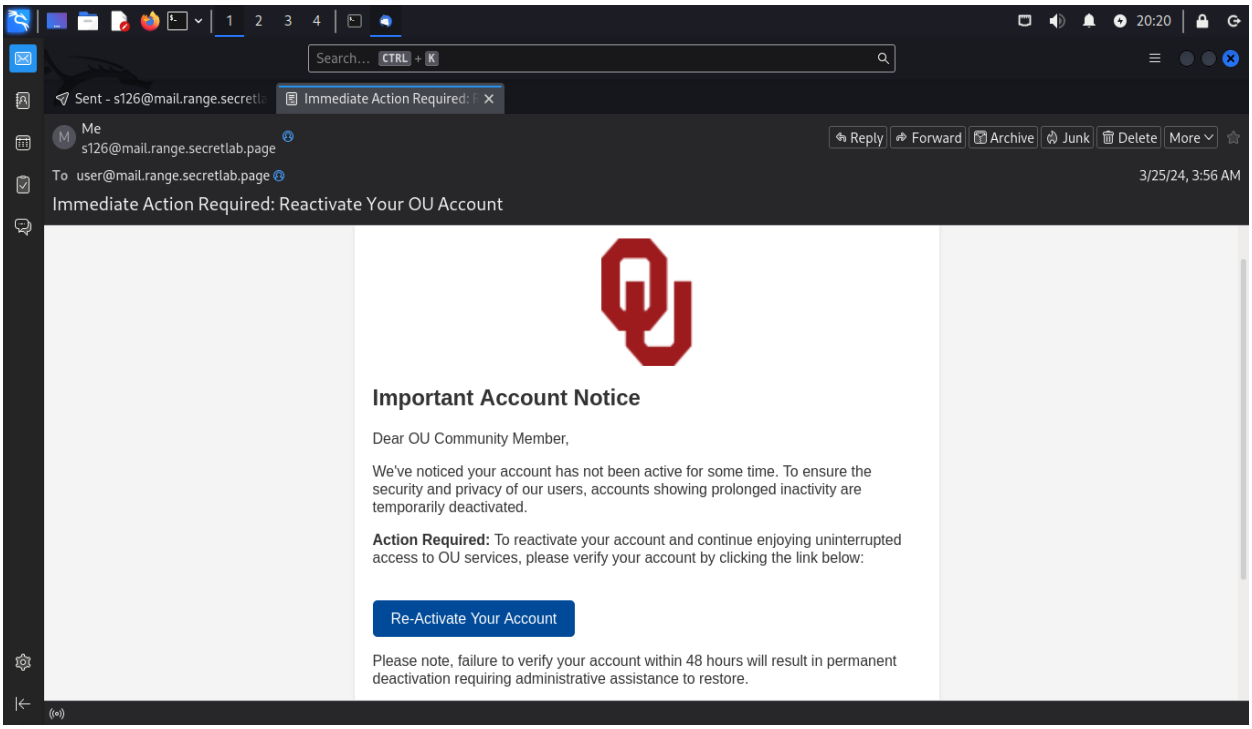
Objective

To craft and send a convincing phishing email that prompts the recipient to click on a link leading to a fake login page designed to harvest credentials.

Process

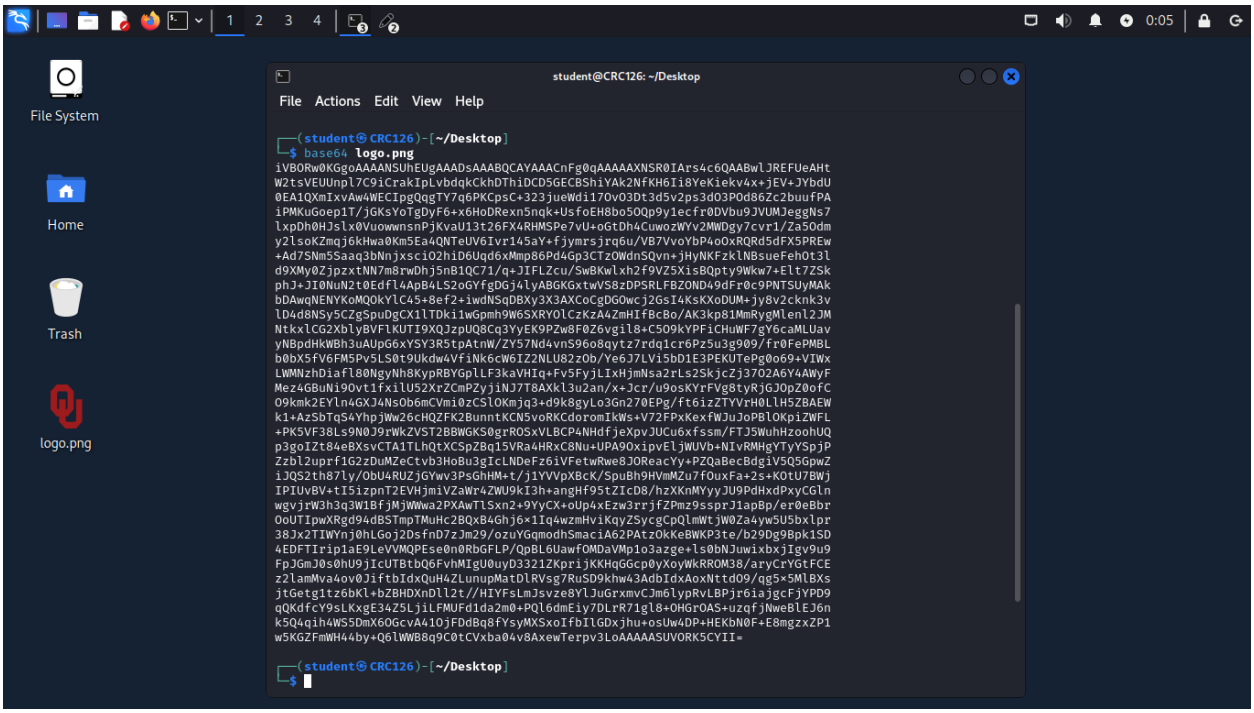
1. **Email Composition**

- Developed the email content with a clear call to action, emulating an official OU communication.
- Created the HTML body of the email with inline styling for a professional appearance.



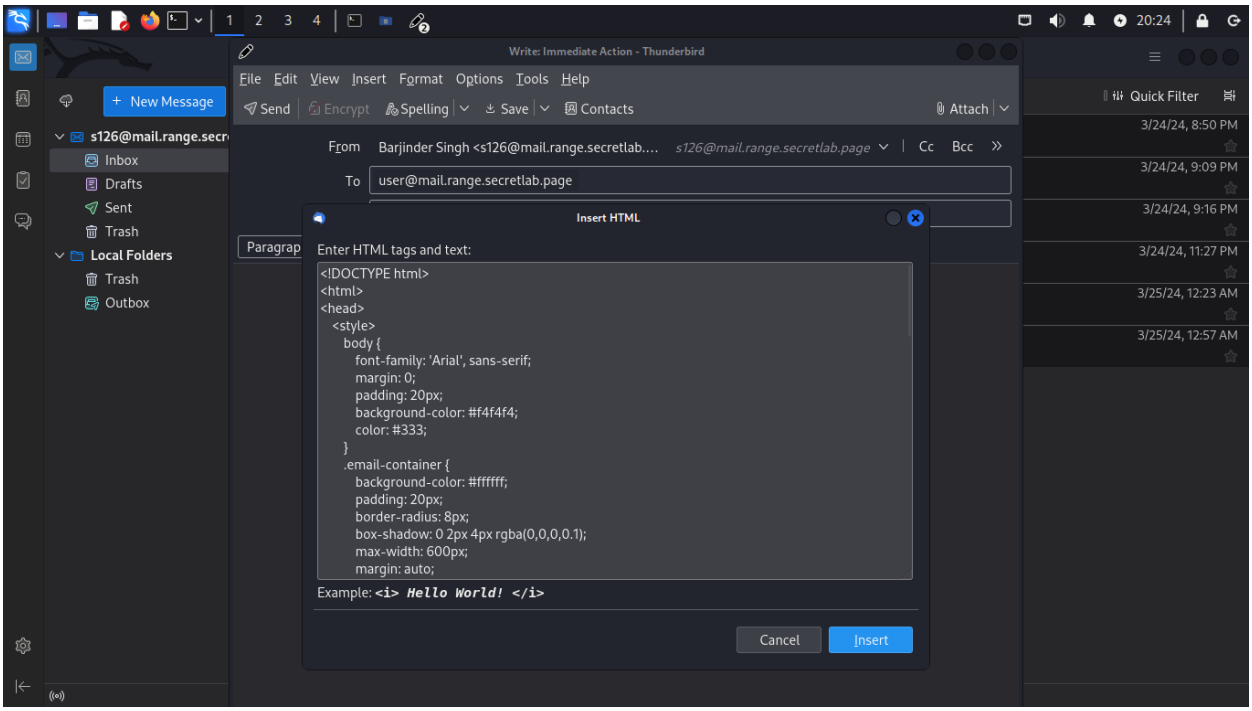
2. Image Embedding

- Encoded the OU logo into a Base64 string using the base64 command.
- Embedded the image directly into the email using the URI scheme.



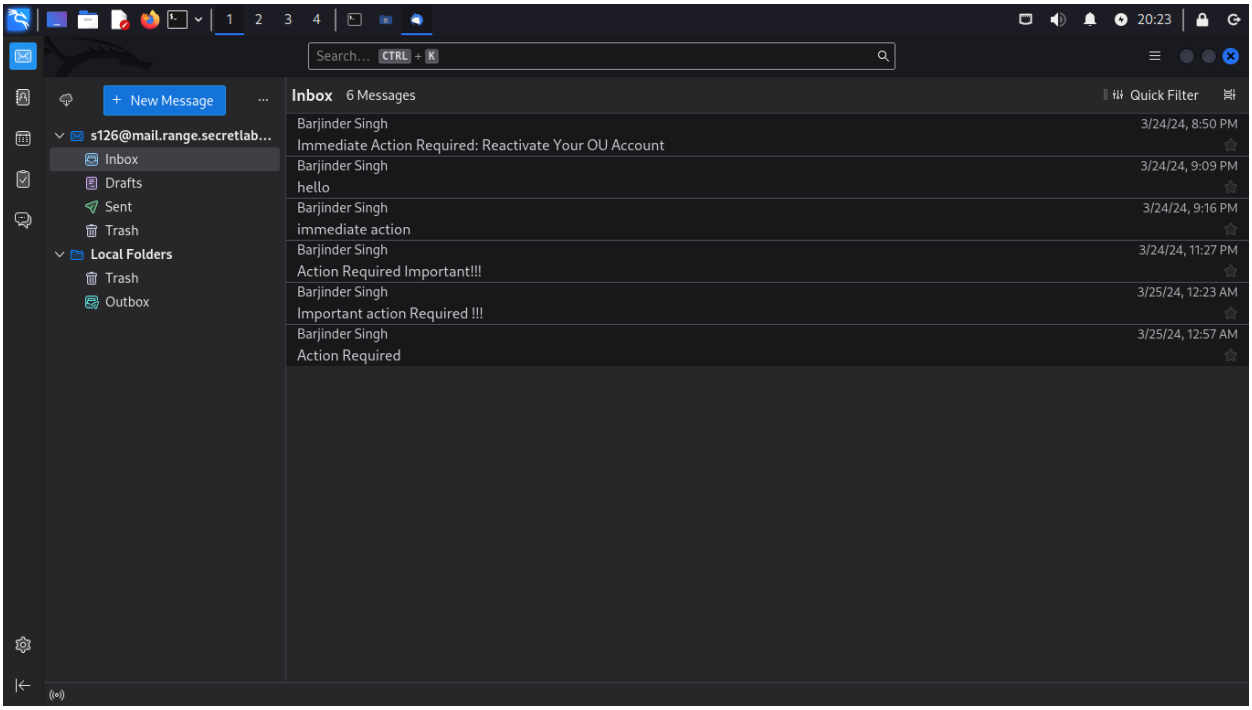
3. Email Client Configuration

- Installed and configured Thunderbird on the Kali Linux VM.
- Composed the email in Thunderbird, switching to the HTML view and inserting the prepared HTML code.



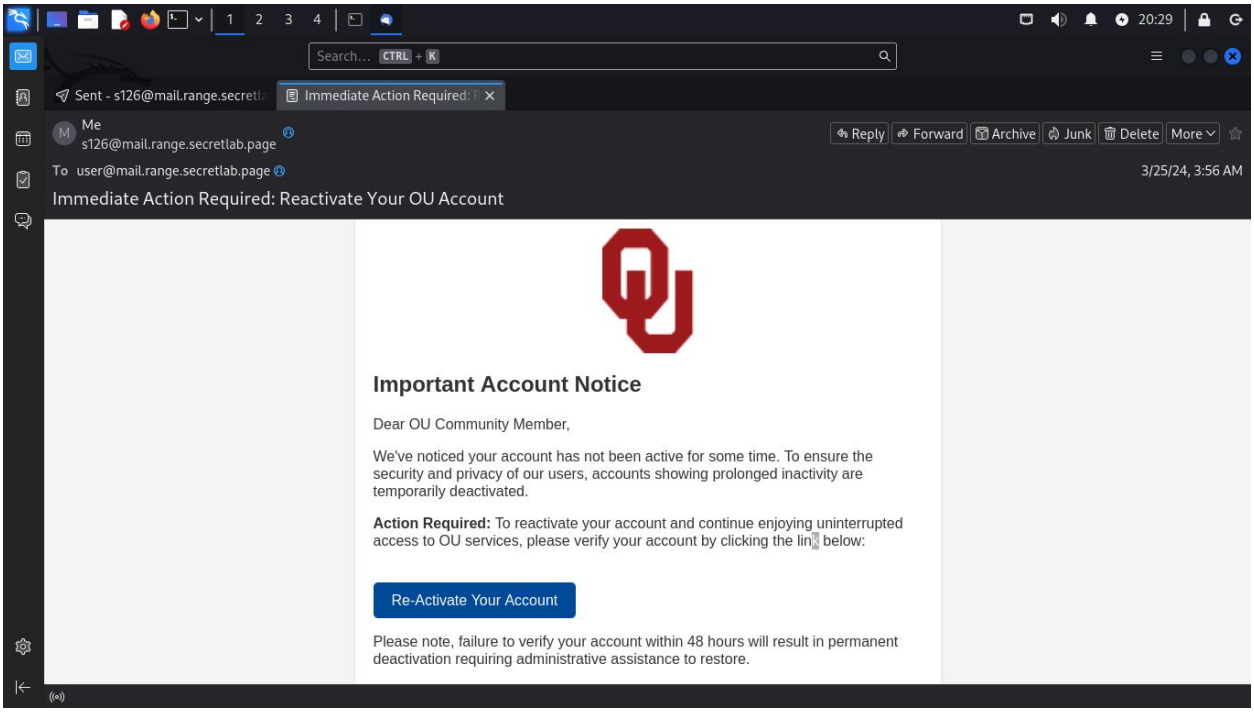
4. Testing

- Sent some test emails to my own inbox s126@mail.range.secretlab.page to ensure proper rendering and functionality.
- Adjusted the HTML code based on the test results.



5. **Sending the Phishing Email**

- Finalized and sent the phishing email to the target address: user@mail.range.secretlab.page.



Tools Used

- Thunderbird Email Client
- Base64 Encoding Utility

Challenges and Solutions

- Initially faced difficulties with remote content blocking in Thunderbird. Solved by embedding the OU logo using a base64-encoded string.
- The base64 string required formatting without line breaks to function correctly in the HTML img tag.

Task 2: Setting Up the Credential Harvester with SET

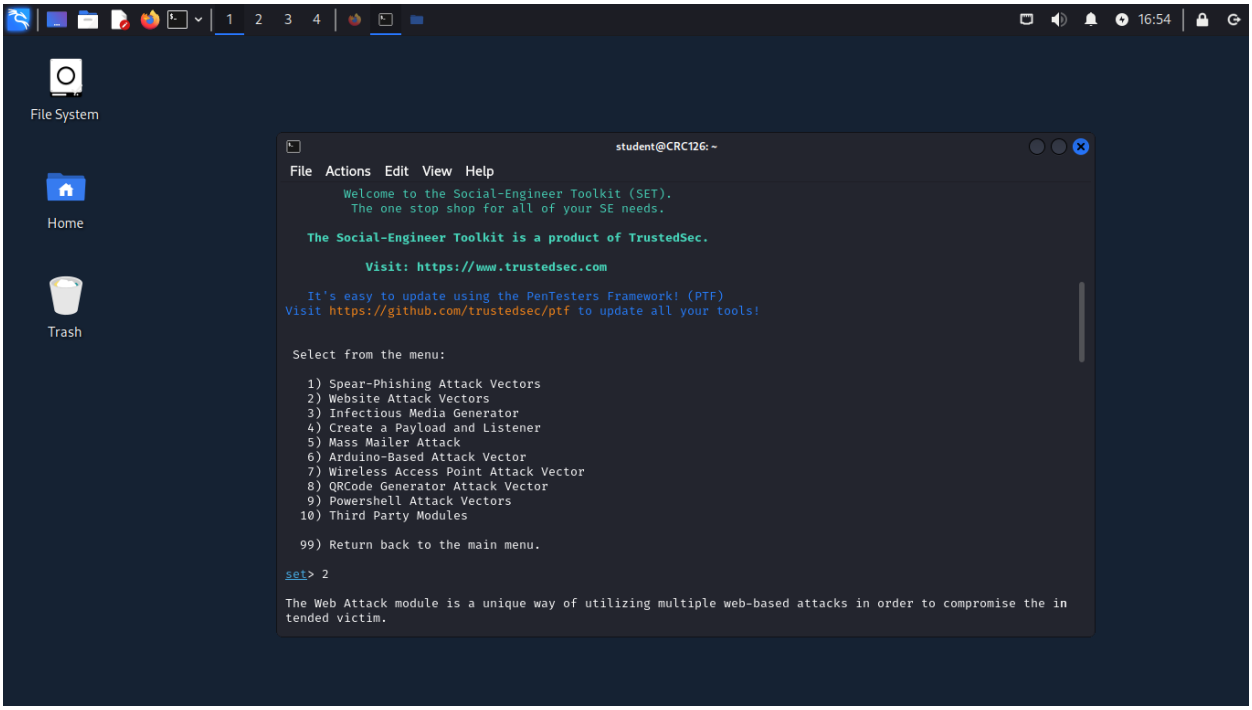
Objective

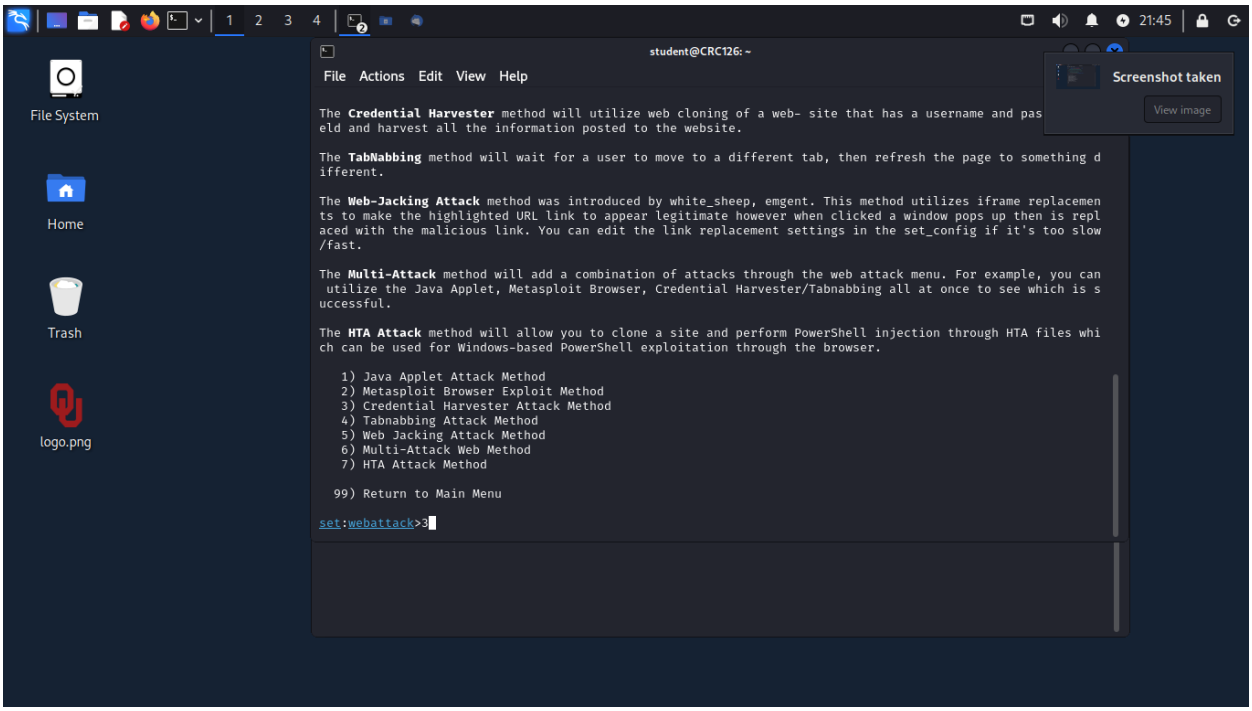
To set up a credential harvesting service using the Social-Engineer Toolkit (SET) that mimics an authentic OU login page and captures any entered credentials.

Process

1. **SET Configuration**

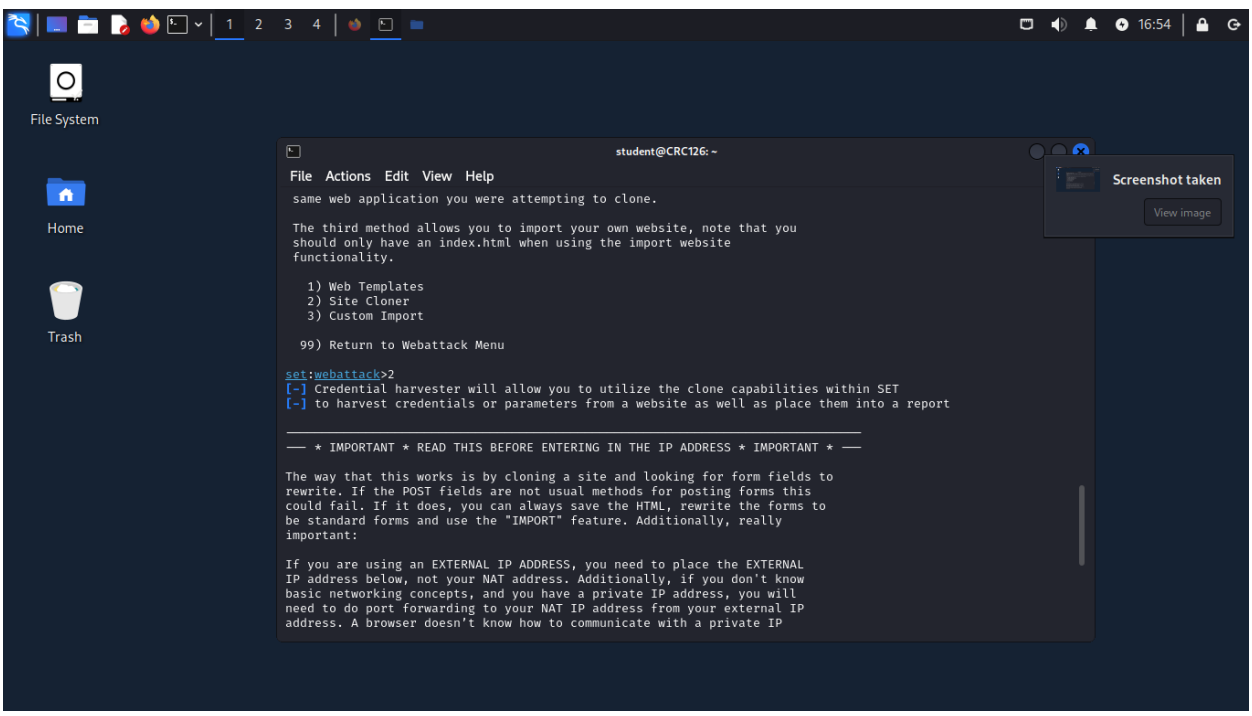
- Launched SET and navigated to the "Website Attack Vectors" and then to the "Credential Harvester Attack Method".





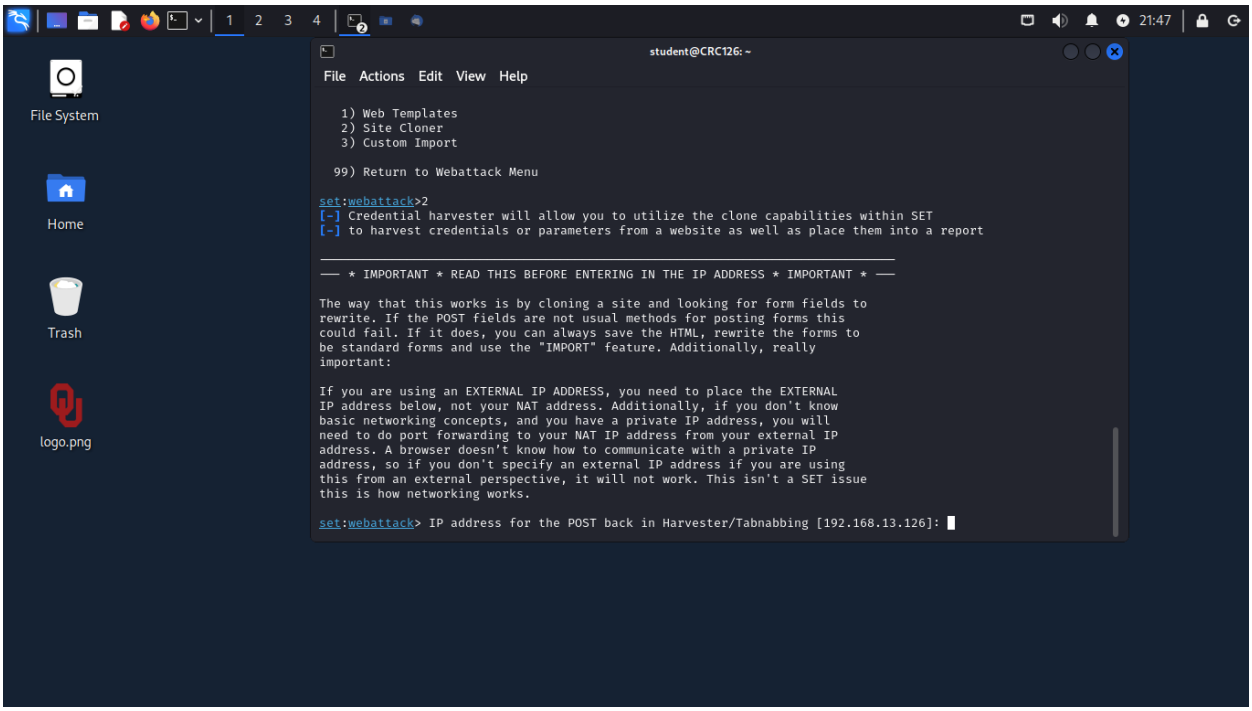
2. Site Cloning

- Selected "Site Cloner" option to clone the legitimate OU login page.



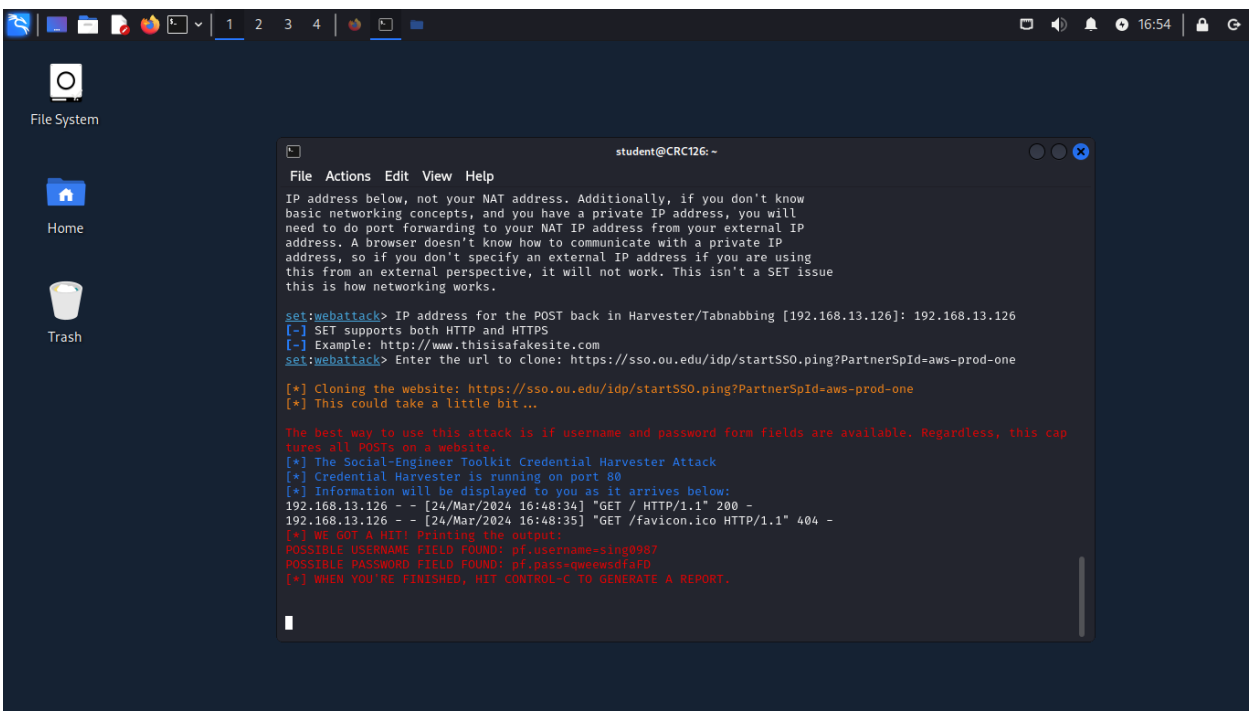
3. IP Configuration

- Configured the local IP (192.168.13.126) for the POST back in Harvester.



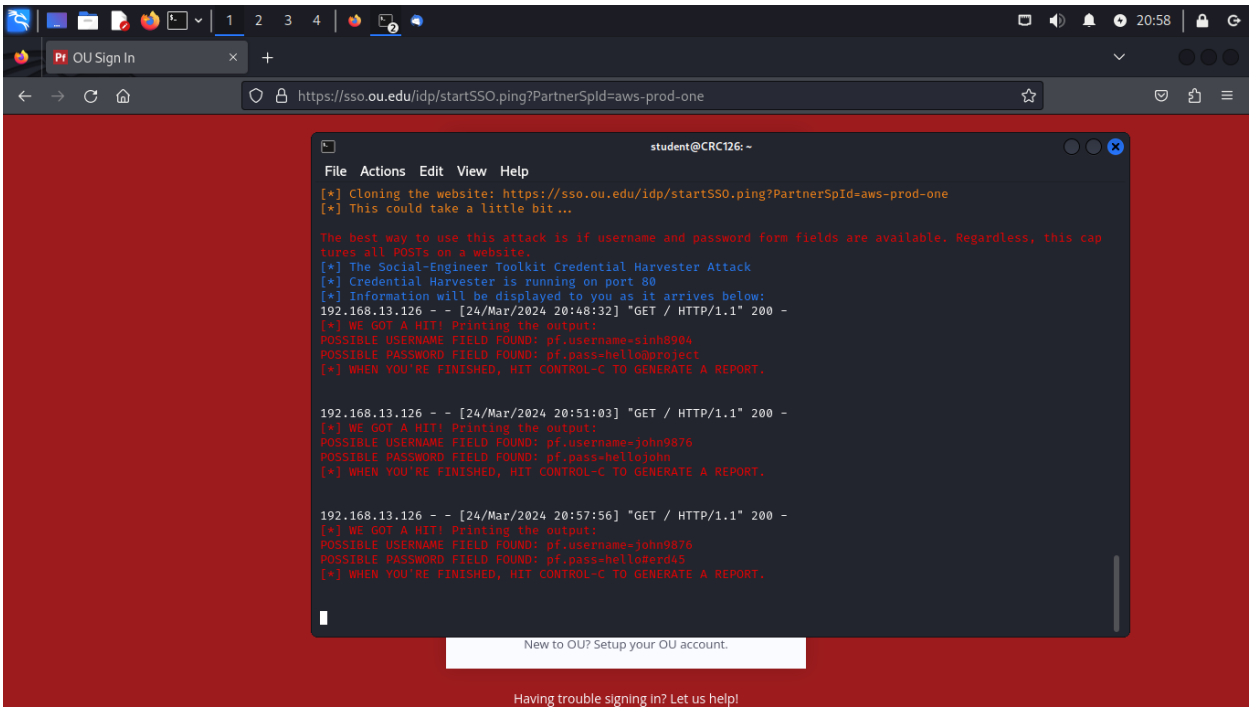
4. Webpage Cloning

- Entered the URL of the OU login page to clone.



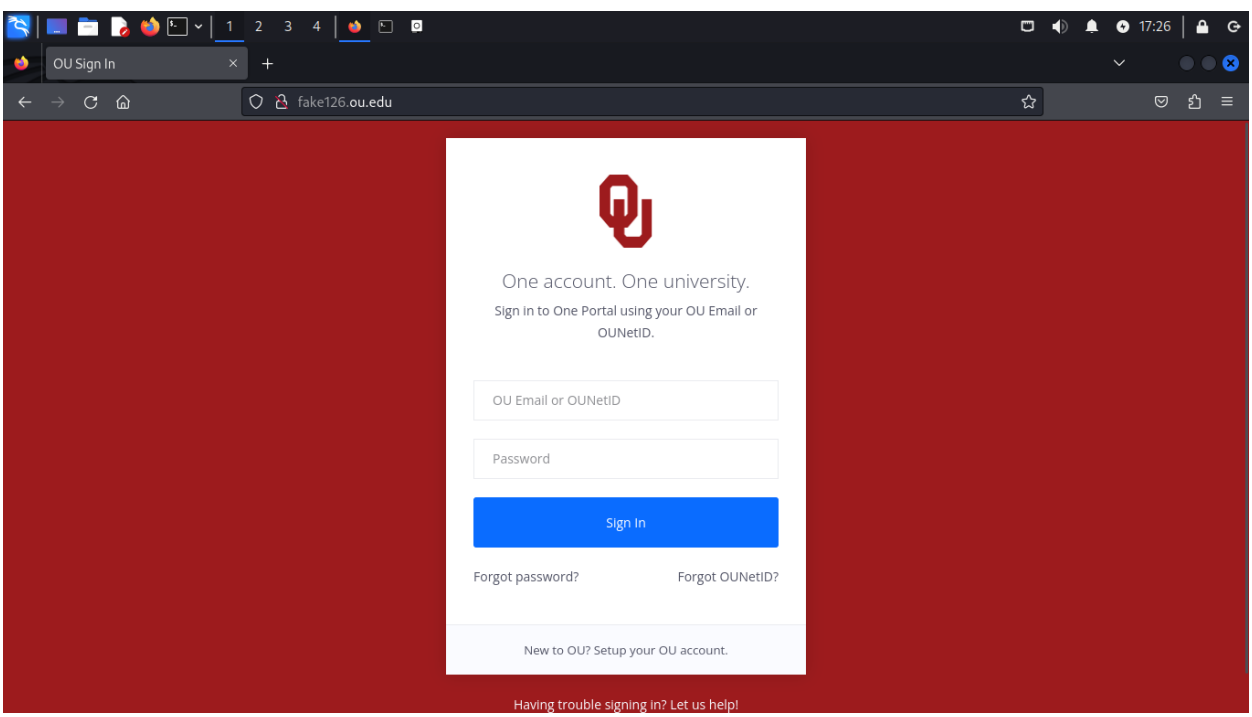
5. Credential Harvester Launch

- Started the credential harvester, which listens for incoming form submissions on the cloned page.



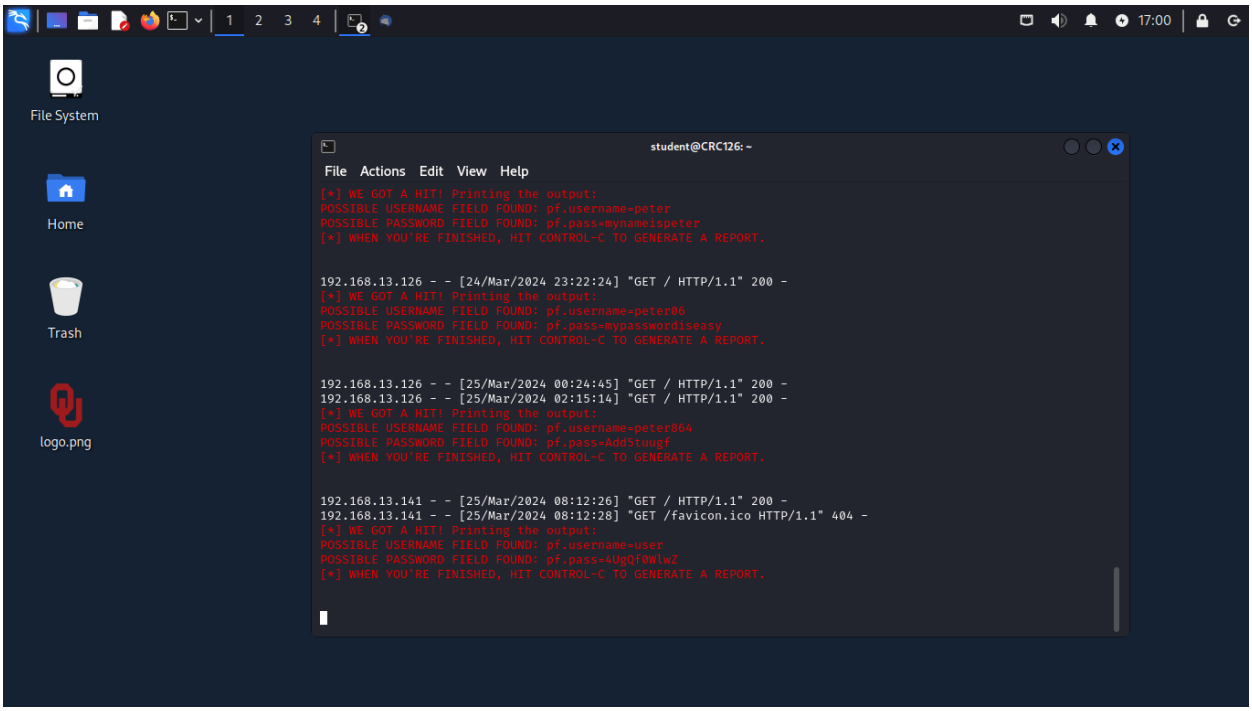
6. Testing

- Opened a browser and navigated to http://192.168.13.126 to ensure the fake login page was a replica of the original and that credentials were being captured by SET.



7. Persistent Monitoring

- Kept the SET terminal open and monitored for any captured credentials.



(The username and password entered by OU employee's email address user@mail.range.secretlab.page. is user for username, and 4UgQf0Wlwz for password.)

Challenges and Solutions

Apache2 conflicts: Initial attempts to use Apache2 led to permission and configuration issues, which were bypassed by using SET's built-in server capabilities.

Conclusion

This exercise demonstrated the process of creating and deploying a phishing attack within a controlled environment. The phishing email was successfully crafted using Thunderbird, and the Social-Engineer Toolkit was utilized effectively to clone a login page and capture credentials. All activities were conducted in compliance with the ethical guidelines, with a focus on simulating a realistic attack scenario to better understand the mechanisms of social engineering threats.