Cyber Security Internship – Task 2 Report:

Task Title: Social Engineering & Phishing Simulation
Track Code: FUTURE_CS_02
Intern Name: Shreya V
Date:15/06/2025

AIM:

- To simulate a phishing attack by cloning a legitimate Google Sign-In page using the Social Engineering Toolkit (SEToolkit) and testing how credential harvesting and redirection techniques work in a controlled lab environment. This helps understand the risks of phishing and the importance of user awareness in cyber defense.

TOOLS USED:

- Social Engineering Toolkit (SEToolkit)
- Kali Linux
- Apache Server (used internally by SET)
- Browser (Chrome/Firefox)
- Ngrok or local IP for testing on other devices

METHOD USED:

1. Launched the SEToolkit from Kali Linux.
2. Selected the following options:
    - ✓ Social-Engineering Attacks
    - ✓ Website Attack Vectors
    - ✓ Credential Harvester Attack Method
    - ✓ Web template
3. The toolkit cloned the original Google login page and hosted it locally.

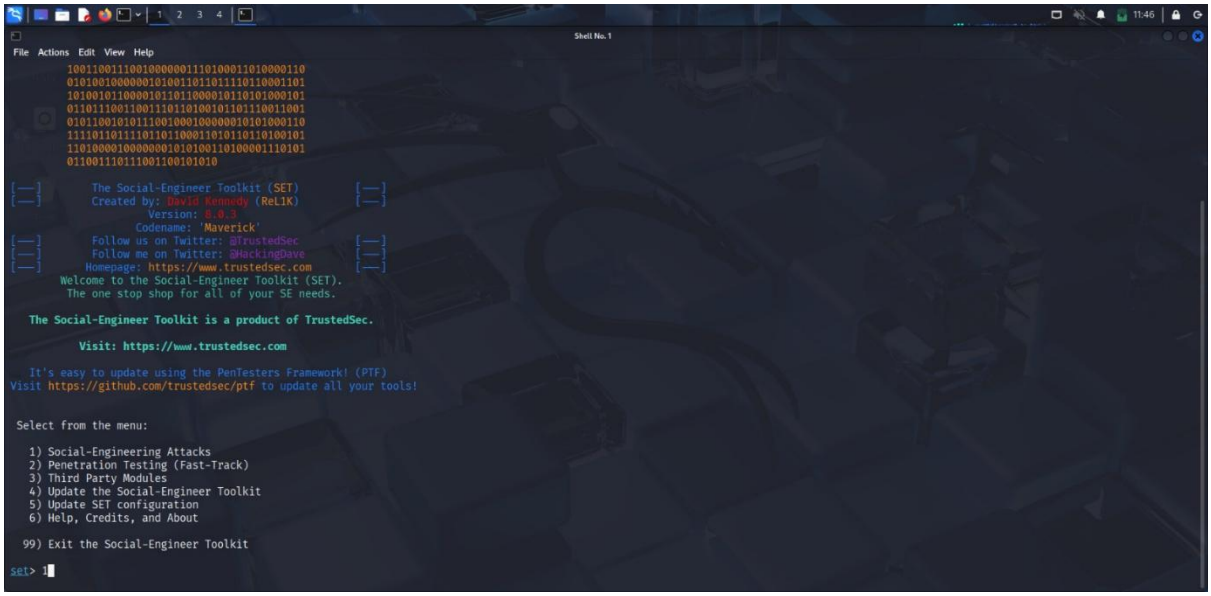
4. When the test user entered credentials into the fake page, the information was captured and saved to a local file (harvester.txt).

4. After submission, the fake page redirected the user to the **real** Google login page to avoid raising suspicion.

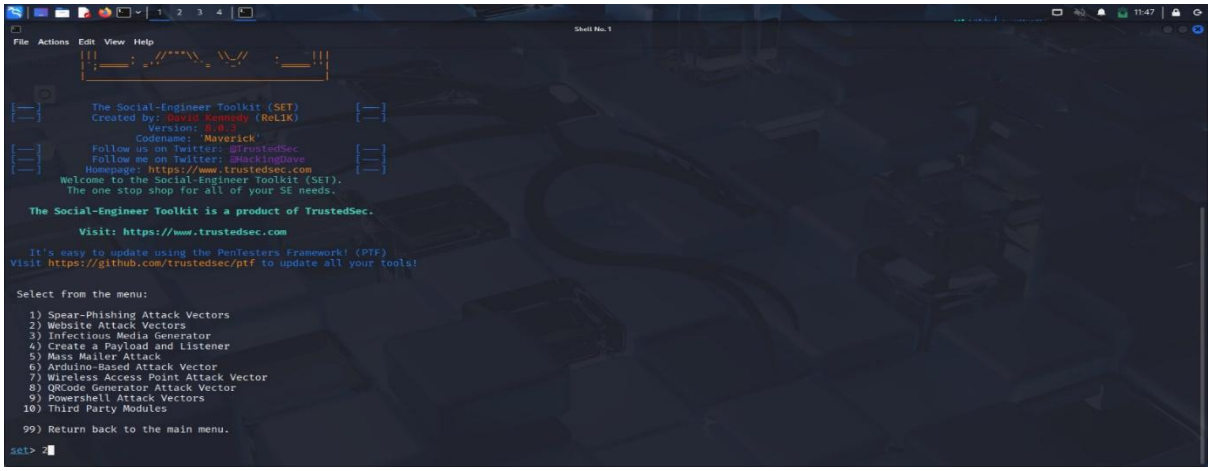
OBSERVATIONS:

- The phishing page appeared visually identical to the real Google login screen.
- Credentials were harvested and saved in cleartext.
- Redirection back to the real site after login made the attack look seamless.
- The attack would be convincing for non-technical users without training.

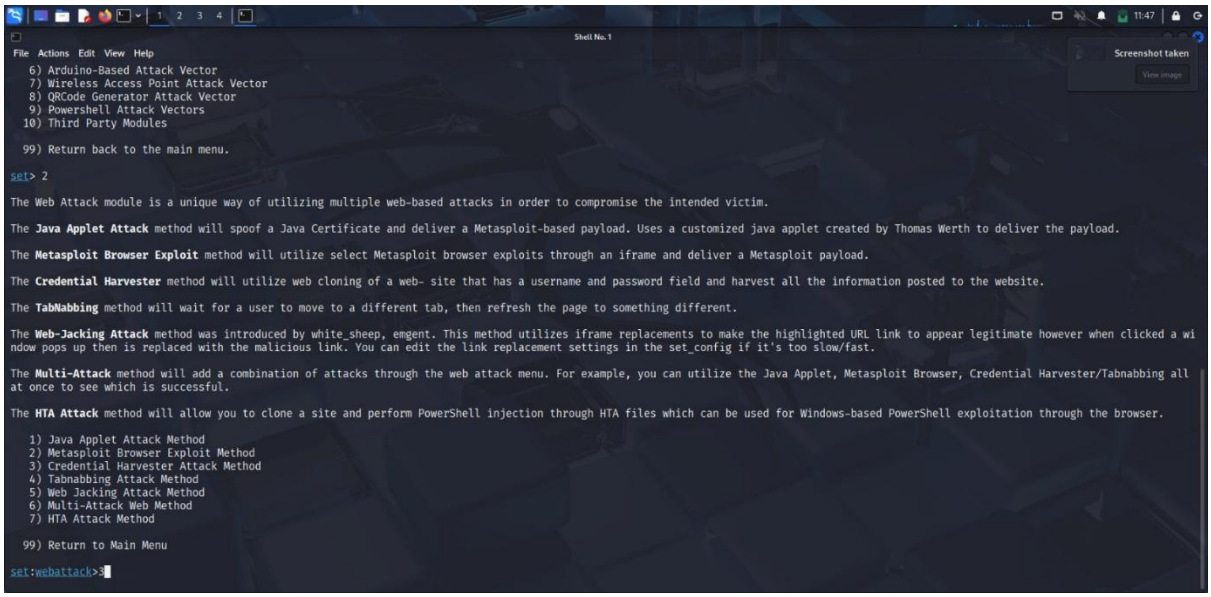
SCREENSHOTS TO ATTACH:



- Select the 1. Social-Engineering Attack



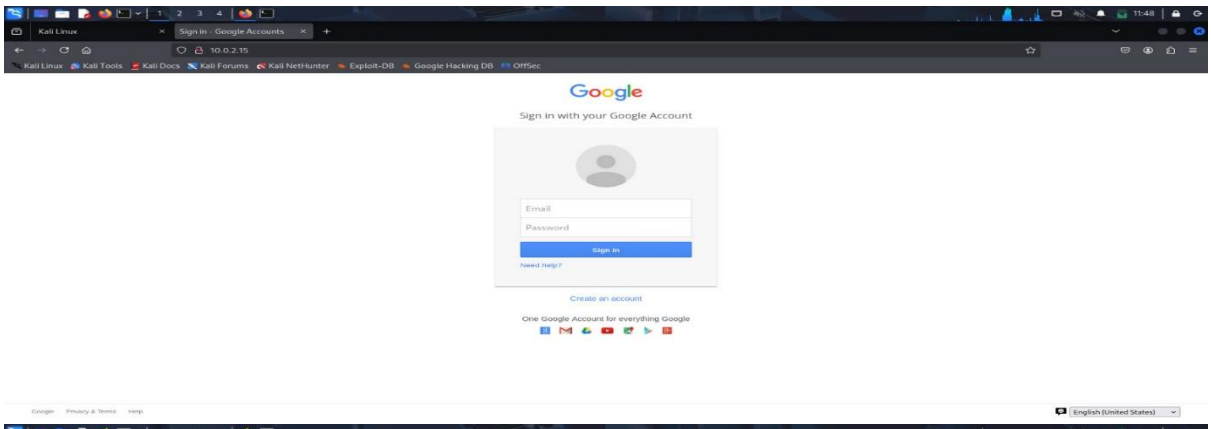
- **Select the Website Attack Vendors**

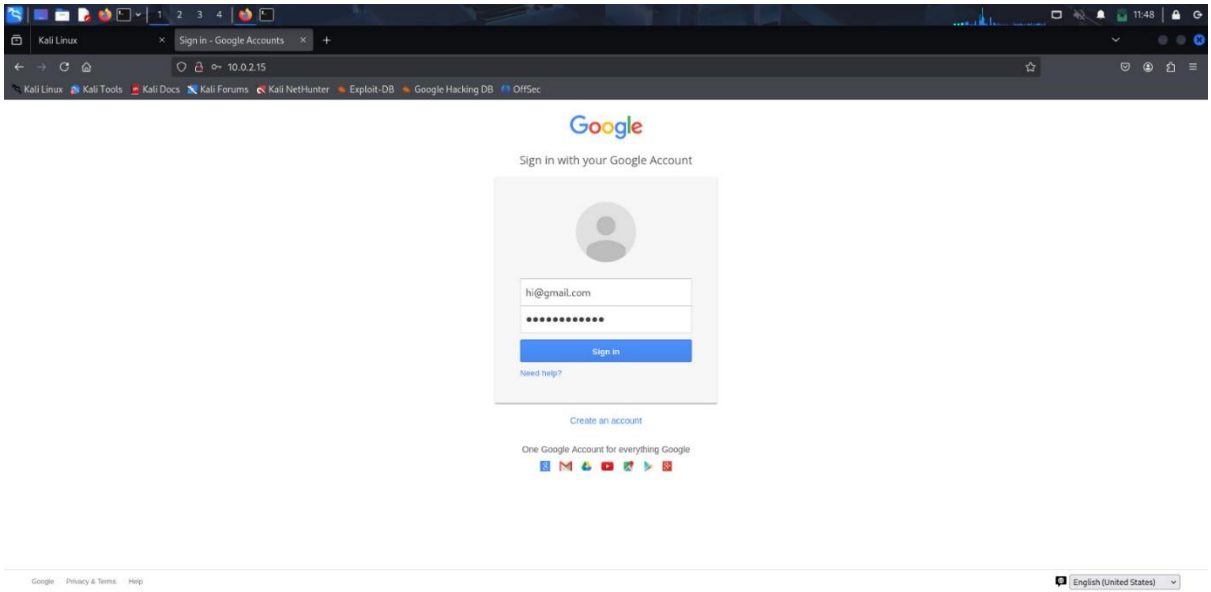


- Select the Credential Harvester Attack Method

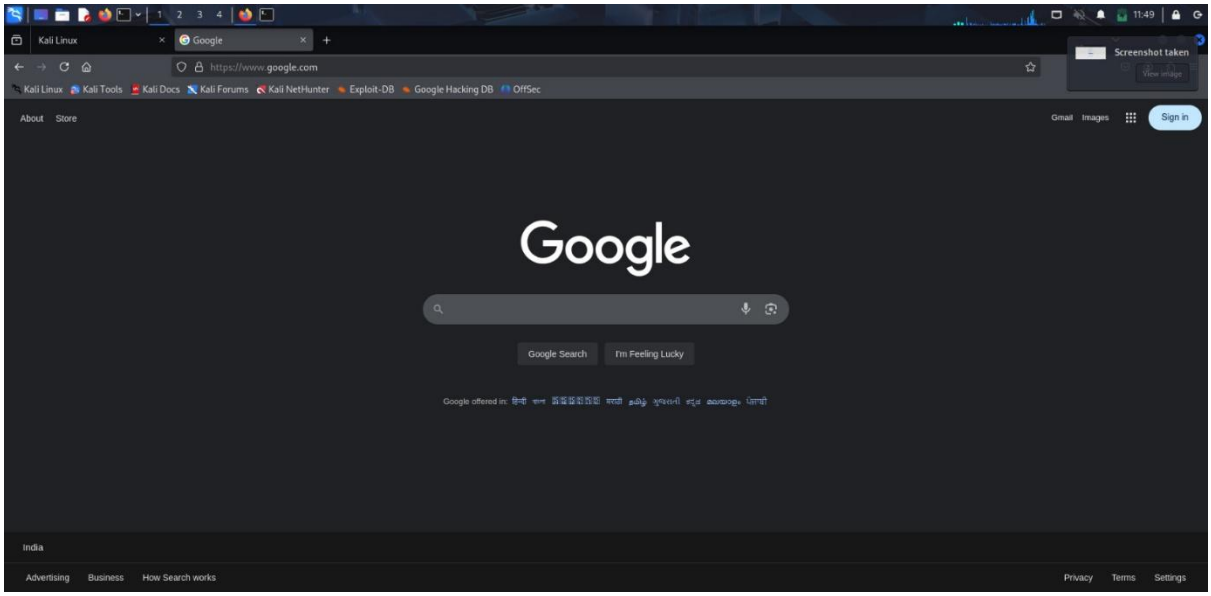
- Select the Web Templates

- Select the Google

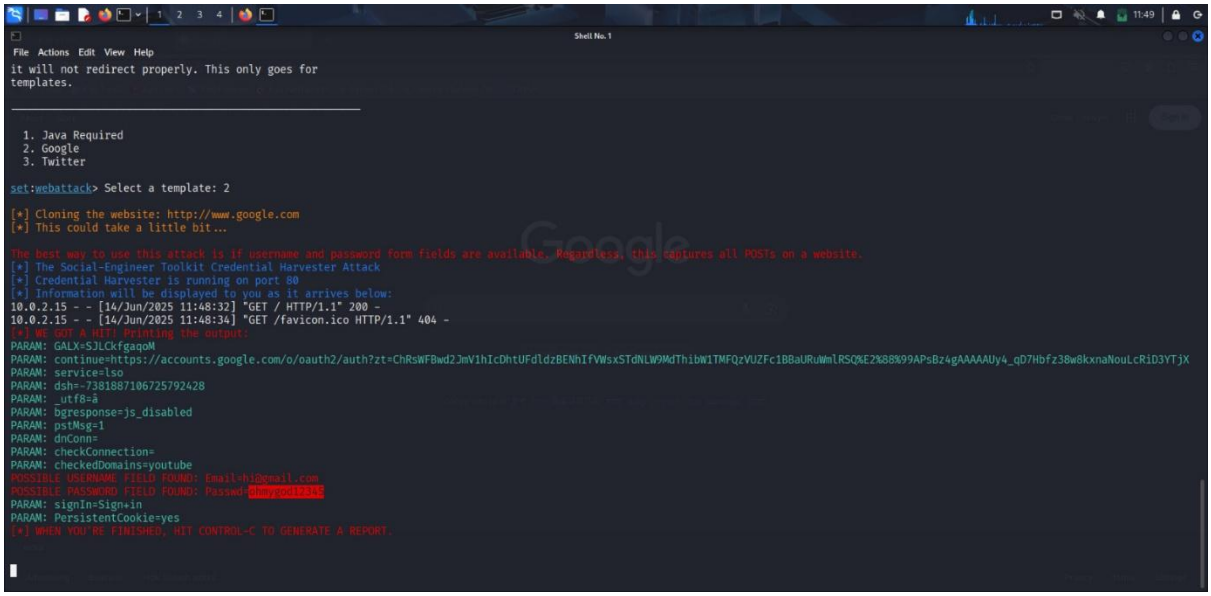




- After sign in they automatically redirect the normal google page



- In SEToolkit they capture username and password.



FINDINGS SUMMARY:

- The phishing setup was effective in capturing login credentials without alerting the user.
- Visual design and redirection increased believability.
- Credential harvesting was successful through cloned page.

- This test shows how easy it is to exploit trust in major brands for malicious purposes.

RECOMMENDATIONS:

- Users should always verify the URL before logging in.
- Avoid clicking unknown or suspicious links, even if the page looks legitimate.
- Enable multi-factor authentication (MFA) to reduce risk of credential misuse.
- IT teams should use email and browser filters to detect phishing pages.
- Organizations must conduct regular phishing awareness training.

LEARNING OUTCOME:

- This task gave me hands-on experience with phishing simulation using SEToolkit. I learned how phishing pages are created, how credentials are harvested, and how redirection adds to the realism of an attack. This exercise improved my understanding of social engineering tactics and highlighted the need for both technical controls and end-user education in defending against phishing threats.
