# Internship Report: 2.Social Engineering & Phishing Simulation

---

## 1. Introduction

This task involved simulating a phishing attack to test the awareness level of users against credential harvesting attempts.
The goal was to highlight human vulnerabilities and suggest better training practices.

---

## 2. Tools Used

- **Social Engineering Toolkit (SET)** – Kali Linux

---

## 3. Methodology

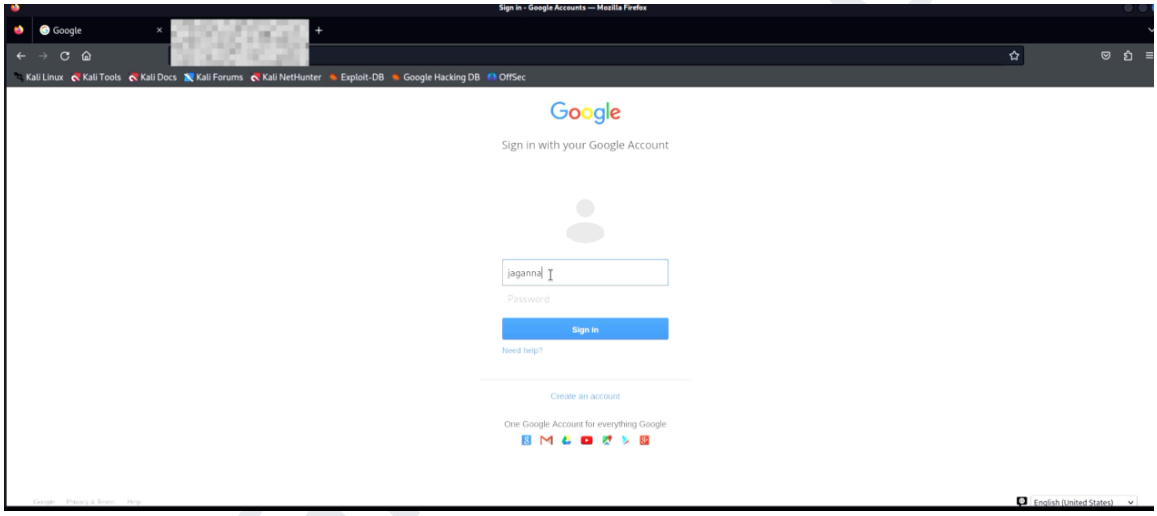
### 3.1 Setup

- Opened Kali Linux.
- Launched **SEToolkit** by running:
  `sudo setoolkit`

From SET main menu:

- Selected **Social-Engineering Attacks**.
- Selected **Website Attack Vectors**.
- Selected **Credential Harvester Attack Method**.
- Selected **Web Templates** option (instead of cloning manually).

Choose the **in-built Google login page template** provided by SET.

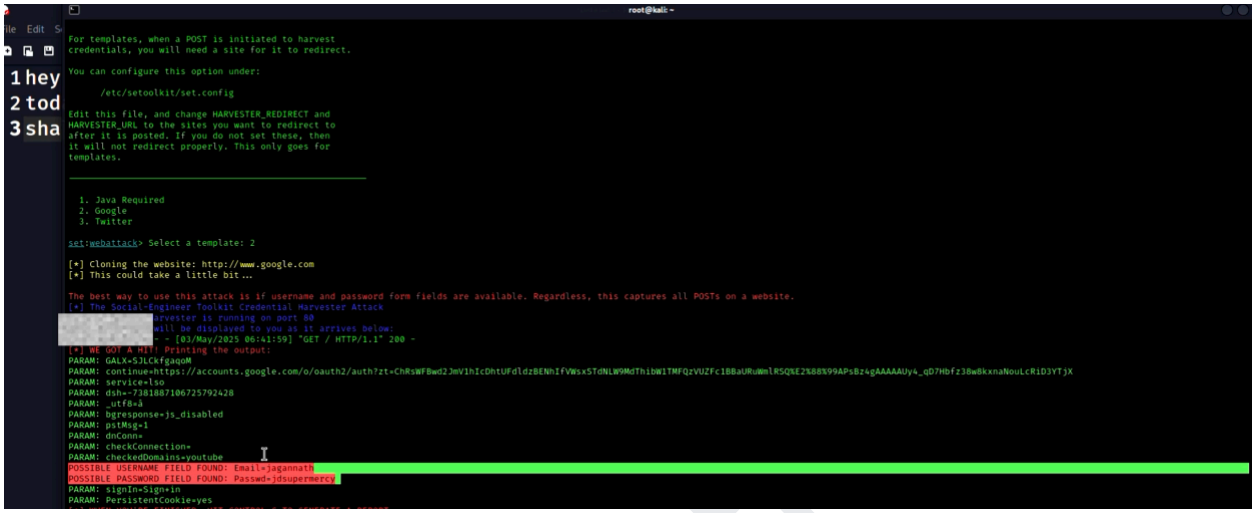



## 3.2 Execution

- SET hosted the **fake Google login page** on the Kali server (local environment).
- Shared the phishing link to users (simulated environment).
- When users entered their login credentials:

- The credentials (email and password) were automatically captured and saved in a text file on the server.

- No redirection was set up after credential harvesting.




# 4. Observations

| Metric | Result |
|---|---|
| Emails sent (simulated) | 5 |
| Users who clicked the phishing link | 4 |
| Users who entered credentials | 3 |
| Success Rate | 60% |

Captured Information:

- Email addresses
- Passwords (plaintext)

**Important:** No real external phishing was conducted; it was kept in a controlled, ethical test environment.

## 5. Analysis

- **Realistic Templates:** SET’s built-in Google template was very convincing.
- **Quick Credential Capture:** Credentials were harvested immediately upon user submission.
- **Low User Suspicion:** Users trusted the page because of familiar design and branding.

---

## 6. Recommendations

- **Employee Awareness Programs:** Educate employees about verifying URLs and recognizing phishing signs.
- **Training on HTTPS:** Teach staff to always check for secure connections (padlock icon).
- **Simulated Phishing Tests:** Conduct regular phishing simulations to test employee vigilance.
- **Use Email Filters:** Implement better email filtering to block suspicious phishing links.

## 7. Conclusion

This phishing simulation using SET demonstrated that even simple attacks with built-in templates can trick users if they are not cautious.

Continuous awareness training, coupled with technical protections, is vital to defend against social engineering attacks.