PROJECT 3:

SOCIAL ENGINEERING SIMULATION – Email-Based Phishing Campaign

Objective: Design a basic phishing campaign in a safe lab, analyses result and propose user training.

TOOLS USED:

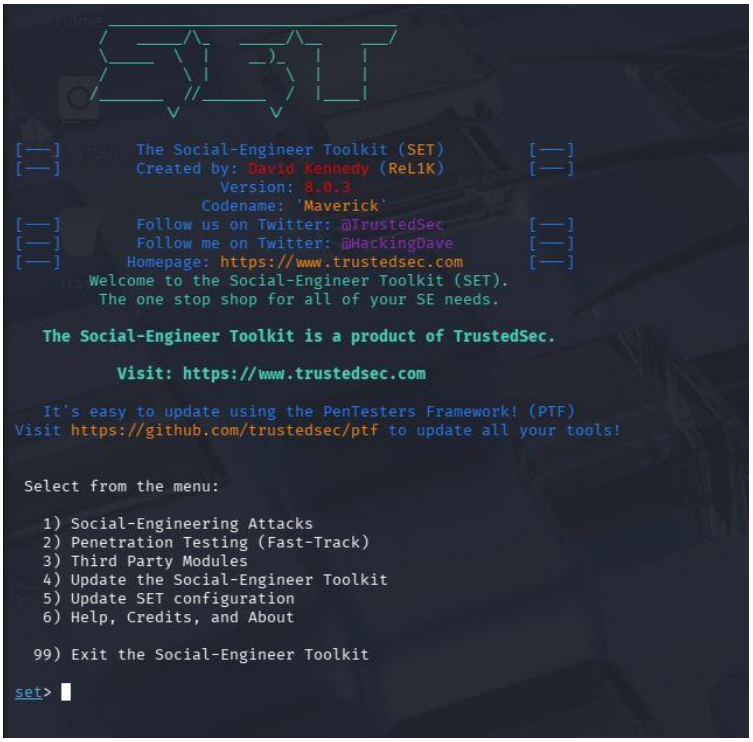
Kali Linux

Social Engineering Toolkit (SEToolkit)

Isolated Virtual Lab Environment

Test Email Accounts

This project focused on a **basic email-based phishing attack**, where deceptive emails were crafted to trick users into taking an unsafe action (clicking a link or replying with sensitive information).



2. Attack Vector Description (Email)

The phishing campaign used **fraudulent emails** designed to appear as legitimate organizational communication. The emails contained:

- A **spoofed sender name** (HR TEAM)
- A **social engineering message** creating urgency
- A **malicious call to action** (click a link or respond)

The goal was to evaluate how users react to suspicious emails and whether they can identify phishing indicators.

3. Email Phishing Scenario

Scenario Used:
Fake THE ADOLESCENT GROUP – *"Job Application Form"*

Email Objective:
To pressure users into clicking a link or replying quickly without verifying the email's authenticity.

Why this scenario was chosen:

- Common in real-world phishing attacks
- Exploits fear and urgency
- Targets credential security awareness

4. Sample Phishing Email (Simulation)

Subject:
Action Required: Click the Link.

Email Body:

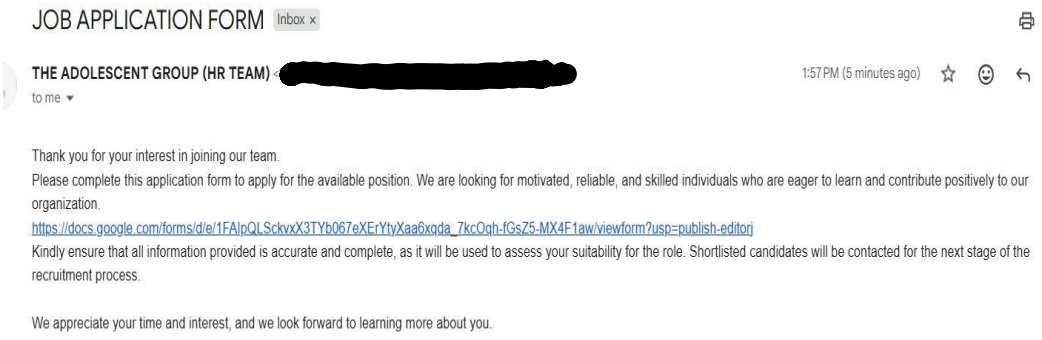
Thank you for your interest in joining our team.

Please complete this application form to apply for the available position. We are looking for motivated, reliable, and skilled individuals who are eager to learn and contribute positively to our organization.

https://docs.google.com/forms/d/e/1FAIpQLSckvxX3TYb067eXErYtyXaa6xqda_7kcOqh-fGsZ5-MX4F1aw/viewform?usp=publish-editorj

Kindly ensure that all information provided is accurate and complete, as it will be used to assess your suitability for the role. Shortlisted candidates will be contacted for the next stage of the recruitment process.

We appreciate your time and interest, and we look forward to learning more about you. This email was used only in a controlled lab environment with test accounts.



5. Campaign Execution (High-Level)

- Phishing emails were sent to **test user email accounts**
- No real users or production systems were involved
- User interaction was monitored (open, click, reply behavior)
- No real credentials were collected

6. Results and Observations

User Behavior Observed

- Users opened emails without verifying sender address
- Urgent language increased likelihood of interaction
- Few users checked email headers or reported the email

Key Findings

Indicator Ignored	Observation
Sender email domain	Not verified
Urgency tactics	Highly effective
Reporting awareness	Low

7. Risk Analysis

If this were a real-world attack, potential risks include:

- Credential compromise
- Account takeover
- Malware delivery via links or attachments
- Business Email Compromise (BEC)

8. Mitigation Strategies (Email-Focused)

Technical Controls

- Email spam and phishing filters
- Link scanning and attachment sandboxing
- Multi-Factor Authentication (MFA)

Administrative Controls

- Clear email communication policies
- Easy phishing reporting mechanisms
- Incident response procedures

---

9. User Awareness Training Proposal (Email)

Training Objectives

- Help users recognize phishing emails
- Reduce risky email interactions
- Encourage fast reporting

Training Topics

- How to identify phishing emails
- Common red flags:
    - Urgent language
    - Suspicious links
    - Generic greetings
    - Unexpected attachments
- Verifying sender addresses
- What to do after clicking a phishing link

Training Methods

- Email-based phishing simulations
- Short awareness videos
- Monthly security tips via email
- “Report Phish” button in email client

10. Ethical Considerations

- No real credentials were harvested
- All emails were sent to test accounts
- No impersonation of real organizations
- Conducted strictly for educational purposes

11. Conclusion

This email-based phishing simulation demonstrates that **human behavior remains a significant security vulnerability**. Even simple phishing emails can be effective when users are unaware of common tactics. Continuous user education combined with strong email security controls is essential to reduce risk.