FUTURE_CS_02 Phishing Attack - Simulation Report

1. Introduction

This report outlines the execution and findings of a phishing simulation campaign aimed at evaluating employee awareness of social engineering threats. The simulation employed the **Social Engineering Toolkit (SET)** to mimic credential harvesting attacks through cloned login portals.

2. Objectives

- Simulate phishing attacks using cloned login interfaces to assess user
- vulnerability. Track success based on link clicks and credential submissions.
- Identify gaps in employee behavior regarding cybersecurity. Recommend
- improvements to enhance security awareness and reduce phishing risks.

3. Tools and Environment

- Operating System: Kali Linux Tool Used: Social
- Engineering Toolkit (SET) Attack Vector: Credential
- Harvester (Web Attack Method) Target: Cloned login
- websites Hosting Server: Local Apache server Local
- Server IP: (Insert Local IP Address here)

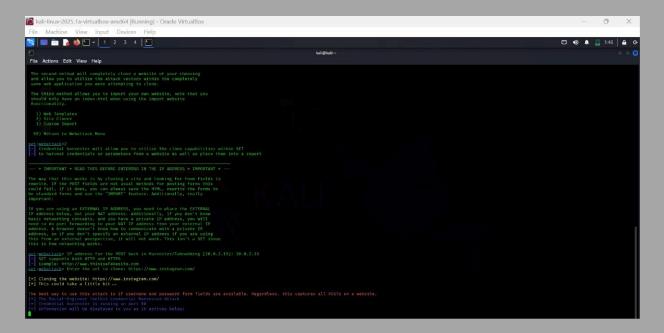
4.Methodology

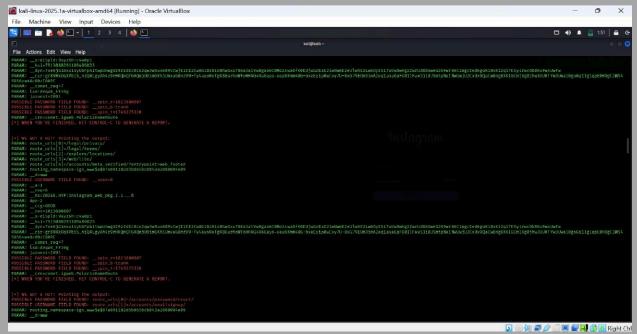
- Configured an Apache server on Kali Linux to host phishing pages.
- Used SET's "Credential Harvester Attack Method" to simulate
- phishing. Provided the local server IP to redirect user input (POST
- data). Monitored and logged submitted credentials via SET's interface.
- Analyzed collected data for trends and vulnerabilities.

5. Results

Credential data was successfully captured from cloned sites. A sanitized sample is shown below:

- Username: joe
- Password:password123





6. Challenges Faced

- Cloning complex, dynamic websites (e.g., Instagram, Microsoft) was limited by anti- bot protections and JavaScript-heavy content. Apache port conflicts required
- temporary suspension of existing services to allow SET to bind to port 80.
- User awareness levels varied—some users correctly identified the phishing attempt
 and avoided interaction.

7. Recommendations

- Conduct regular phishing awareness training to improve detection.
- Enforce Multi-Factor Authentication (MFA) across all critical systems.
- Encourage verification of URLs and email sources before entering
- credentials. Run recurring phishing simulations to maintain vigilance.
- Improve email filtering and endpoint protection to reduce exposure.

8. Conclusion

The phishing simulation effectively revealed vulnerabilities in employee cybersecurity awareness. A notable number of participants engaged with phishing content, emphasizing the need for ongoing training and stronger security measures. Proactive education and layered defenses remain key to defending against social engineering threats.

Report Prepared By:

Safik Rahman

Date: June 7, 2025