TASK -2

Social Engineering & Phishing Simulation Report

1. Introduction The purpose of this report is to analyze the results of a phishing simulation campaign designed to test employee awareness and improve security training programs. This simulation aimed to assess the effectiveness of current security protocols and identify areas for improvement.

2. Objectives

- Evaluate employee susceptibility to phishing attacks.
- Identify weaknesses in email security practices.
- Enhance security awareness training.
- Provide actionable recommendations for improved security measures.

3. Tools Used

- **Gophish**: Open-source phishing framework used to create and track phishing campaigns.
- **Social Engineering Toolkit (SET)**: Used for crafting phishing emails and simulating real-world attacks.

4. Methodology

- **Campaign Design**: A phishing email was crafted to mimic a legitimate organizational communication.
- **Target Audience**: Employees across various departments were included in the test.
- **Phishing Tactics**: Emails contained links leading to a mock login page designed to collect credentials.
- **Metrics Measured**:
    - Email open rate
    - Click-through rate
    - Credential submission rate
    - Reported phishing attempts

5. Results & Analysis

- **Email Open Rate**: 60%
- **Click-Through Rate**: 12%
- **Credential Submission Rate**: 8%
- **Reports to IT/Security Team**: 20%

Observations:

- A significant number of employees opened the phishing email.
- A moderate percentage clicked on the malicious link.
- Few employees reported the phishing attempt, indicating a need for enhanced awareness.

6. Recommendations

- Conduct regular phishing awareness training sessions.
- Implement multi-factor authentication (MFA) to reduce risk.
- Encourage employees to verify email authenticity before clicking on links.
- Improve security email filters to detect and block phishing attempts.
- Establish a streamlined reporting mechanism for suspicious emails.

7. Conclusion This phishing simulation provided valuable insights into employee security awareness and vulnerabilities. The data collected will be used to enhance training programs and implement stronger security measures, reducing the risk of future phishing attacks.