Phishing Attack Simulation & Detection Report

Cyber Security Internship – Task 11

Objective

To simulate a phishing attack in a controlled lab environment to understand how phishing campaigns are created, executed, tracked, and detected.

Tools Used

- GoPhish (Phishing simulation framework)
- Gmail SMTP
- Windows Operating System

Introduction to Phishing

Phishing is a social engineering attack where attackers send fraudulent emails pretending to be trusted entities to steal sensitive information such as login credentials, banking details, and personal data.

Types of Phishing

- Email Phishing
- Spear Phishing
- Whaling
- Smishing (SMS phishing)
- Vishing (Voice phishing)

Practical Implementation

- Installed GoPhish and accessed admin panel at https://127.0.0.1:3333.
- Created phishing email template with dynamic URL.
- Designed fake login landing page and enabled data capture.

- Configured Gmail SMTP using App Password.
- Created target group and launched campaign.
- Monitored campaign statistics and captured credentials.

Red Flags Identified

- Urgent language in subject line.
- Suspicious verification link.
- Generic greeting.
- Request for sensitive information.

Prevention Methods

- Enable Two-Factor Authentication (2FA).
- Verify sender email address.
- Hover over links before clicking.
- Use spam filters and email security tools.
- Conduct security awareness training.

Conclusion

This simulation demonstrated how phishing attacks exploit human psychology and highlighted the importance of awareness and preventive security measures.