Cyber Security Internship – Task 11 Phishing Attack Simulation & Detection (Detailed Report)

Objective

The objective of this task is to practically understand phishing attacks by simulating a real-world phishing scenario. This task focuses on how attackers trick users, how victims respond, and how organizations can detect and prevent such attacks.

Introduction to Phishing

Phishing is a social engineering attack where attackers impersonate trusted entities to steal sensitive data such as usernames, passwords, or financial information. It is one of the most common causes of data breaches globally.

Tool Used – GoPhish

GoPhish is an open-source phishing simulation framework used by security teams to conduct awareness campaigns. It allows email template creation, landing page hosting, and user interaction tracking.

Phishing Simulation Process

A fake IT support email was created requesting users to reset their password. A landing page resembling a real login page was configured. The campaign was executed in a controlled environment for learning purposes only.

Observations & Red Flags

Several indicators such as suspicious sender email, urgent language, and mismatched URLs were identified. Users who clicked links demonstrated lack of phishing awareness.

Detection & Prevention

Organizations can prevent phishing by user awareness training, email filtering, URL scanning, and implementing Multi-Factor Authentication (MFA).

Conclusion

This task highlights that phishing attacks rely more on human psychology than technical vulnerabilities. Continuous awareness is the strongest defense.

Phishing Email Template Screenshot

Screenshot Phishing Email Template (GoPhish)

Phishing Landing Page Screenshot