Cyber Security Internship – Task 11

Phishing Attack Simulation & Detection

Objective

The objective of this task is to understand phishing attacks, simulate a phishing scenario in a safe and controlled environment, identify phishing indicators, and learn methods to detect and prevent phishing attacks.

What is Phishing?

Phishing is a type of social engineering attack where attackers impersonate trusted entities to trick users into revealing sensitive information such as usernames, passwords, banking details, or personal data. These attacks are commonly delivered through emails, messages, or fake websites.

Types of Phishing

- Email phishing
- Spear phishing
- Whaling
- Smishing (SMS phishing)
- Vishing (voice phishing)

Tools Used

- Manual phishing templates (safe simulation)
- Text editor
- Web browser

(GoPhish was studied conceptually as suggested, but manual simulation was used as a free alternative.)

Phishing Simulation Performed

The following steps were performed as part of the phishing simulation:

1. Created a **fake phishing email template** using urgent and generic language.
2. Designed a **fake login landing page** to demonstrate credential harvesting.
3. Analyzed the phishing email to identify **red flags**.
4. Studied **phishing detection and prevention techniques**.

⚠ No real phishing emails were sent and no real users were targeted.

Phishing Email Analysis

The phishing email contained:

- Urgent message requesting immediate action
- Generic greeting instead of personalized name
- Suspicious or fake link
- Request for account verification

These are common characteristics of phishing emails.

Landing Page Simulation

A fake login page was created to demonstrate how attackers attempt to collect login credentials by mimicking legitimate websites. This highlights how users can be deceived if they do not verify website authenticity.

Red Flags Identified

- Urgent or threatening language
- Generic greetings (e.g., “Dear User”)
- Suspicious or shortened URLs
- Requests for sensitive information
- Lack of official contact details

How to Detect Phishing

- Check sender email address carefully

- Hover over links before clicking
- Look for spelling and grammar mistakes
- Avoid opening unknown attachments
- Verify website URLs and HTTPS usage

Prevention Methods

- Never share passwords via email or messages
- Enable two-factor authentication (2FA)
- Use spam filters and email security tools
- Regular user awareness training
- Report suspicious emails immediately