Task 11: Phishing Attack Simulation & Detection (Solved)

🎯 Objective

Simulate a **controlled phishing attack** using **GoPhish** to understand:

- How phishing works
- How users fall for it
- How to **detect, analyze, and prevent** phishing attacks

This task focuses on **defensive security & awareness**, which is exactly what companies want.

🛠 Tools Used

- **Primary:** GoPhish (Open-source phishing simulation framework)
- **Alternative:** Manual phishing templates (for learning only)

⚠️ Important Rule

✓ Only test on:

- Your own email
- Dummy/test email accounts
- Lab environment
  ❌ Never target real users without permission

🧠 1️⃣ Understanding Phishing Attacks

What is Phishing?

Phishing is a **social engineering attack** where attackers impersonate trusted entities to trick users into:

- Clicking malicious links
- Entering credentials
- Downloading malware

📌 Phishing targets **humans**, not systems.

🧪 LAB SETUP (Safe & Ethical)

Environment

- Kali Linux / Ubuntu / Windows
- GoPhish running locally
- Test email accounts (example: test1@mail.com)

Components

- Fake email (educational)
- Fake landing page (no real credential storage)
- Tracking enabled

🐟 PART A: GoPhish Simulation (High-Level & Safe)

2️⃣ Install & Start GoPhish

```
wget https://github.com/gophish/gophish/releases

tar -xvf gophish-*.tar.gz

cd gophish

sudo ./gophish
```

Access dashboard:

https://127.0.0.1:3333

3️⃣ Create a Fake Email Template (Educational)

⚠️ DO NOT use real company names or brands

Example (Redacted & Safe)

Subject: Action Required – Account Verification

Hello User,

We noticed unusual login activity on your account.

Please verify your account to avoid temporary suspension.

[Verify Account]

Thank you,

Security Team

🔍 Phishing Red Flags (Intentional)

- Urgency
- Generic greeting
- Suspicious link
- Fear-based language

4️⃣ Setup Landing Page (Simulation Only)

Landing page purpose:

- Record **click**
- Show **education message**

Example Page Content:

This was a phishing simulation.

Never enter credentials on suspicious links.

📌 No real passwords stored (important for ethics).

5️⃣ Send Test Phishing Email

- Target: Your own test email

- SMTP: Local or test SMTP
- Campaign mode: Test

GoPhish tracks:

- Email opened
- Link clicked
- Page visited

6️⃣ Track & Analyze Responses

GoPhish Metrics:

Metric	Meaning
Email Sent	Reach
Email Opened	Curiosity
Link Clicked	Vulnerability
Reported	Awareness

📊 Example Result

- Sent: 1
- Opened: 1
- Clicked: 1

7️⃣ Identify Phishing Red Flags (Detection)

🚩 Common Indicators

- Misspelled sender domain
- Urgent language
- Suspicious links
- Attachments

- Generic greetings
- HTTPS ≠ Safe

8️⃣ Prevention & Defense Measures

🛡 Technical Controls

- Email filtering (SPF, DKIM, DMARC)
- Secure Email Gateways
- URL rewriting
- MFA

🧑 Human Controls

- Security awareness training
- Phishing simulations
- Reporting mechanisms

📄 PHISHING SIMULATION REPORT (Deliverable)

Simulation Overview

- Tool: GoPhish
- Type: Credential harvesting (simulated)
- Target: Test email account
- Date: DD/MM/YYYY

Attack Flow

1. Phishing email sent
2. User opened email
3. User clicked link
4. Redirected to awareness page

Findings

- User clicked suspicious link
- Indicates lack of phishing awareness

Risk Level

High – Human factor vulnerability

Recommendations

- Conduct regular phishing training
- Enable MFA
- Improve email filtering
- Promote “Report Phish” culture