STEP 1: Install GoPhish

▶ On Kali / Ubuntu Linux

sudo apt update

sudo apt install unzip -y

Download GoPhish:

wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip

Unzip:

unzip gophish-v0.12.1-linux-64bit.zip

cd gophish*

Give permission:

chmod +x gophish

Start GoPhish:

sudo ./gophish

✓ You should see:

Listening on https://0.0.0.0:3333

🔹 **STEP 2: Open GoPhish Admin Panel**

Open browser:

https://127.0.0.1:3333

Login using credentials shown in terminal:

Username: admin

Password: <auto-generated>

⚠️ Accept SSL warning (lab only)

🔹 **STEP 3: Create User Group (Target Users)**

Go to **Users & Groups → New Group**

Example:

- Group Name: Test_Users
- Add User:
    - First Name: Test

- Email: testuser@mailhog.local

Click **Save changes**

🔹 **STEP 4: Create Email Template (Phishing Email)**

Go to **Email Templates → New Template**

Fill:

- Name: Password Expiry Alert
- Subject:

Urgent: Your Password Will Expire Today

Email Body:

Dear User,

Your account password is about to expire.

Please verify immediately to avoid account suspension.

Verify Account

Security Team

✓ Click **Save Template**

🔹 **STEP 5: Create Landing Page (Fake Login Page)**

Go to **Landing Pages → New Page**

Fill:

- Name: Fake Login Page
- Check:
  ✓ Capture Submitted Data
  ✓ Redirect to URL after submit

Page HTML:

<h2>Login Required</h2>

<form method="POST">

Username: <input name="username">

Password: <input type="password" name="password">

<input type="submit" value="Login">

</form>

Redirect URL:

https://example.com/training

✓ Save page

🔹 **STEP 6: Create Sending Profile (Mail Server)**

Option A (Recommended for Lab): MailHog

sudo apt install mailhog

mailhog

In GoPhish → **Sending Profiles → New Profile**

- Name: Local SMTP
- SMTP Server: 127.0.0.1:1025
- From: security@testlab.com
- No username/password

✓ Save

🔹 **STEP 7: Create Campaign (Actual Attack Simulation)**

Go to **Campaigns → New Campaign**

Fill:

- Name: Awareness Test
- Email Template: Password Expiry Alert
- Landing Page: Fake Login Page
- Sending Profile: Local SMTP
- Groups: Test_Users
- URL:

http://127.0.0.1

Click **Launch Campaign**

🔹 **STEP 8: Check Phishing Email (Victim Side)**

Open MailHog:

http://127.0.0.1:8025

✓ Open received email
✓ Click phishing link
✓ Enter dummy credentials

🔹 **STEP 9: View Results (Tracking)**

Back in GoPhish → **Campaigns**

You'll see:

- Email sent ✓
- Email opened ✓
- Link clicked ✓
- Credentials captured ✓

📊 This shows **user behavior tracking**

🔹 **STEP 10: Identify Red Flags (Write This)**

- Urgent message
- Unknown sender
- Suspicious link
- Generic greeting

🔹 **STEP 11: Prevention (Mandatory in Exam)**

- User awareness training
- Email filtering
- SPF / DKIM / DMARC
- Multi-factor authentication
- Regular phishing simulations

📝 **FINAL LAB RECORD FORMAT (Short)**

Aim:
To simulate a phishing attack using GoPhish for awareness training.

Tool:
GoPhish

Result:
Phishing email was sent and user interaction was successfully tracked.