

Task 11: Phishing Attack Simulation & Detection

Objective: To simulate a controlled phishing attack using GoPhish in order to understand social engineering techniques, analyze user behavior, and learn effective phishing detection and prevention strategies.

Tools Used:

- GoPhish (Primary phishing simulation framework)
- Test SMTP service (MailHog / Local SMTP)

Simulation Workflow:

1. Configured GoPhish admin panel.
2. Designed a realistic phishing email template (Password Expiry Alert).
3. Created a fake credential-harvesting landing page.
4. Launched a test phishing campaign on dummy users.
5. Tracked clicks and credential submissions via dashboard.

Observations:

- Users clicked links due to urgency-based messaging.
- Credential submission occurred when branding appeared legitimate.

Prevention Measures:

- User awareness training
- Email authentication (SPF, DKIM, DMARC)
- Multi-Factor Authentication (MFA)

Conclusion:

Phishing simulations are effective in improving social engineering awareness and reducing organizational risk.