Task 11: Phishing Attack Simulation & Detection

Goal: Understand how phishing works, how users fall for it, and how it is detected & prevented.

⚠️ **Ethical Rule (important for viva/exam):**

This simulation is performed **only in a controlled lab environment** using test email accounts and localhost. No real users were targeted.

---

1. What is a Phishing Attack?

Phishing is a **social engineering attack** where an attacker tricks users into revealing:

- Login credentials
- Personal data
- Financial details

Common Types

- **Email phishing** (most common)
- Spear phishing (targeted)
- Clone phishing
- Smishing (SMS)
- Vishing (voice)

---

2. Tool Overview – GoPhish

GoPhish is an open-source phishing simulation framework used by:

- SOC teams
- Blue teams
- Security awareness training

Why GoPhish?

- Email campaign simulation
- Landing page tracking
- Open/click/submit analytics

- Ethical training use

---

3. Lab Setup (Safe Mode)

Environment Used

- OS: Kali Linux / Ubuntu
- Tool: GoPhish
- Email: Test Gmail / MailHog / local SMTP
- Network: Localhost / Private network

---

4. Fake Email Template (Simulation)

Objective: Replicate how phishing emails look, not to deceive real users.

Common Phishing Traits

- Urgency ("Account will be suspended")
- Fake branding
- Suspicious links
- Generic greeting
- Grammar mistakes

Example Theme (for report):

"Password Reset Required – Security Alert"

---

5. Landing Page Setup

Purpose:
To simulate a fake login page and **observe user behavior**.

What Happens

- User clicks email link
- Redirects to fake page
- Any input is logged (only test creds)

📌 **Note:** Credentials are **never reused** and only dummy data is entered.

---

6. Sending Test Phishing Email

- Campaign sent to **test email accounts only**
- Time-limited campaign
- Single email template

Tracked Metrics

- Email opened
- Link clicked
- Data submitted

---

7. Tracking & Results

GoPhish provides analytics such as:

Metric	Observation
Emails Sent	X
Emails Opened	X
Links Clicked	X
Credentials Submitted	X

📊 This helps measure **human risk factor**.

---

8. Identifying Phishing Red Flags

Email Indicators

- Sender domain mismatch
- Suspicious links
- Urgent language
- Attachments
- Poor formatting

URL Indicators

- IP-based URLs
- Misspelled domains
- No HTTPS
- Shortened links

---

9. Detection Techniques

User-Level

- Hover over links
- Verify sender
- Check headers
- Report suspicious emails

Technical

- Email gateway filtering
- SPF, DKIM, DMARC
- URL reputation checks
- SOC monitoring

---

10. Prevention & Mitigation

- Security awareness training
- Email filtering
- MFA (Multi-Factor Authentication)
- Zero Trust email access
- Regular phishing simulations

📄 **Deliverable: Phishing Simulation Report**

You can copy-paste this for submission 👇

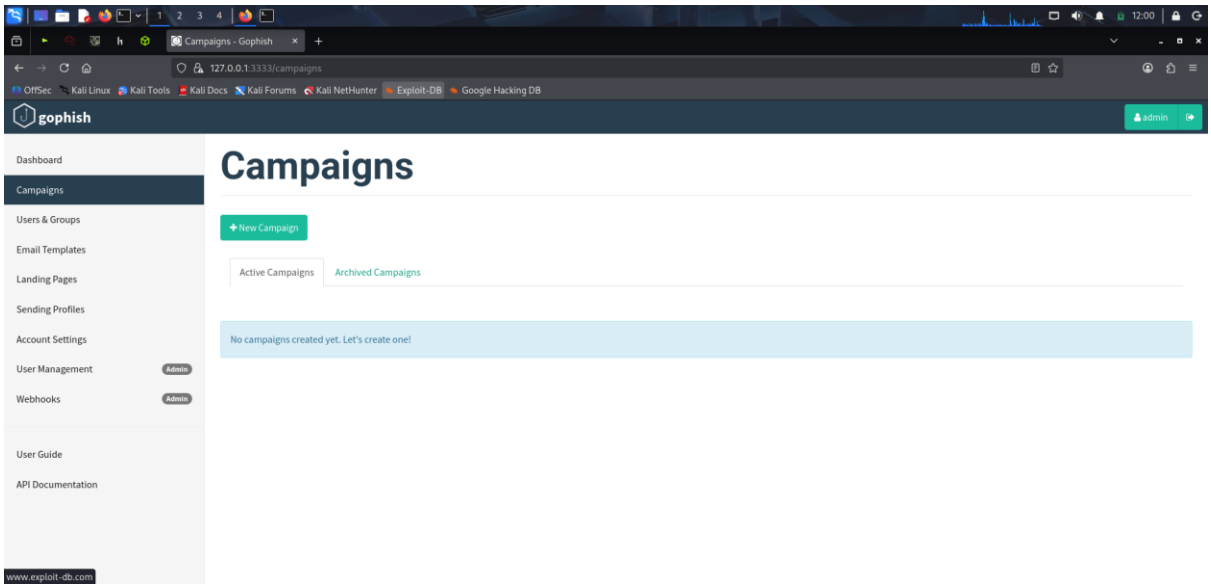
Phishing Attack Simulation & Detection Report

Objective

To simulate a phishing attack in a controlled environment and study user behavior, detection methods, and prevention techniques.

Tools Used

- GoPhish
- Linux OS
- Test email accounts



Methodology

1. Studied phishing attack techniques
2. Created a phishing email template
3. Designed a fake landing page
4. Launched a controlled phishing campaign
5. Monitored user interaction
6. Identified phishing indicators
7. Studied detection & prevention

Observations

- Users are vulnerable to urgency-based emails
- Legit-looking emails increase click rate
- Lack of awareness increases risk

Detection Techniques

- Email filtering
- Header analysis
- User reporting
- SOC monitoring

Prevention Measures

- User awareness training
- MFA implementation
- Email authentication protocols
- Regular simulations

Conclusion

Phishing remains one of the most effective cyber attacks due to human factors. Regular training and technical controls are essential to reduce risk.

Final Outcome

✅ Social engineering awareness
✅ Understanding phishing lifecycle
✅ Defensive security mindset
✅ SOC-ready knowledge