Task 11: Phishing Simulation Report

Name: Mohammed Fadil PK **Date:** February 2, 2026

1. Introduction

Social engineering, particularly phishing, is a leading cause of security breaches. This task involved setting up a controlled phishing simulation using **GoPhish** on Kali Linux to understand the mechanics of these attacks and how to detect them.

2. Attack Configuration (The Setup)

I configured the three core components of the phishing attack:

- **A. The Hook (Sender Identity):** I created a trusted "IT Support" persona to make the email look legitimate.

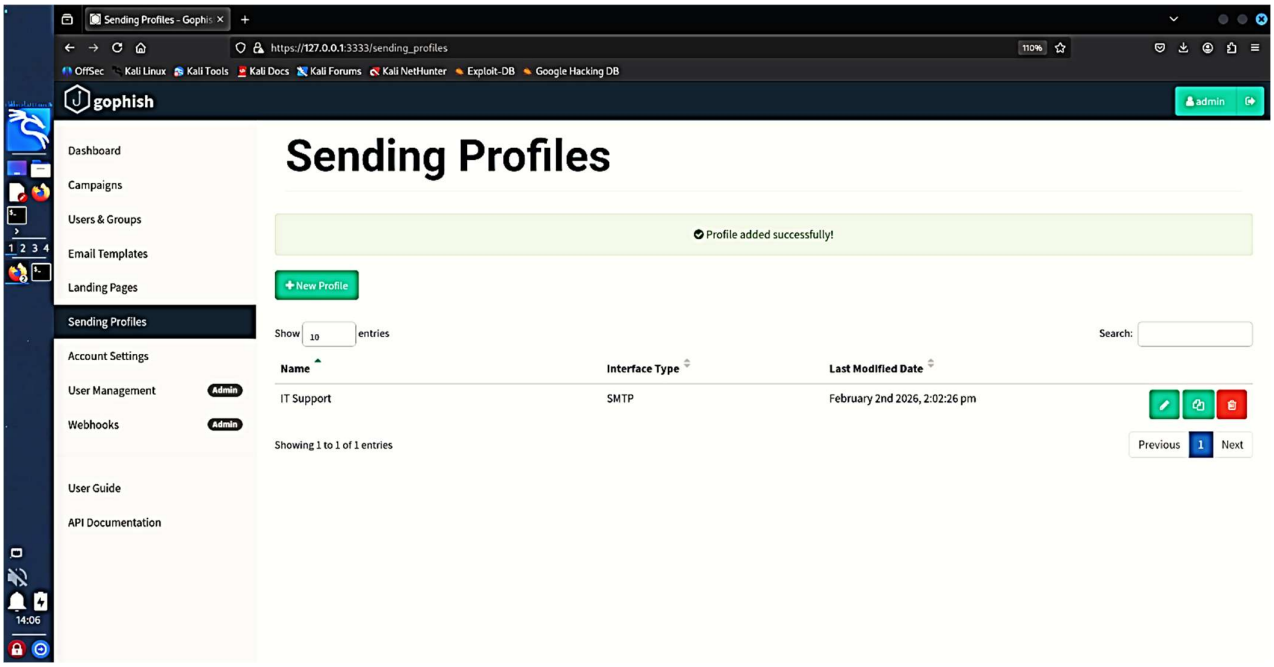

Fig 1: Sending Profiles

- **B. The Trap (Landing Page):** I set up a fake login page that mimics a standard Google sign-in screen to capture credentials.

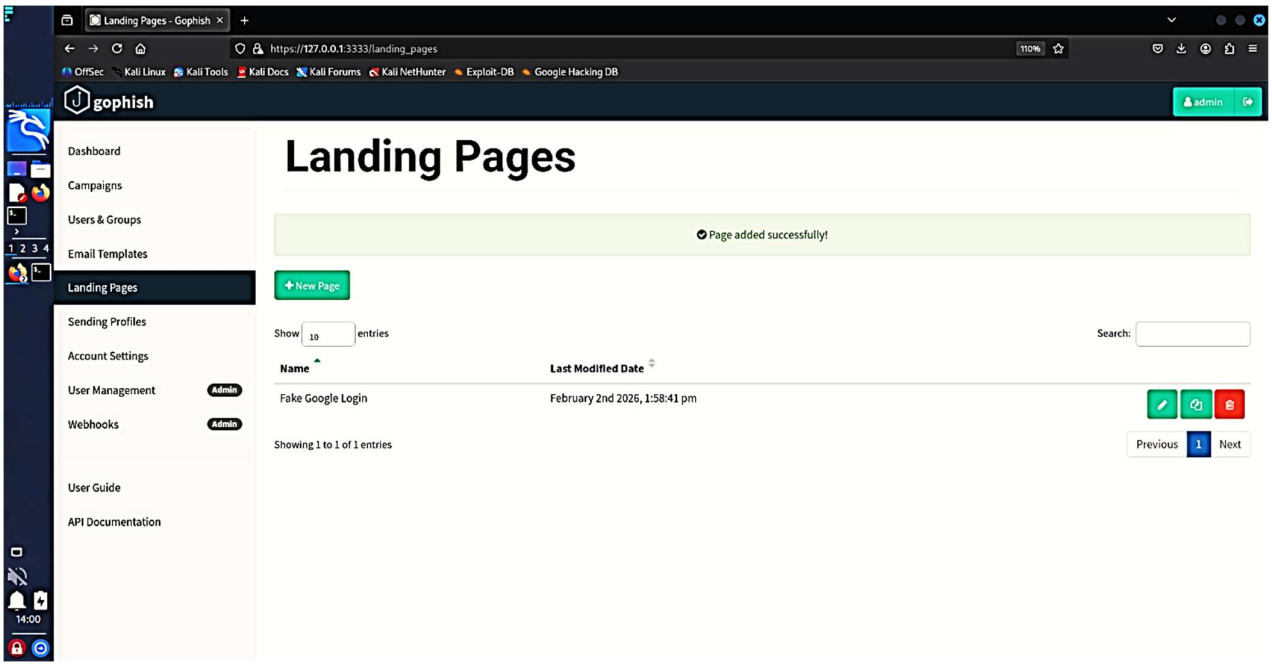

Fig 2: Landing Pages

- **C. The Bait (Email Template):** I drafted an "Urgent Security Alert" email containing the malicious link {{.URL}} to trigger a sense of urgency.

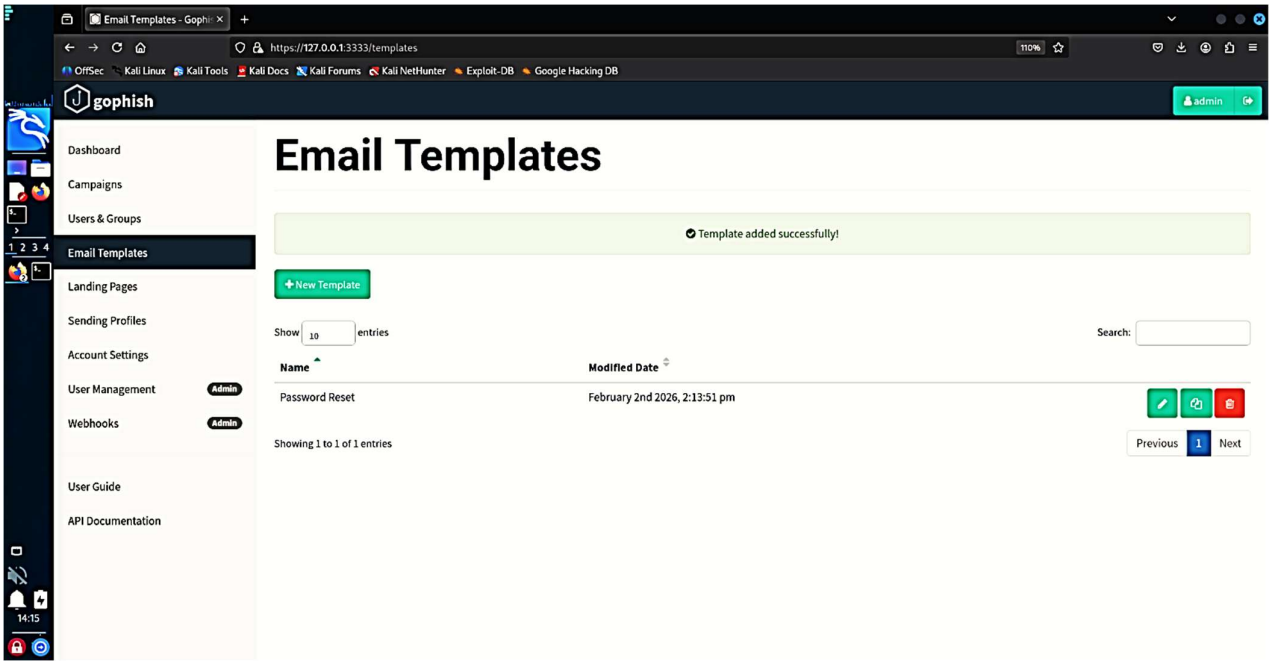

Fig 3: Email Templates

3. Execution & Results

The campaign "Simulation 1" was launched successfully. The dashboard below confirms the campaign status is "In Progress", and tracking is active.

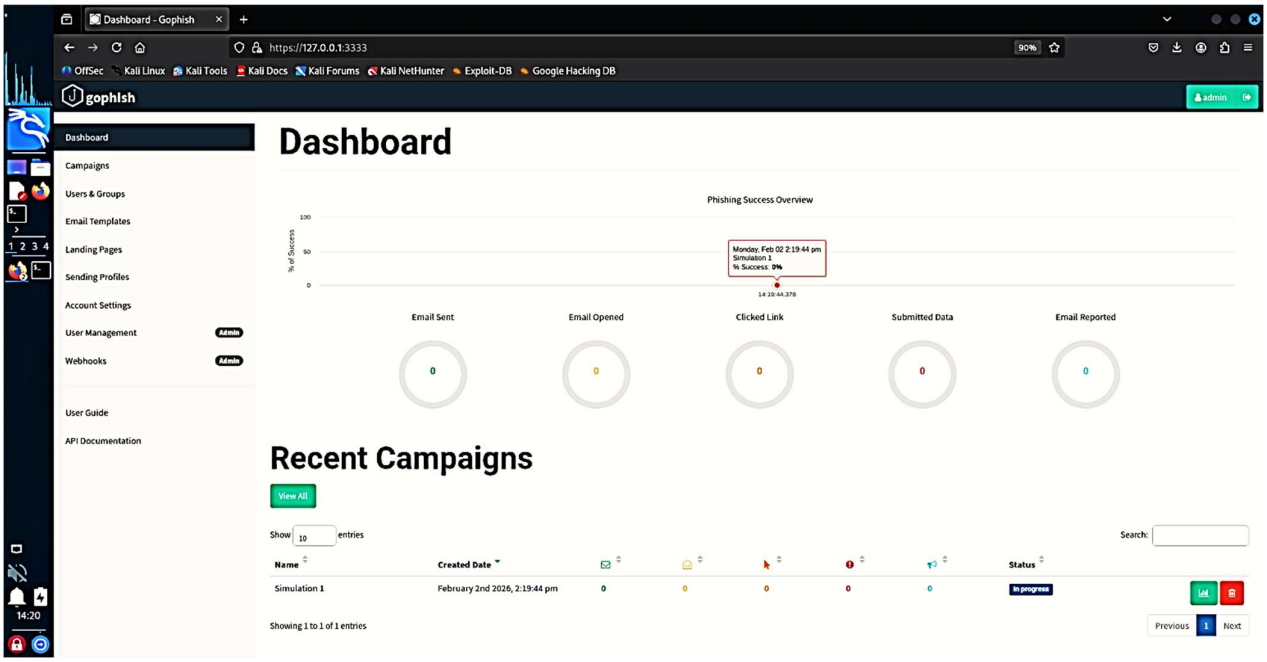

Fig 4: Dashboard

4. Interview Questions

- **What is phishing?** A cybercrime where attackers pose as legitimate institutions (via email, SMS, or phone) to trick individuals into revealing sensitive data like passwords or banking details.
- **Types of Phishing?**
    - **Spear Phishing:** Targeted at a specific person.
    - **Whaling:** Targeted at high-profile executives (CEOs).
    - **Vishing:** Phishing via voice calls.
    - **Smishing:** Phishing via SMS text messages.
- **How to detect phishing?** Check for mismatched URLs (e.g., g00gle.com), urgent/threatening language, generic greetings ("Dear Customer"), and spelling errors.
- **Why is it dangerous?** It bypasses technical defences (firewalls/antivirus) by exploiting human psychology. A single click can compromise an entire organisation.

5. Conclusion

This simulation demonstrated how easily attackers can replicate trusted brands. The most effective defence is user awareness training and multi-factor authentication (MFA).