Gophish Simulated Phishing Campaign Report

Prepared by: AKHIL NS

Date: October 18, 2025

Executive Summary

This document serves as a detailed record of a simulated phishing exercise, executed using the open-source Gophish platform within a protected Kali Linux virtual environment. Screenshots illustrate every step for comprehensive understanding.

---

1 Gophish Setup

Using the web interface on Kali Linux, we connected to the Gophish dashboard. This control panel provided real-time campaign statistics, detailing the lifecycle of the phishing emails from being sent to being opened, clicked, submitted (data), and reported.

Figure 1: Gophish Dashboard Overview

2 Creating Users and Groups

A test group was created in the "Users & Groups" section. This group contained test accounts which acted as phishing targets for the campaign.

3 Email Creation

A phishing email template was designed in the "Email Templates" section. The email was made to look urgent and professional, tricking users into clicking a malicious link.

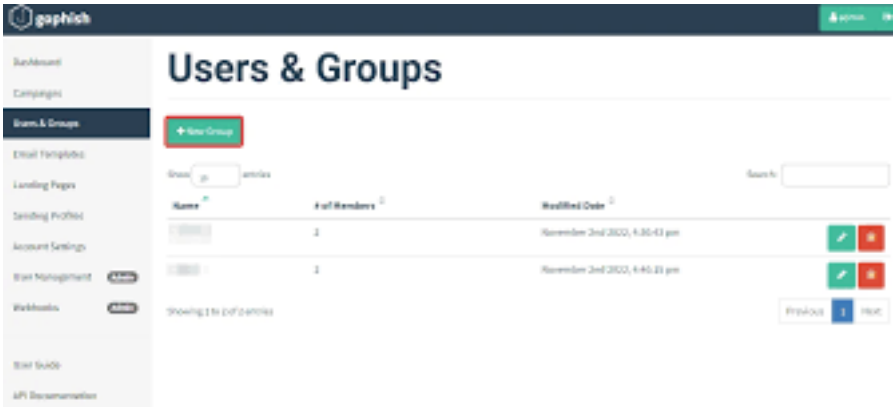

Figure 2: Test User Group Creation

4 Setting Profile

A sending profile was set up with SMTP details so that the phishing emails appeared to come from a legitimate account. This helped make the attack more convincing.

5 Campaign Creation

A phishing campaign was launched using the configured group, template, sending profile, and landing page. The campaign ran successfully and allowed live tracking of user interactions.

5.1 Receiving the Phishing Email

The targeted inbox received the phishing email. The message contained the fake warning and link to the landing page.

5.2 Target Mailbox Snapshot

The phishing email appeared in the inbox alongside other real emails, making it look genuine.

6 Gophish Dashboard Results

The Gophish dashboard displayed campaign results, showing whether emails were opened, links clicked, credentials submitted, or emails reported.

7 Conclusion

This simulation successfully demonstrated how a phishing attack is structured and tracked using Gophish. By creating groups, templates, sending profiles, and landing pages, the campaign showed the end-to-end flow of phishing attempts. Conducting such exercises in a controlled environment helps understand attacker methods and highlights the importance of **user awareness** in cybersecurity.

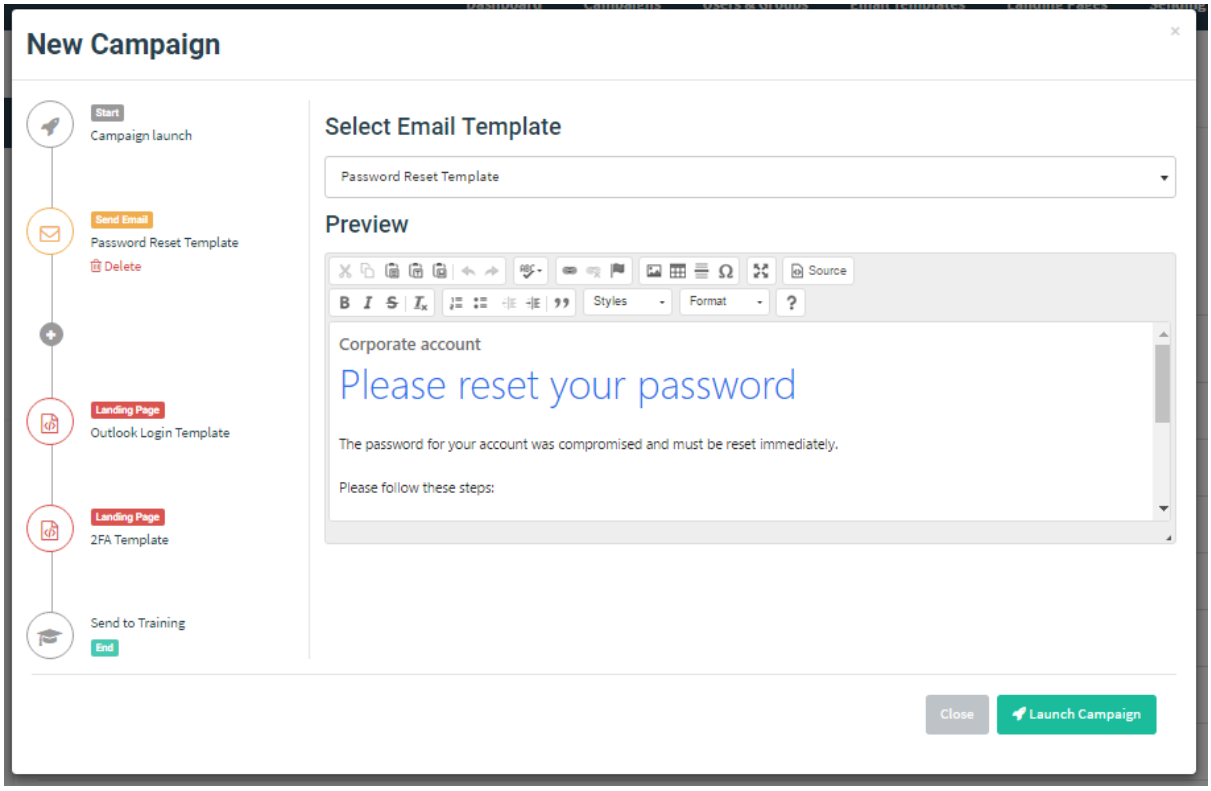

Figure 3: Phishing Email Template Design

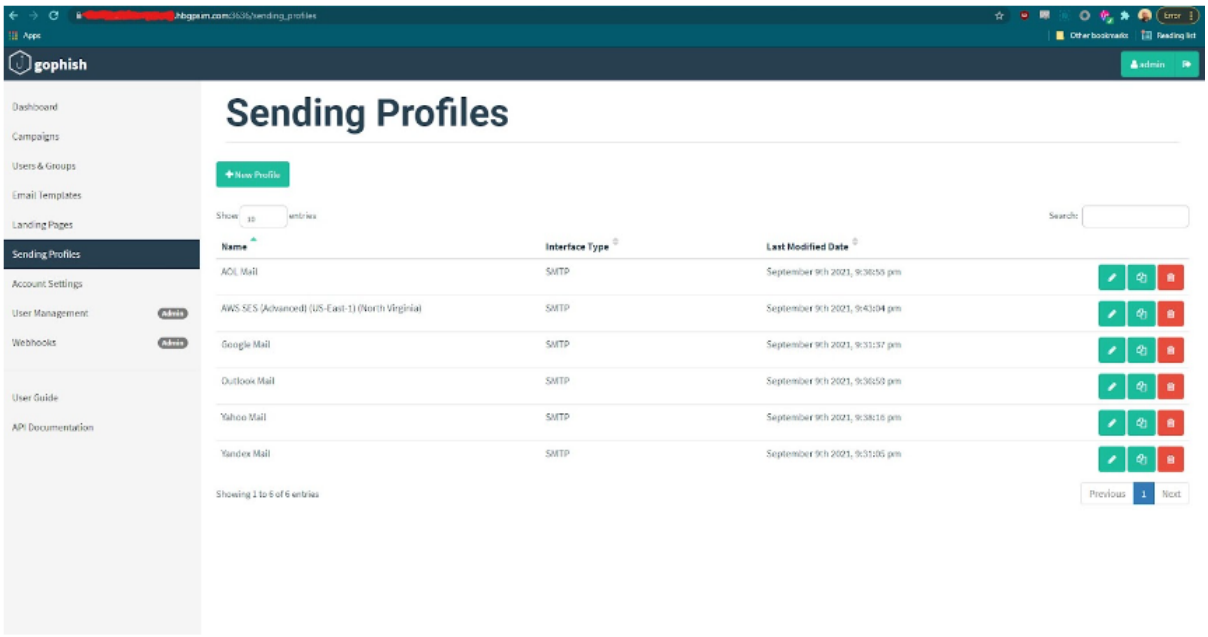

Figure 4: SMTP Sending Profile Configuration

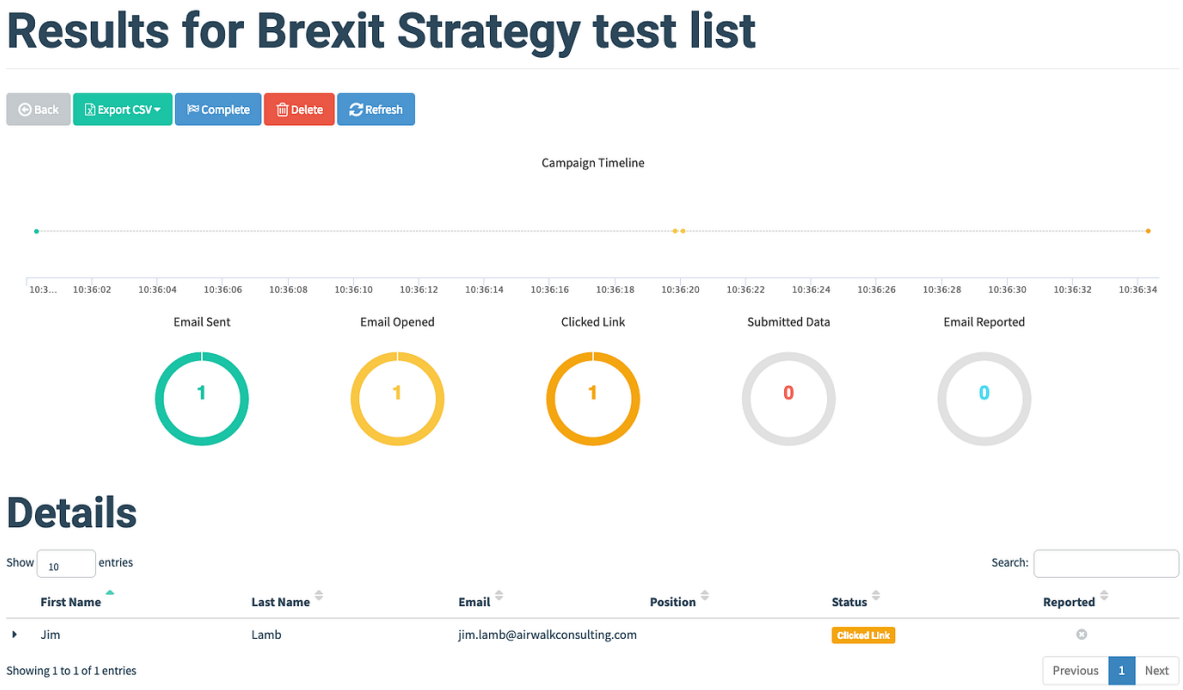

Figure 5: Live Campaign Results Dashboard