SCRATCH AND SCRIPT
IGNITE Cybersecurity Program
Cohort 2

Kibet Cleophas

Group 6

Week 2 Assignment

Question 3 will be a class **mini-project** you will do as a group. For the group work, **create a phishing campaign and write a report.** I will direct the group leaders to create a GitHub account where you will upload your group report, which will serve as your portfolio.

Project Title:

Phishing for Awareness: Simulating a Social Engineering Attack

Phishing Campaign:

Instagram Phishing

Date:

October 9th 2024.

1. Introduction

This report outlines the design, execution, and analysis of a phishing campaign carried out as part of our cybersecurity training. **The objective was to simulate a phishing attack to raise awareness and understand the effectiveness of phishing techniques.**

2. Campaign Overview

Campaign Type: Credential Harvesting & Awareness Training.

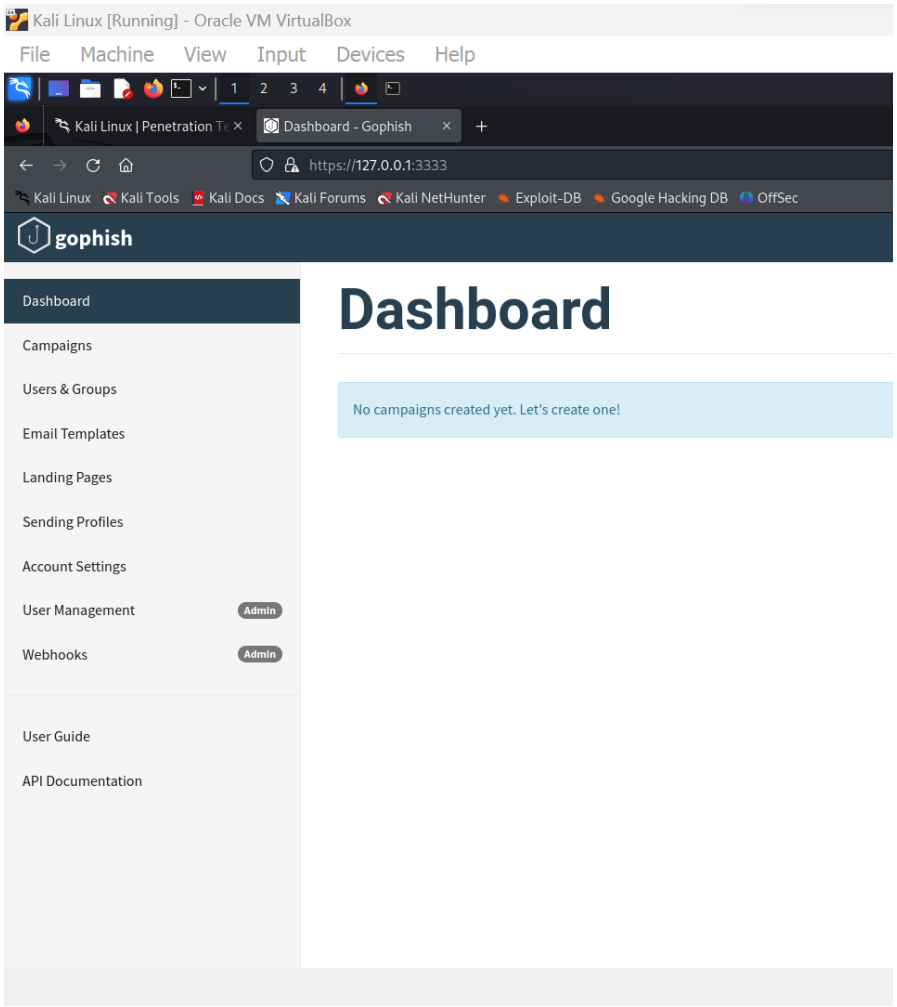
Target Audience: Friends and classmates.

Number of Recipients: Four

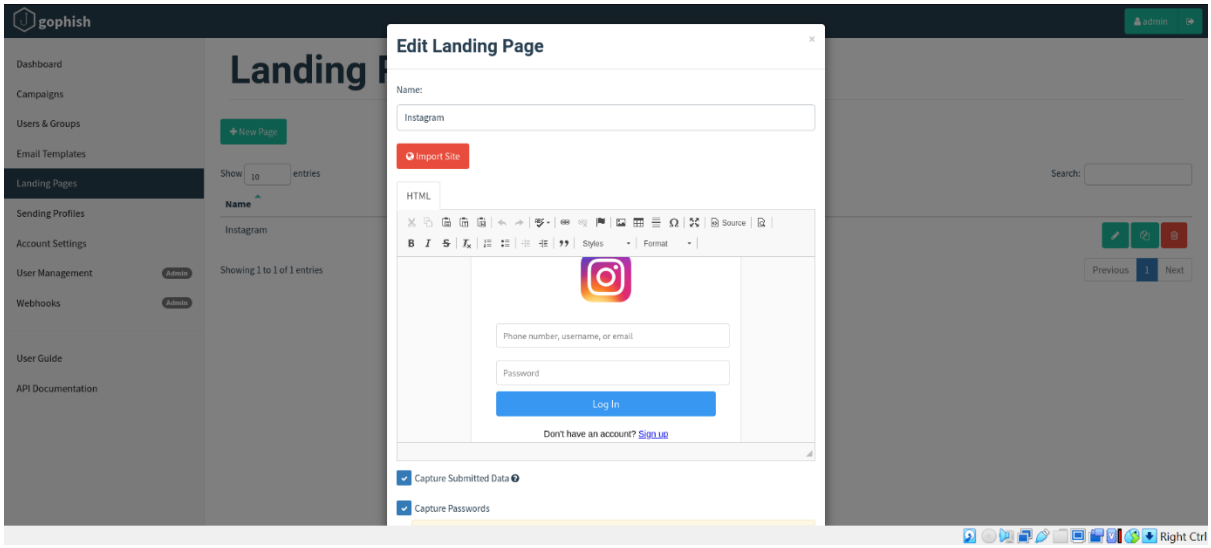
Phishing Methodology: Email-based phishing attack with a malicious link directing to a fake landing page resembling **Instagram login page.**

3. Technical Setup

Platform Used: GoPhish

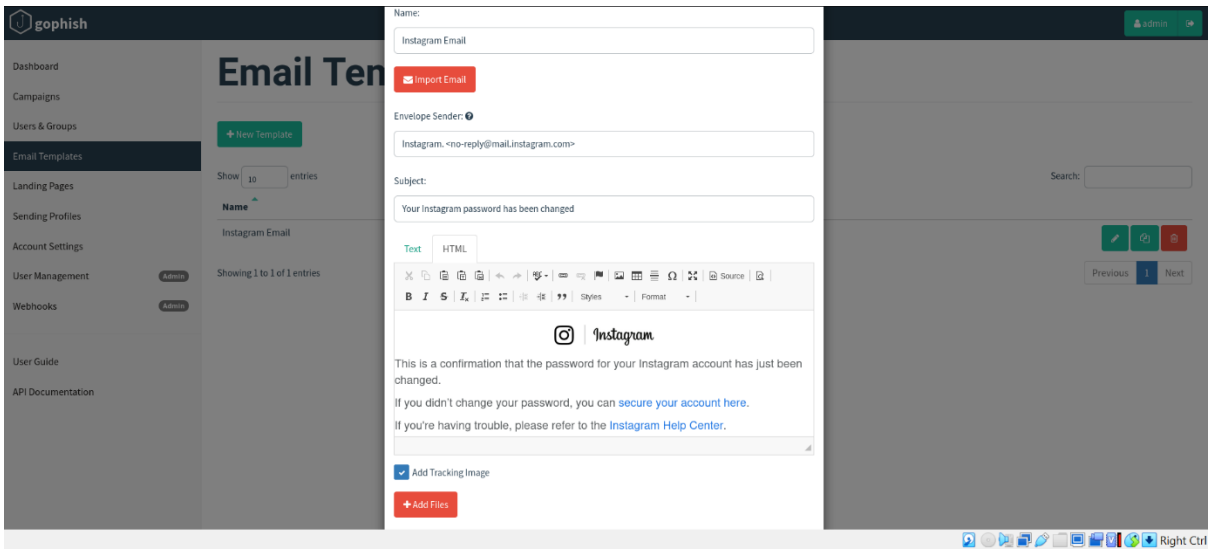


Landing Page: Custom-built page mimicking Instagram's login page



SMTP Server: I used my google account

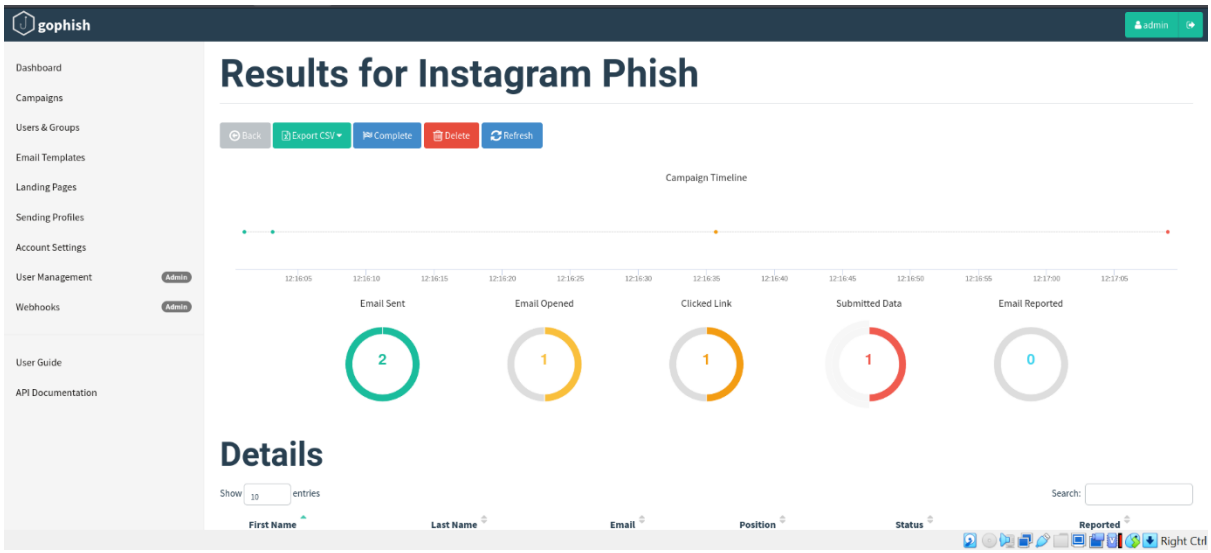
Email Template



Subject Line: Your Instagram password has been changed

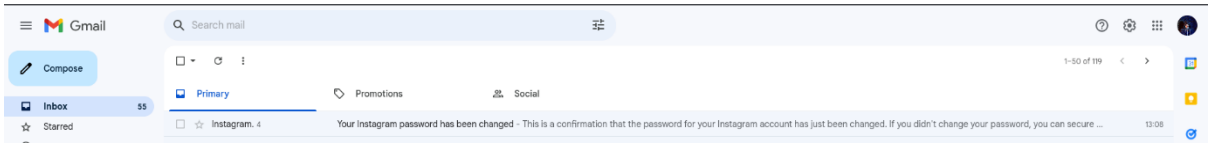
Body Content: A phishing email that appeared as a password reset confirmation from Instagram. The email included a link directing recipients to the fake login page.

4. Execution

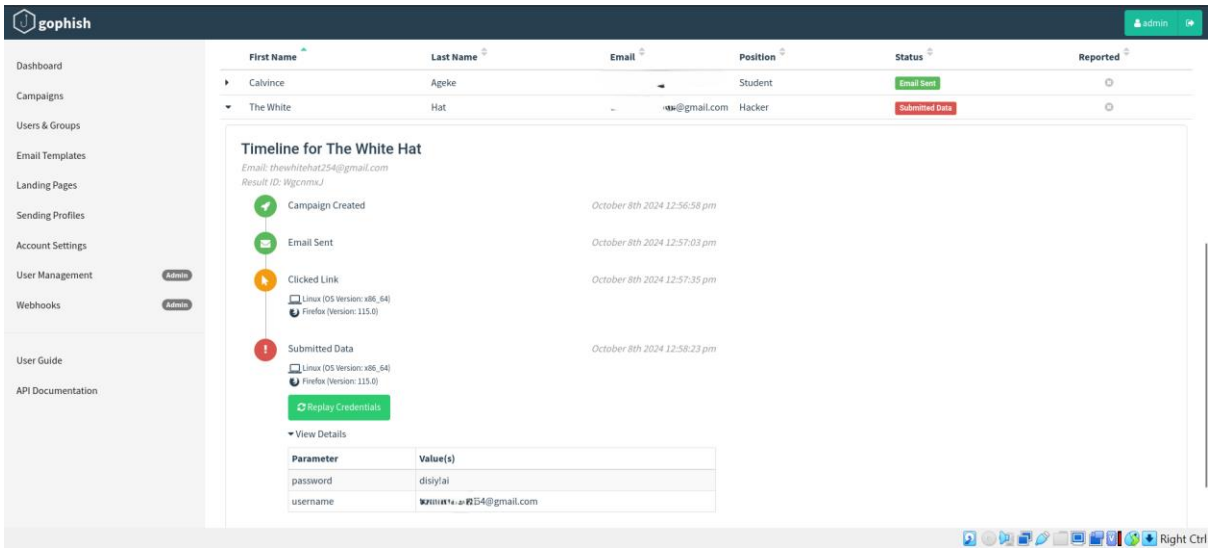


The phishing campaign was launched on October 3rd 2024 and ran for a duration of four days. During this period, the campaign achieved a delivery rate of 100 percent, ensuring that the majority of emails reached their targets. The open rate, which reflects the percentage of recipients who engaged with the email by opening it, stood at 50 percent.

Message Delivered



Credentials Harvested



5. Landing Page Metrics

Landing Page: The page was designed to resemble Instagram's login page to trick users into entering their credentials.
Credential Submission Rate: 50 percent of users submitted their login credentials

Total Clicks: 50 percent clicks

6. Phishing Email Example

7. Key Findings

Effectiveness of Phishing Attack: The phishing attack demonstrated a notable level of success, as evidenced by a click rate of 50%, indicating that a significant portion of recipients engaged with the malicious content. Furthermore, the credential submission rate reached 50%, highlighting the effectiveness of the campaign in deceiving users into providing sensitive information. Overall, the high engagement levels underscored the vulnerabilities present in user awareness regarding phishing threats.

Common Mistakes of Users: A common trend observed during the campaign was that many users clicked on the links without adequately verifying the sender's identity or scrutinizing the URL. This lack of vigilance often stemmed from a misplaced trust in recognizable branding and familiar email formats, ultimately leading to the submission of personal credentials.

Technical Difficulties: Throughout the campaign, several technical challenges arose. One significant issue was related to the SMTP "From" field, which presented difficulties in configuring the sender's identity to avoid revealing the true source of the email. Additionally, there were challenges in ensuring that the email template links correctly directed users to the landing page upon clicking. These issues required troubleshooting and adjustments to

enhance the functionality of the campaign while minimizing disruption to the overall effectiveness of the phishing simulation.

8. Lessons Learned

- **Importance of User Education:** Many users fell for the attack, indicating a need for awareness training.
- **Common Red Flags:** Educating users to check email headers, URLs, and report suspicious content can greatly reduce the success of phishing attacks.

9. Conclusion and Recommendations

The phishing campaign successfully demonstrated how easily users could be tricked into divulging sensitive information. To mitigate the risk of such attacks, we recommend the following:

- Regular phishing awareness training.
- Implementation of two-factor authentication.
- Tightening email security measures (e.g., SPF, DKIM, DMARC).