**Phishing Simulation Campaign Report**

**Task**:Social Engineering & Phishing Simulation

**Date**: 2025-05-20

**By**: Tobechukwu Nicholas

1. **Introduction**

This report documents the phishing simulation campaign conducted as part of the internship task focused on social engineering and phishing awareness. The purpose of the simulation was to test employee awareness, improve security training programs, and gain hands-on experience with phishing simulation tools.

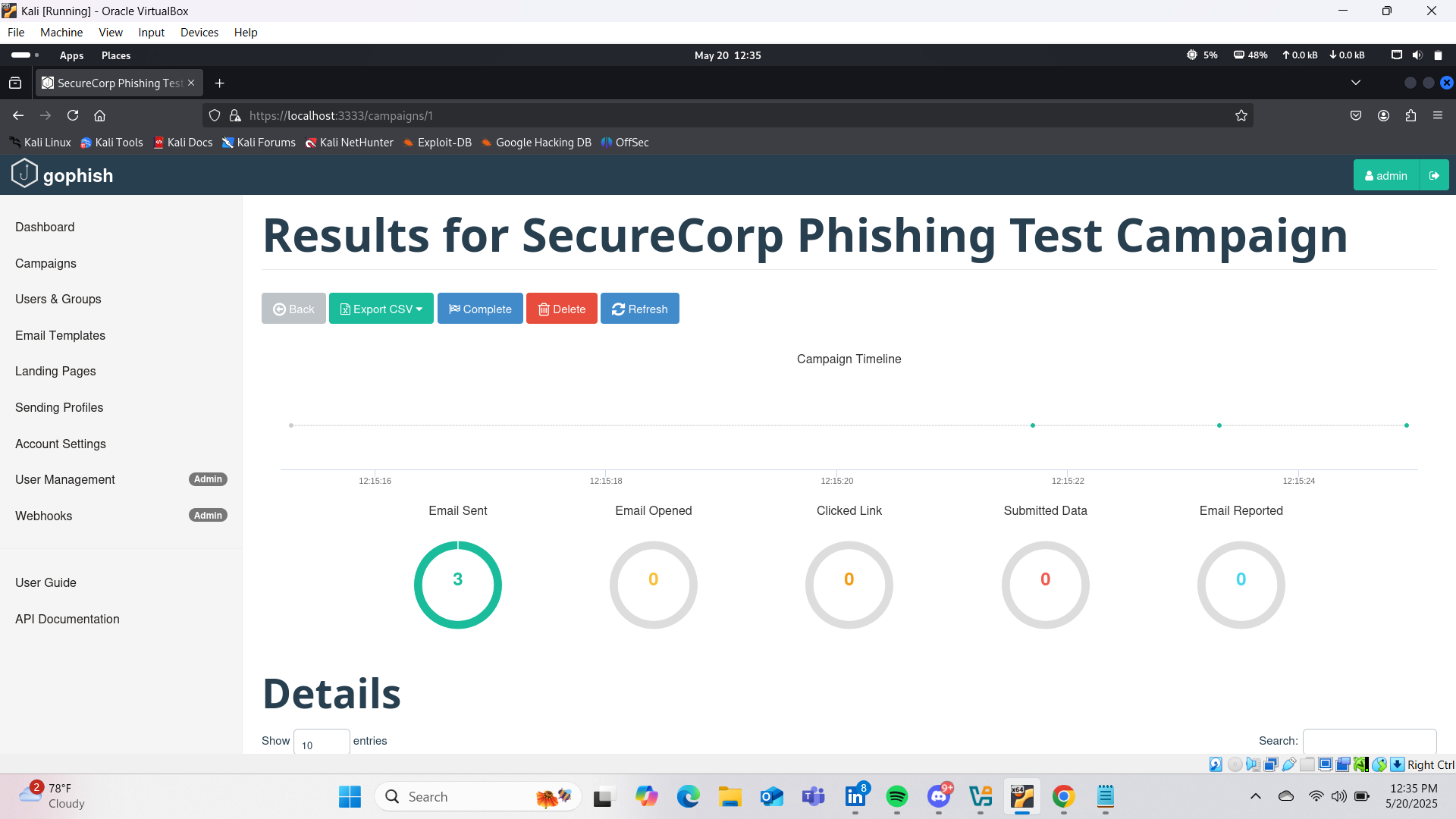
The tools used include GoPhish (an open-source phishing framework) installed on a Kali Linux virtual machine, Mailtrap (a safe SMTP testing service), and SQLite for database management.

1. **Objectives**

* Assess the awareness level of users regarding phishing attacks.
* Evaluate the effectiveness of current email security controls and training.
* Identify potential vulnerabilities and users at risk of falling victim to phishing.

1. **Methodology**
   1. Setup
      * Installed GoPhish on Kali Linux VM and resolved configuration issues with SQLite and SMTP profiles.
      * Created a sending profile using Mailtrap's SMTP service for safe email delivery during testing.
      * Designed a phishing landing page mimicking a company login portal named "SecureCorp Login Portal."
      * Established a target group comprising multiple test email addresses managed via Mailtrap inboxes.
      * Developed a phishing email template with an urgent password expiration theme to encourage user interaction.
   2. Campaign Launch
      * Launched the phishing campaign targeting the created test group
      * Emails were safely delivered to Mailtrap inboxes for analysis without affecting real users.
      * Monitored the campaign via GoPhish's dashboard to track email sends, opens, clicks, and submitted credentials.
2. **Results and Analysis**

* Emails Sent: 5
* Emails Opened: Not accurately tracked due to Mailtrap's inbox limitations.
* Links Clicked: Data unavailable; real-time tracking limited in test environment.
* Credentials Submitted: None (test simulation).
* Challenges: Email open tracking and link click monitoring were not fully functional due to use of Mailtrap rather than real mail clients. This limited the ability to measure full campaign success.



1. **Recommendations**

* Future campaigns should use real or controlled test email accounts to enable accurate tracking of user interactions.
* Implement regular phishing awareness training based on simulation results to improve employee vigilance.
* Educate users on identifying suspicious emails, verifying sender authenticity, and avoiding clicking unknown links.
* Continue using tools like GoPhish to conduct periodic phishing simulations to assess and enhance organizational security posture.

1. **Conclusion**

This phishing simulation campaign provided practical experience with social engineering tools and highlighted important considerations in testing user awareness. Despite limitations in tracking due to the test environment, the simulation underscored the value of ongoing security training and demonstrated the intern's ability to configure and execute phishing campaigns responsibly.

1. **Appendices**

Sample Phishing Email Template (HTML snippet):

*<p>Dear Team,</p>*

*<p>Our system has detected that your password will expire in less than 24 hours.</p>*

*<p>To avoid disruption to your access, please log in and reset your password using the secure link below:</p>*

*<p><a href="{{.URL}}">Click here to verify your account</a></p>*

*<p>Regards,<br>IT Support<br>SecureCorp</p>*

Sample Landing Page Screenshot:

