Phishing Simulation Project with SIEM & EDR Mapping

1. Project Objective

- **The objective of this project was to simulate a real-world phishing attack, observe user behavior, and map the attack lifecycle to SOC detection and response mechanisms using SIEM, EDR, and SOAR concepts**

2. Lab Environment

- **Operating System: Kali Linux (VMware)**
- **Phishing Framework: GoPhish**
- **Campaign Type: Credential Harvesting**
- **Target Test User: (Local Simulation)**

3. Attack Simulation Flow

- **A phishing email containing a password reset link was simulated using GoPhish. The user opened the email, clicked the malicious link, and submitted credentials on a fake login page. All interactions were tracked and logged by the framework**

4. Campaign Results

- **Email Sent: 1**
- **Email Opened: 1**
- **Link Clicked: 1**
- **Credentials Submitted: 1**

5. SIEM Mapping (Detection & Correlation)

Log Source	Observed Event
Email Gateway	Spoofed sender and phishing email
Web Proxy / Firewall	Access to phishing URL
Application Logs	Credential submission event Potential account misuse

- **The SIEM correlates these events to generate a high-severity phishing alert.**

6. EDR Mapping (Endpoint Visibility)

EDR Signal	Behavior
Browser Activity	User opened phishing URL
Credential Handling	Password entered into browser

Network Behavior	**Suspicious outbound connection**

7. SOAR Automated Response

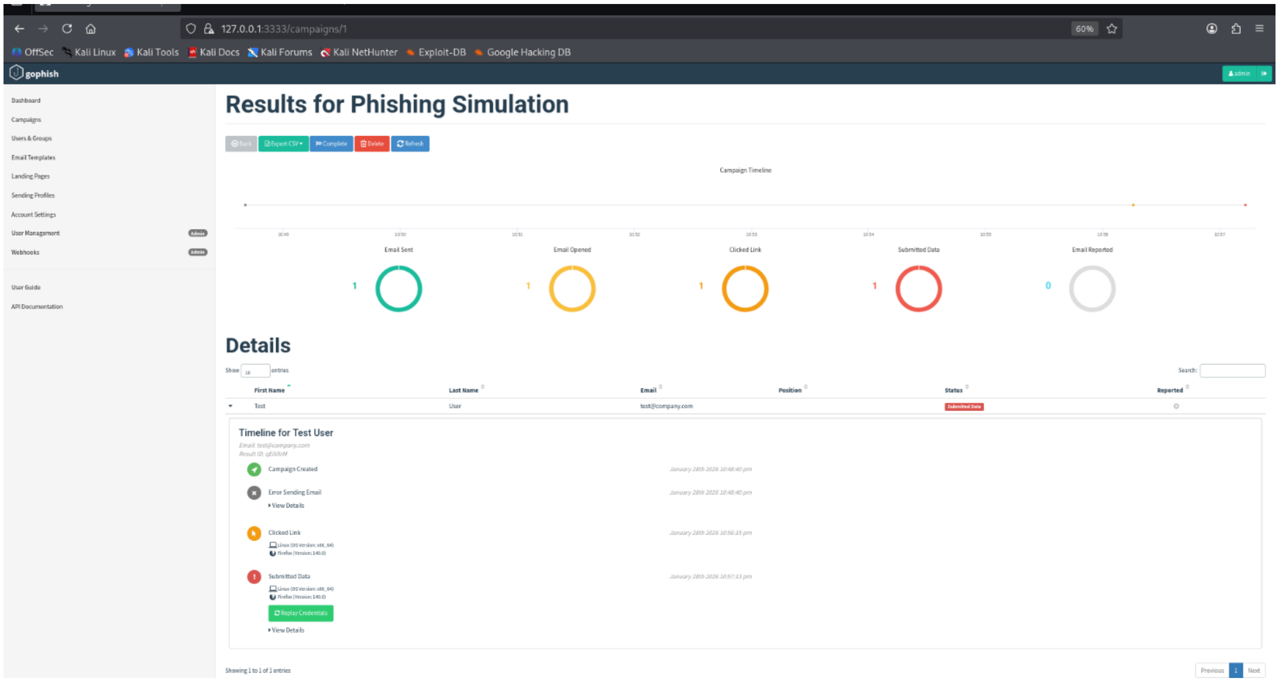
- **Upon confirmation of phishing, automated actions would include blocking the phishing URL, resetting the affected user's password, notifying the SOC team, and initiating user awareness training.**

8. MITRE ATT&CK; Mapping

Tactic	**Technique**
Initial Access	**Phishing (T1566)**
Credential Access	**Credential Harvesting**

9. Conclusion

- **This project demonstrates a complete phishing attack lifecycle and SOC-style detection and response workflow. It highlights practical knowledge of attack techniques, security monitoring, and incident response**



Results for Phishing Simulation

Details

First Name	Last Name	Email	Position	Status	Reported
Test	User	test@company.com		Submitted Data	

Timeline for Test User

Email: test@company.com
Result ID: qEAXoM

Campaign Created	*January 28th 2026 10:48:40 pm*
Error Sending Email	*January 28th 2026 10:48:40 pm*
Clicked Link Linux (OS Version: x86_64) Firefox (Version: 140.0)	*January 28th 2026 10:56:15 pm*
Submitted Data Linux (OS Version: x86_64) Firefox (Version: 140.0)	*January 28th 2026 10:57:13 pm*

Showing 1 to 1 of 1 entries