GOPHISH — Simulated Phishing Campaign (Concise Technical Summary)

Author: TOM SHINJJO THOMAS
Environment: Gophish running in a virtualized VM (Windows/Linux)

Objective

Objective: Execute a controlled phishing simulation using Gophish to measure user susceptibility, capture engagement metrics, and produce data for targeted security training.

Setup & Configuration

Installation & Access: Gophish deployed on a VM. Web UI accessible at https://localhost:3333; SMTP profile configured for outbound mail delivery.
Templates & Landing Pages: Custom email templates and realistic credential-capture landing pages were created to simulate common phishing techniques.
Targeting: A controlled test group of recipient addresses was defined to limit the campaign to authorized participants.

Campaign Execution

• Campaign launched against the test recipient group using the configured SMTP profile.
• Gophish dashboard monitored real-time metrics: email deliveries, opens, link clicks, and credentialsubmissions.
• Activity timelines captured per-recipient events from delivery to form submission.

Educational Impact

• Identified user behaviors that increase phishing susceptibility.
• Provided tailored training opportunities to reduce credential-sharing.
• Reinforced the need for phishing reporting procedures and periodic drills.

Limitations & Ethical Notes

• Campaign executed in a closed environment with prior authorization.
• Real-world effectiveness depends on template realism and appropriate targeting practices.
• Ensure strict legal and ethical compliance for any live deployments.

Conclusion

Gophish proved effective for simulating phishing scenarios within a VM environment. The tool's analytics and customization capabilities allow security teams to quantify human risk and design targeted awareness programs. When executed ethically, Gophish is a cost-effective solution for ongoing phishing resilience testing.
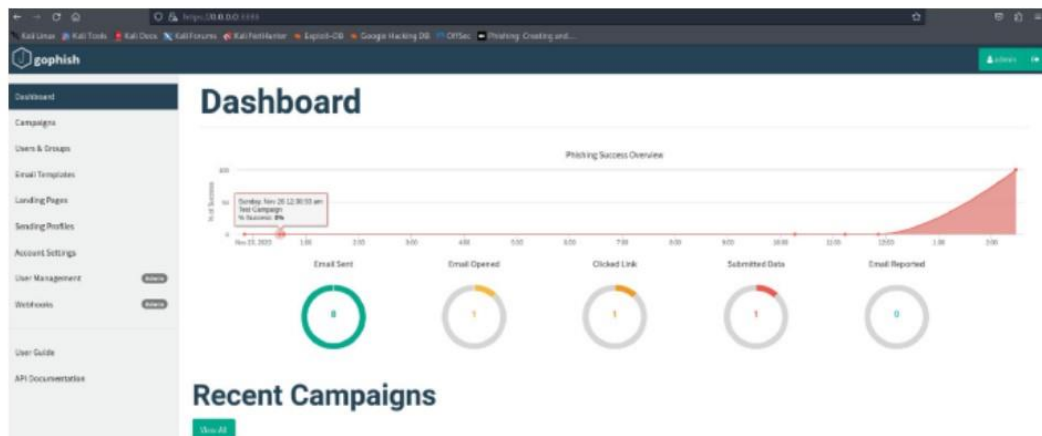
Screenshots: