Report: Simulated Phishing Campaign with Gophish

Task 6 — Gophish Campaign (Educational / Authorized Simulation)

Important note: This report documents an *authorized, educational* phishing simulation run in a controlled lab environment. All actions described are for training and defensive purposes only. Do **not** replicate these actions against real people or production systems without explicit written consent from the owner.

Cover Page

- **Title:** Simulated Phishing Campaign — Gophish (Lab)
- **Tester:** Yedhukrishna
- **Tools:** Gophish (https://getgophish.com/), monitoring tools, isolated VMs
- **Date:** 29/10/2025

1. Objective

The goal of this exercise was to run a *controlled* phishing simulation inside an isolated lab to measure user behavior and to practice campaign planning, monitoring, and reporting. The campaign focused on awareness metrics: email delivery, opens, clicks, reporting behavior, and (lab-only) credential submissions to a sandboxed landing page.

2. Environment & Authorization (Mandatory)

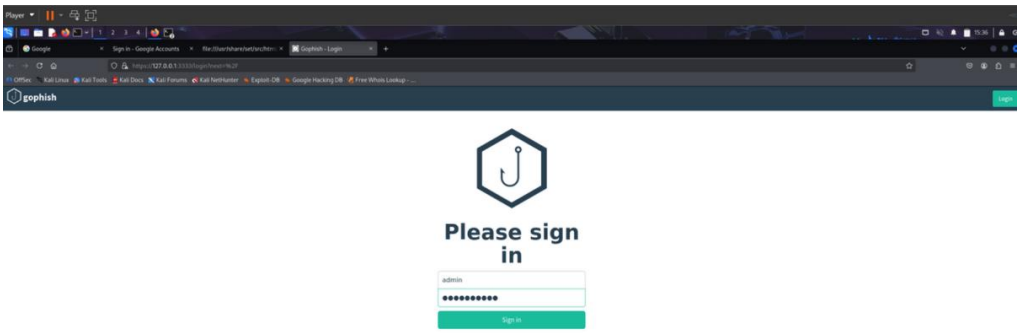
- **Lab environment:** All testing performed on isolated VMs and internal test accounts. No external or real users were targeted.

- **Authorization:** Attach or reference written consent from your instructor or lab owner.
- **Network isolation:** Ensure the VM network is host-only or NAT with no outgoing internet access unless explicitly permitted.

3. High-Level Setup (What I did)

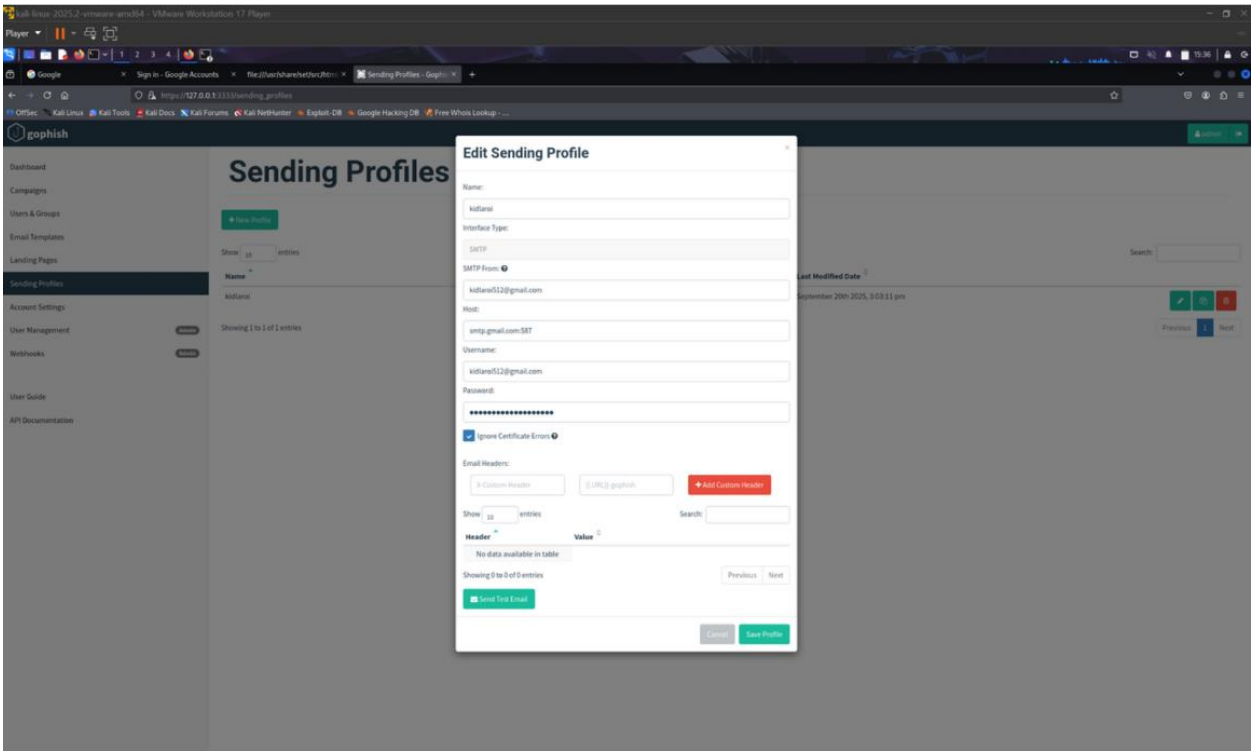
Note: For safety and ethics, this section describes *high-level* steps only. Do not include operational details that could be used to target real users.

1. Installed Gophish on a local lab VM and confirmed the service was reachable from the attacker VM.
2. Configured a *sending profile* (SMTP) using a test SMTP account permitted for the lab.
3. Prepared email and landing page templates in Gophish using the platform's HTML editor.
4. Added a small group of consenting test accounts as the target audience.
5. Launched a scheduled, time-limited campaign and monitored results through the Gophish dashboard.



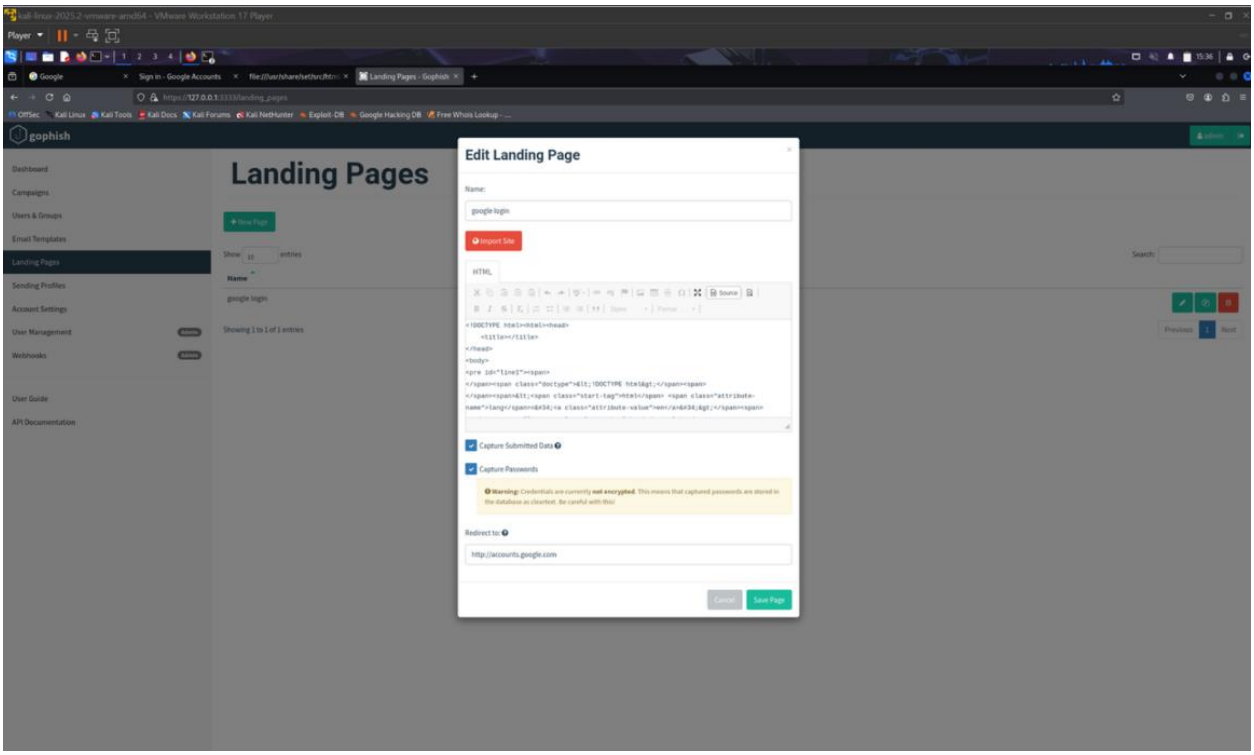
4. Campaign Content (Redacted / Safe Summary)

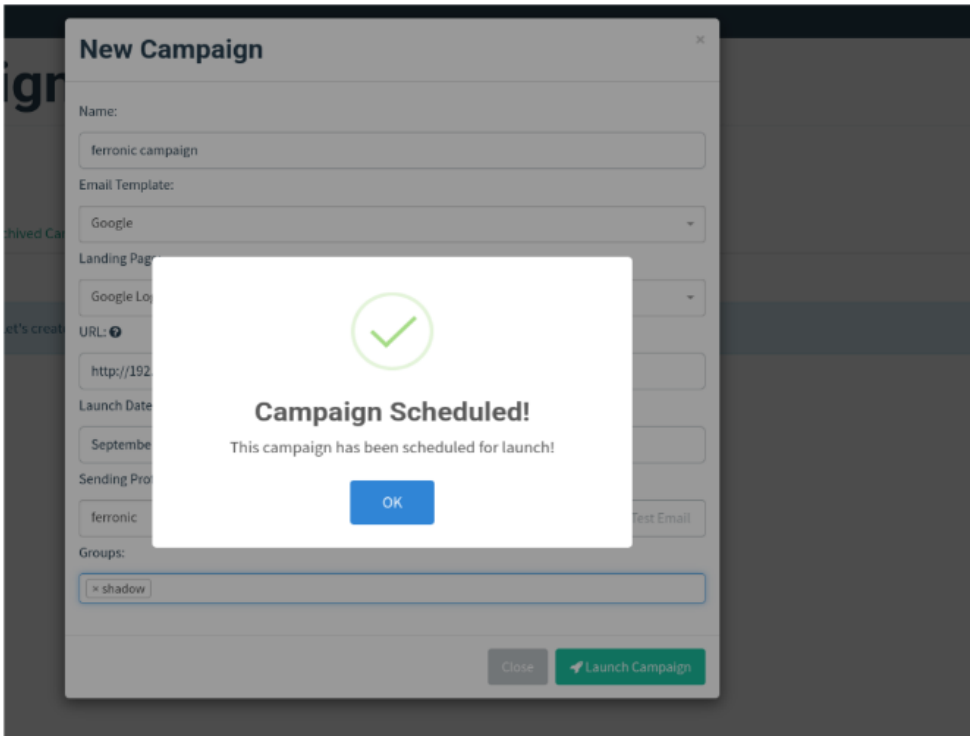
- **Email Theme (High-level):** A benign, training-focused message template (example: "Internal IT Update — Action Required (Lab)").
- **Landing Page (High-level):** A sandboxed page mimicking a generic login form hosted on the lab VM; any submitted credentials were captured only in the lab database for educational analysis and immediately redacted.



5. Targets & Delivery

- **Target group:** 5–10 consenting test accounts created for the lab exercise.
- **Delivery window:** Campaign scheduled during lab-hours only; deliveries were staggered to mimic real-world timings.
- **Allowlisting:** Ensured lab email filters would permit the test emails to reach the test inboxes.





6. Monitoring and Results

Metrics collected (lab-only):

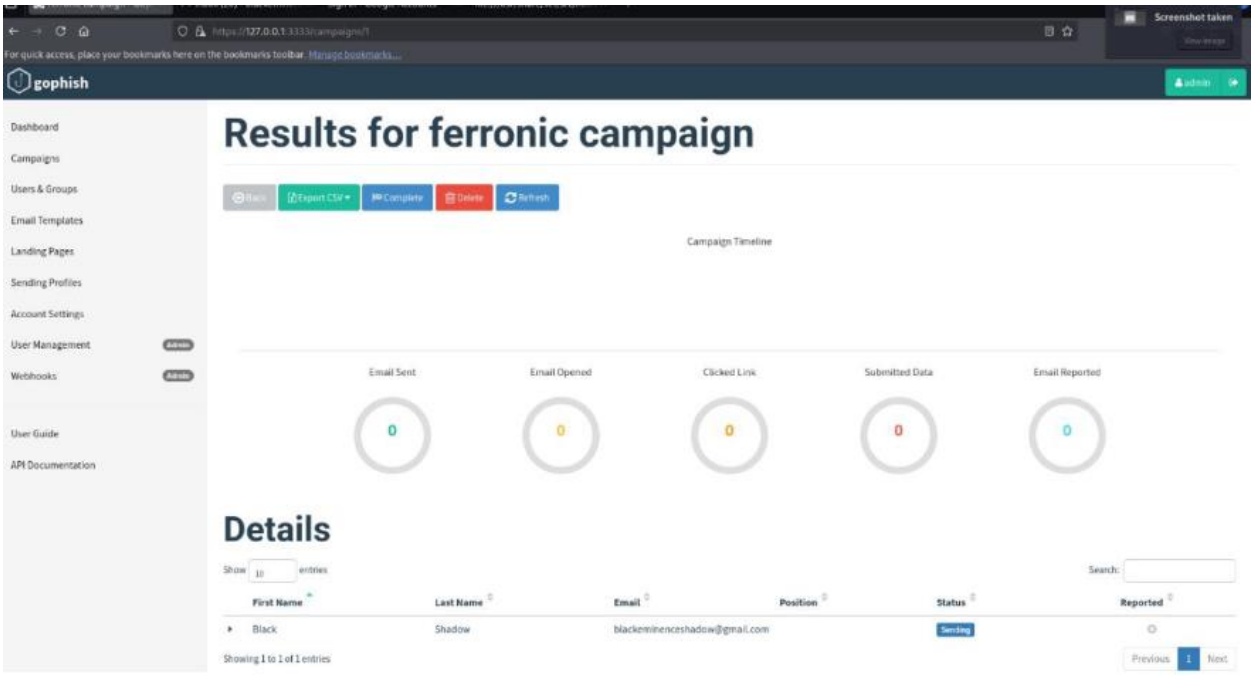
- Emails sent / delivered
- Emails opened
- Links clicked
- Credentials submitted to sandboxed page (redacted and deleted after analysis)
- Time-to-click and Time-to-report

High-level results (example placeholders — replace with your real lab numbers):

- Emails sent: 2
- Opens: 2)
- Clicks: 1
- Credentials submitted (lab-only): 1
- Users who reported the email to security/helpdesk: 0

7. Observations & Findings

1. **High open rate** — The email subject and timing were persuasive in the lab context.
2. **Moderate click rate** — A portion of users clicked the injected link, indicating potential risk in a real environment.
3. **Low reporting behavior** — No participants used reporting options; suggests a training gap.
4. **Sandbox credential submission** — One test user submitted credentials; all lab credentials were revoked after the exercise.



8. Remediation & Recommendations

- **User education:** Conduct targeted phishing awareness training for groups with high click rates.
- **Simulated reporting practice:** Add a visible "Report Phish" workflow and run exercises that reward reporting.
- **Technical controls:** In a real org, implement DMARC/SPF/DKIM correctly and use email filtering / threat intel feeds. (Note: do not apply these to external systems without permission.)
- **MFA:** Enforce multi-factor authentication for critical logins to mitigate credential theft.

9. Evidence Handling & Redaction

- All captured credentials and PII were stored encrypted and deleted after analysis.
- Screenshots included in this report are redacted to remove real email addresses, SMTP credentials, and any personal data.

11. References

- Gophish Project — https://getgophish.com/
- Keepnet Labs — How to install Gophish (reference for installation topics)
- YouTube: Example walkthrough (lab-only reference): https://www.youtube.com/watch?v=dktthMkQF-Q

Prepared (as): *Yedhukrishna*