# Task 6: Simulated Phishing Campaign Analysis - GoPhish
Prepared for: MuLearn Bootcamp
Prepared by: Sreehari Vinod
Platform: Virtual Machine (Self-hosted GoPhish)
Task Type: Ethical Hacking, Social Engineering

## Introduction

GoPhish, an open-source phishing toolkit, enables security experts to simulate phishing attacks for training purposes. This report outlines a controlled campaign conducted in a VM to assess user susceptibility and enhance security awareness.

## Purpose

The aim was to simulate a phishing attack using GoPhish, gaining insights into social engineering tactics to strengthen organizational defenses through practical learning.

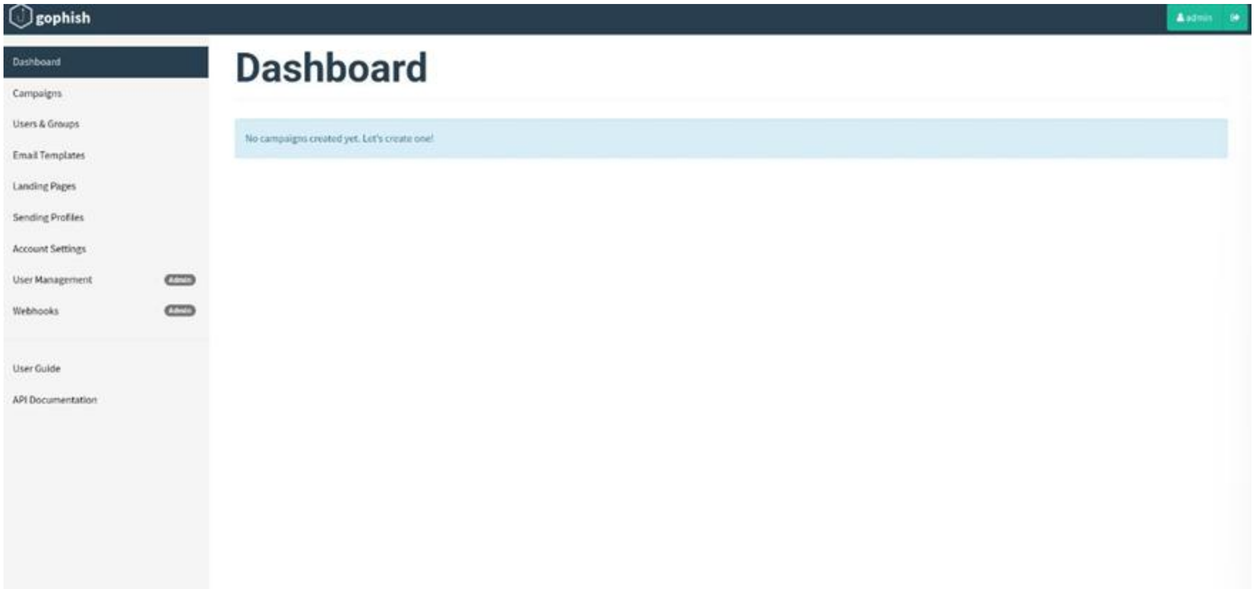
## Tools Utilized

- **GoPhish:** A robust platform offering a web interface for crafting emails, designing fake pages, and monitoring campaign outcomes in real-time.

## Execution Steps

### Step 1: System Configuration

- Installed and launched GoPhish on a Kali Linux VM, accessing the dashboard via the default browser.



Dashboard

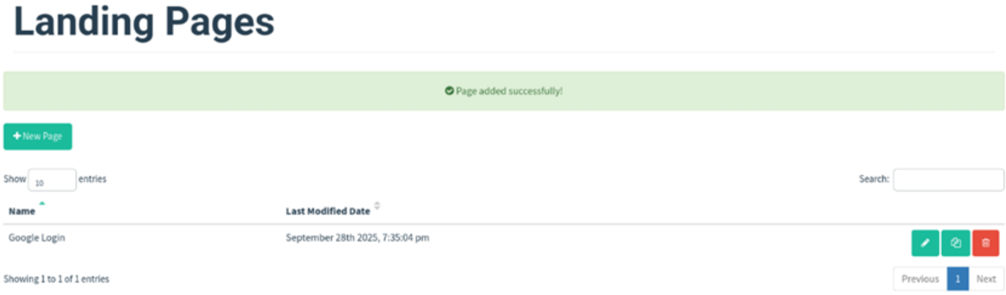
No campaigns created yet. Let's create one!

### Step 2: Crafting the Decoy

- **Landing Page:** Replicated a Google login page using /usr/share/set/src/html/templates/google/index.template, with a redirect to https://accounts.google.com.
- **Email Template:** Designed a bait email mimicking a 2-step verification alert.
- **Screenshot:** [Image of landing page setup from "Task -6:" Page 3]
- **Screenshot:** [Image of email template design from "Task -6:" Page 4]

### Step 3: Target Setup and Dispatch

- **User Grouping:** Created a target group with test users.
- **Email Dispatch:** Configured an SMTP profile and sent a test email to verify functionality.
- **Screenshot:**



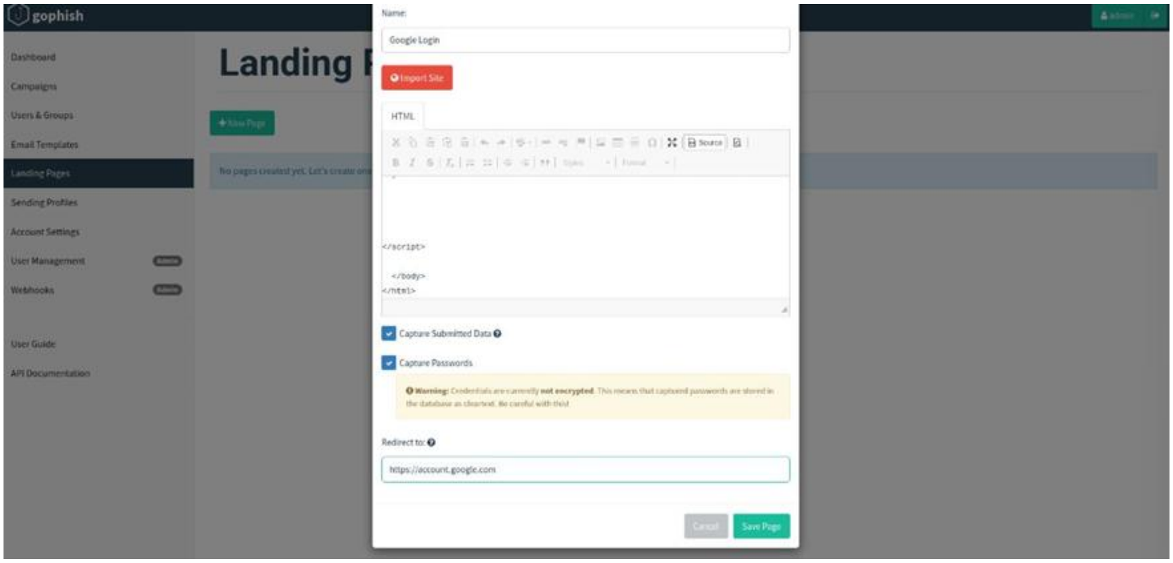
Landing Pages

Page added successfully!

| Name | Last Modified Date |
|---|---|
| Google Login | September 28th 2025, 7:35:04 pm |

Showing 1 to 1 of 1 entries

- **Screenshot:**



Name: Google Login

```
</script>

  </body>
</html>
```

☑ Capture Submitted Data

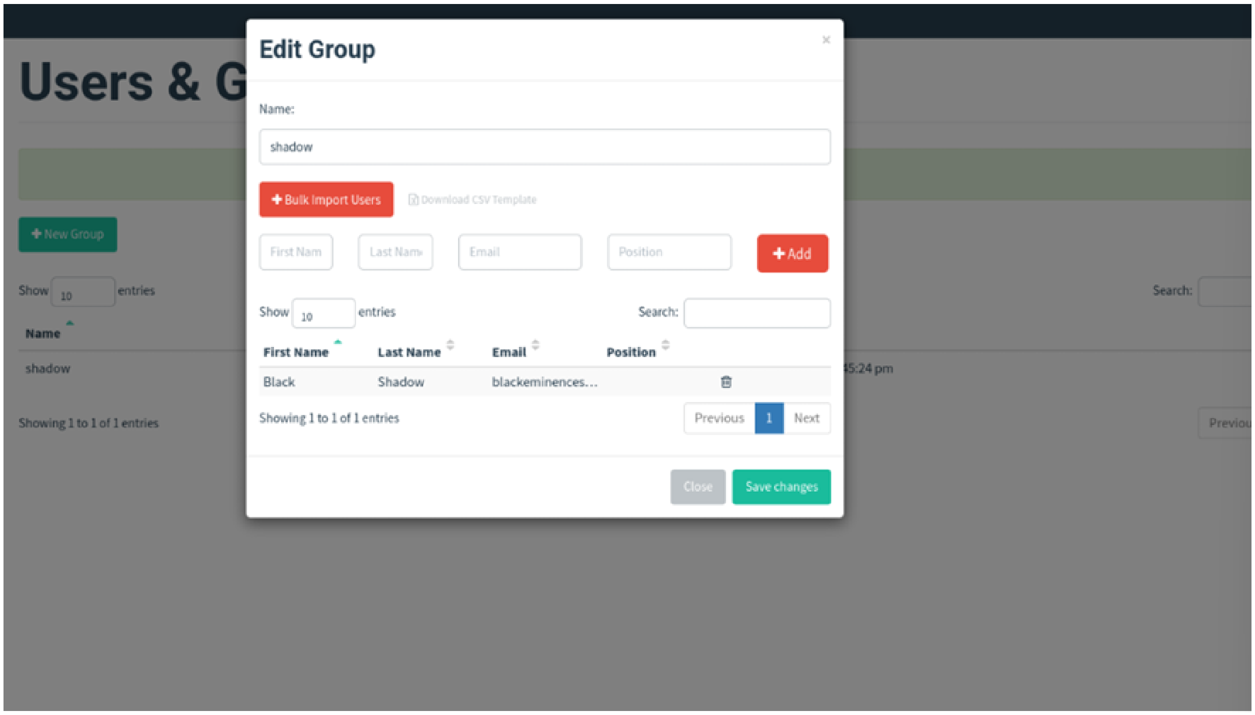
☑ Capture Passwords

**Warning:** Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: https://account.google.com

### Step 4: Campaign Execution and Review

- **Launch:** Initiated a campaign named "Google Security Alert" targeting the group.
- **Monitoring:** Tracked results showing both emails opened and links clicked.
- **Screenshot:**



Edit Group

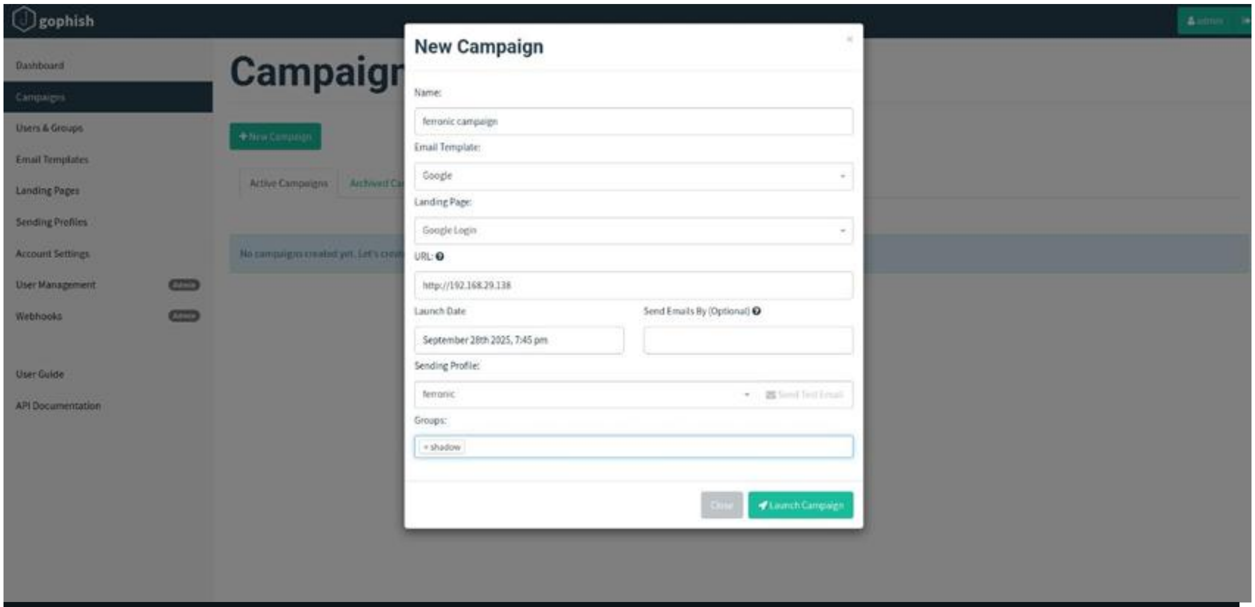
Name: shadow

Show 10 entries    Search:

| First Name | Last Name | Email | Position |
|---|---|---|---|
| Black | Shadow | blackeminences... | |

Showing 1 to 1 of 1 entries

- **Screenshot:**



New Campaign

Name: ferronic campaign

Email Template: Google

Landing Page: Google Login

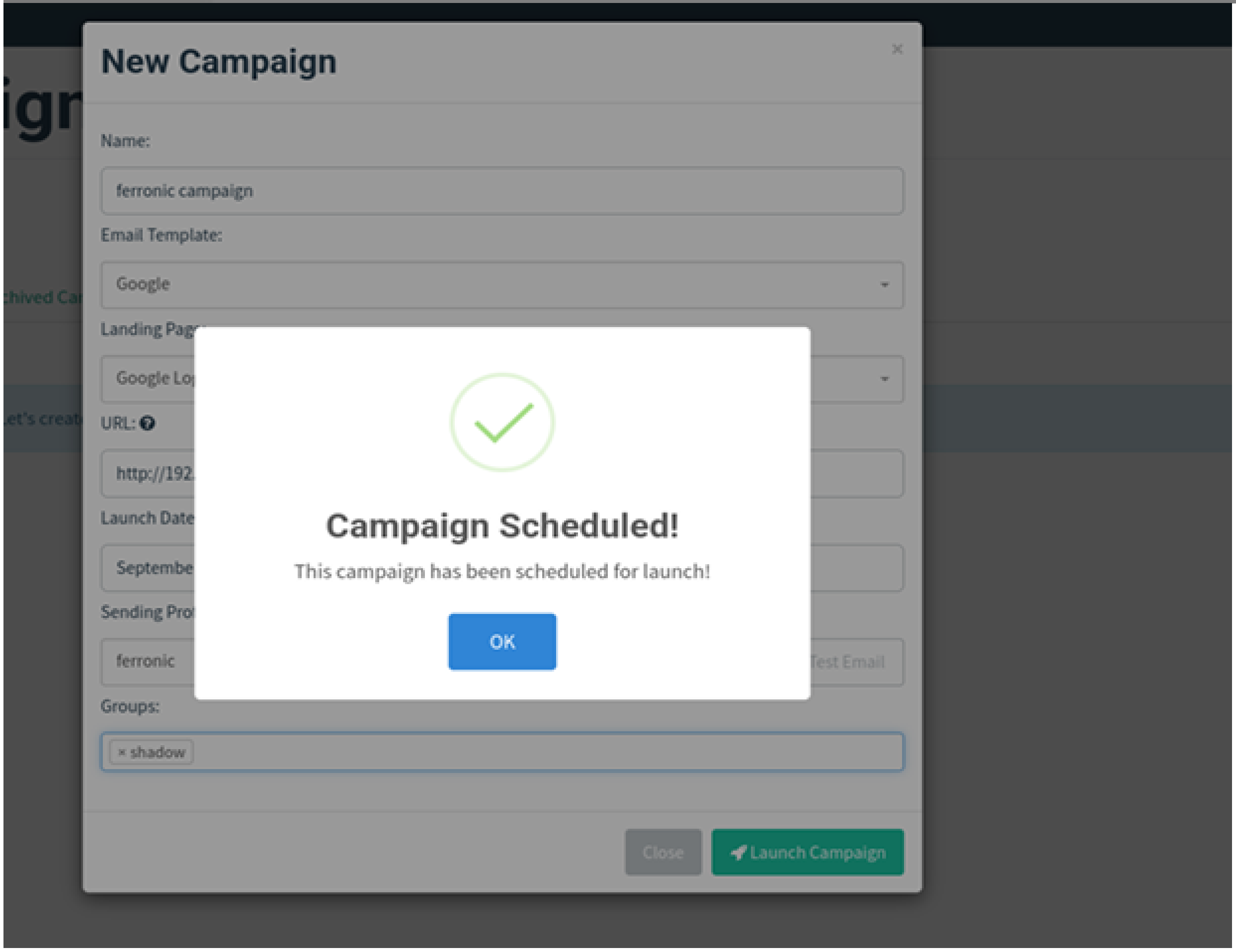
URL: http://192.168.29.138

Launch Date: September 28th 2025, 7:45 pm

Send Emails By (Optional):

Sending Profile: ferronic

Groups: × shadow



New Campaign

Name: ferronic campaign

Email Template: Google

Landing Pag Google Lo

URL: http://192.

Launch Date Septembe

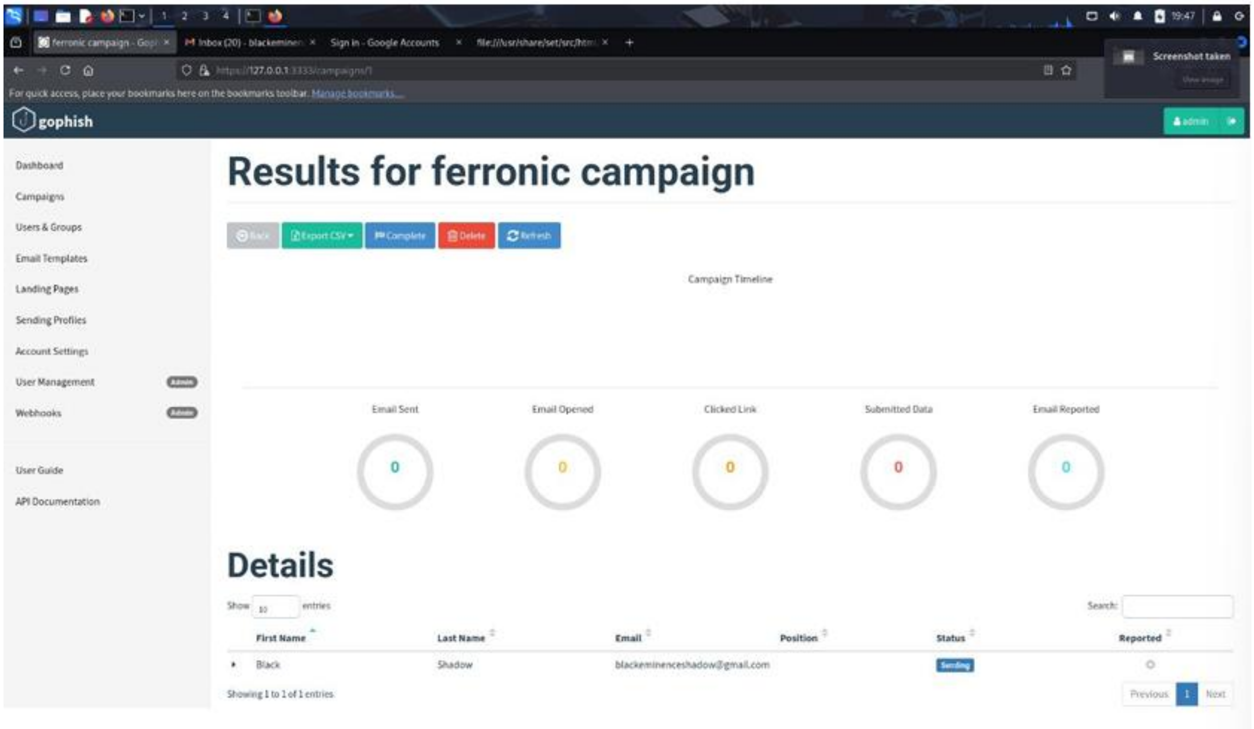
Sending Prof ferronic

Groups: × shadow

Campaign Scheduled!

This campaign has been scheduled for launch!

-



Results for ferronic campaign

| Email Sent | Email Opened | Clicked Link | Submitted Data | Email Reported |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |

Details

Show 10 entries

Search:

| | First Name | Last Name | Email | Position | Status | Reported |
|---|---|---|---|---|---|---|
| ▸ | Black | Shadow | blackeminenceshadow@gmail.com | | Sending | ○ |

Showing 1 to 1 of 1 entries

Previous 1 Next

-

**Results**

The campaign successfully engaged targets, with both opening emails and clicking the link, underscoring the potency of social engineering tactics. No real data was compromised due to the controlled VM environment.

**Reflection**

This simulation highlighted the ease of phishing success through human error. GoPhish proved valuable for educational purposes, emphasizing the need for ongoing training and robust email validation to mitigate such risks.