

Task -6:

GoPhish Simulated Phishing Campaign Report

Prepared for: MuLearn Bootcamp

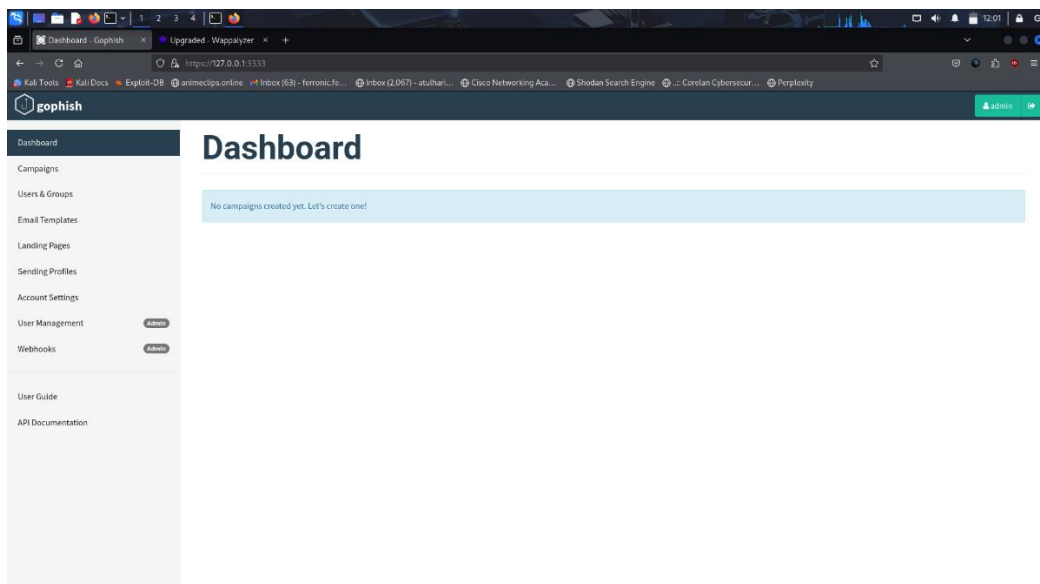
Prepared By: Atul H

Introduction:

[Gophish](#) is a powerful, open-source phishing framework used by security professionals to conduct phishing campaigns and security awareness training. It allows organizations to test their workforce for vulnerabilities by simulating real-world phishing attacks, tracking employee responses, and analyzing the results.

Steps proceeded:

In Kali Linux there is a pre installed tool called GoPhish in it. As we open the GoPhish tool, we would be asked to enter the password for the system to grant the root access to the terminal for running. After the command gets executed a windows of the GoPhish via our default browser pops up.



Navigate through the left side. We then select and create the new sending profile.

The left screenshot shows the 'New Sending Profile' form. It includes fields for Name, Profile name, Interface Type (SMTP), SMTP From (First Last <test@example.com>), Host (smtp.example.com:25), Username, Password, and a checkbox for 'Ignore Certificate Errors'. There is also a section for Email Headers with a table showing 'X-Custom-Header' and '[[URL]]-gopish'. The right screenshot shows the 'Send Test Email' dialog. It has a green bar at the top saying 'Email Sent!'. Below it, there are input fields for 'Send Test Email to:' with values 'ferronic', 'ferro', and 'ferronic.ferro@gmail.com', and a 'Position' field. There are 'Cancel' and 'Send' buttons.

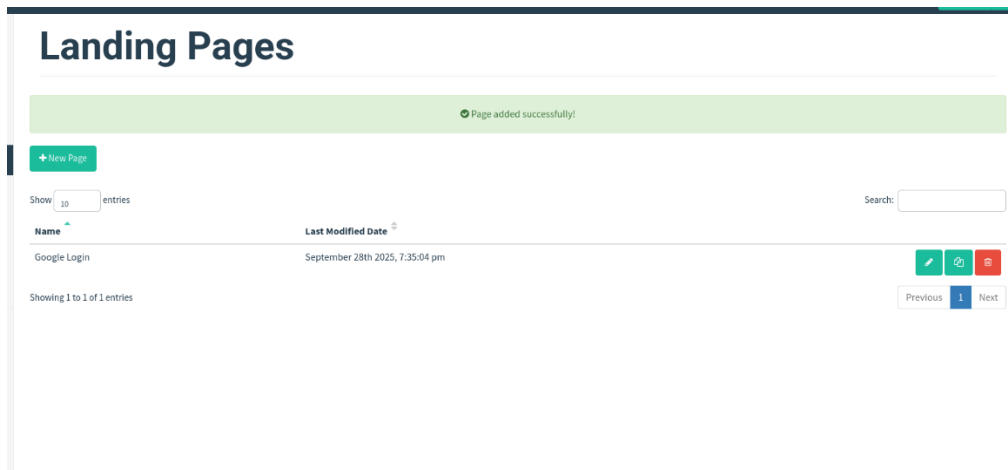
After we fill out the sending profile form, we get to verify our mail is working properly by sending a test mail. Once the email sent! Popup comes we can be sure that our sending profile is all set to go.

Once this process is done we move on to the setting of our landing page:

The screenshot shows the Gopish web interface with the 'Landing Pages' section selected in the sidebar. A modal window is open for creating a new landing page. The modal has a title 'Name: Google Login' and a red 'Import Site' button. Below that is a text area for HTML code. There are checkboxes for 'Capture Submitted Data' and 'Capture Passwords'. A warning message states: 'Warning: Credentials are currently not encrypted. This means that captured passwords are stored in the database as plaintext. Be careful with that!'. There is a 'Redirect to:' field with the value 'https://account.google.com'. At the bottom are 'Cancel' and 'Save Page' buttons.

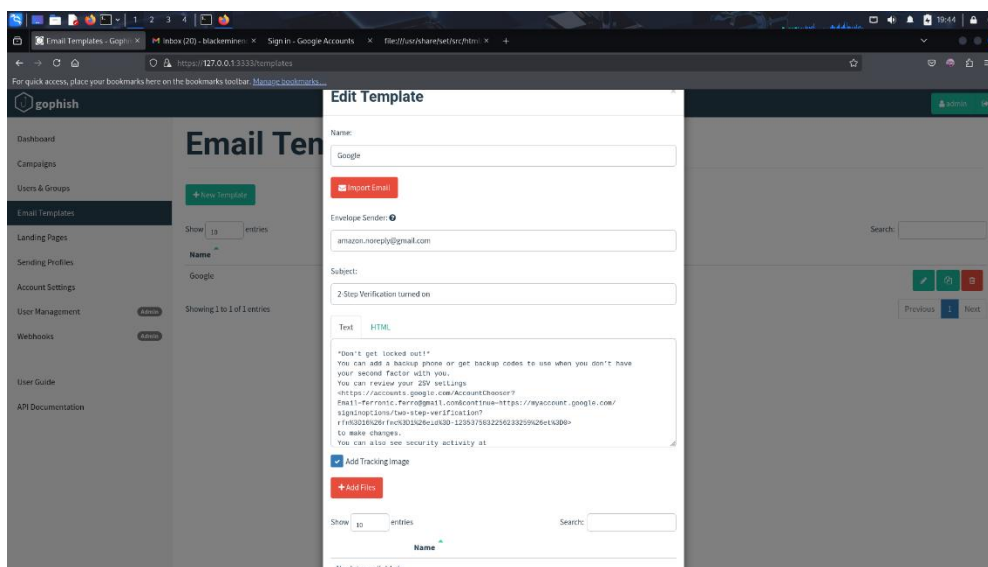
In this example I have copied a google template by using the command :

“cd /usr/share/set/src/html/templates/google “. We can see a file “index.template”. Use the command open “index.template” to open it in your default browser. We can see the UI of google, we copy the source code and then we paste that in our landing page. Then we fill the redirect box to “ <https://accounts.google.com> ” for making it look legitimate after they login. We save this as our current landing page.



We now successfully created the landing page.

We go to the edit template section and by copying an existing email’s original message (In this case I copied the original text of the 2 step verification from my email) we paste it on the import email section.



We then navigate to User and Group section then fill out the details.

The screenshot shows the 'Edit Group' modal in the Gophish application. The modal is titled 'Edit Group' and has a close button in the top right corner. It contains the following fields and options:

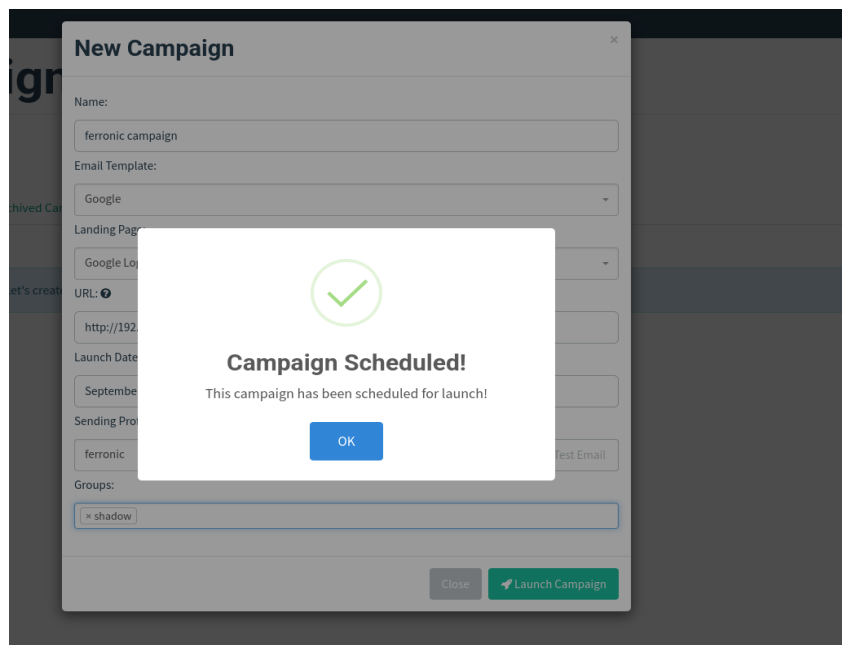
- Name:** A text input field with the value 'shadow'.
- + Bulk Import Users** and **Download CSV Template** buttons.
- First Name**, **Last Name**, **Email**, and **Position** input fields, followed by an **+ Add** button.
- Show** 10 entries and a **Search:** input field.
- A table with columns: **First Name**, **Last Name**, **Email**, and **Position**. The table contains one entry: Black, Shadow, blackeminences..., and a trash icon.
- Showing 1 to 1 of 1 entries** and **Previous** 1 **Next** pagination controls.
- Close** and **Save changes** buttons at the bottom.

In the campaign section we can see the details of our page already retrieved, provide the host's ip address as URL, rename it and select the group to send mails.

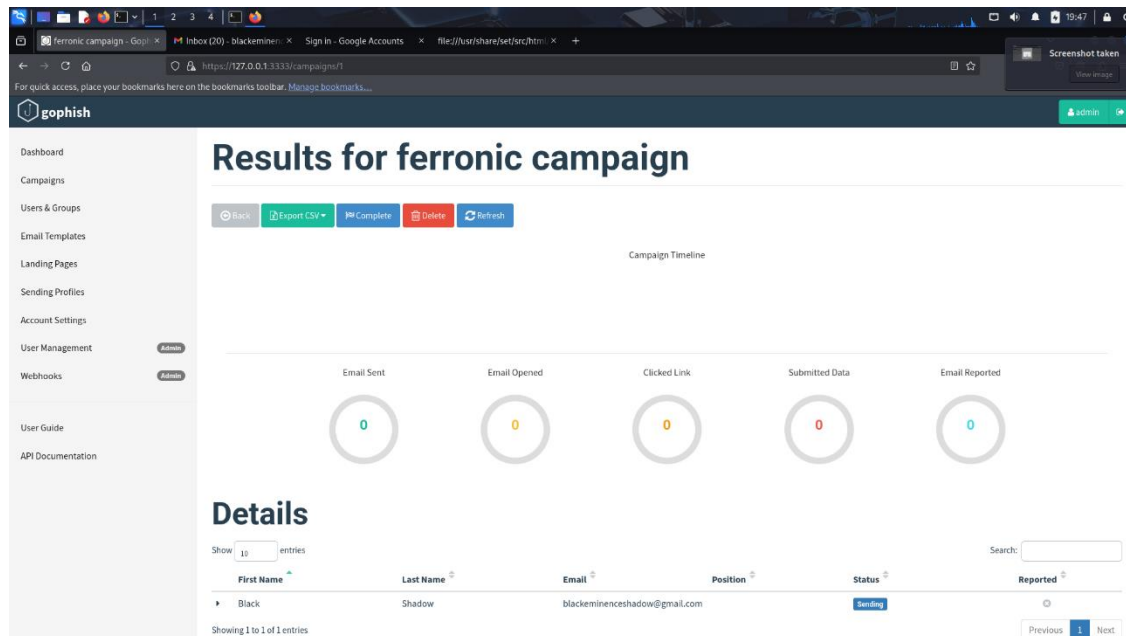
The screenshot shows the 'New Campaign' modal in the Gophish application. The modal is titled 'New Campaign' and has a close button in the top right corner. It contains the following fields and options:

- Name:** A text input field with the value 'ferronic campaign'.
- Email Template:** A dropdown menu with the value 'Google'.
- Landing Page:** A dropdown menu with the value 'Google Login'.
- URL:** A text input field with the value 'http://192.168.29.138'.
- Launch Date:** A date and time picker showing 'September 28th 2025, 7:45 pm'.
- Send Emails By (Optional):** An empty text input field.
- Sending Profile:** A dropdown menu with the value 'ferronic' and a **Send Test Email** button.
- Groups:** A dropdown menu with the value 'shadow'.
- Close** and **Launch Campaign** buttons at the bottom.

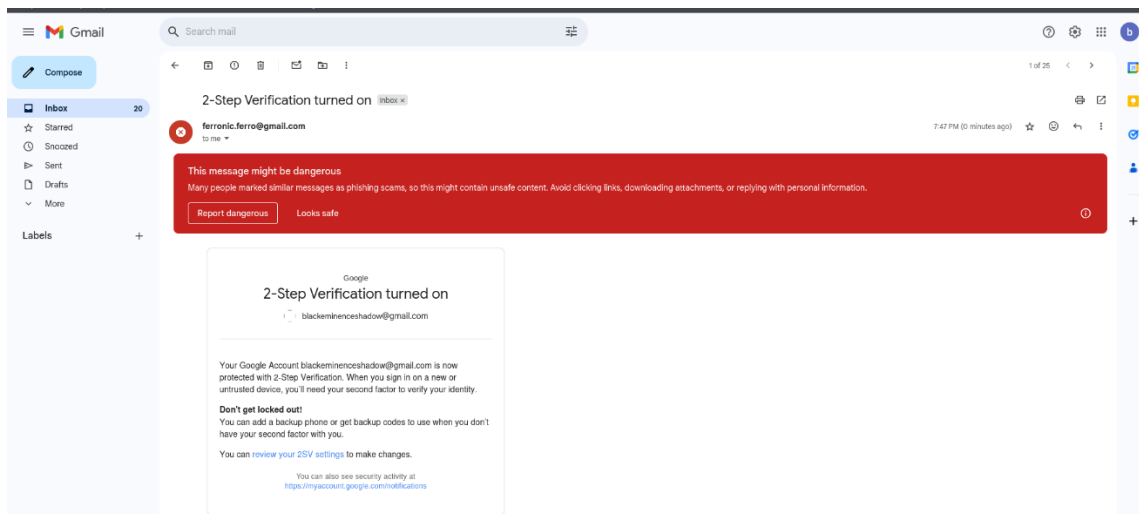
Once we are done with our campaign setup. We can now launch our campaign.



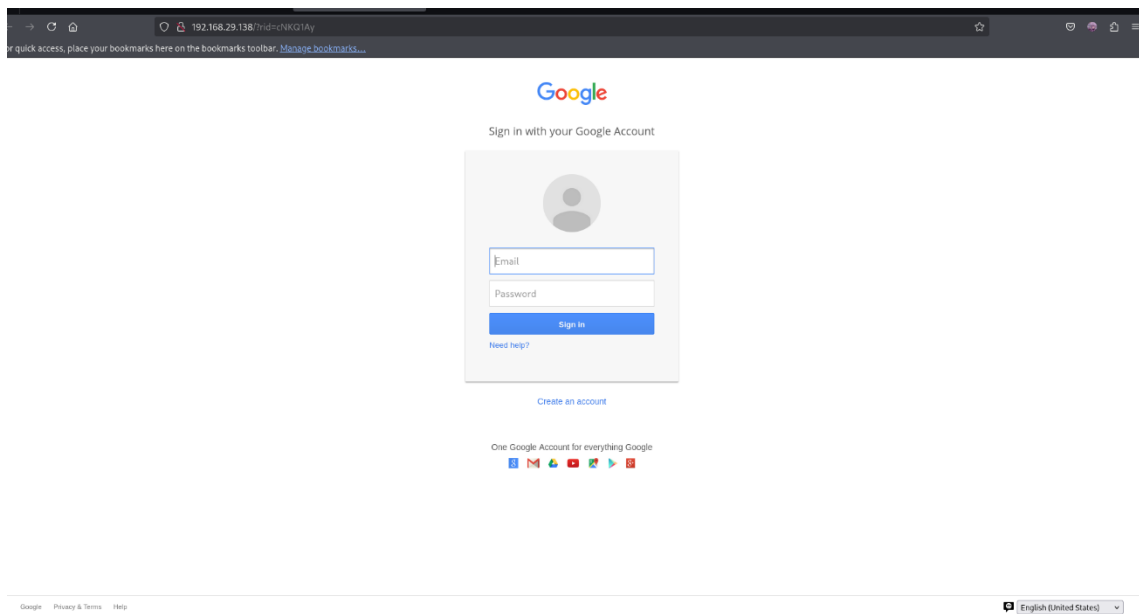
We can then monitor the live reports of the report in our dashboard:



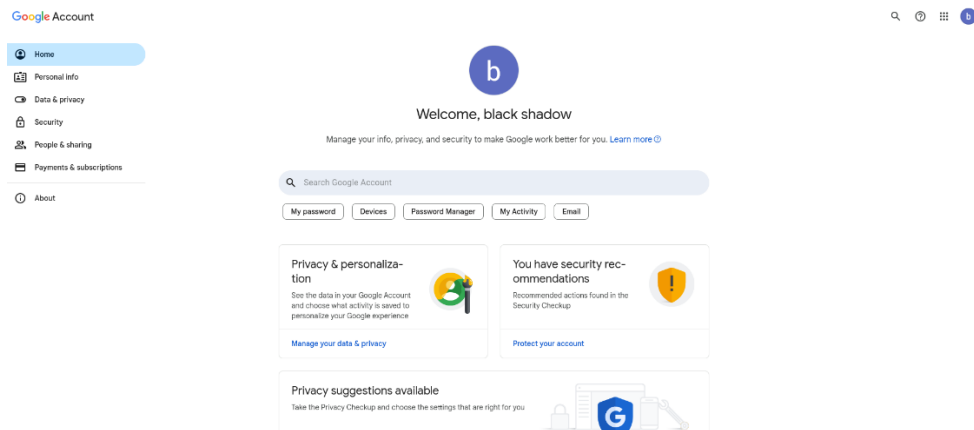
After a quick refresh we can see one mail is sent. When we open the mail we can see the mail we received with a link.



When we click on the link we will then be redirected to the template of the landing page which we created.



Once we enter the credentials, we go to the redirected page of our own Google accounts.



Come back and check the dashboard. We'll get the results for this phishing simulation.

