Task -6:

GoPhish Simulated Phishing Campaign Report

Prepared for: MuLearn Bootcamp

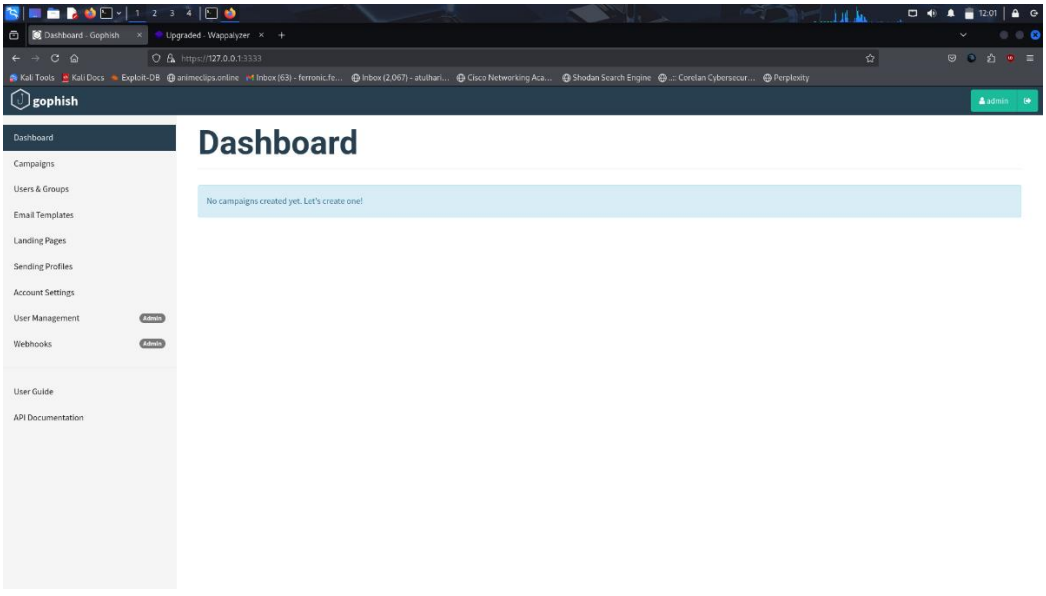
Prepared By: Atul H

Introduction:

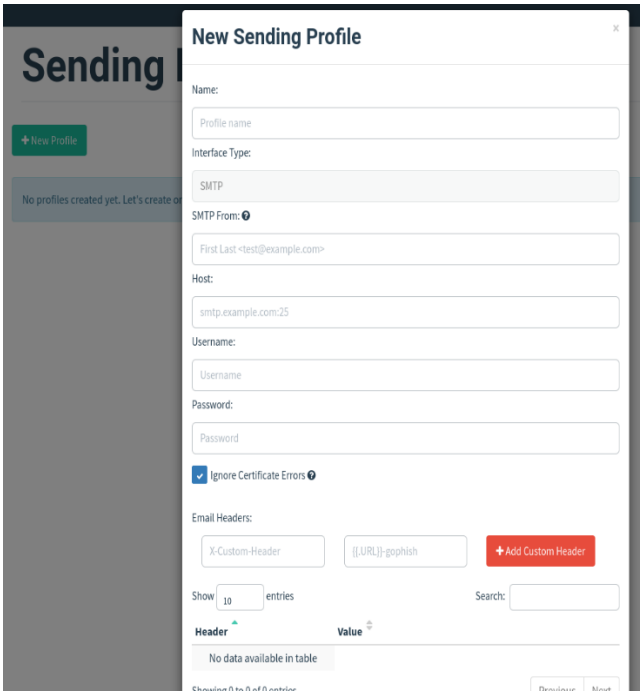
Gophish is a powerful, open-source phishing framework used by security professionals to conduct phishing campaigns and security awareness training. It allows organizations to test their workforce for vulnerabilities by simulating real-world phishing attacks, tracking employee responses, and analyzing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

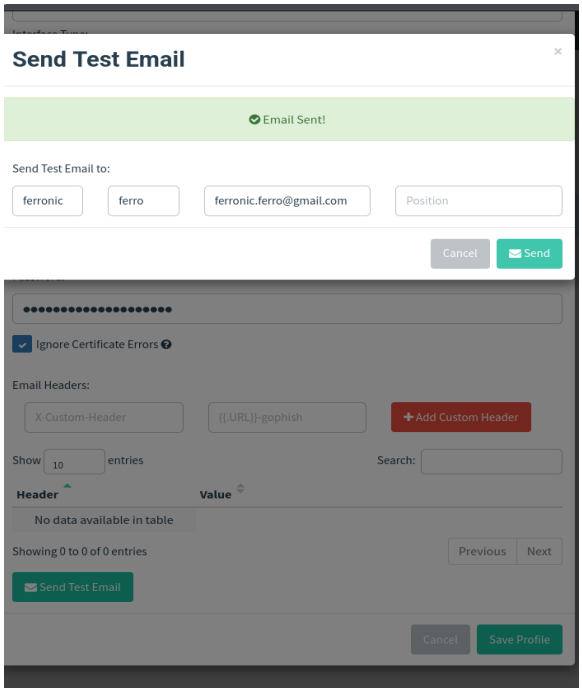
Steps proceeded:

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.



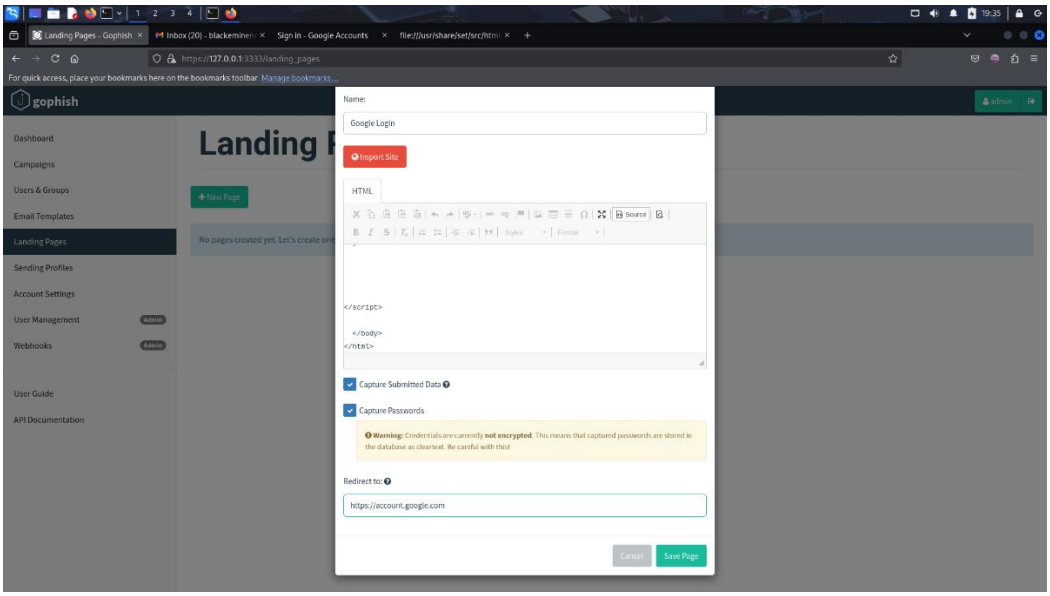
Navigate through the left side. We then select and create the new sending profile.





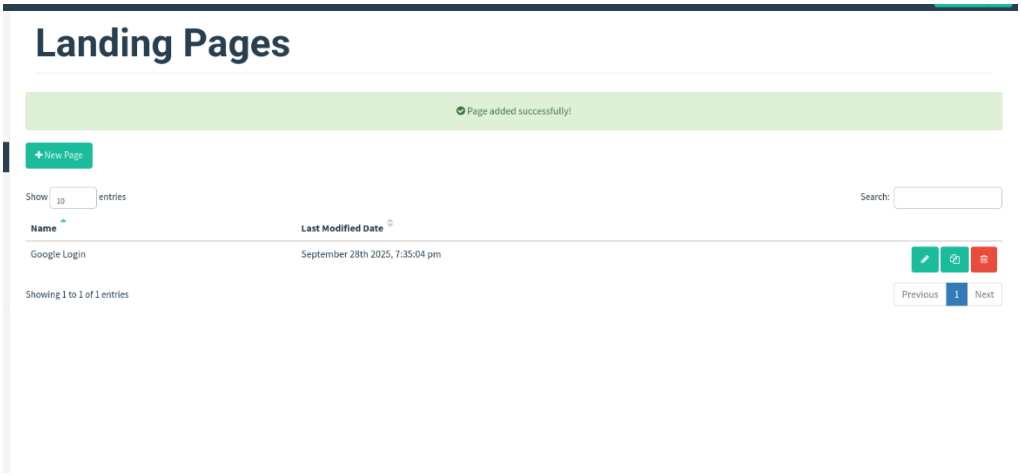
After we fill out the sending profile form, we get to verify our mail is working properly by sending a test mail. Once the email sent! Popup comes we can be sure that our sending profile is all set to go.

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



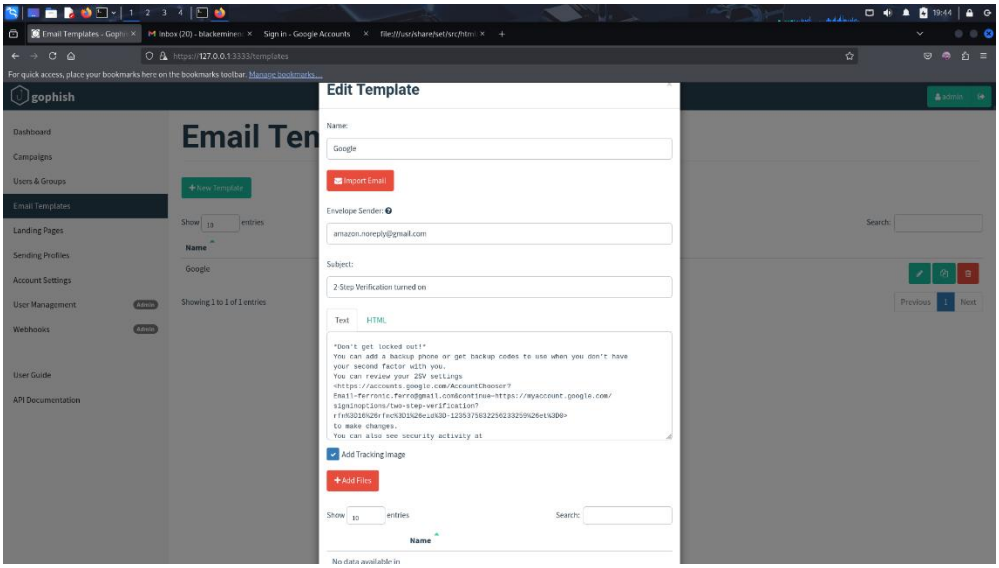
In this example I have copied a google template by using the command :

“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.

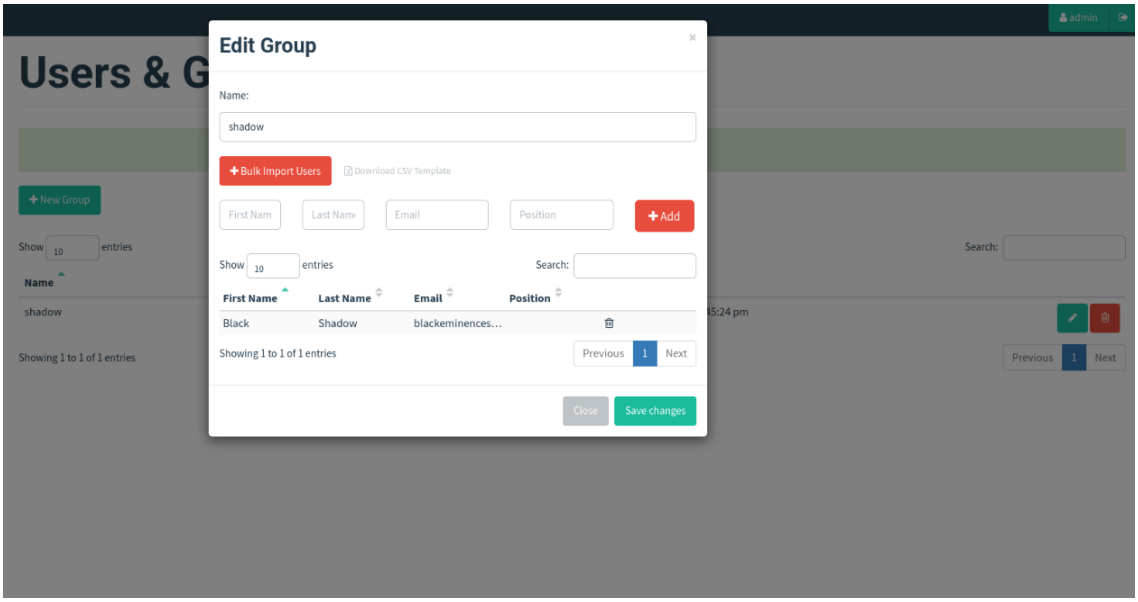


We now successfully created the landing page.

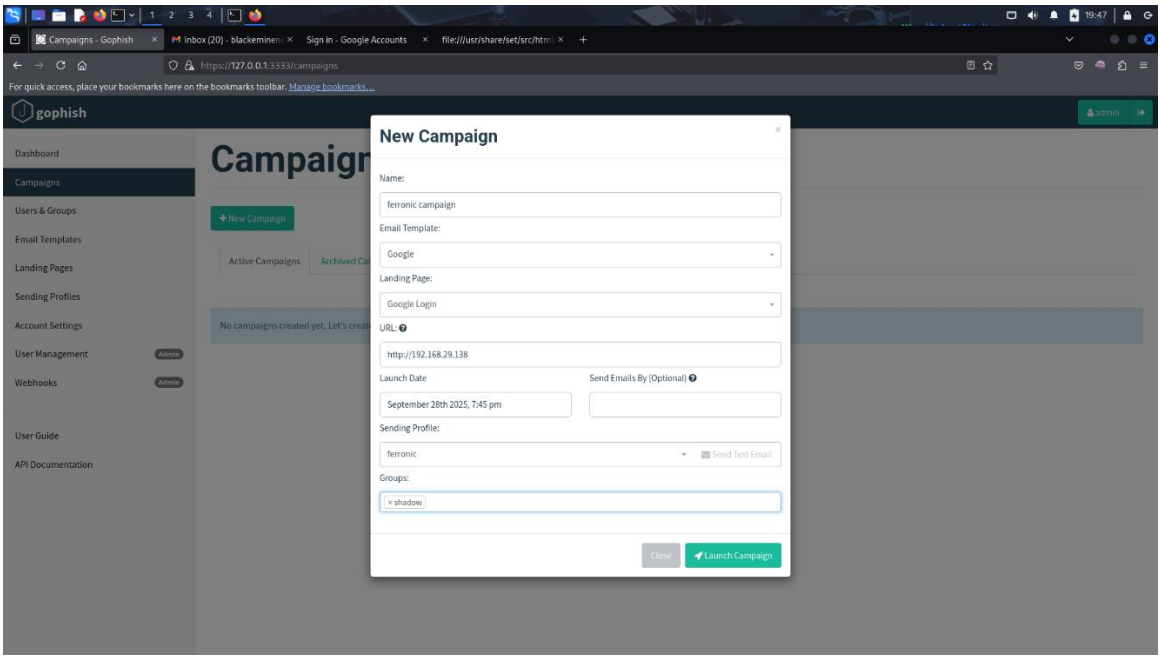
We go to the edit template section and by copying an existing email’s original message (In this case I copied the original text of the 2 step verification from my email) we paste it on the import email section.



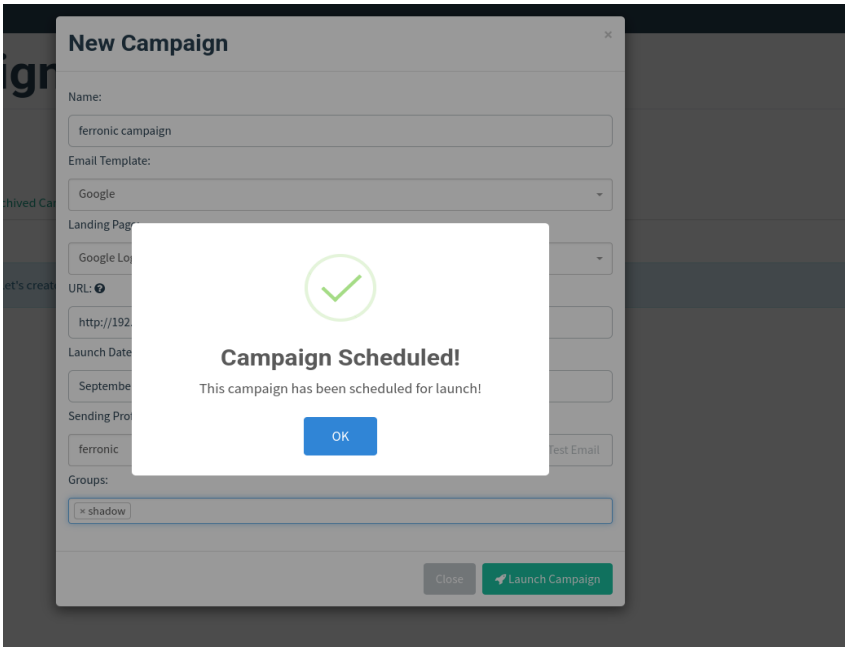
We then navigate to User and Group section then fill out the details.



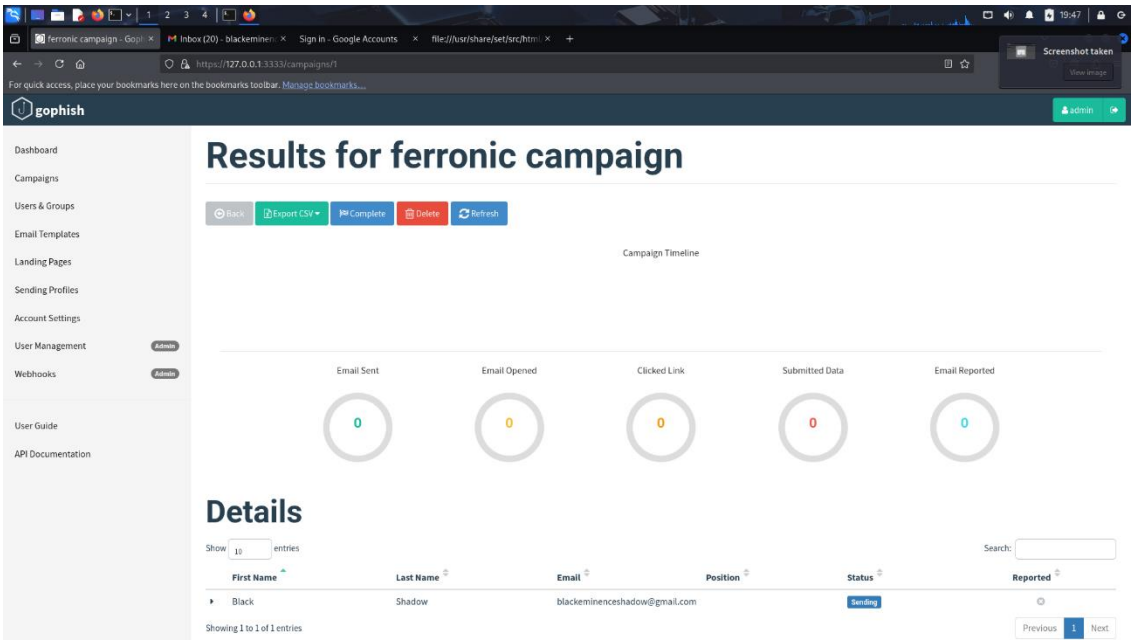
In the campaign section we can see the details of our page already retrieved, provide the host's ip address as URL, rename it and select the group to send mails.



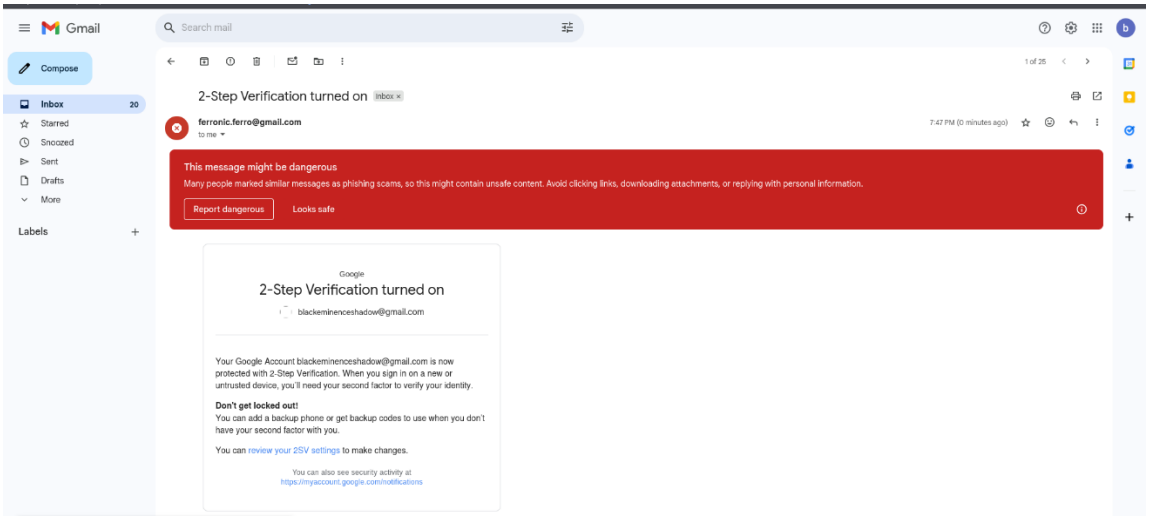
Once we are done with our campaign setup. We can now launch our campaign.



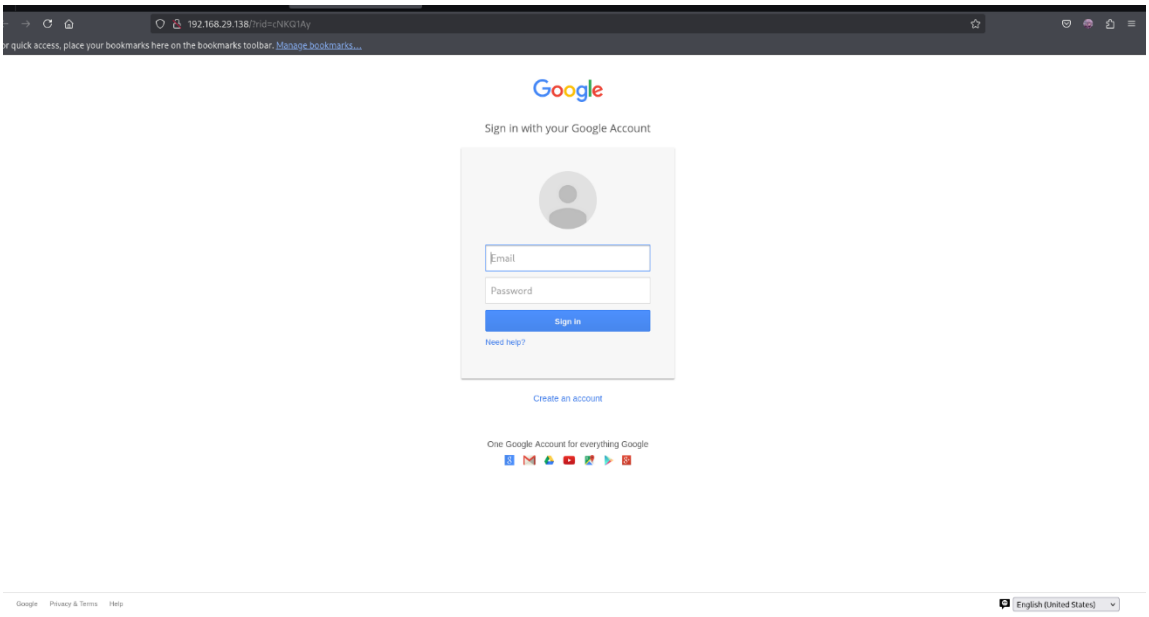
We can then monitor the live reports of the report in our dashboard:



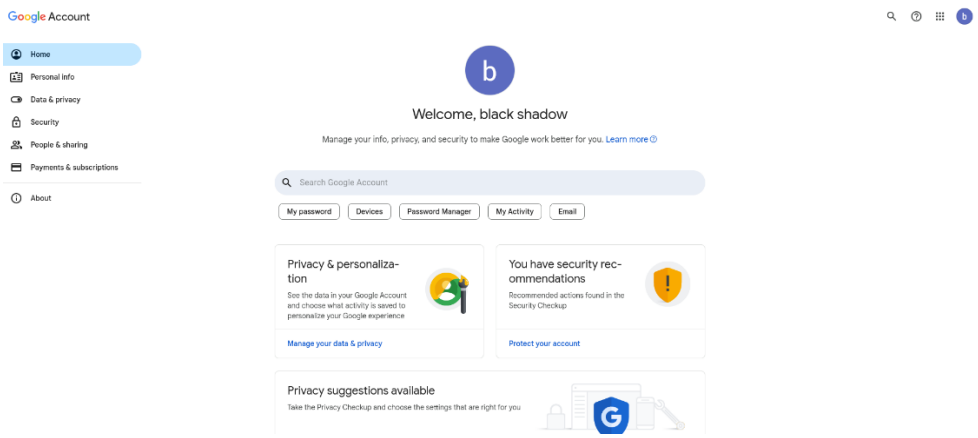
After a quick refresh we can see one mail is sent. When we open the mail we can see the mail we received with a link.



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 goes to the redirected page of our own google accounts.



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