



# CHAMELEON

FOR OUR SMARTER WORLD

Phishing Report  
By Harrison Tierney

## Contents

### Contents

Executive summary: .....	3
Introduction: .....	4
Tools used: .....	4
Kali Linux .....	4
Gophish .....	4
Scope of Testing .....	4
Methodology .....	5
Gophish Utilisation and Methods .....	6
Users and Groups .....	6
Email Template .....	7
Sending Profile .....	8
Campaign Launch .....	10
Results .....	13
Recommendations .....	14
Conclusion .....	14
References .....	15

## Executive summary:

This report acts as a guide to setup a phishing campaign and reports on the need of training and active testing of Chameleon students to aid in the protection of Chameleon assets.

- Tools that are used are covered with pros and cons of the technology and how they can be used to further the cyber security posture of Chameleon.
- Methodology of the testing is covered as we look to engage phishing by utilising a high-profile university lecturer that holds power over the project, promising new services that are needed for the Chameleon team.
- A step-by-step guide in how a phishing campaign can be setup to test student knowledge of phishing practices and how they can protect themselves, and Chameleon assets.
- Recommendations are to begin training of phishing tactics and setup internal phishing campaigns to allow students to determine the need and wants of the training that can be provided later in Chameleons life cycle.

## Introduction:

In this report, we look to test Chameleon students on their knowledge of phishing attacks and tactics that could compromise credentials, leading to damage of Chameleon assets, websites, and source code. This campaign looks to act as a baseline test for the Chameleon group, looking to garner initial data on what is needed from training in the future for Juniors that look to be onboarded in the coming trimesters. This report also details how to setup a campaign through the open-source program Gophish, and how it can be aligned to the needs and wants of Chameleon for future campaigns.

## Tools used:

### Kali Linux

"Kali Linux is an open source, Debian-based Linux distribution geared towards various information tasks such as Penetration testing, Security Research, Computer Forensics and Reverse Engineering." (Kali, n.d.) With previous familiarity with the Kali distribution of Linux, I decided to utilise it for the testing purposes of this report. Not only does Gophish come preinstalled within the distribution, I am also able to run Kali as a virtual machine, aiding in the cost of having a purpose machine with Kali installed to perform the setup, hosting and active launch of a phishing campaign. Kali Linux remains one of, if not, the best environment to perform security testing is.

### Gophish

"Gophish is a powerful, open-source phishing framework that makes it easy to test an organisations exposure to phishing." (Gophish, n.d.) Being an open-source program, it is inherently free to use, helping to cut down overall costs for the project. The ability to locally host Gophish also helps to cut down running costs as the rent or purchase of a new system in the cloud is not needed. Cons of using this program is the lack of end support, due to it being free to use, there is no support line that you can call for assistance other than forums. Along with this, updates to Gophish may come sparingly as those who are working on the program are not paid to do so, leading to longer wait times for bug patching and new features. Another limitation would be the necessity of having all computers/ emails on the same network to be able to successfully utilise the email obfuscation techniques used to get through network defences.

## Scope of Testing

The scope of the testing would be to test emails that have accounts with GitHub that have direct access to the repositories used to build MOP and Chameleon websites. This would be completed by testing either personal emails or emails attached to Deakin. This would utilise a virtual machine to setup the necessary Gophish component.

## Methodology

“Social engineering is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information.” (Carnegie Mellon University, n.d.) Phishing falls directly in line with social engineering, creating a scam tactic to lure in the victim and steal their credentials through faux websites.

Utilising Gophish to craft a phishing email, the attack will contain a link to a credential theft site (hosted locally for test purposes) and will look to lure in Chameleon members and staff with the promise of a new website where they can collaborate and build from in a live environment.

Phishing is ‘a technique for attempting to acquire sensitive data through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person’ (NIST, n.d) Phishing is primarily used for account theft, allowing attackers access to sensitive information or systems without the need to brute force credentials to gain access.

I decided to undertake the phishing campaign to test whether GitHub accounts with access to the source code of the GOP and Chameleon websites were secure from account theft. With the GitHub repository being open to many students, both active and inactive, it is deemed a risk for those students to have insecure passwords that could be brute forced. With all students being within the School of I.T with Deakin, it is assumed that their password roster and rotation is secure and strong, along with necessary precautions and lockouts from GitHub to aid in securing accounts from being brute forced by attackers.

The initial decision was to originally masquerade as one of the Security team leads to build rapport with the email receiver. With this approach, the scope was limited to the Chameleon Security team as most of the other teams within the Chameleon group would not know of the CS Leaders names till notified through the fake email. Instead, Michelle Yu’s current position, power, and knowledge of the internal going’s on of the project to leverage authority to the entire Chameleon team.

Being within the Chameleon team whilst undertaking this campaign, I was able to utilise current pressure points within the team to aid in click through rate and credential submission. These pressure points, at least for the Security team, were the under-utilisation of live test environments and proper infrastructure surrounding the websites currently used for testing. Understanding that most students would like to see new testing environments implemented, the email promised new testing servers, with access coming to those who have signed into their GitHub account through the fake website.

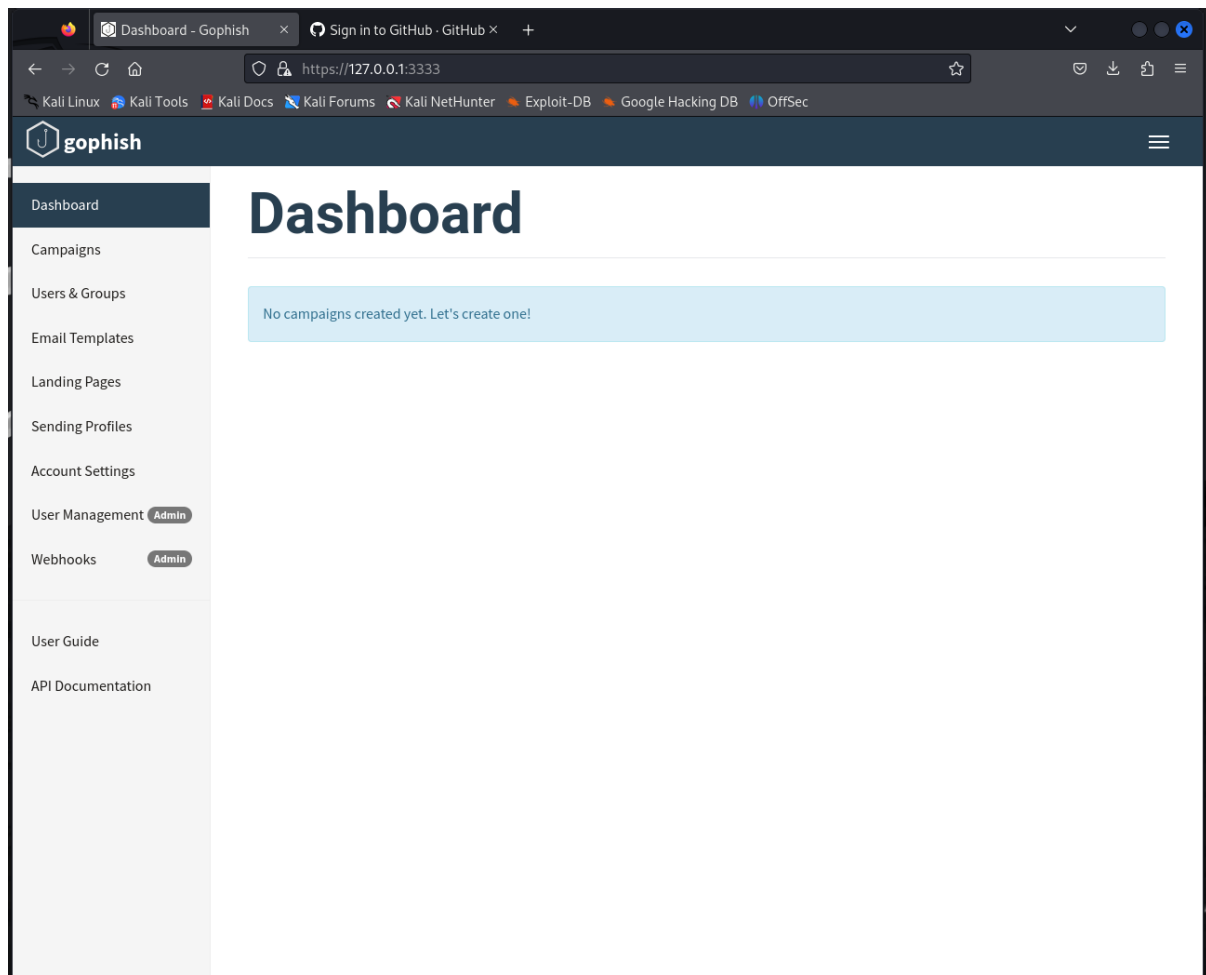
Being that we are already within the team through a controlled environment, we were able to pull the current contributors of the Chameleon and MOP websites and cross reference to ensure correct email addresses were used for targeting. Most students sign up to GitHub with a personal email address. This would provide a barrier for an actual phishing campaign as the attacker won’t be able to guess the standard structure that is provided to Deakin students through their given email (first initial, full last name, @deakin.edu.au)

The initial campaign looks to get a baseline of student’s actions regarding the email, being reporting, clicking through to view the website, or credential input. The results of this will help garner new rules and training that come with being a Chameleon team member.

## Gophish Utilisation and Methods

To aid in the theorisation of the phishing campaign, this will section of the report will be a guide though the steps in how it would be created if it were to go ahead.

Gophish is locally hosted and utilises a graphical interface that allows the user to craft multiple phishing campaigns at one time to help target different subsets of employees.



*Landing Page*

## Users and Groups


When starting from scratch, you first need to create a new “Users” group to be able to send the phishing emails to. I first created a “Chameleon Current Members” group and began to populate the group with current members. This can be done using a CSV file for ease of use, allowing large companies to input employees into Gophish using existing data frames.

Users & Groups - Gophish

Sign in to GitHub - GitHub

https://127.0.0.1:3333/groups

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

gophish

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User Management Admin

Webhooks Admin

User Guide

API Documentation

# Users & Groups

+ New Group

Show  entries

Search:

Name	# of Members	Modified Date
Chameleon Current Members	5	April 10th 2024, 12:52:18 am

Showing 1 to 1 of 1 entries

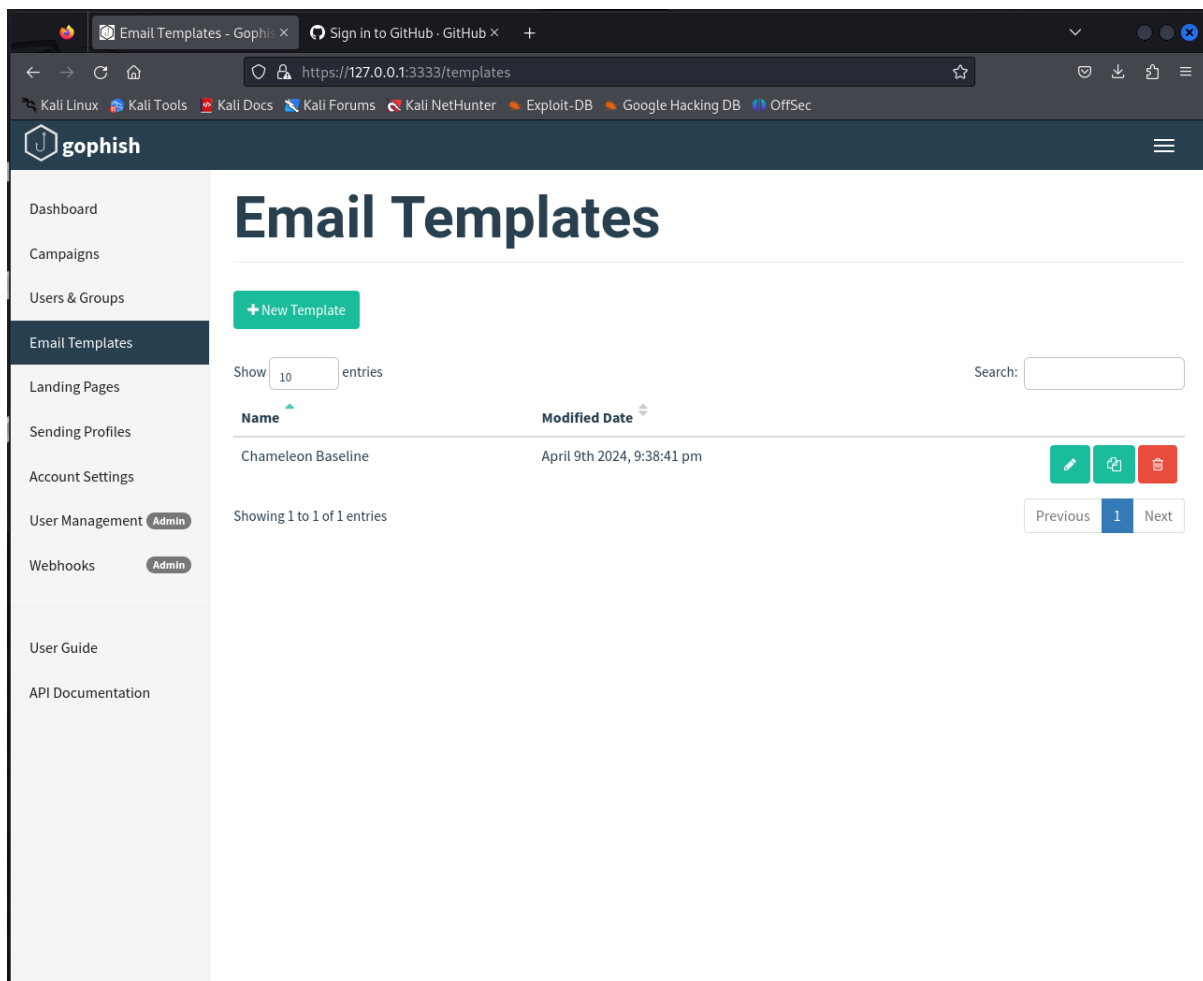
Previous

1

Next

## Email Template

Once a User group has been populated, an email template can be made. Multiple templates can be created to test different groups of users to enhance credibility. For example, testing Graphics Design teams of a business with a free year of Adobe products, as it would be something they would use everyday and are an expensive item.



## Sending Profile

The next action is to create a sending profile, that is used to send the email out to the User within the selected User Group. This is where an admin can custom make a profile to aid in the believability of the email and to ensure that it is not picked up by any network defences that may already be in place. Admins can setup the host for which the emails will be sent from as well as the address that they will come from. This is another step to ensure the campaign is not stopped by network defences before reaching employee inboxes. One is already populated for Michelle Yu, as we will be utilising her identity to make the bait email seem like it is coming from a reputable source.



# New Sending Profile



Name:

Profile name

Interface Type:

SMTP

SMTP From: ?

First Last <test@example.com>

Host:

smtp.example.com:25

Username:

admin

Password:

●●●●●●●●

☒ Ignore Certificate Errors ?

Email Headers:

X-Custom-Header

{{.URL}}-gophish

+ Add Custom Header

Show 10 entries

Search:

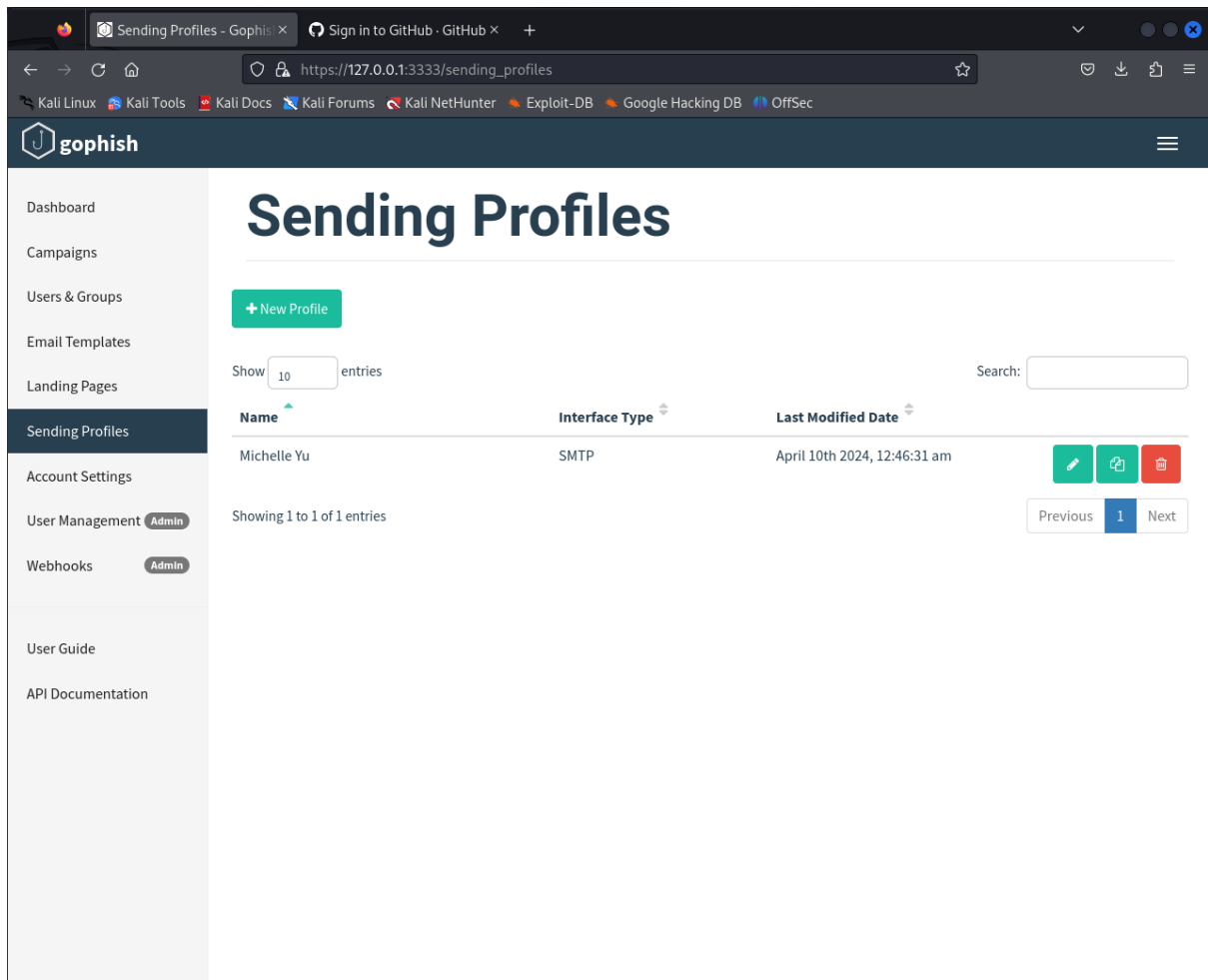
Header	Value
No data available in table	

Showing 0 to 0 of 0 entries

Previous

Next

Send Test Email



## Campaign Launch

One of the last parts of a successful campaign is the creation of a local 'landing page' to assist in the capture of credentials. This is where the link that is sent through the bait email will take anyone that decides to click through. This website is locally, or cloud hosted and needs to imitate the form that would be the desired website that the victim would like to go to. Gophish can import sites that may already be hosted, but the best way is to create your own copy of the target website and host it using local resources. For this example, I am using the GitHub Login page as the imported site, to show its functionality. This page will capture any credentials and passwords that are entered a store them in plaintext on the host system.

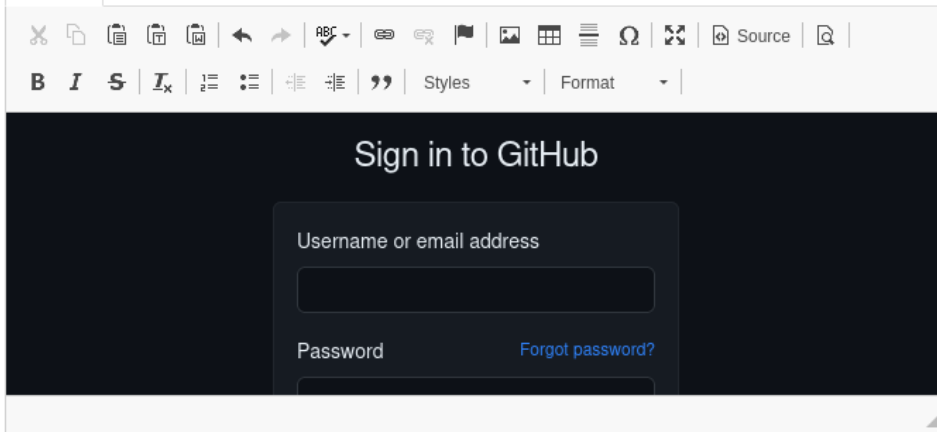
## New Landing Page ✕

Name:

<https://github.com/login>

 Import Site

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: ?

[http://testsite.com/landing\\_page\\_sketchy](http://testsite.com/landing_page_sketchy)

Cancel

Save Page

Campaign launch is the last step to begin the campaign. This is where all the previous setup comes together to from the campaign, making sure to include a listening port on the local device to be able to pick up on activities made during the campaign (click through, reports, credential input etc.) With Gophish, there is the ability to set the campaign to slowly send emails over the course of many days which can help dissuade calls for the email being spam or illegitimate. I have chosen not to do this as the email is crafted to be an announcement, giving it better rapport being an email that is sent out all at once.

## New Campaign



Name:

Chameleon Baeline #1

Email Template:

Chameleon Baseline

Landing Page:

GitHub.com Login Page

URL: ?

http://192.168.1.104

Launch Date

April 10th 2024, 9:42 pm

Send Emails By (Optional) ?

Sending Profile:

Michelle Yu

 Send Test Email

Groups:

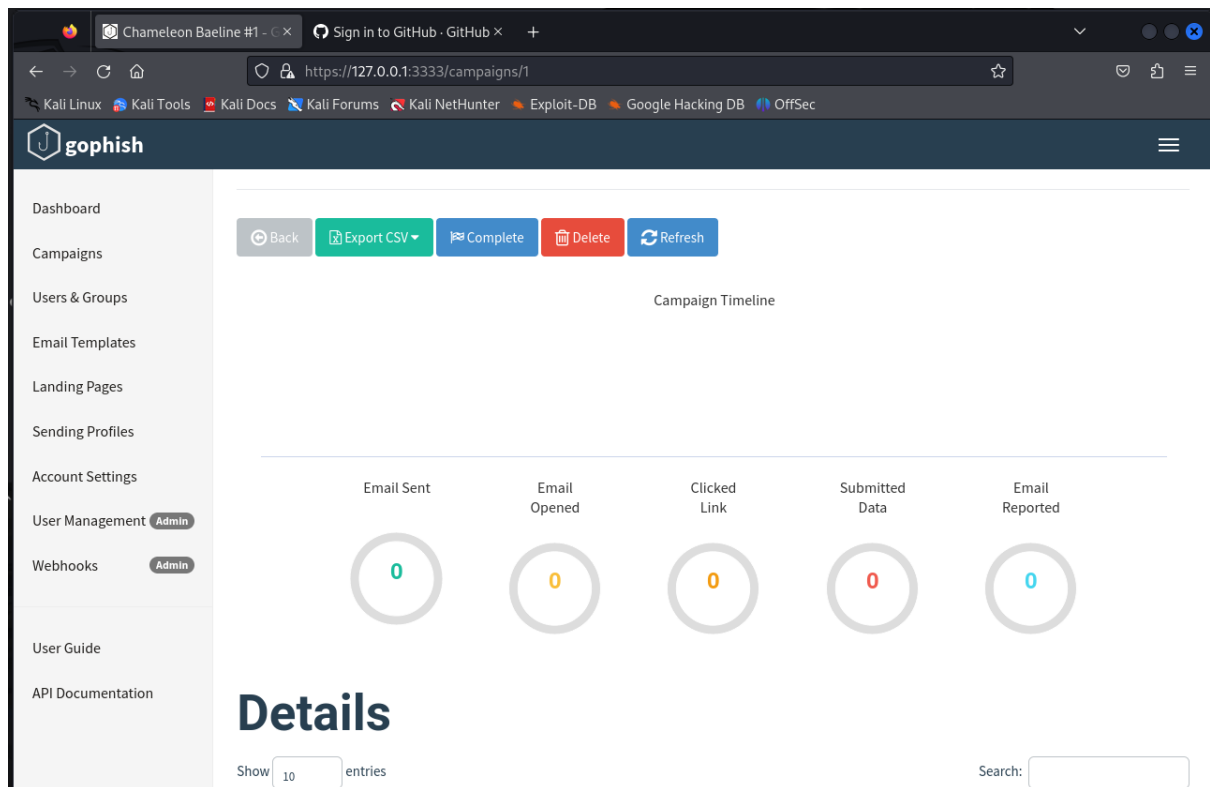
× Chameleon Current Members

Close

 Launch Campaign

## Results

Due to personal email's being the main target of this exercise, we have decided to not undertake the attack as this could compromise personal GitHub accounts. We have instead decided to step through the necessary steps to create the campaign, up to a point of nearly being able to run the campaign. Prior approval would be needed for the campaign to go ahead from every student as it looks to attack a personal email service along with a Deakin email service.



The results page would detail the emails sent and opened, clicked links, data submitted and those who reported the email as suspicious.

## Recommendations

Current recommendations would be to start an internal phishing campaign that tests current students that are part of Chameleon, and to start educating students during the onboarding process to be mindful for fraudulent emails that may want access to Chameleon connected accounts, such as GitHub.

As of this trimester, there is no education around phishing and its practices. For those in the Security division of Chameleon, it comes as second nature how to spot a suspicious email, but we cannot guarantee the safety of other students that occupy positions in other departments. With a safety pack that assists students in understanding the risks of phishing, Chameleon can become more cybersecure and help to cover the necessary knowledge of phishing attempts to protect students and Chameleon from harm that comes from threat actors.

The use of open-source programs would be best suited due to the no cost nature of the software. Gophish has plenty of features to be able to test Chameleon, in terms of its current number of students, and compile data to help shape the training contents for the next group of Junior students that join Chameleon.

## Conclusion

Overall, I believe that Chameleon can benefit from phishing training and subsequent testing to ensure that all Chameleon students are knowledgeable of the dangers that come with phishing scams and the knowledge to protect themselves from credential theft that can lead to damage of Chameleon projects, source code and websites. The use of open-source software enables Chameleon to efficiently setup and test the knowledge of student in how to pick a phishing email, along with keeping running costs of Chameleon down as none of the software previously mentioned has any paywalls for their services.

## References:

National Institute of Standards and Technology (NIST), C.C., n.d. phishing - Glossary | CSRC [WWW Document]. URL <https://csrc.nist.gov/glossary/term/phishing> (accessed 4.10.24).

Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution [WWW Document], 2024. . Kali Linux. URL <https://www.kali.org/> (accessed 4.12.24).

University, C.M., n.d. Social Engineering - Information Security Office - Computing Services - Carnegie Mellon University [WWW Document]. URL <http://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html> (accessed 4.12.24).