

Open-source tools for Social Engineering

AN INTRODUCTION TO TOOLS
AND TECHNIQUES EMPLOYED
FOR SOCIAL ENGINEERING
ATTACKS

Saroj Gopali

June 1, 2023





Social Engineering Tools

- **Social Engineering Toolkit (SET)**
- **Sherlock**
- **Zphisher**
- **Gophish**
- **Maltego**
- **Metasploit Framework (MSF)**

Sherlock

- A robust command-line tool offered by the Sherlock Project
- A tool that allows you to search for social media accounts associated with a specific username across multiple social networks.
- <https://github.com/sherlock-project/sherlock>

```
(root@kali)-[/home/saroj/Downloads/workshop/sherlock]
# python3 sherlock hackerman
[*] Checking username hackerman on:

[+] 9GAG: https://www.9gag.com/u/hackerman
[+] About.me: https://about.me/hackerman
[+] Academia.edu: https://independent.academia.edu/hackerman
[+] Anilist: https://anilist.co/user/hackerman/
[+] Apple Developer: https://developer.apple.com/forums/profile/hackerman
[+] Apple Discussions: https://discussions.apple.com/profile/hackerman
[+] Archive of Our Own: https://archiveofourown.org/users/hackerman
[+] Archive.org: https://archive.org/details/@hackerman
[+] Asciinema: https://asciinema.org/~hackerman
[+] AskFM: https://ask.fm/hackerman
[+] Bandcamp: https://www.bandcamp.com/hackerman
[+] Behance: https://www.behance.net/hackerman
[+] BitBucket: https://bitbucket.org/hackerman/
[+] Blogger: https://hackerman.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/hackerman
[+] CGTrader: https://www.cgtrader.com/hackerman
[+] Career.habr: https://career.habr.com/hackerman
[+] Championat: https://www.championat.com/user/hackerman
[+] Chess: https://www.chess.com/member/hackerman
[+] Clapper: https://clapperapp.com/hackerman
[+] Clubhouse: https://www.clubhouse.com/@hackerman
[+] Codecademy: https://www.codecademy.com/profiles/hackerman
[+] Codeforces: https://codeforces.com/profile/hackerman
[+] Codewars: https://www.codewars.com/users/hackerman
[+] Crowdin: https://crowdin.com/profile/hackerman
```


Zphisher

- Zphisher is a powerful open-source tool an automated Phishing Tool.
- Zphisher is a tool of Kali Linux.
- Zphisher creates phishing pages of popular sites such as Facebook, Instagram, Google, Snapchat, Github, Yahoo, Protonmail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc
- <https://github.com/htr-tech/zphisher>

```

Zphisher
Version : 2.3.5
[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch          [21] DeviantArt
[02] Instagram     [12] Pinterest       [22] Badoo
[03] Google        [13] Snapchat        [23] Origin
[04] Microsoft     [14] LinkedIn        [24] DropBox
[05] Netflix       [15] Ebay            [25] Yahoo
[06] Paypal        [16] Quora           [26] Wordpress
[07] Steam         [17] Protonmail      [27] Yandex
[08] Twitter       [18] Spotify         [28] StackoverFlow
[09] Playstation  [19] Reddit          [29] Vk
[10] Tiktok        [20] Adobe           [30] XBOX
[31] Mediafire     [32] Gitlab          [33] Github
[34] Discord       [35] Roblox

[99] About        [00] Exit

[-] Select an option : █
```

Hands on Experience Zphisher -Facebook

```
root@kali: ~/home/saroj/Downloads/workshop/zphisher
File Actions Edit View Help
Zphisher
Version : 2.3.5
[-] Tool Created by htr-tech (tahmid.rayat)
[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch      [21] DeviantArt
[02] Instagram     [12] Pinterest  [22] Badoo
[03] Google        [13] Snapchat   [23] Origin
[04] Microsoft     [14] LinkedIn   [24] DropBox
[05] Netflix       [15] Ebay       [25] Yahoo
[06] Paypal        [16] Quora      [26] Wordpress
[07] Steam         [17] Protonmail [27] Yandex
[08] Twitter       [18] Spotify    [28] StackoverFlow
[09] Playstation  [19] Reddit     [29] Vk
[10] Tiktok        [20] Adobe      [30] XBOX
[31] Mediafire     [32] Gitlab     [33] Github
[34] Discord       [35] Roblox

[99] About        [00] Exit

[-] Select an option : 01

[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page

[-] Select an option : 01
```

```
root@kali: ~/home/saroj/Downloads/workshop/zphisher
File Actions Edit View Help
ZPHISHER
2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]

[-] Select a port forwarding service : 02

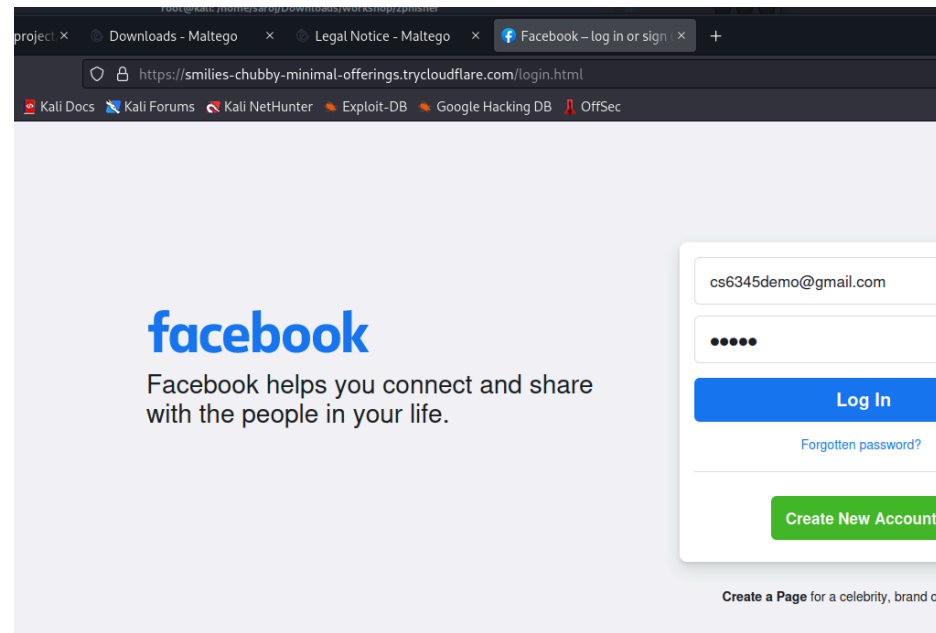
[?] Do You Want A Custom Port [y/N]: N

[-] Using Default Port 8080 ...

[-] Initializing... ( http://127.0.0.1:8080 )
```

Hands on Experience Zphisher -Facebook

```
root@kali: /home/saroj/Downloads/workshop/zphisher
File Actions Edit View Help
ZPHISHER 2.3.5
[-] URL 1 : https://smilies-chubby-minimal-offerings.trycloudflare.com
[-] URL 2 : https://is.gd/T7sCZw
[-] URL 3 : https://faceboook.com@is.gd/T7sCZw
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP : 99.64.54.20
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
34.83.203.92IP : 34.83.203.92
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : cs6345demo@gmail.com
[-] Password : saroj
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit. █
```



* ONLY FOR EDUCATION PURPOSE

Gophish

- A phishing toolkit with the aim of making robust security awareness training accessible to all individuals..
- A phishing framework simplifies the simulation of real-world phishing attacks..
- Gophish is an open-source software that offers free accessibility, making it an affordable option for all users.
- Accessible - Gophish, written in Go, provides easy installation with compiled binaries and no dependencies, simplifying the process to just "download and run"!
- <https://github.com/gophish/gophish>



Hands on Experience Gophish

- Start gophish server in local .
- https://SERVER_IP:3333
- enter the default login credentials
- Default username: Admin
- Default password: random text

```
root@kali: /home/saroj/Downloads/workshop/gophish
File Actions Edit View Help
(root@kali)~/Downloads/workshop/gophish
# ./gophish
time="2023-05-22T21:30:41-05:00" level=warning msg="No contact address has been configured."
time="2023-05-22T21:30:41-05:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2023-05-22T21:30:41-05:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
time="2023-05-22T21:30:41-05:00" level=info msg="Starting IMAP monitor manager"
time="2023-05-22T21:30:41-05:00" level=fatal msg="listen tcp 127.0.0.1:3333: bind: address already in use"
(root@kali)~/Downloads/workshop/gophish
#
```



**Please sign
in**

Username
Password
Sign in

Hands on Experience

Gophish

- Create Email template .
- Provide the template name.
- Provide subject.
- Provide template email body.

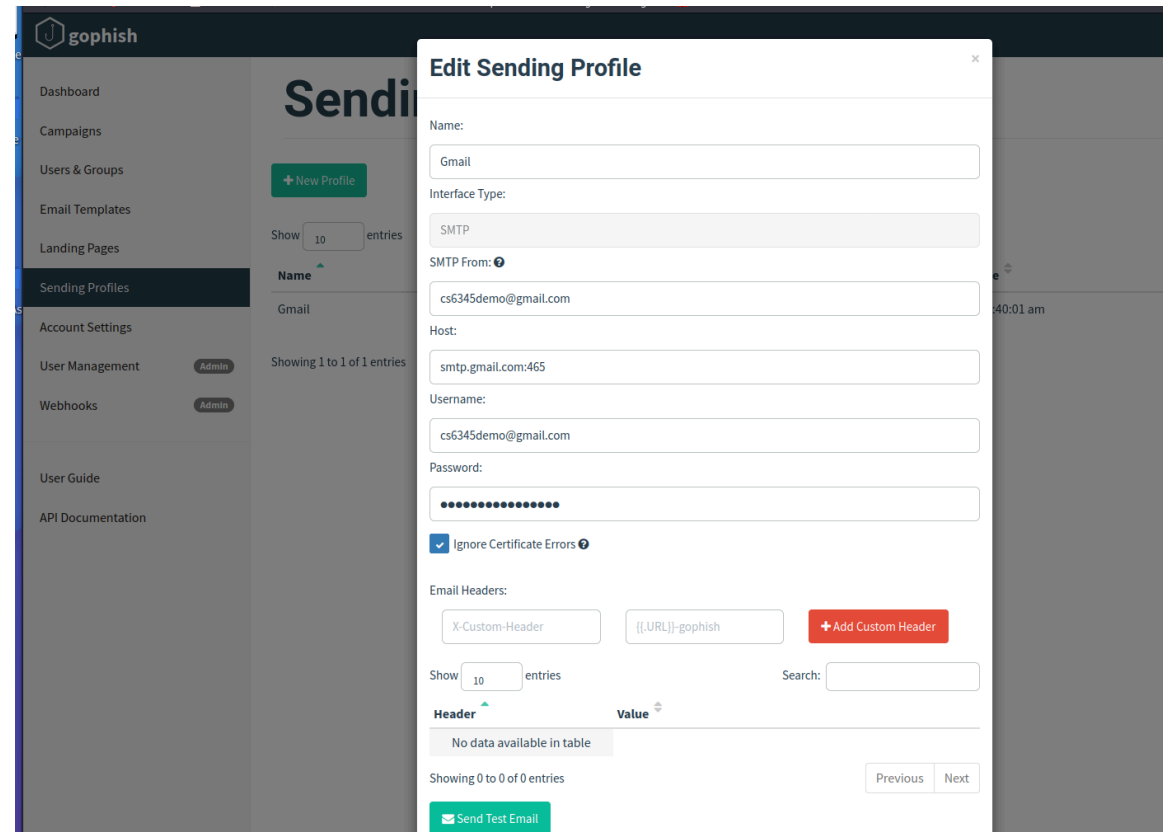
The screenshot displays the Gophish web interface with the 'Email Templates' section active. An 'Edit Template' modal is open, showing the following fields and options:

- Name:** Password Reset for {{.Email}}
- Import Email:** A red button to import an existing email template.
- Envelope Sender:** First Last <test@example.com>
- Subject:** Password Reset for {{.Email}}
- Text/HTML:** A toggle switch with 'HTML' selected.
- Body:** A text area containing the email body:

```
{{.FirstName}},  
The password for {{.Email}} has expired. Please reset your password here.  
Thanks,  
Your IT Team
```
- Add Tracking Image:** An unchecked checkbox.
- Add Files:** A red button to add files to the email.
- Show:** A dropdown menu set to '10' entries.
- Search:** A search bar.
- Name:** A dropdown menu.
- No data available in:** A message at the bottom of the modal.

Hands on Experience Gophish

- Create Sending Profile.
- Provide the template name.
- Provide SMTP from .
- Provide Host to send email.
- Provide your email as username.
- Provide password not login one, one from app password.



The screenshot shows the Gophish web interface with the 'Edit Sending Profile' modal open. The left sidebar contains navigation links: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles (active), Account Settings, User Management, Webhooks, User Guide, and API Documentation. The main content area shows the 'Sending Profiles' section with a '+ New Profile' button and a table listing existing profiles. The 'Edit Sending Profile' modal is a white box with a close button in the top right. It contains the following fields: 'Name' (text input with 'Gmail' entered), 'Interface Type' (dropdown menu with 'SMTP' selected), 'SMTP From' (text input with 'cs6345demo@gmail.com' entered), 'Host' (text input with 'smtp.gmail.com:465' entered), 'Username' (text input with 'cs6345demo@gmail.com' entered), 'Password' (password input field with dots), and a checked checkbox for 'Ignore Certificate Errors'. Below these is an 'Email Headers' section with a table showing one header: 'X-Custom-Header' with value '{{URL}}-gophish'. There is a '+ Add Custom Header' button. At the bottom of the modal are 'Previous' and 'Next' buttons, and a green 'Send Test Email' button.

Edit Sending Profile

Name:

Interface Type:

SMTP From:

Host:

Username:

Password:

☒ Ignore Certificate Errors

Email Headers:

Header	Value
X-Custom-Header	{{URL}}-gophish

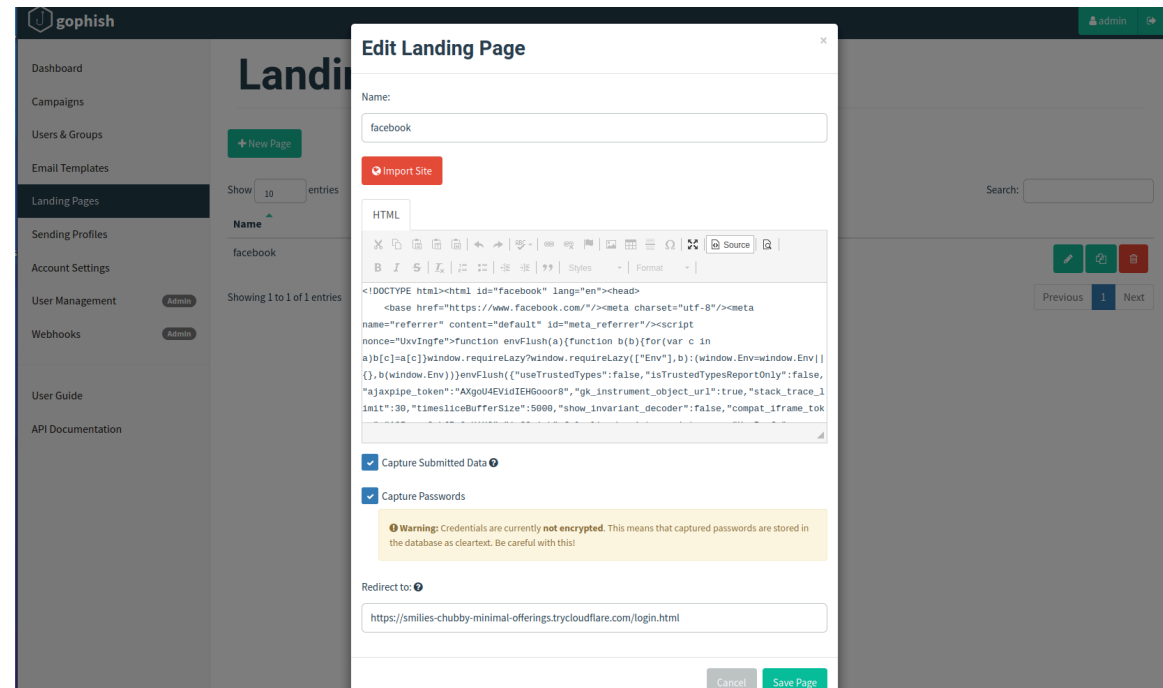
Show entries Search:

No data available in table

Showing 0 to 0 of 0 entries

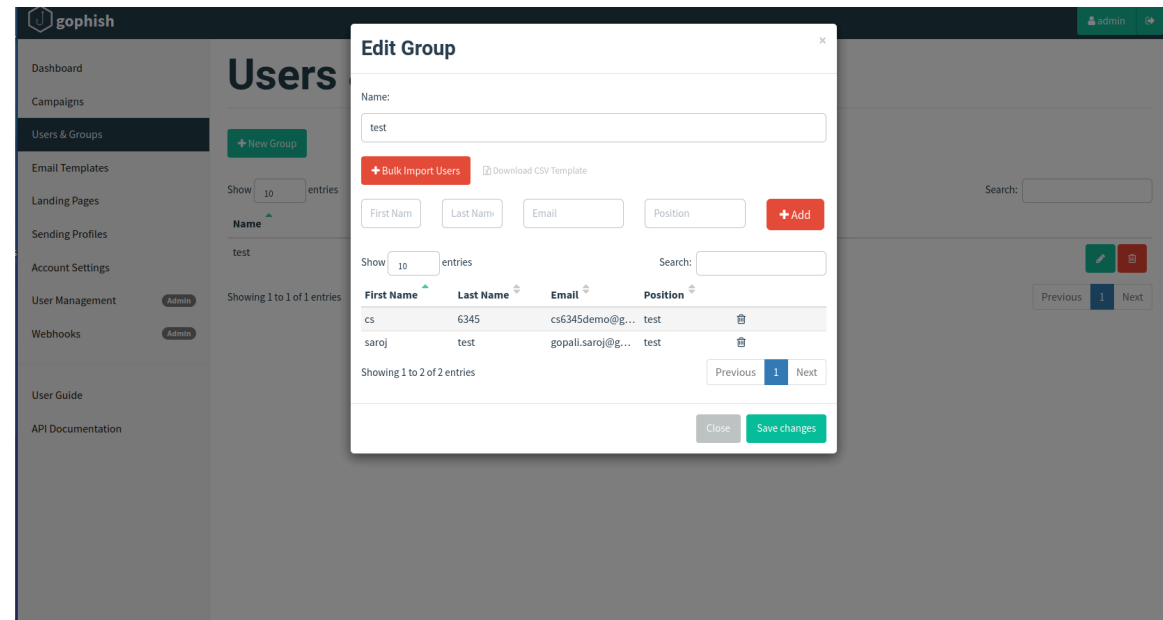
Hands on Experience Gophish

- Create Landing page.
- Provide the template name.
- Provide source of simulate page or real page where users will attempt to log in to change password in the example .



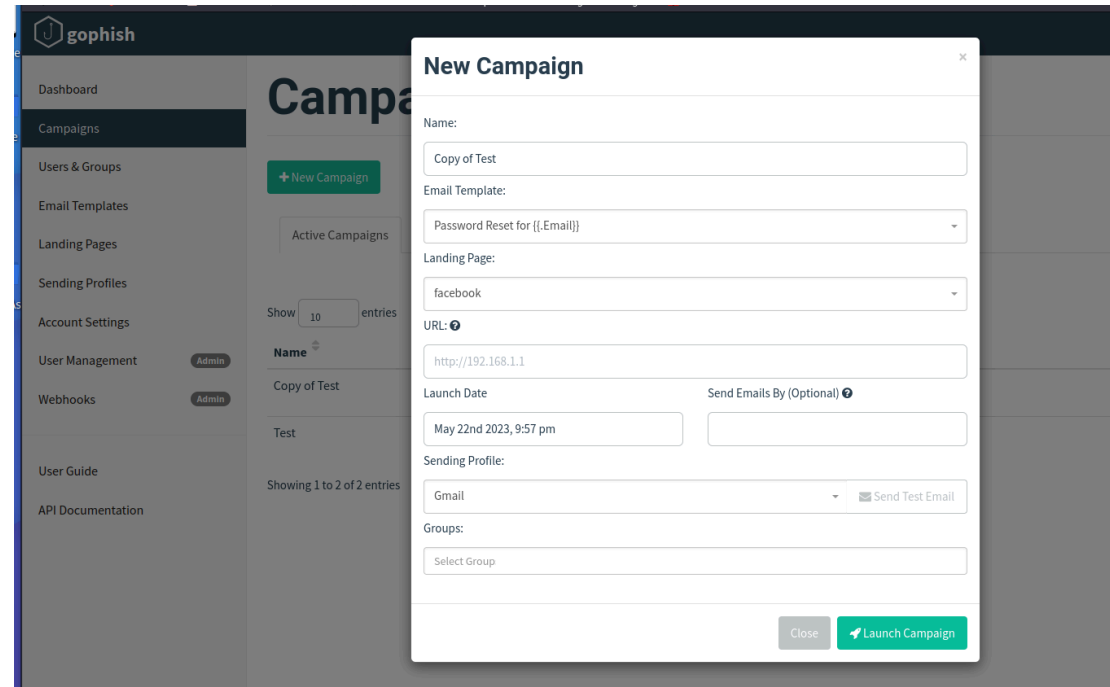
Hands on Experience Gophish

- Create users and group.
- Add the emails where you want to send emails during campaign .



Hands on Experience Gophish

- Create campaign.
- Provide the campaign name for monitor.
- Provide email template from email template section.
- Provide url where user is redirected once click.
- Provide sending profile.
- Provide groups to send the email.



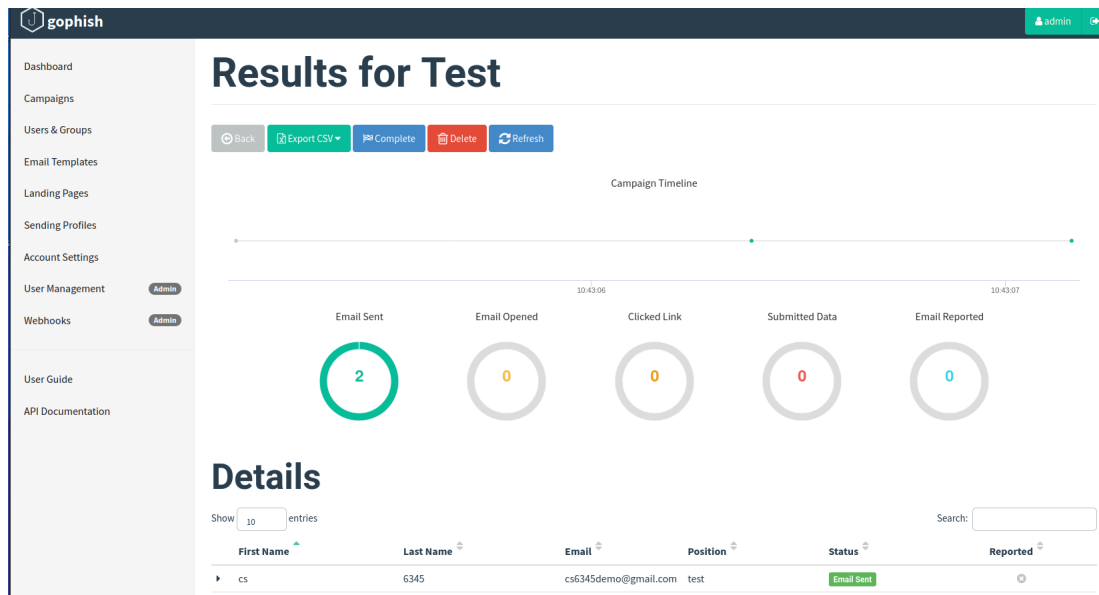
The screenshot shows the Gophish web interface with a 'New Campaign' modal open. The modal contains the following fields and options:

- Name:** Text input with 'Copy of Test' entered.
- Email Template:** Dropdown menu with 'Password Reset for {{.Email}}' selected.
- Landing Page:** Dropdown menu with 'facebook' selected.
- URL:** Text input with 'http://192.168.1.1' entered.
- Launch Date:** Date and time picker showing 'May 22nd 2023, 9:57 pm'.
- Send Emails By (Optional):** Empty text input.
- Sending Profile:** Dropdown menu with 'Gmail' selected, and a 'Send Test Email' button.
- Groups:** Text input with 'Select Group' placeholder.

At the bottom right of the modal are 'Close' and 'Launch Campaign' buttons.


Hands on Experience Gophish

- Monitor campaign.



- Test email from campaign.

Password Reset for cs6345demo@gmail.com Inbox x

 cs6345demo@gmail.com
to me ▾

CS ,

The password for cs6345demo@gmail.com has expired. Please reset your password here.

[Click here!!](#)

Thanks,

Your IT Team