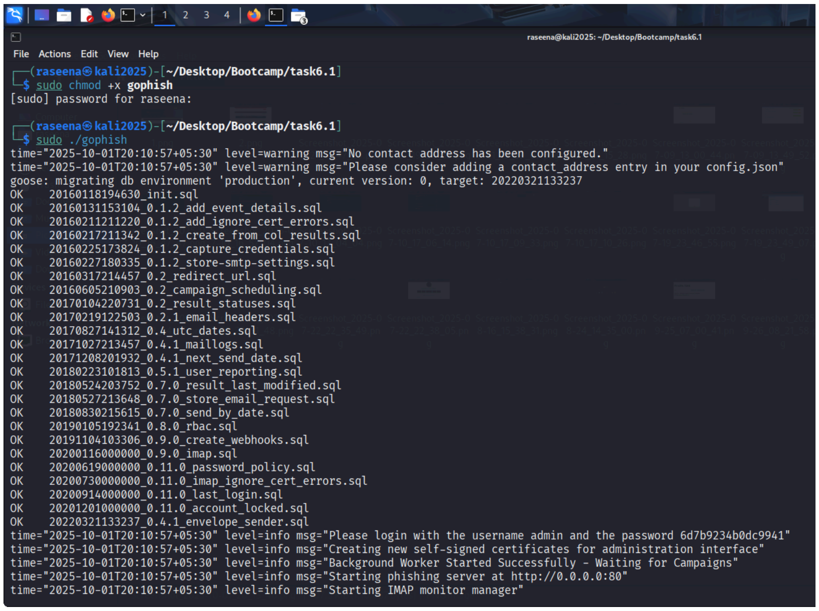
Gophish Simulated Phishing Campaign Report

Prepared by: Raseena. R

Date: October 1, 2025

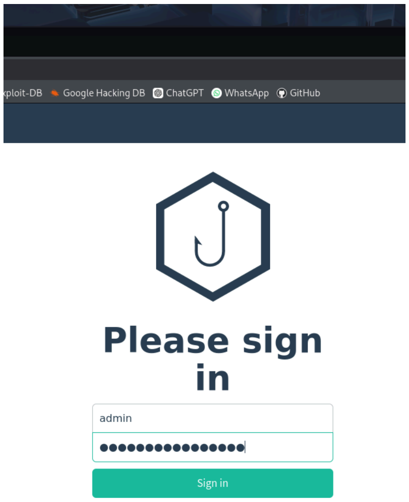
Executive Summary

This report documents the execution of a simulated phishing campaign using the **Gophish** open-source framework inside a controlled **Kali Linux virtual machine** environment. Each step is explained and supported with screenshots for clarity.



raseena@kali2025: ~/Desktop/Bootcamp/task6.1
File Actions Edit View Help

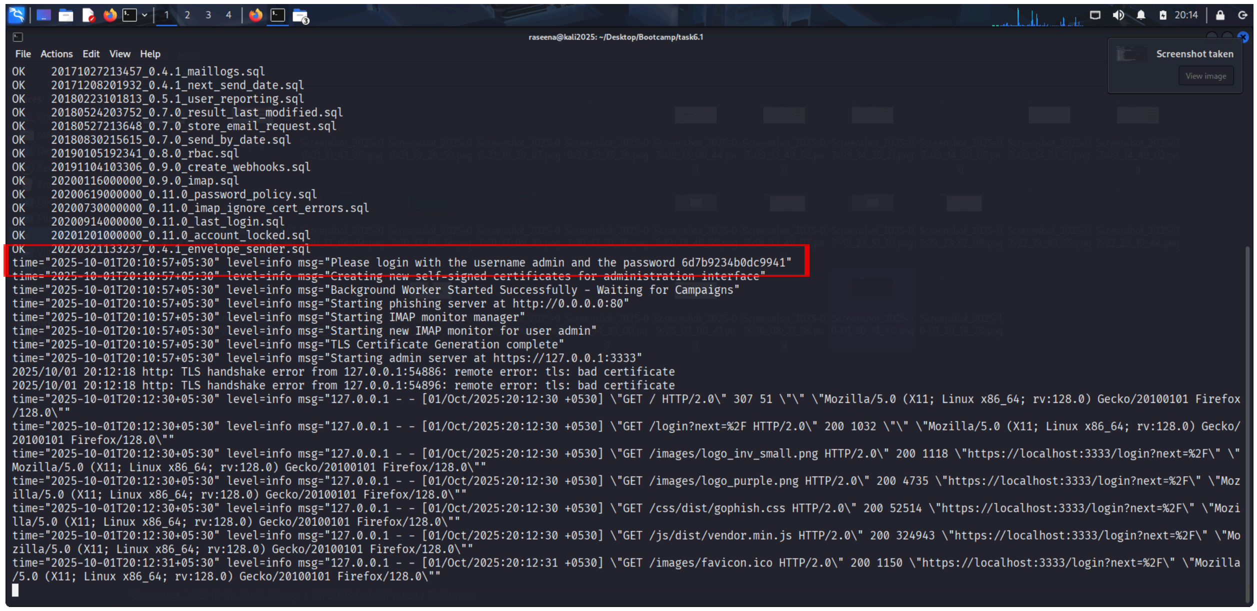
```
┌──(raseena㉿kali2025)-[~/Desktop/Bootcamp/task6.1]
└─$ sudo chmod +x gophish
[sudo] password for raseena:

┌──(raseena㉿kali2025)-[~/Desktop/Bootcamp/task6.1]
└─$ sudo ./gophish
time="2025-10-01T20:10:57+05:30" level=warning msg="No contact address has been configured."
time="2025-10-01T20:10:57+05:30" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: migrating db environment 'production', current version: 0, target: 20220321133237
OK    20160118194630_init.sql
OK    20160131153104_0.1.2_add_event_details.sql
OK    20160211211220_0.1.2_add_ignore_cert_errors.sql
OK    20160217211342_0.1.2_create_from_col_results.sql
OK    20160225173824_0.1.2_capture_credentials.sql
OK    20160227180335_0.1.2_store-smtp-settings.sql
OK    20160317214457_0.2_redirect_url.sql
OK    20160605210903_0.2_campaign_scheduling.sql
OK    20170104220731_0.2_result_statuses.sql
OK    20170219122503_0.2.1_email_headers.sql
OK    20170827141312_0.4_utc_dates.sql
OK    20171027213457_0.4.1_maillogs.sql
OK    20171208201932_0.4.1_next_send_date.sql
OK    20180223101813_0.5.1_user_reporting.sql
OK    20180524203752_0.7.0_result_last_modified.sql
OK    20180527213648_0.7.0_store_email_request.sql
OK    20180830215615_0.7.0_send_by_date.sql
OK    20190105192341_0.8.0_rbac.sql
OK    20191104103306_0.9.0_create_webhooks.sql
OK    20200116000000_0.9.0_imap.sql
OK    20200619000000_0.11.0_password_policy.sql
OK    20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK    20200914000000_0.11.0_last_login.sql
OK    20201201000000_0.11.0_account_locked.sql
OK    20220321133237_0.4.1_envelope_sender.sql
time="2025-10-01T20:10:57+05:30" level=info msg="Please login with the username admin and the password 6d7b9234b0dc9941"
time="2025-10-01T20:10:57+05:30" level=info msg="Creating new self-signed certificates for administration interface"
time="2025-10-01T20:10:57+05:30" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-10-01T20:10:57+05:30" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-10-01T20:10:57+05:30" level=info msg="Starting IMAP monitor manager"
```



Please sign in

admin

●●●●●●●●●●●●●●●●

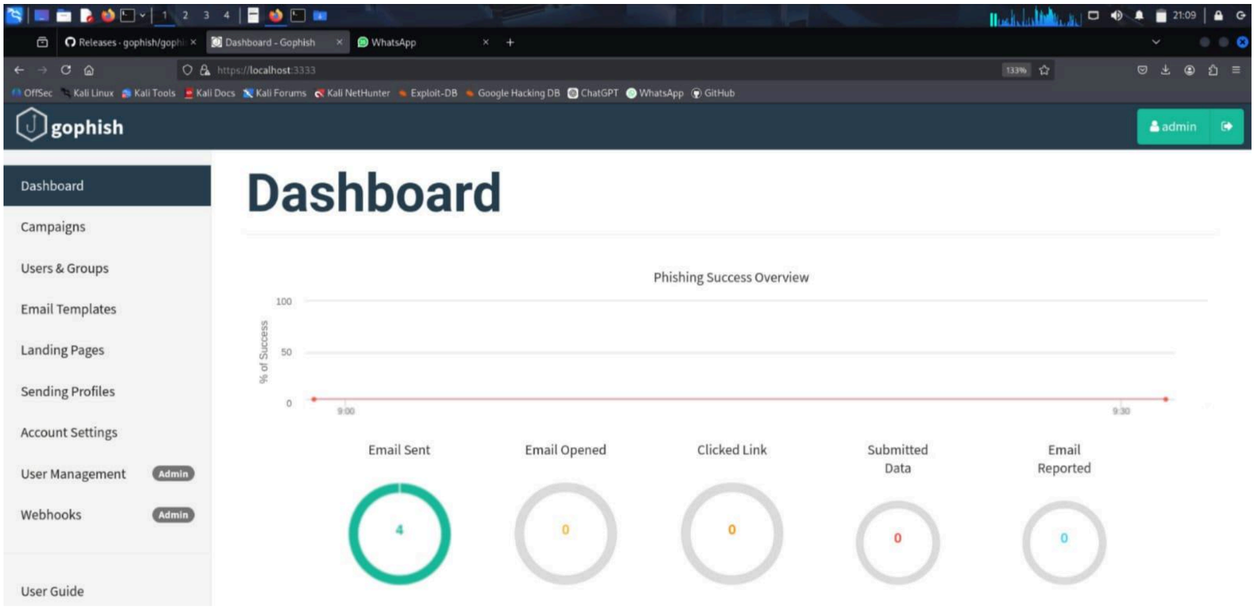


20:14
raseena@kali2025: ~/Desktop/Bootcamp/task6.1
File Actions Edit View Help
Screenshot taken
View image

```
OK    20171027213457_0.4.1_maillogs.sql
OK    20171208201932_0.4.1_next_send_date.sql
OK    20180223101813_0.5.1_user_reporting.sql
OK    20180524203752_0.7.0_result_last_modified.sql
OK    20180527213648_0.7.0_store_email_request.sql
OK    20180830215615_0.7.0_send_by_date.sql
OK    20190105192341_0.8.0_rbac.sql
OK    20191104103306_0.9.0_create_webhooks.sql
OK    20200116000000_0.9.0_imap.sql
OK    20200619000000_0.11.0_password_policy.sql
OK    20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK    20200914000000_0.11.0_last_login.sql
OK    20201201000000_0.11.0_account_locked.sql
OK    20220321133237_0.4.1_envelope_sender.sql
time="2025-10-01T20:10:57+05:30" level=info msg="Please login with the username admin and the password 6d7b9234b0dc9941"
time="2025-10-01T20:10:57+05:30" level=info msg="Creating new self-signed certificates for administration interface"
time="2025-10-01T20:10:57+05:30" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-10-01T20:10:57+05:30" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-10-01T20:10:57+05:30" level=info msg="Starting IMAP monitor manager"
time="2025-10-01T20:10:57+05:30" level=info msg="Starting new IMAP monitor for user admin"
time="2025-10-01T20:10:57+05:30" level=info msg="TLS Certificate Generation complete"
time="2025-10-01T20:10:57+05:30" level=info msg="Starting admin server at https://127.0.0.1:3333"
2025/10/01 20:12:18 http: TLS handshake error from 127.0.0.1:54886: remote error: tls: bad certificate
2025/10/01 20:12:18 http: TLS handshake error from 127.0.0.1:54896: remote error: tls: bad certificate
time="2025-10-01T20:12:30+05:30" level=info msg="127.0.0.1 - - [01/Oct/2025:20:12:30 +0530] \"GET / HTTP/2.0\" 307 51 \"\" \"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox
/128.0\""
time="2025-10-01T20:12:30+05:30" level=info msg="127.0.0.1 - - [01/Oct/2025:20:12:30 +0530] \"GET /login?next=%2F HTTP/2.0\" 200 1032 \"\" \"Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/
20100101 Firefox/128.0\""
time="2025-10-01T20:12:30+05:30" level=info msg="127.0.0.1 - - [01/Oct/2025:20:12:30 +0530] \"GET /images/logo_inv_small.png HTTP/2.0\" 200 1118 \"https://localhost:3333/login?next=%2F\" \"
Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\""
time="2025-10-01T20:12:30+05:30" level=info msg="127.0.0.1 - - [01/Oct/2025:20:12:30 +0530] \"GET /images/logo_purple.png HTTP/2.0\" 200 4735 \"https://localhost:3333/login?next=%2F\" \"Moz
illa/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\""
time="2025-10-01T20:12:30+05:30" level=info msg="127.0.0.1 - - [01/Oct/2025:20:12:30 +0530] \"GET /css/dist/gophish.css HTTP/2.0\" 200 52514 \"https://localhost:3333/login?next=%2F\" \"Mozi
lla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\""
time="2025-10-01T20:12:30+05:30" level=info msg="127.0.0.1 - - [01/Oct/2025:20:12:30 +0530] \"GET /js/dist/vendor.min.js HTTP/2.0\" 200 324943 \"https://localhost:3333/login?next=%2F\" \"Mo
zilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\""
time="2025-10-01T20:12:31+05:30" level=info msg="127.0.0.1 - - [01/Oct/2025:20:12:31 +0530] \"GET /images/favicon.ico HTTP/2.0\" 200 1150 \"https://localhost:3333/login?next=%2F\" \"Mozilla
/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\""
```

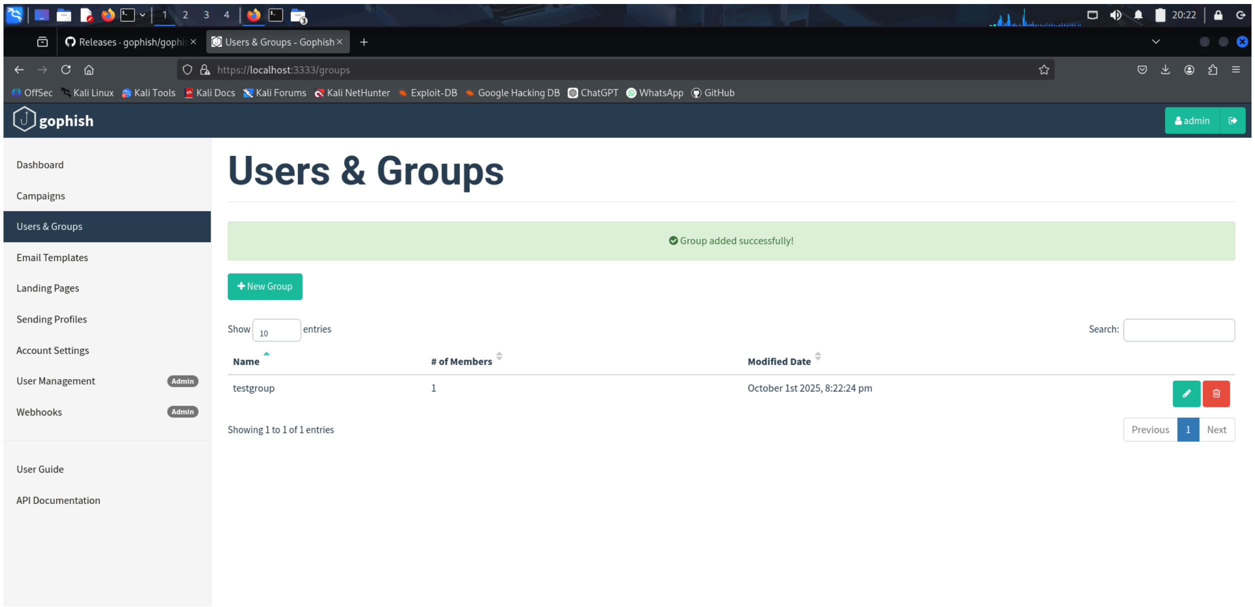
1. Gophish Setup and Dashboard

Gophish was accessed through its **web-based dashboard** on Kali Linux. The dashboard provides an overview of campaigns, including email statistics such as **sent, opened, clicked, submitted, and reported**.



2. Creating User Groups

A test group was created in the "**Users & Groups**" section. This group contained test accounts which acted as phishing targets for the campaign.



Users & Groups

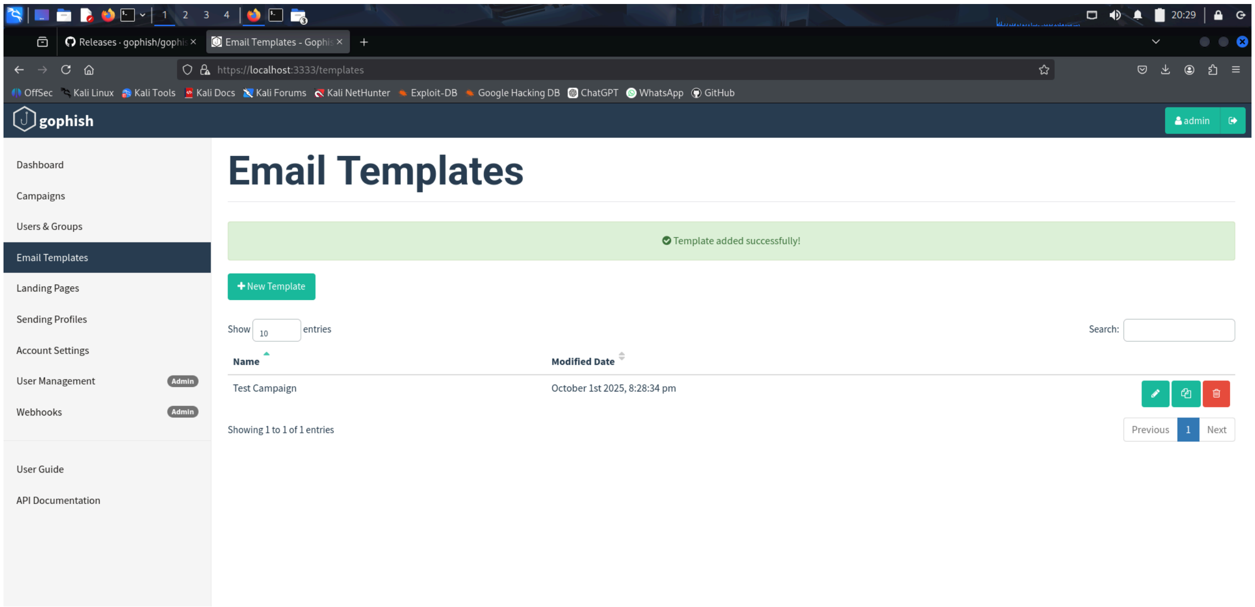
Group added successfully!

Name	# of Members	Modified Date
testgroup	1	October 1st 2025, 8:22:24 pm

Showing 1 to 1 of 1 entries

3. Email Template Creation

A phishing **email template** was designed in the “Email Templates” section. The email was made to look urgent and professional, tricking users into clicking a **malicious link**.



Email Templates

Template added successfully!

+ New Template

Show 10 entries

Search:

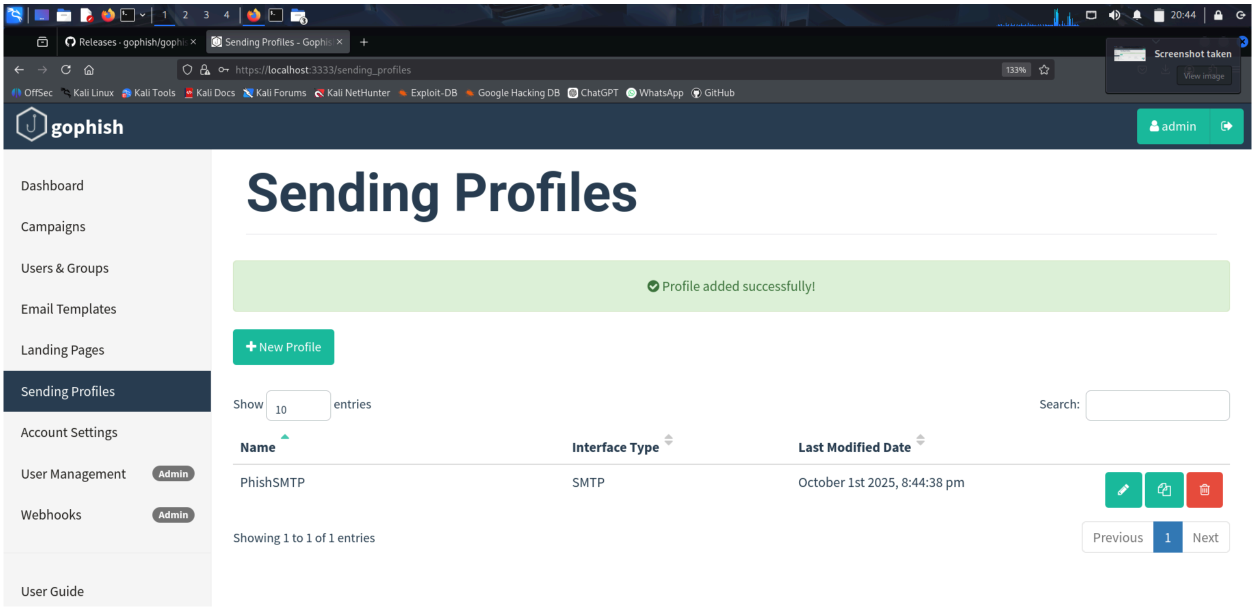
Name	Modified Date
Test Campaign	October 1st 2025, 8:28:34 pm

Showing 1 to 1 of 1 entries

Previous 1 Next

4. Sending Profile Configuration

A **sending profile** was set up with SMTP details so that the phishing emails appeared to come from a legitimate account. This helped make the attack more convincing.



Sending Profiles

Profile added successfully!

+ New Profile

Show 10 entries

Search:

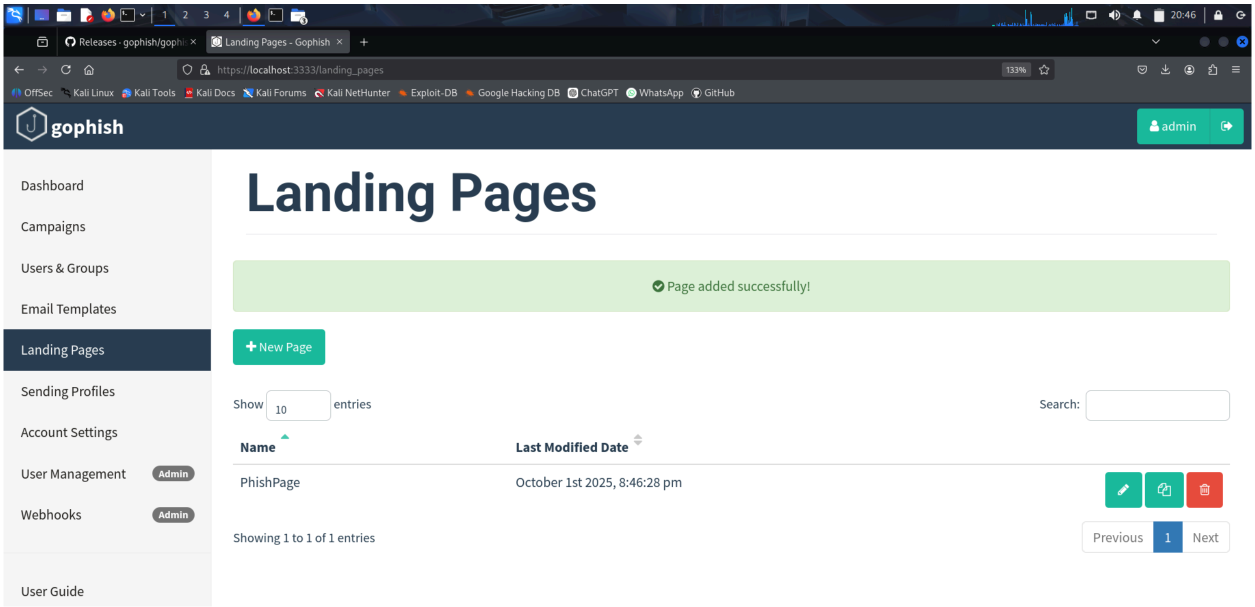
Name	Interface Type	Last Modified Date
PhishSMTP	SMTP	October 1st 2025, 8:44:38 pm

Showing 1 to 1 of 1 entries

Previous 1 Next

5. Landing Page Design

A custom **landing page** was created for harvesting credentials. If a target clicked the phishing link, they were redirected to this page and prompted to submit sensitive information.



Landing Pages

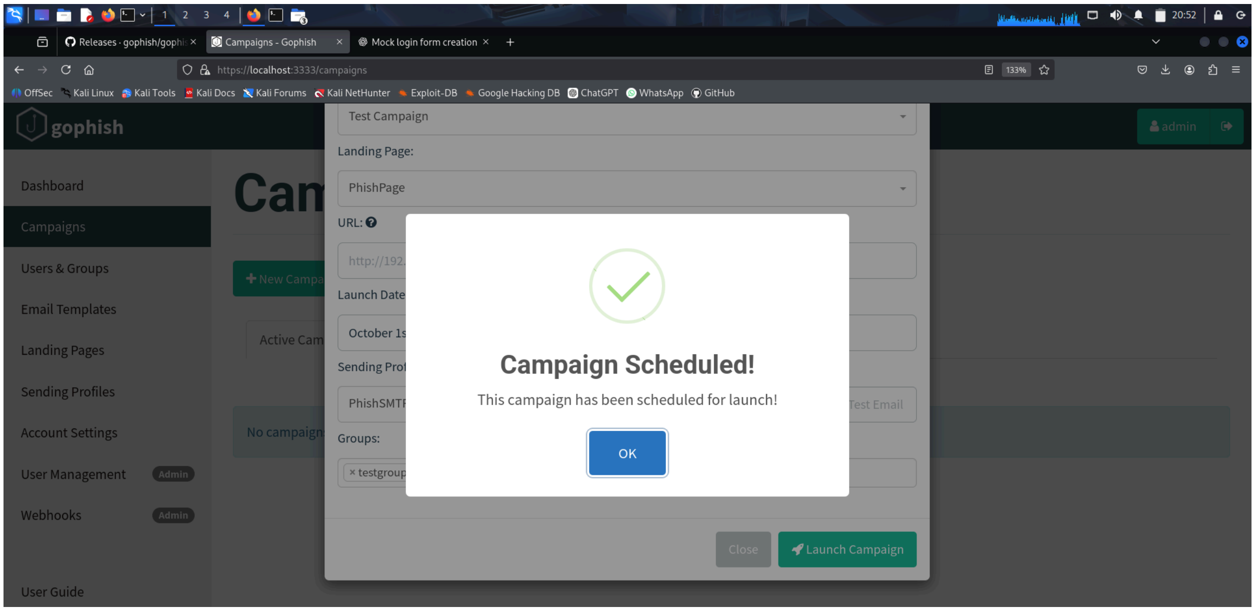
Page added successfully!

Name	Last Modified Date
PhishPage	October 1st 2025, 8:46:28 pm

Showing 1 to 1 of 1 entries

6. Campaign Creation and Execution

A phishing campaign was launched using the configured group, template, sending profile, and landing page. The campaign ran successfully and allowed live tracking of user interactions.



Test Campaign

Landing Page: PhishPage

URL: http://192.

Launch Date: October 1s

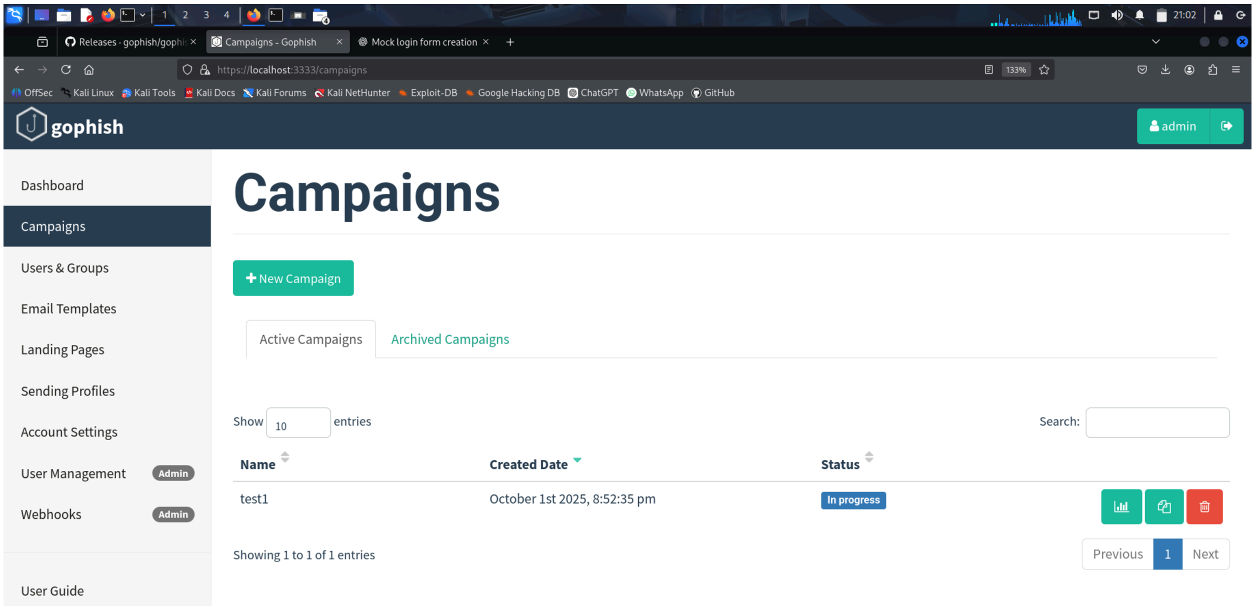
Sending Prof: PhishSMTF

Groups: × testgroup

Campaign Scheduled!

This campaign has been scheduled for launch!

OK



Campaigns

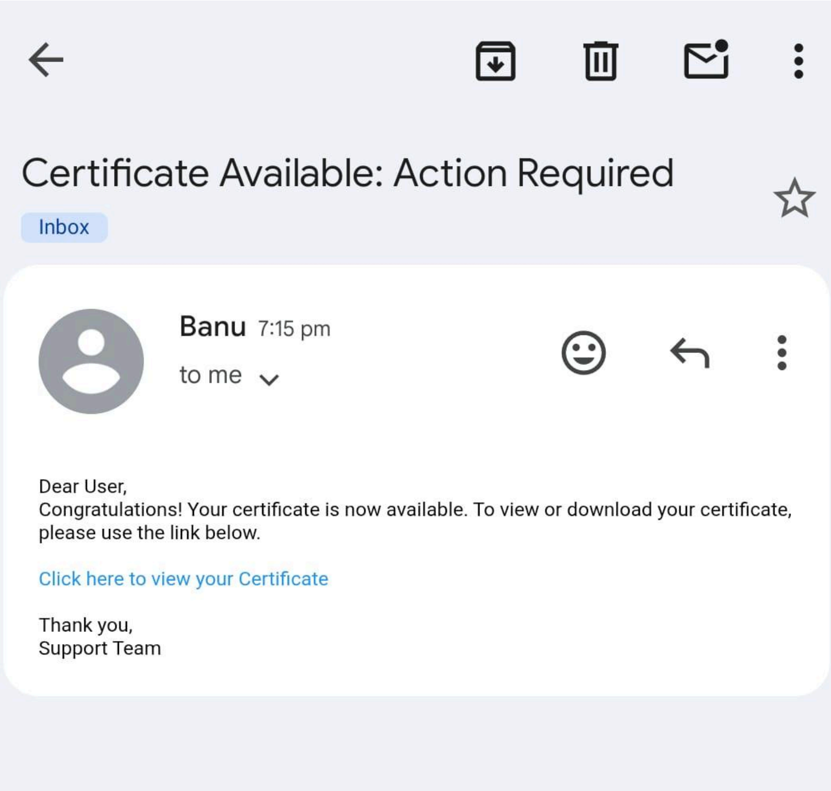
Show 10 entries

Name	Created Date	Status
test1	October 1st 2025, 8:52:35 pm	In progress

Showing 1 to 1 of 1 entries

7. Receiving the Phishing Email

The targeted inbox received the phishing email. The message contained the **fake warning** and link to the landing page.



Certificate Available: Action Required

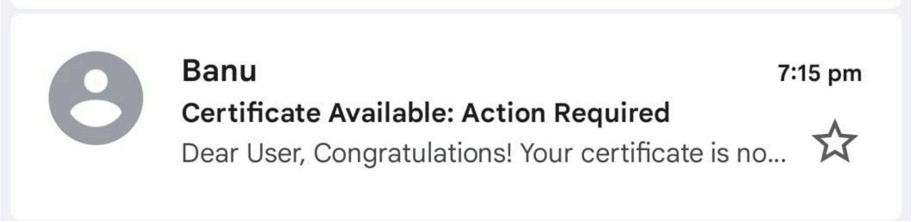
Dear User,
Congratulations! Your certificate is now available. To view or download your certificate, please use the link below.

Click here to view your Certificate

Thank you,
Support Team

8. Target Mailbox Snapshot

The phishing email appeared in the inbox alongside other real emails, making it look genuine.



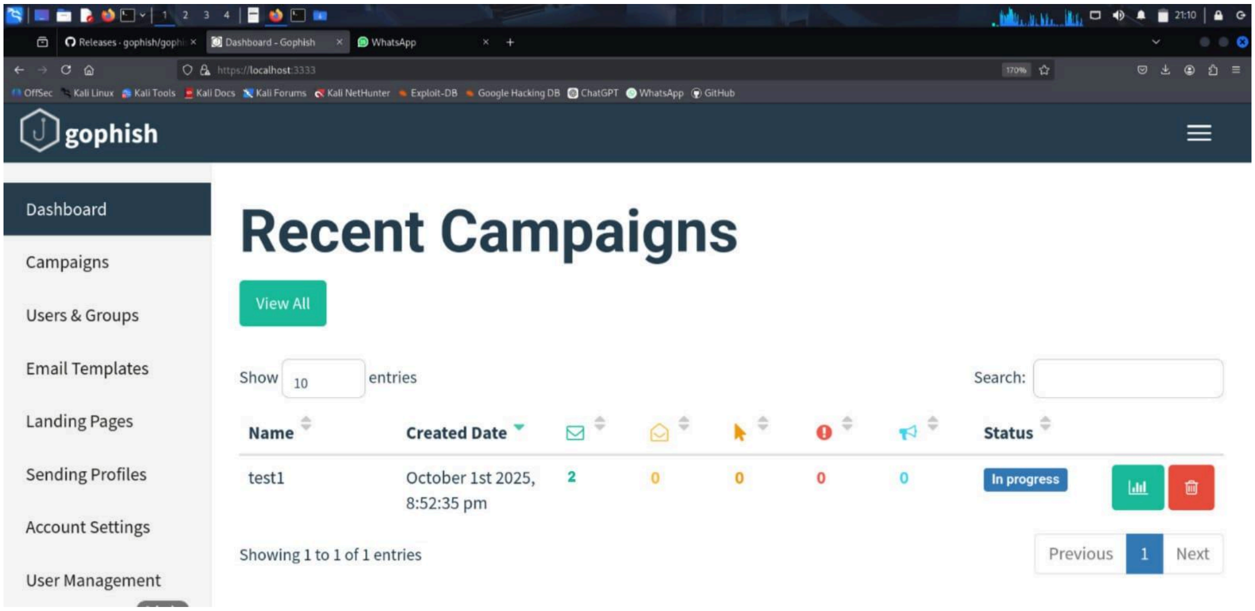
Banu 7:15 pm

Certificate Available: Action Required

Dear User, Congratulations! Your certificate is no...

9. Gophish Dashboard Results

The Gophish dashboard displayed campaign results, showing whether emails were opened, links clicked, credentials submitted, or emails reported.



Recent Campaigns

Show 10 entries Search:

Name	Created Date	✉	✉	➤	!	📢	Status
test1	October 1st 2025, 8:52:35 pm	2	0	0	0	0	In progress

Showing 1 to 1 of 1 entries

Conclusion

This simulation successfully demonstrated how a phishing attack is structured and tracked using Gophish. By creating groups, templates, sending profiles, and landing pages, the campaign showed the **end-to-end flow** of phishing attempts. Conducting such exercises in a **controlled environment** helps understand attacker methods and highlights the importance of user awareness in cybersecurity.