PHISHING ATTACK SIMULATION & DETECTION REPORT

1. Title

Phishing Attack Simulation & Detection Using GoPhish on Kali Linux

2. Objective

The objective of this task is to understand how phishing attacks work, simulate a phishing campaign in a controlled lab environment, identify phishing red flags, and learn methods to prevent phishing attacks using awareness and security practices.

3. Introduction

Phishing is a type of social engineering attack where attackers trick users into revealing sensitive information such as usernames, passwords, or personal data through fake emails or websites.
 This task focuses on simulating a phishing attack using the GoPhish framework in Kali Linux to understand attacker techniques and defensive awareness.

4. Tool Used

- **GoPhish** – Open-source phishing framework
- **Operating System** – Kali Linux
- **Browser** – Firefox

5. Methodology

Step 1: GoPhish Setup

- GoPhish was executed on Kali Linux using the terminal.
- The admin server was started on https://127.0.0.1:3333.
- The phishing server was configured to run on port 8080.

Step 2: Email Template Creation

- A phishing-style email template was created.
- The email contained a generic message requesting the user to review account information.
- A phishing URL placeholder was included to redirect users to the landing page.

Step 3: Landing Page Creation

- A fake login page was created to simulate a credential-harvesting website.
- Username and password fields were added.
- Credential capture option was enabled to record submitted data.

Step 4: Target User Configuration

- A user group was created using a test email address.
- No real users were targeted during the simulation.

Step 5: Campaign Launch

- A phishing campaign was launched using the created email template, landing page, and user group.
- The campaign status showed **Error** due to SMTP restrictions.

Step 6: Manual Phishing Simulation

- Due to email delivery restrictions, the phishing landing page was accessed manually via browser.
- Dummy credentials were entered and submitted.
- GoPhish successfully recorded user interaction and data submission.

6. Observations

- The GoPhish framework successfully simulated a phishing environment.
- Email delivery failed due to SMTP restrictions and email provider security controls.
- Credential capture and campaign tracking worked correctly through manual interaction.
- The simulation demonstrated how phishing attacks can collect sensitive data.

```
┌──(kali㉿kali)-[~]
└─$ unzip gophish-v0.12.1-linux-64bit.zip

Archive:  gophish-v0.12.1-linux-64bit.zip
  inflating: gophish
   creating: static/js/dist/
   creating: static/js/dist/app/
  inflating: static/js/dist/app/sending_profiles.min.js
  inflating: static/js/dist/app/campaign_results.min.js
  inflating: static/js/dist/app/gophish.min.js
  inflating: static/js/dist/app/campaigns.min.js
  inflating: static/js/dist/app/autocomplete.min.js
  inflating: static/js/dist/app/settings.min.js
  inflating: static/js/dist/app/users.min.js
  inflating: static/js/dist/app/webhooks.min.js
  inflating: static/js/dist/app/dashboard.min.js
  inflating: static/js/dist/app/passwords.min.js
  inflating: static/js/dist/app/templates.min.js
  inflating: static/js/dist/app/groups.min.js
  inflating: static/js/dist/app/landing_pages.min.js
  inflating: static/js/dist/vendor.min.js
   creating: static/js/src/vendor/ckeditor/
  inflating: static/js/src/vendor/ckeditor/CHANGES.md
   creating: static/js/src/vendor/ckeditor/skins/
   creating: static/js/src/vendor/ckeditor/skins/moono-lisa/
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/editor_ie.css
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/editor_gecko.css
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/icons.png
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/readme.md
   creating: static/js/src/vendor/ckeditor/skins/moono-lisa/images/
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/images/refresh.png
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/images/arrow.png
   creating: static/js/src/vendor/ckeditor/skins/moono-lisa/images/hidpi/
 extracting: static/js/src/vendor/ckeditor/skins/moono-lisa/images/hidpi/refresh.png
```

```
cd: no such file or directory: gophish-v0.12.1-linux-64bit

┌──(kali㉿kali)-[~]
└─$ chmod +x gophish


┌──(kali㉿kali)-[~]
└─$ sudo ./gophish

time="2026-02-09T01:16:42-05:00" level=warning msg="No contact address has been configured."
time="2026-02-09T01:16:42-05:00" 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    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="2026-02-09T01:16:43-05:00" level=info msg="Please login with the username admin and the password 0c52e29f8b2b784d"
time="2026-02-09T01:16:43-05:00" level=info msg="Starting IMAP monitor manager"
time="2026-02-09T01:16:43-05:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2026-02-09T01:16:43-05:00" level=info msg="Starting new IMAP monitor for user admin"
time="2026-02-09T01:16:43-05:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2026-02-09T01:16:43-05:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2026-02-09T01:16:43-05:00" level=info msg="TLS Certificate Generation complete"
time="2026-02-09T01:16:43-05:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
time="2026-02-09T01:16:43-05:00" level=fatal msg="listen tcp 0.0.0.0:80: bind: address already in use"
```

127.0.0.1:3333/login?next=%2F

OffSec | Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB

gophish

Login

Please sign in

admin

●●●●●●●●●●●●●●●

Sign in
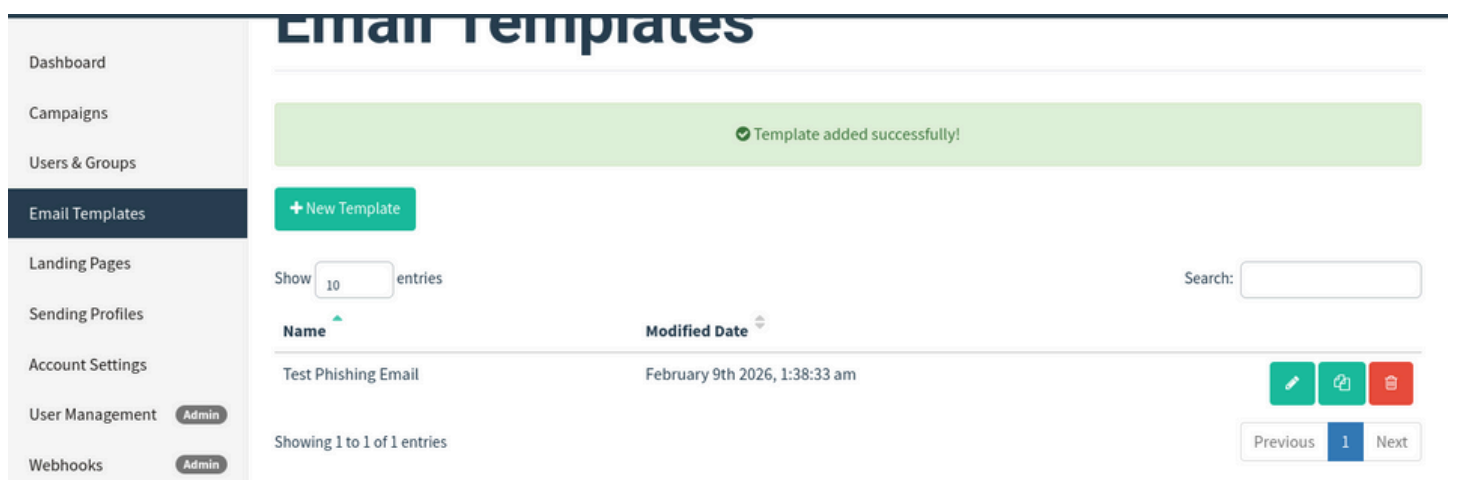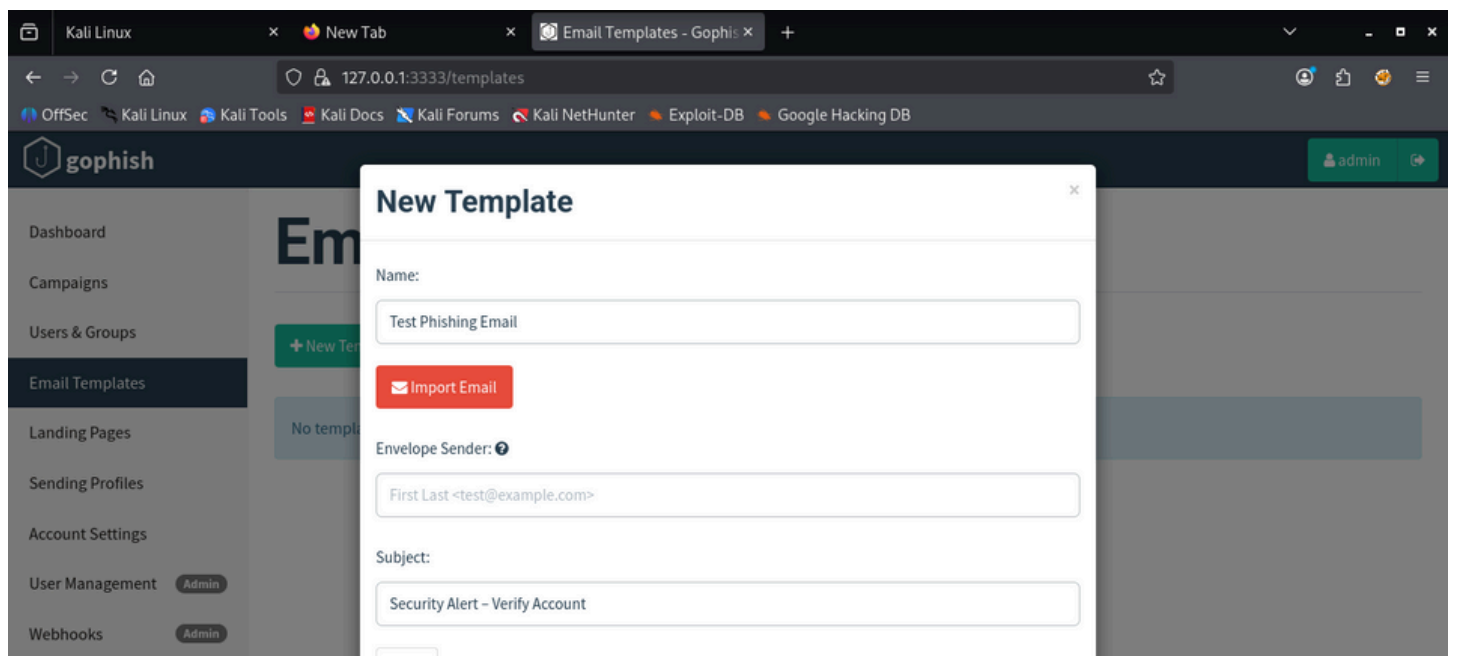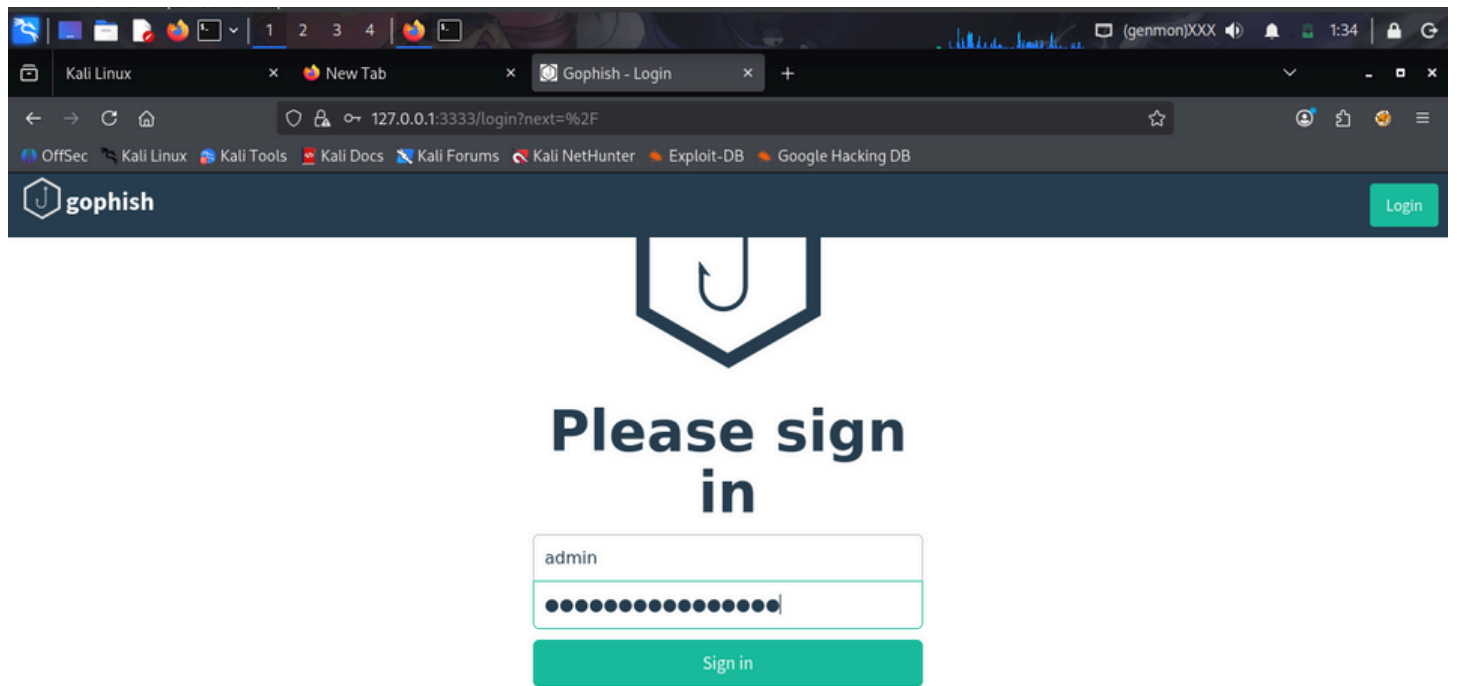
Kali Linux | New Tab | Email Templates - Gophish | +

127.0.0.1:3333/templates

OffSec | Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB

gophish

admin

- Dashboard
- Campaigns
- Users & Groups
- Email Templates
- Landing Pages
- Sending Profiles
- Account Settings
- User Management **Admin**
- Webhooks **Admin**

Em

New Template

+ New Te

No templa

Name:

Test Phishing Email

✉ Import Email

Envelope Sender: ❓

First Last <test@example.com>

Subject:

Security Alert – Verify Account

Email Templates

- Dashboard
- Campaigns
- Users & Groups
- Email Templates
- Landing Pages
- Sending Profiles
- Account Settings
- User Management **Admin**
- Webhooks **Admin**

✓ Template added successfully!

+ New Template

Show 10 entries   Search:

Name	Modified Date	
Test Phishing Email	February 9th 2026, 1:38:33 am	✏ 🗐 🗑

Showing 1 to 1 of 1 entries   Previous 1 Next

Users & Groups

admin

+ New Group

Show 10 entries

Search:

Name	# of Members	Modified Date	
Test Group	1	February 9th 2026, 1:48:58 am	✏ 🗑

Showing 1 to 1 of 1 entries

Previous 1 Next

Fake Login Page

URL: ❓

http://192...

Launch Date

February 9

Sending Prof

Test Profile

Groups:

× Test Grou

✓ Campaign Scheduled!

This campaign has been scheduled for launch!

OK

Close ✈ Launch Campaign

Details

Show 10 entries

Search:

First Name	Last Name	Email	Position	Status	Reported
▸ aaaaa	bbb	vaishwith123@gmail.com		Sending	⊘

Showing 1 to 1 of 1 entries

Previous 1 Next

7. Phishing Red Flags Identified

- Urgent or suspicious email messages
- Generic greetings instead of personal names
- Unexpected links asking for login details
- Requests for sensitive information
- Unverified sender email addresses

8. Why Phishing Is Dangerous

- Leads to credential theft
- Causes financial fraud
- Enables identity theft
- Can result in malware infection
- Compromises organizational security

9. Phishing Prevention Methods

- Verify sender email addresses
- Avoid clicking unknown links
- Check URLs carefully
- Use multi-factor authentication (MFA)
- Conduct user awareness training
- Use email filtering and security tools

10. Result

The phishing attack simulation was successfully demonstrated using GoPhish.
Although real email delivery was blocked by SMTP and provider security policies, the phishing workflow, landing page interaction, and credential capture were validated through manual testing.

11. Conclusion

This task provided hands-on understanding of phishing attacks, their detection, and prevention methods. The simulation improved awareness of social engineering threats and emphasized the importance of cybersecurity awareness in real-world environments.