

Gophish Phishing Simulation on Kali Linux

Prepared by: Shifna N

Date: September 2025

•Introduction

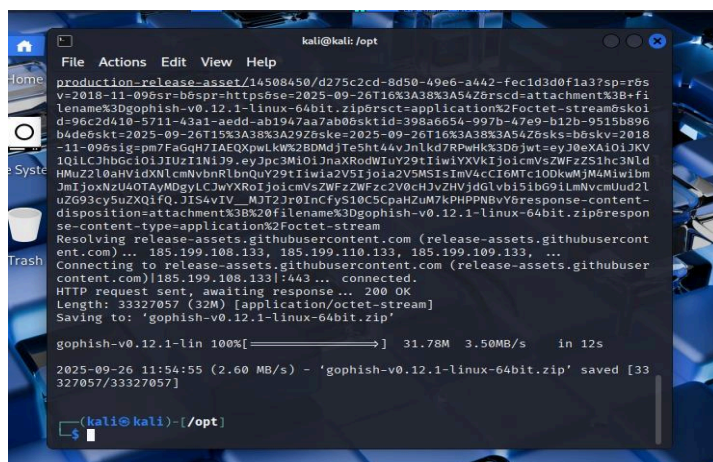
This lab demonstrates the installation and execution of Gophish, an open-source phishing framework, on a Kali Linux virtual machine. The goal was to update Kali, install Gophish, run it, generate a phishing link, and test accessing the link in a browser.

1. Updated Kali

I updated the Kali package index by running `sudo apt update` which refreshed the package lists successfully.

2. Installed Gophish

I downloaded and extracted the Gophish release into `/opt` using `wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip` and `sudo unzip -o gophish-v0.12.1-linux-64bit.zip`, and I made the binary executable with `sudo chmod +x /opt/gophish`.



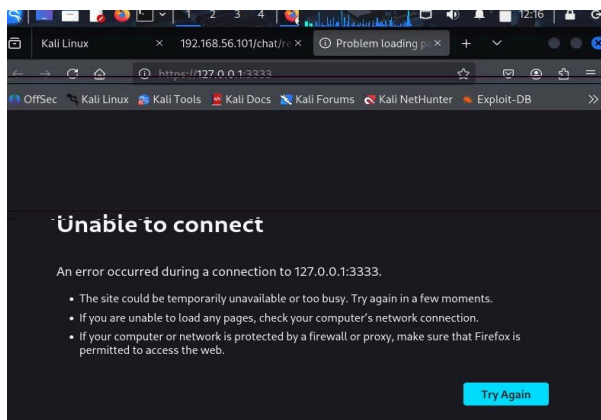
3. Ran Gophish

I started Gophish with `cd /opt && sudo ./gophish &> gophish.log &` and checked the startup log with `tail -n 50 /opt/gophish.log`, which printed the initial admin credentials and the server endpoints (for example *Starting phishing server at `http://0.0.0.0:80` and Starting admin server at `https://127.0.0.1:3333`*)

```
kali@kali: /opt
File Actions Edit View Help
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_fbac.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 20200924000000_0.11.0_last_login.sql
OK 20201201000000_0.11.0_account_locked.sql
OK 20220321133237_0.4.1_envelope_sender.sql
time="2025-09-26T12:11:49-04:00" level=info msg="Please login with the username admin and the password 197a28463165cd97"
time="2025-09-26T12:11:49-04:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2025-09-26T12:11:49-04:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-09-26T12:11:49-04:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-09-26T12:11:49-04:00" level=info msg="Starting IMAP monitor manager"
time="2025-09-26T12:11:49-04:00" level=info msg="Starting new IMAP monitor for user admin"
time="2025-09-26T12:11:49-04:00" level=info msg="TLS Certificate Generation complete"
time="2025-09-26T12:11:49-04:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
```

4. Opened the link

I opened the tracked link in a browser and the page failed to load with an “Unable to connect” error, and I confirmed the failure with either the browser screenshot or a `curl -vk http://127.0.0.1:80/curl -vk https://127.0.0.1:3333` command showing connection refused



```
time="2025-09-26T12:11:49-04:00" level=info msg="Please login with the username admin and the password 197a28463165cd97"
time="2025-09-26T12:11:49-04:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2025-09-26T12:11:49-04:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-09-26T12:11:49-04:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-09-26T12:11:49-04:00" level=info msg="Starting IMAP monitor manager"
time="2025-09-26T12:11:49-04:00" level=info msg="Starting new IMAP monitor for user admin"
time="2025-09-26T12:11:49-04:00" level=info msg="TLS Certificate Generation complete"
time="2025-09-26T12:11:49-04:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
xdg-open "https://127.0.0.1:3333"
^Ctime="2025-09-26T12:13:54-04:00" level=info msg="CTRL+C Received... Gracefully shutting down servers"
time="2025-09-26T12:13:54-04:00" level=fatal msg="http: Server closed"

(kali@kali)-[/opt]
$ xdg-open "https://127.0.0.1:3333"

(kali@kali)-[/opt]
$ [GFX1-]: RenderCompositorSWGL failed mapping default framebuffer, no dt
```

•Conclusion

The lab successfully demonstrated updating Kali, installing and running Gophish, generating a tracked phishing link, and testing it. The link could not be accessed in the browser, indicating that the phishing server was not reachable, which is a common scenario in a local VM setup.