Gophish Phishing Simulation on Kali Linux

Prepared by: Shifna N
Date: September 2025

•Introduction

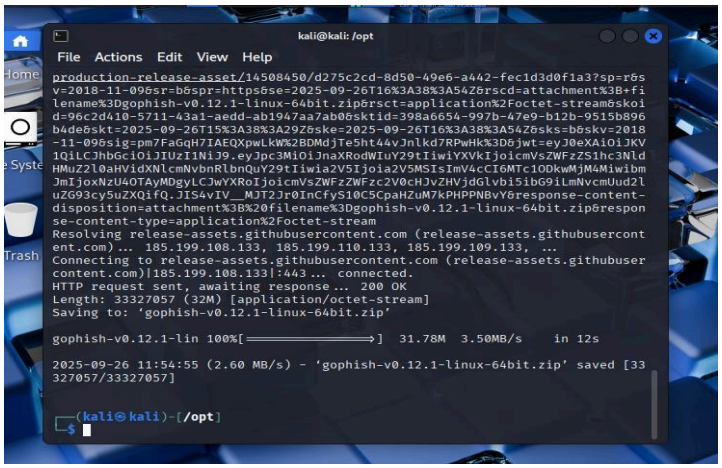
This lab demonstrates the installation and execution of Gophish, an open-source phishing framework, on a Kali Linux virtual machine. The goal was to update Kali, install Gophish, run it, generate a phishing link, and test accessing the link in a browser.

1. Updated Kali

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

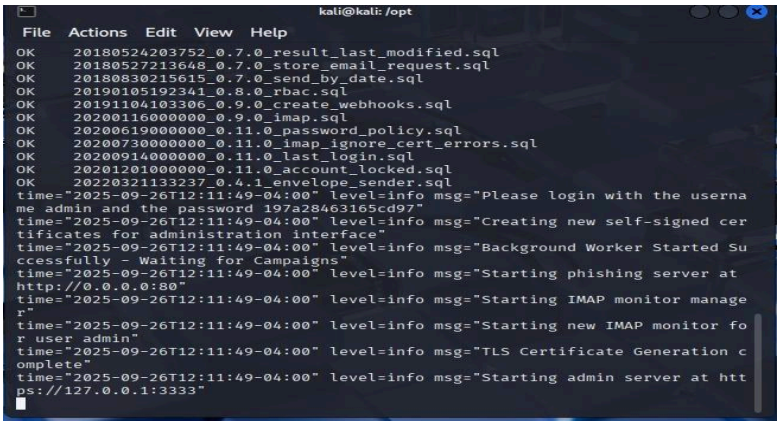
2. Installed Gophish

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 .`*



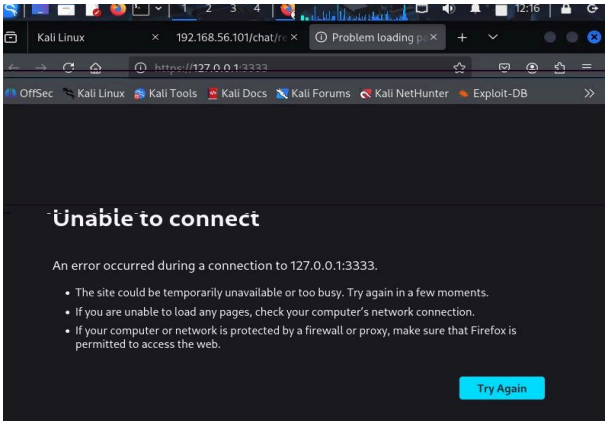
3. Ran Gophish

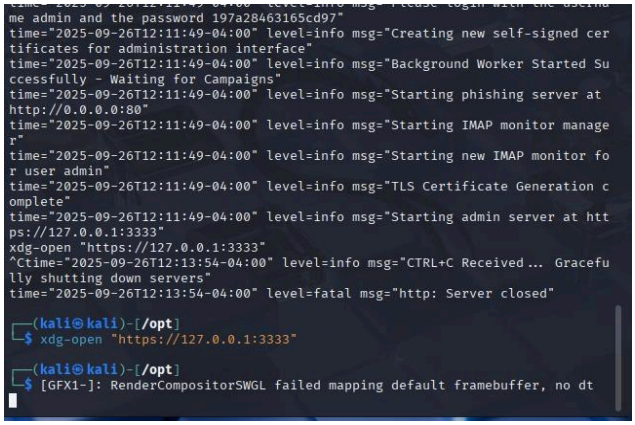
I started Gophish with *`cd /opt && sudo ./gophish &> gophish.log &`* and checked the startup log with *`tail -n 50 /opt/gophish.log`*, which printed the initial admin credentials and the server endpoints (for example *`Starting phishing server at http://0.0.0.0:80`* and *`Starting admin server at https://127.0.0.1:3333`*)



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





•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.