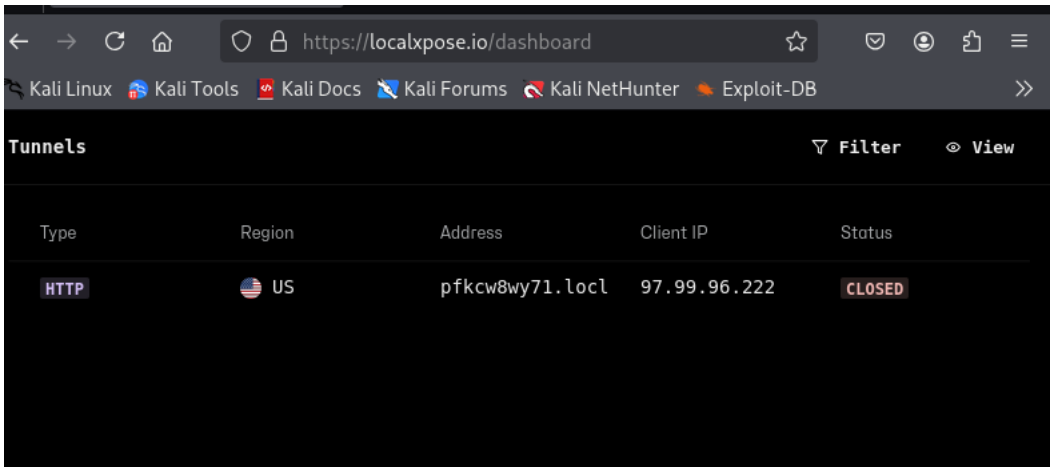
Steps In Generating a PayPal Phishing Link with Zphisher

This document records the exact steps I followed to build and deliver a PayPal -style phishing page for an internal security exercise.

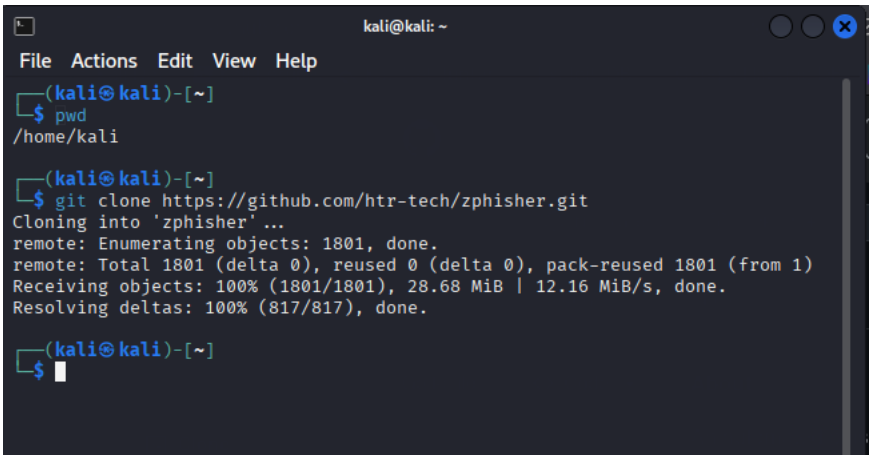
1 Prerequisites I Confirmed

- I secure written approval and defined scope for stimulation.
- I prepared a dedicated kali Linux virtual machine with outbound internet access.
- I set up a localxpose account for external port forwarding.



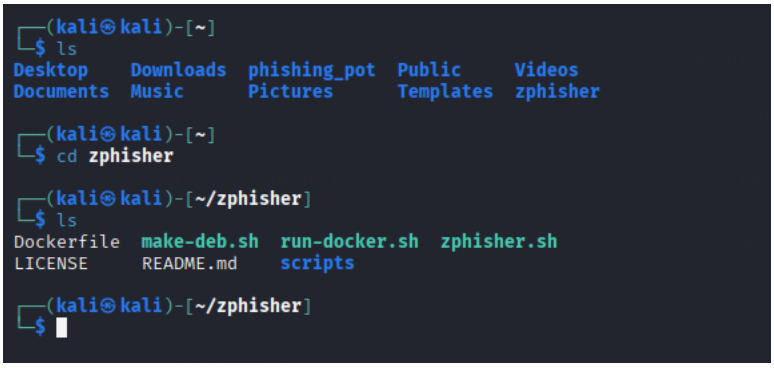
2 Installing Zphisher Tools

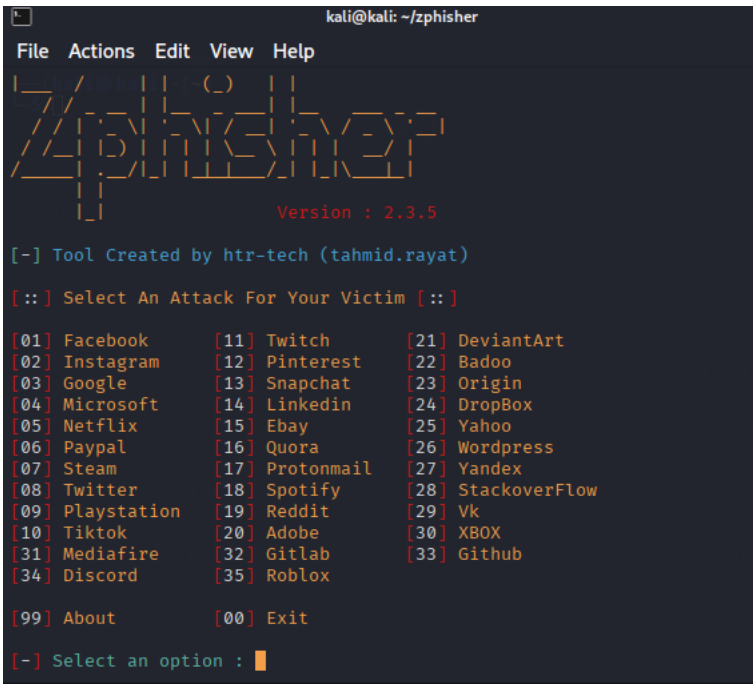
- Using the code 'git clone' with the link https://gitclone.com/htr-tech/zphisher.git~zphisher. I cloned the project to my home directory.
- I confirmed the script was launched without errors:



3 Launching Zphisher

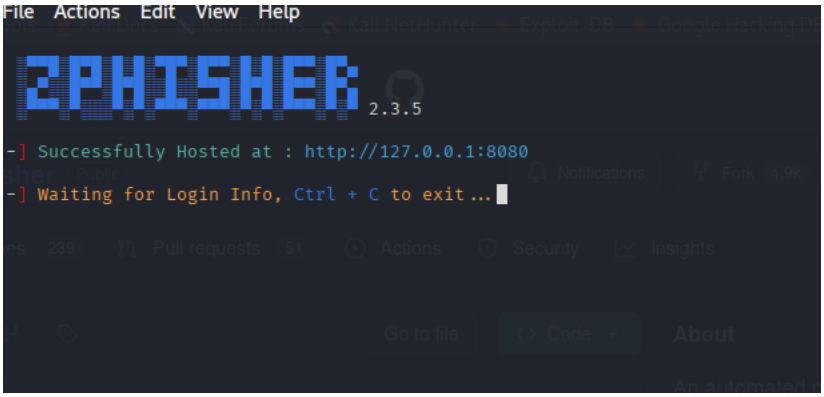
- I navigated into Zphisher directory
- I checked for the files in zphisher using ls command
- I located the bash file ‘zphisher.sh
- I started the script with ‘./zphisher.sh’





4 Selecting the PayPal template

- I selected the PayPal login template option 6



5 Sending the phishing email

- I drafted an email requesting for urgent password change for security purpose.
- I embedded the link behind a 'link ' button
- I scheduled mail delivery during business hours for authenticity

Subject: Urgent: Immediate PayPal Password Change Required for Security

Dear [Samuel],

We have detected unusual activity related to your PayPal account and, as a precautionary measure, we strongly recommend that you change your password immediately.

To help ensure the continued security of your account, please follow these steps:

1. Log in to your PayPal account directly at http://127.0.0.1:8080
2. Navigate to **Settings > Security > Password**.
3. Create a strong, unique password that you haven't used before.

Please **do not click any suspicious links** and avoid sharing your login details with anyone. If you did not initiate any recent changes or suspect unauthorized access, contact PayPal Support right away.

Protecting your information is our top priority. Thank you for your prompt attention to this matter.

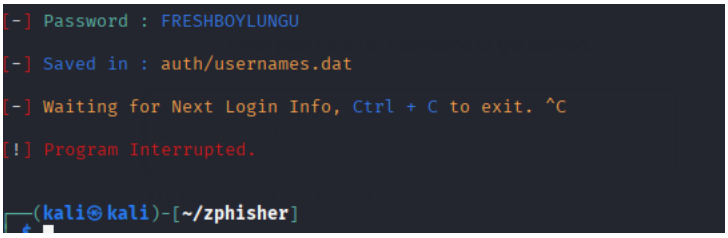
Sincerely,
James
PayPal

6 Monitoring interaction

- I monitored the credential log
- I captured logs for each link clicked

7 Terminating and cleaning up

- I stopped zphisher using CTRL+ C



8 Analysing Result

- I analysed the KPI data (clicks, credential submissions, reports) in google sheets
- I included the findings in the final simulation report and updated the risk register

KPI	Baseline (before- campaign	Post Campaign
link clicks	90%	20%
credential submission	70%	10%
Reports	20%	90%

Prepared By: Rasheed O. Odubayo (Jnr. Cybersecurity Analyst)