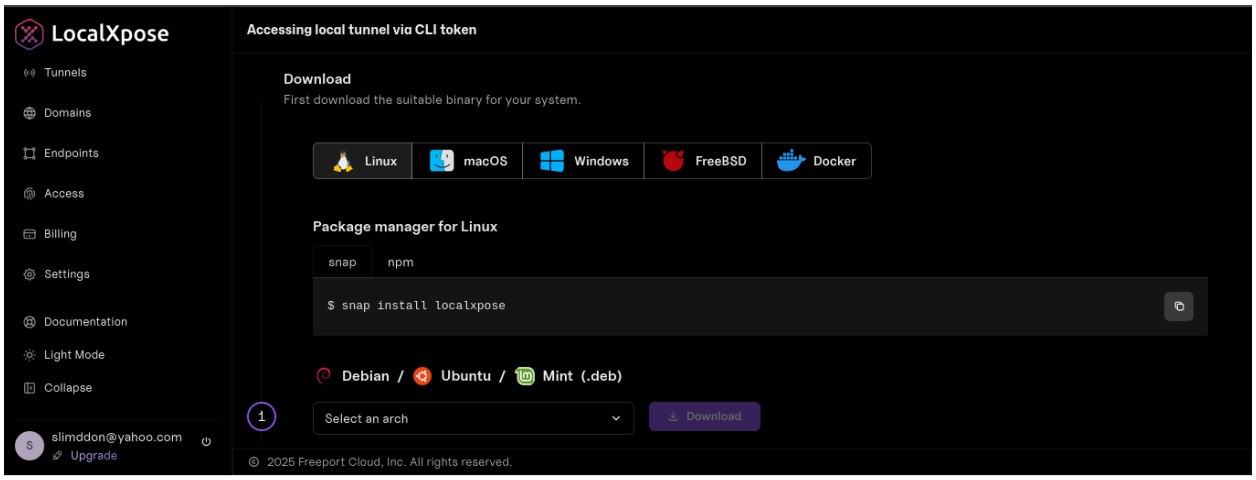
Generating Google Link with Zphisher

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

1. Prerequisites I confirmed

- I prepared a dedicated Kali Linux VM with outbound internet access
- I secured written approval and defined scope for the simulation
- I set up a Localxpose account for external port forwarding



2. Installing Zphisher

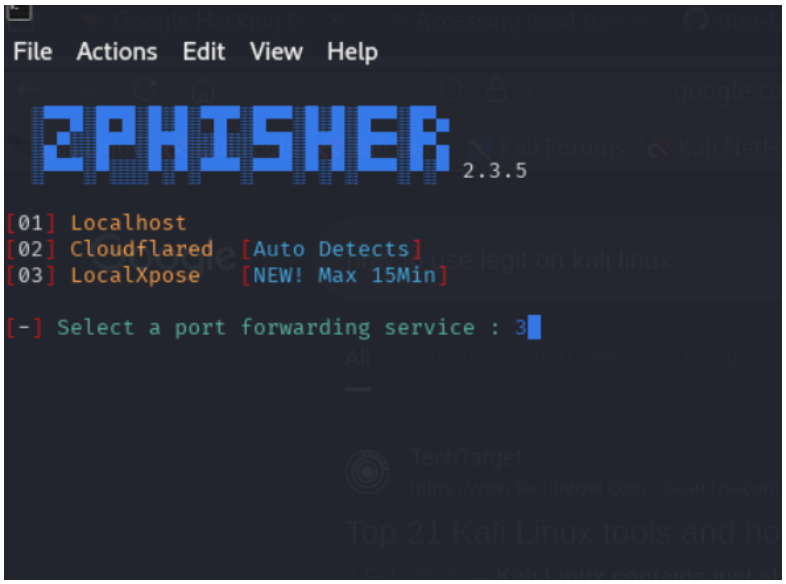
- I cloned the project to my home directory: git clone https://github.com/htr-tech/zphisher.git~/zphisher`.
- I confirmed the script launched without errors: `~/zphisher/zphisher.sh –h`.

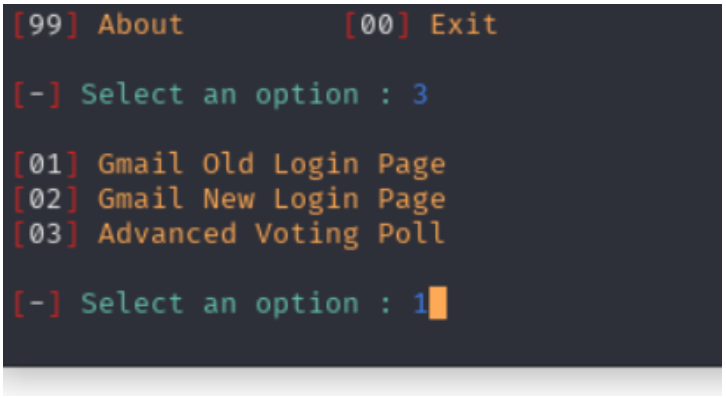
3. Launching zphisher

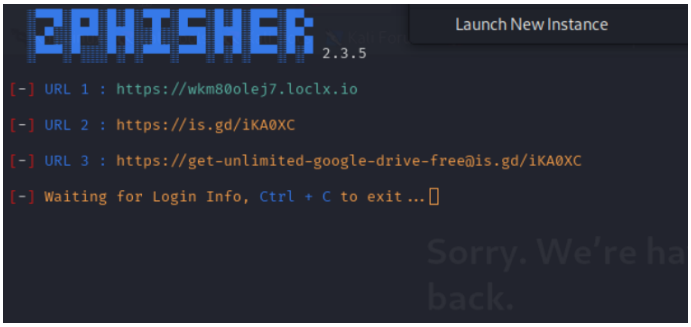
- I changed into the tool directory: cd ~/zphisher
- I started the script with sudo: `sudo ./zphisher.sh`.

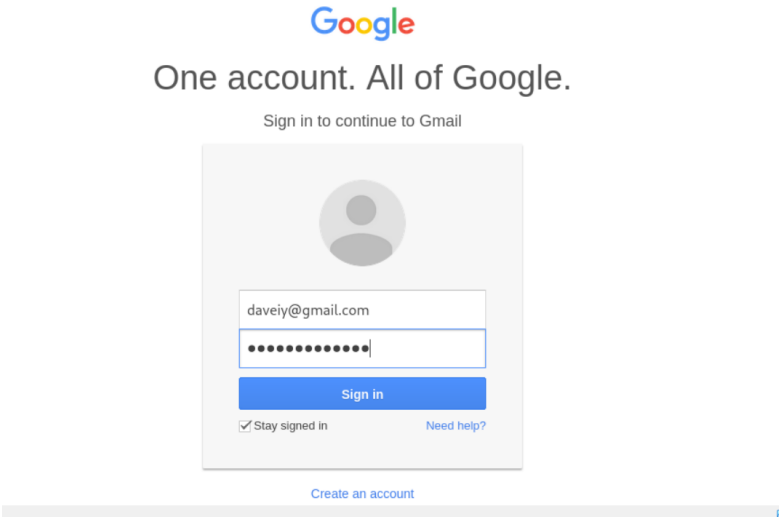
4. Selecting or importing the google template

- I chose the google login template (option number displayed as 03 in my session).
- Zphisher presented a local URL, https://wkm80olej7.loclx.io` which I noted for the email









Dear Team,

As part of our ongoing efforts to enhance security and protect user data, Google will be implementing new security measures for Google account holders. We want to ensure that all team members are aware of these changes and take necessary steps to update their accounts.

Action Required:

1. Review your Google account settings to ensure that your account information is up-to-date and secure. Click the link to learn more.
2. Familiarize yourself with the new security features and best practices for protecting your account.

If you have any questions or concerns, please don't hesitate to reach out to our IT department. We're here to support you.

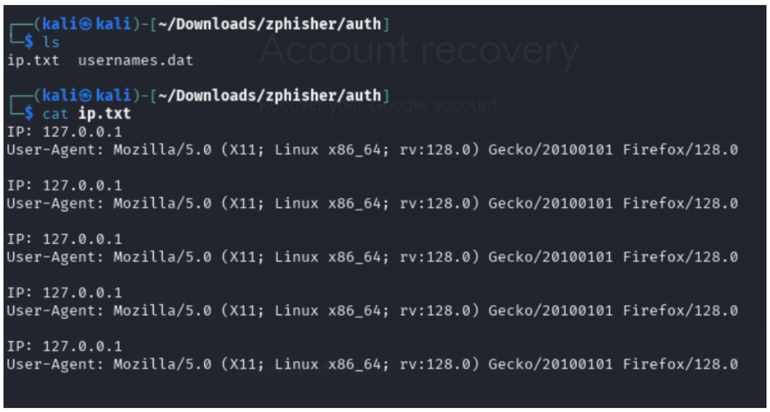
Best regards,
IT Manager

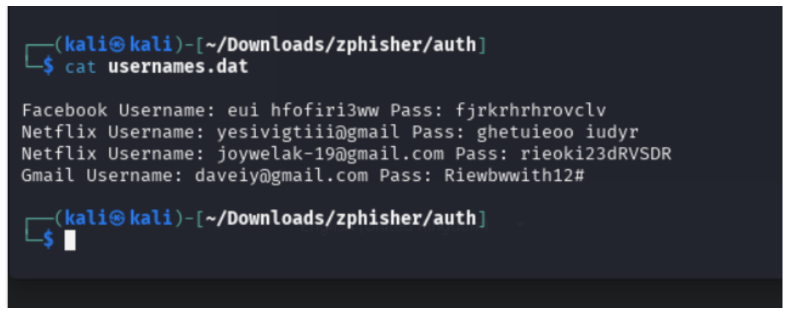
6. Monitoring Interaction

- I monitored the credential log
- I captured logs for each link click submission

7. Terminating and clean up

- I stopped zphisher with CTRL+C.
- I closed the localhost with CTRL+C if it was running.
- I confirmed the captured credentials are truly saved.





8. Next Steps

- 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

Measured Outcomes

KPI	Baseline (before campaign)	Post campaign
Link clicks	80%	30%
Credential submission	60%	20%
Reports	10%	80%

Prepared by: Oladapo Fredrick (Cybersecurity Analyst)