BABU BANARASI DAS UNIVERSITY

SCHOOL OF Computer Application

Department of Cybersecurity and forensics

Identity and Access Management.
(BCACSN13102)
Session 2025-26

PRACTICAL LAB FILE

SUBMITTED BY: -

NAME – PRATEEK SAHU
Roll No - 1240264
SECTION– BCACS 22

SUBMITTED TO: -

Mr. Anand Kumar Gupta

INDEX

REPORT: - SIMULATED PHISING EXERCISE

Title: Simulated Phishing Exercise Report (Zphisher-based)

Author: [PRATEEK SAHU]

Client / Faculty: IBM Faculty (Practice Exercise)

Date of Report: [2025-10-10]

Scope / Target(s):

- Target group: [Normal web users]
- Number of target accounts tested: [1]
- Test window: [09/10/2025 — 10/10/2025]
- Authorization: Activity performed under explicit written authorization from [IBM FACULTY]. This exercise is part of an approved security training and red-team/blue-team exercise.

1.) EXECUTIVE SUMMARY

This report summarizes the results of a simulated phishing campaign executed to evaluate user susceptibility and the effectiveness of current email security controls. The campaign targeted [1] accounts within the NORMAL WEB USER between [09/10/2025-10/10/2025]. Key findings show that targets interacted with the test phish (opened email, clicked link, submitted credentials), indicating a moderate/high risk posture. Remediation focuses on technical controls, user training, and policy updates.

2.) OBJECTIVES

- To perform the use of zphisher software for practicing and make phishing e mails

3.) Rules of Engagement s Authorization

- Test approved by: [IBM FACULTY] on [10/10/2025].

- Explicit limitations: No malicious payloads were used; no real credential harvesting was retained; any submitted credentials were simulated/redacted and not stored.

- **Note:** This exercise adhered to ethical guidelines and local policies. Ensure all future exercises carry similar written authorization.

4. Methodology (High-level)

Step1) open Firefox or any other browser in kali Linux or any present vm.

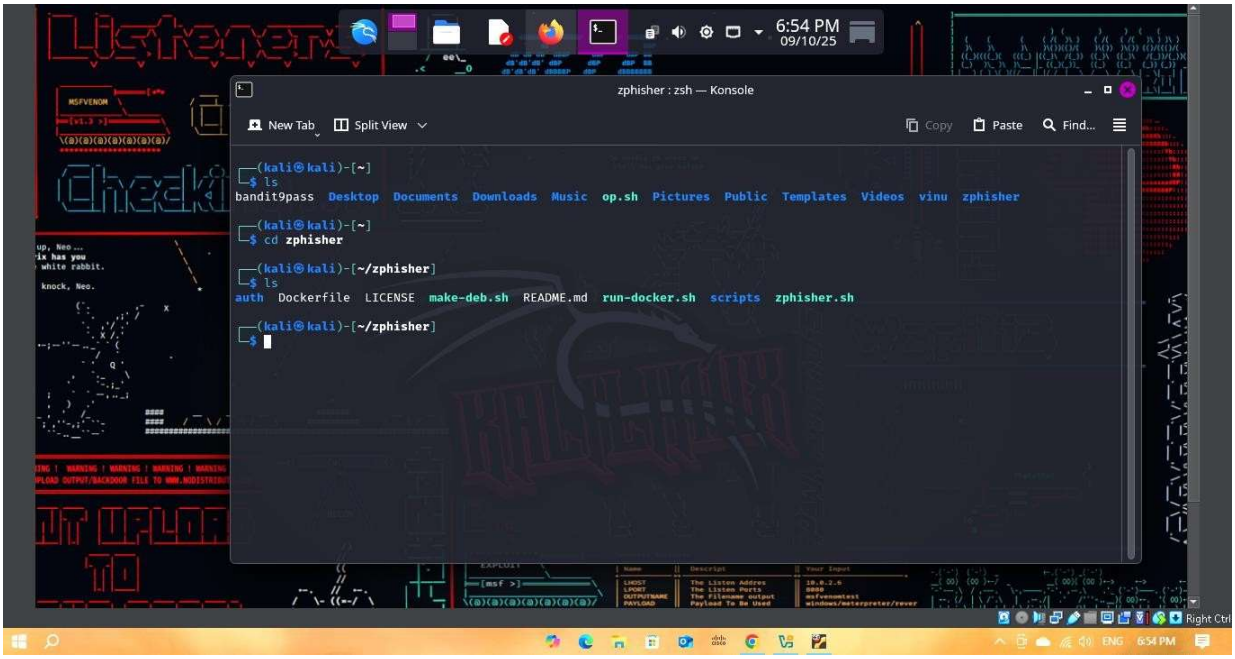
Step2) type z phisher and click on the first link

Step3) clone the git into the terminal (this will install the zphisher application)

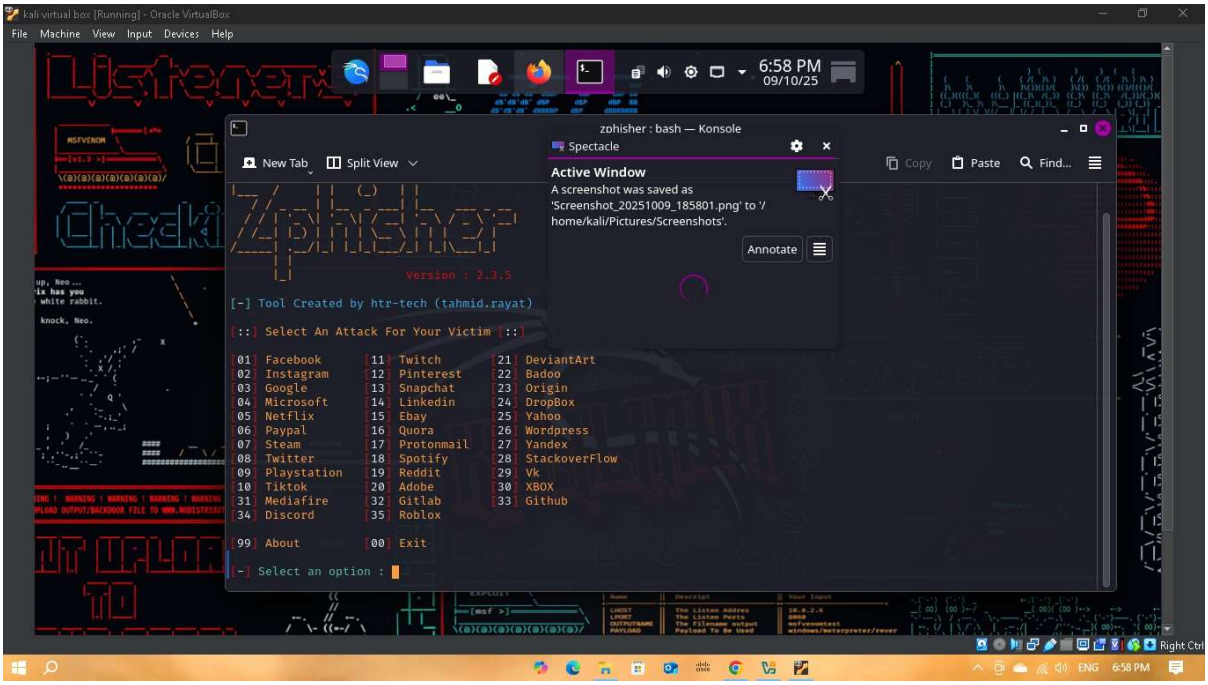
Git link: - “git clone --depth=1 https://github.com/htr-tech/zphisher.git”

Step4) type the “ls” command to see the zphisher folder

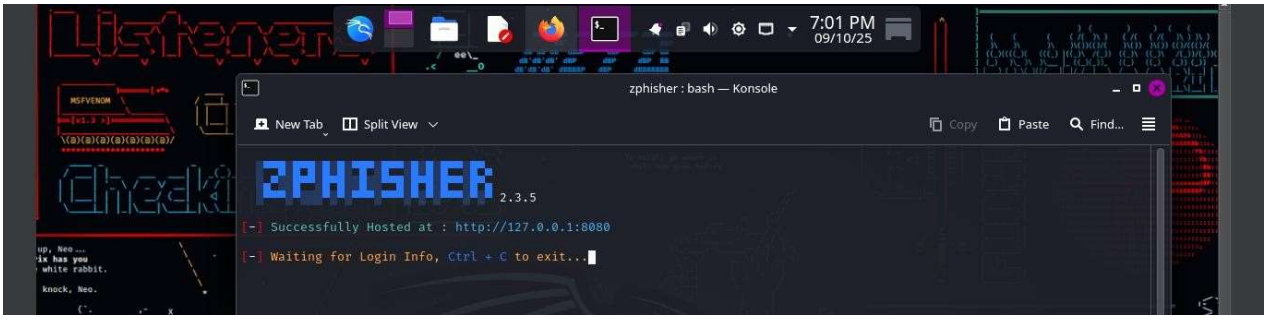
Step5) type the “cd command to enter the zphisher folder



Step6) after seeing the shell file “zphisher.sh”, type “bash zphisher.sh” || ./zphisher.sh (this will execute the zphisher tool.

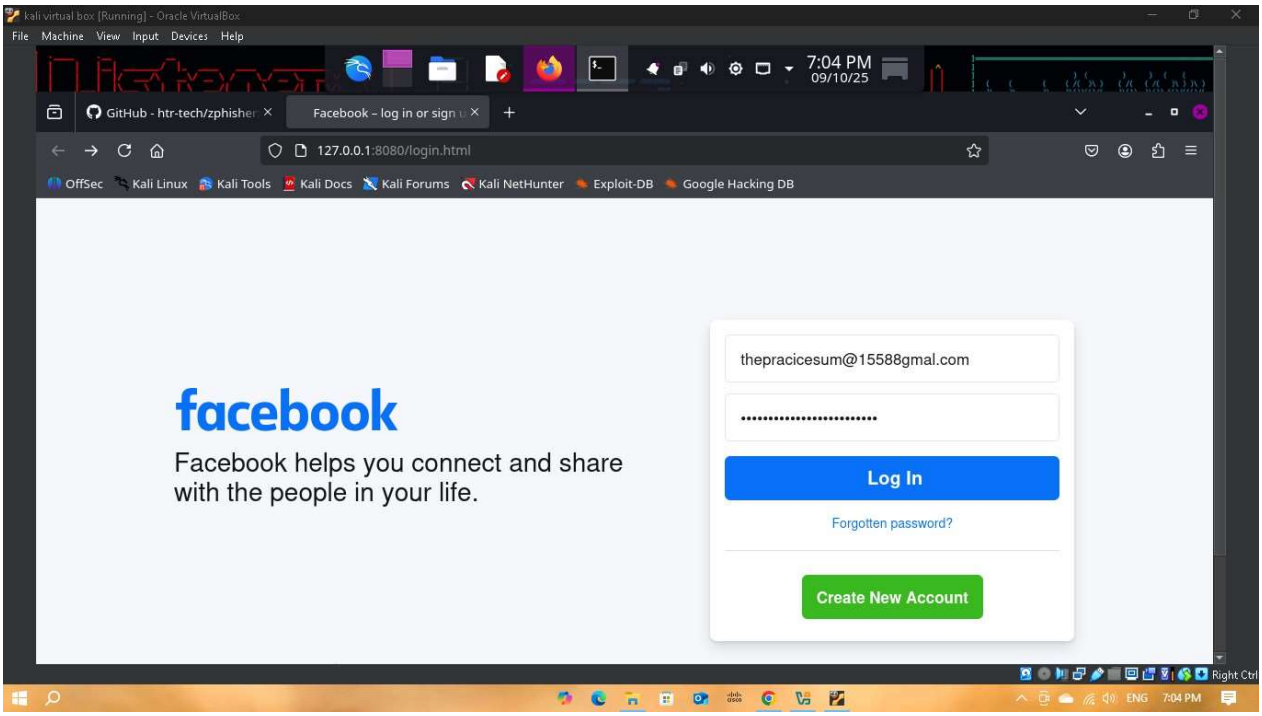


Step7) type the number you want to create a phishing login page or anything (follow along the step with the tool), you will be given a link like this after following along

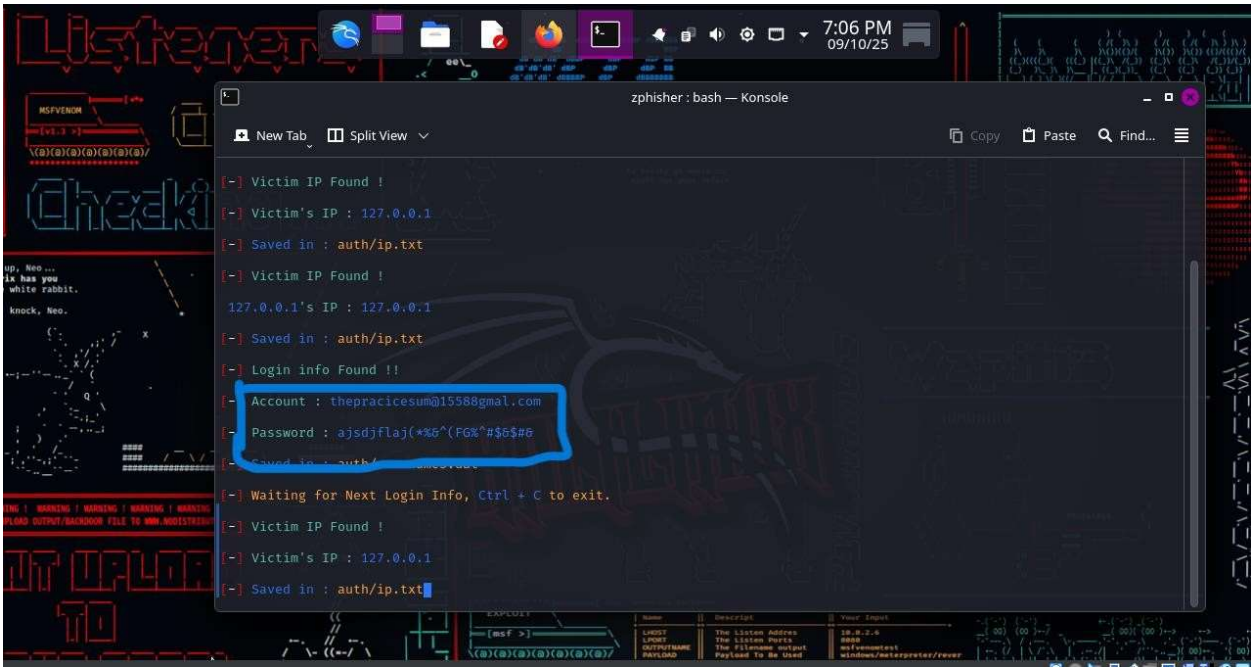


Step8) click on the link -->> your phishing page will be created, like here for testing we have used the Facebook phishing login page -->> now you want to add some details for e.g. has

been seen below in the image



Step8) once done click on terminal again -->> you will see the login credentials victim has entered



8. Conclusions

Reiterate that the exercise was simulated, authorized, and intended to improve security posture and awareness.

10. Tools s References

- Testing tool used (training platform): [Zphisher — used as an approved training Tool, Kali Linux- the attacking machine]

Notes s Safe-practice reminders

- Never retain real credentials gathered during a simulation. If credentials were captured accidentally, record the event and securely destroy the data, and notify the appropriate compliance officer.
- Keep the exercise non-punitive — the goal is to improve awareness, not penalize users.