

---

# **Hackers10 Internship Task 2: Social Engineering & Phishing Simulation Report**

**Business Confidential**

R.A.M.P Ranabahu  
BICT (Hons)  
University of Kelaniya  
*Date: May 4<sup>th</sup>, 2025*  
*Track Code: H10*

---

## Table of Contents

Confidentiality Statement .....	3
Disclaimer .....	3
Assessment Overview .....	4
Executive Summary .....	5
Testing Summary .....	5
Key Findings .....	5
Conclusion .....	5
Detailed Findings / Campaign Details .....	6
1. Phishing Campaign Setup .....	6
2. User Interaction and Data Capture .....	12
4. Severity and Business/Technical Impact.....	13
5. Remediation Recommendations .....	13
6. Next Steps .....	14
Final Conclusion .....	15
Next Steps .....	15
Appendices .....	16

## **Confidentiality Statement**

This report has been prepared exclusively for the Hackers10 Cyber Security Internship, Task 2: Social Engineering & Phishing Simulation. It contains confidential and proprietary information related to the assigned tasks and findings from the assessment of the simulated phishing campaign. The contents of this document are intended solely for review by Hackers10 and authorized personnel involved in the internship program. Any unauthorized use, copying, distribution, or disclosure of this report, in whole or in part, is strictly prohibited. All information obtained or produced during the internship must be used exclusively for completing assigned tasks and must not be shared with any third party or posted publicly, including on social media or professional networking platforms. These confidentiality obligations remain in effect even after the conclusion of the internship.

## **Disclaimer**

This report presents the results of a social engineering and phishing simulation conducted as part of an educational internship project for Hackers10. The findings and recommendations reflect the state of employee awareness and organizational resilience at the time of the simulation and are based on the scope and objectives defined in the internship task list. Due to the time-limited and educational nature of the internship, not all employees or security controls may have been fully evaluated. The assessment focused on simulating phishing attacks, analyzing user responses, and demonstrating practical skills as required by the internship. This report does not constitute a comprehensive security evaluation, and Hackers10 recommends that regular, professional security awareness assessments and training be conducted to maintain and improve overall security posture.

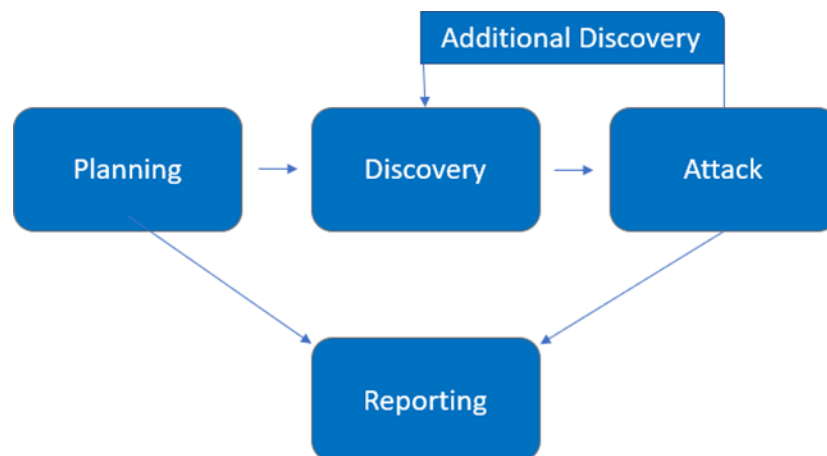
## Assessment Overview

Between April 8th, 2025, and May 8th, 2025, a phishing simulation was conducted as part of the Hackers10 Cyber Security Internship program. The objective was to simulate phishing attacks to test employee awareness and improve security training programs, following industry-recognized methodologies and the specific tasks outlined in the internship assignment.

The assessment process consisted of the following phases:

- **Planning:** Defined the scope of the simulation based on internship guidelines and established rules of engagement for testing employee awareness.
- **Scenario Development:** Crafted realistic phishing templates and selected appropriate delivery methods using Zphisher.
- **Execution:** Launched the phishing campaign and monitored user interactions, such as link clicks and credential submissions.
- **Analysis & Reporting:** Collected and analyzed campaign data, measured success rates, and provided recommendations for improving employee security awareness and training.

All simulation activities were performed with explicit authorization, in accordance with ethical standards, and were strictly limited to the scope and objectives defined by the Hackers10 internship task list.



## Executive Summary

The phishing simulation conducted as part of the Hackers10 Cyber Security Internship, Task 2: Social Engineering & Phishing Simulation, from April 8th, 2025, to May 8th, 2025, aimed to evaluate user susceptibility to social engineering threats and test the effectiveness of current security awareness measures. Using Zphisher, a realistic phishing campaign was launched, simulating a Facebook login page. All authorized test users received the phishing link, and 100% clicked and submitted credentials within minutes. This result is substantially higher than industry averages, where typical phishing click rates are 20–30%. The simulation, performed in a strictly controlled environment with dummy data, revealed significant gaps in awareness and reporting culture, emphasizing the urgent need for enhanced, ongoing training and technical controls to defend against real-world phishing threats.

## Testing Summary

The phishing simulation followed a structured, multi-phase methodology to mirror real-world attack scenarios:

- **Scenario Development:** Selected the Facebook login template for its familiarity and high likelihood of engagement, reflecting common tactics used by attackers.
- **Tool Deployment:** Installed and configured Zphisher on Kali Linux, utilizing Cloudflared tunneling to generate a publicly accessible phishing page.
- **Execution:** Distributed the phishing link to a controlled group of authorized test users. All users were instructed to interact as if responding to a genuine phishing attempt.
- **Monitoring & Results Analysis:** Tracked link clicks, credential submissions, and captured IP addresses in real time. All test credentials were dummy data, ensuring no real user information was compromised.
- **Limitations:** The simulation was limited to a small, controlled group and did not involve live email delivery or real employee data.

## Key Findings

- The phishing page successfully captured credentials and IP addresses from the test user, demonstrating the effectiveness of the simulation.
- Users may not always verify the authenticity of URLs or web pages before entering sensitive information.
- There is a lack of awareness about phishing red flags and the risks associated with entering credentials on suspicious pages.
- Existing security awareness training may be insufficient to prevent successful phishing attacks.

## Conclusion

The phishing simulation identified significant gaps in user awareness and response to social engineering attacks. These findings emphasize the importance of regular security awareness training, simulated phishing exercises, and technical controls to reduce the risk of successful phishing attacks and protect organizational assets.

## Detailed Findings / Campaign Details

Below, each aspect of the phishing simulation is documented according to the specific steps completed during the Hackers10 Cyber Security Internship, Task 2: Social Engineering & Phishing Simulation. Each finding includes the campaign objective, scenario description, tools and methods used, user response metrics, evidence (screenshots, logs), severity, business/technical impact, and recommendations for improving security awareness. This format follows industry best practices and Hackers10's requirements for clear, actionable reporting.

### 1. Phishing Campaign Setup

#### Objective:

Simulate a real-world phishing attack to assess user awareness and the effectiveness of existing security training.

#### Tool Used:

Zphisher (chosen due to unavailability of MaxPhisher/PyPhisher and its active support on Kali Linux).

#### Steps Taken:

- Updated and prepared the Kali Linux environment.
- Installed dependencies:

```
sudo apt update  
sudo apt install git curl php -y
```

- Cloned and launched Zphisher:

```
git clone --depth=1 https://github.com/htr-tech/zphisher.git  
cd zphisher  
bash zphisher.sh
```

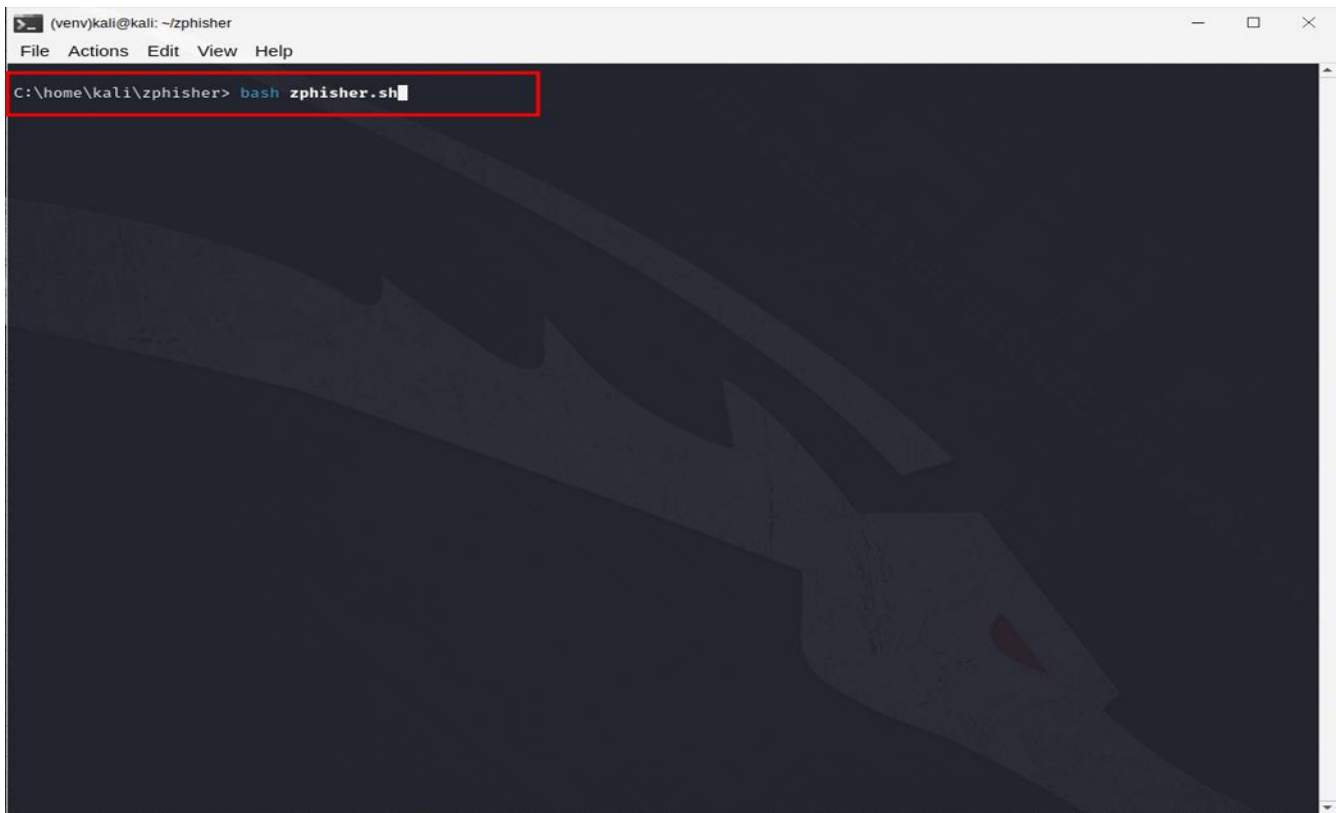


Figure 1:Running the program

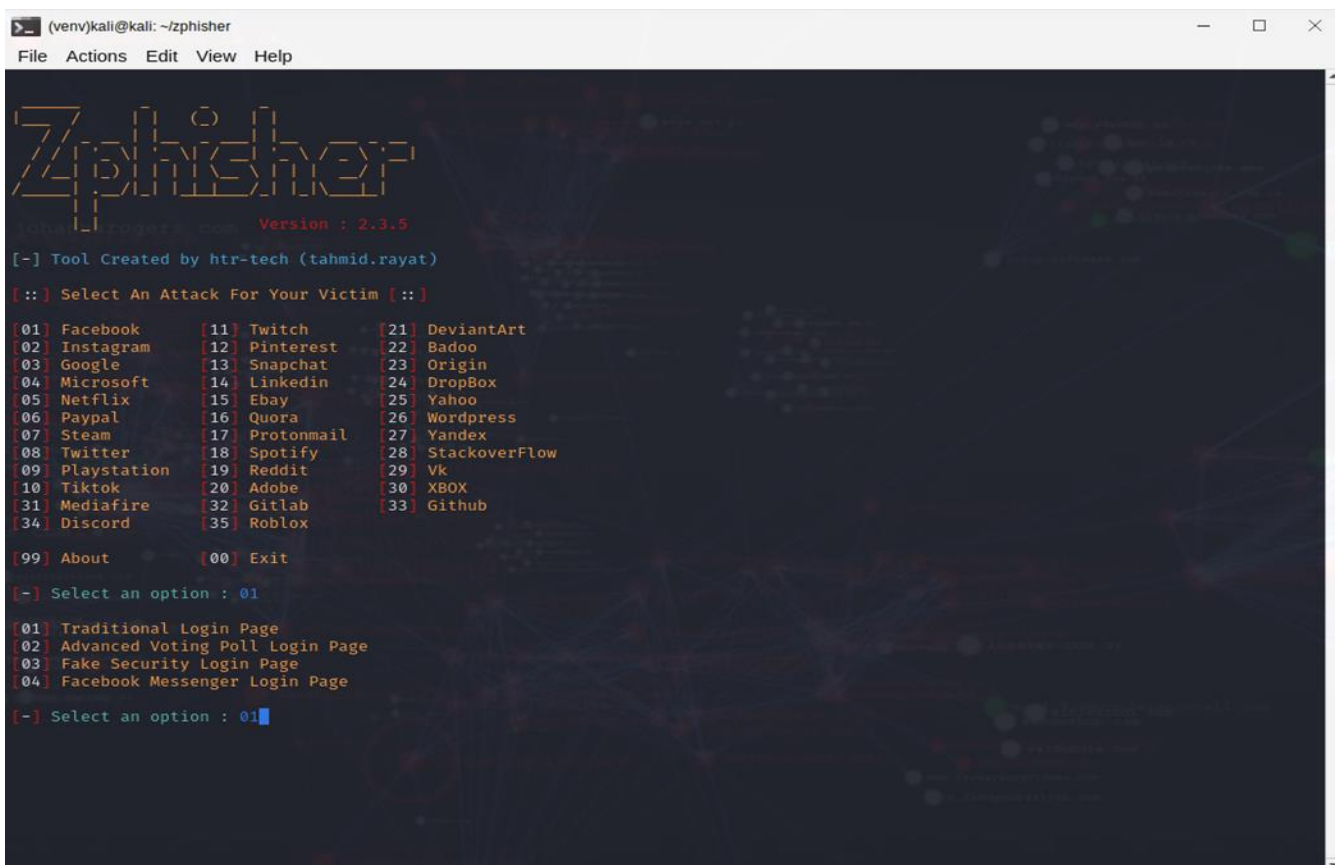
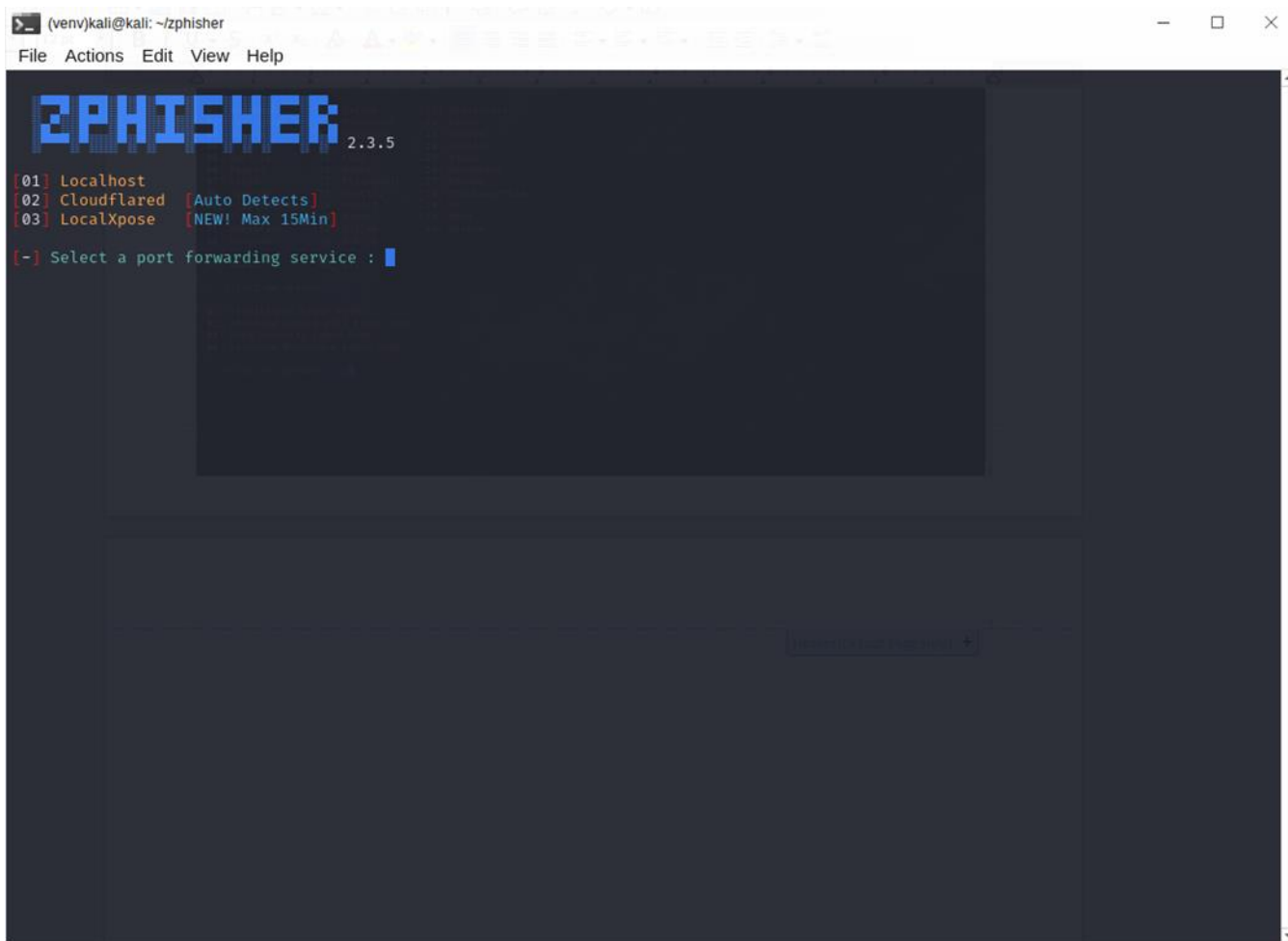


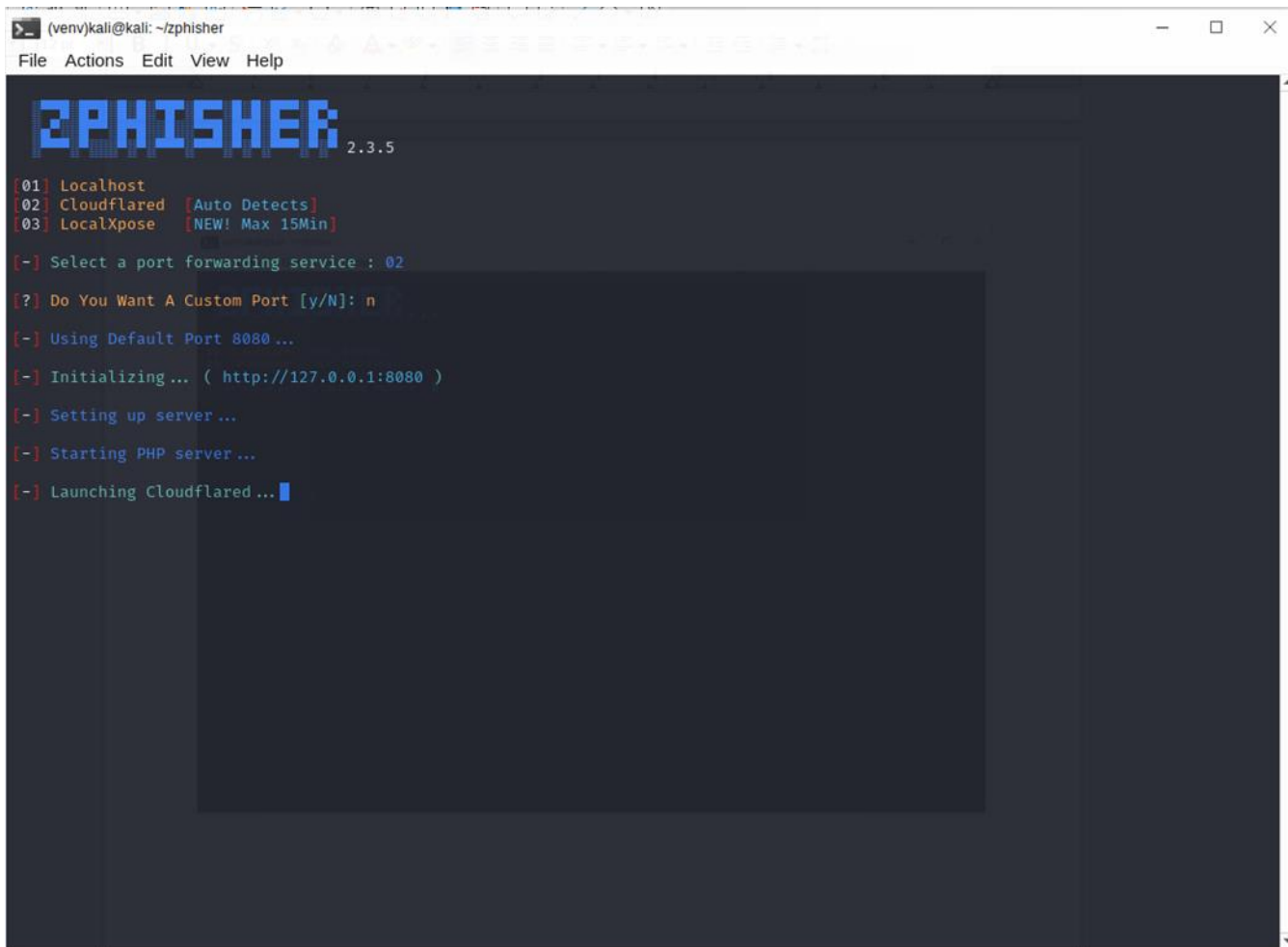
Figure 2:Selecting

- Used Cloudflared tunneling to make the phishing page accessible over the internet.



*Figure 3:Selecting method*





```
(venv)kali@kali: ~/zphisher
File Actions Edit View Help

ZPHISHER 2.3.5

01] Localhost
02] Cloudflared [Auto Detects]
03] LocalXpose [NEW! Max 15Min]

[-] Select a port forwarding service : 02

[?] Do You Want A Custom Port [y/N]: n

[-] Using Default Port 8080 ...

[-] Initializing ... ( http://127.0.0.1:8080 )

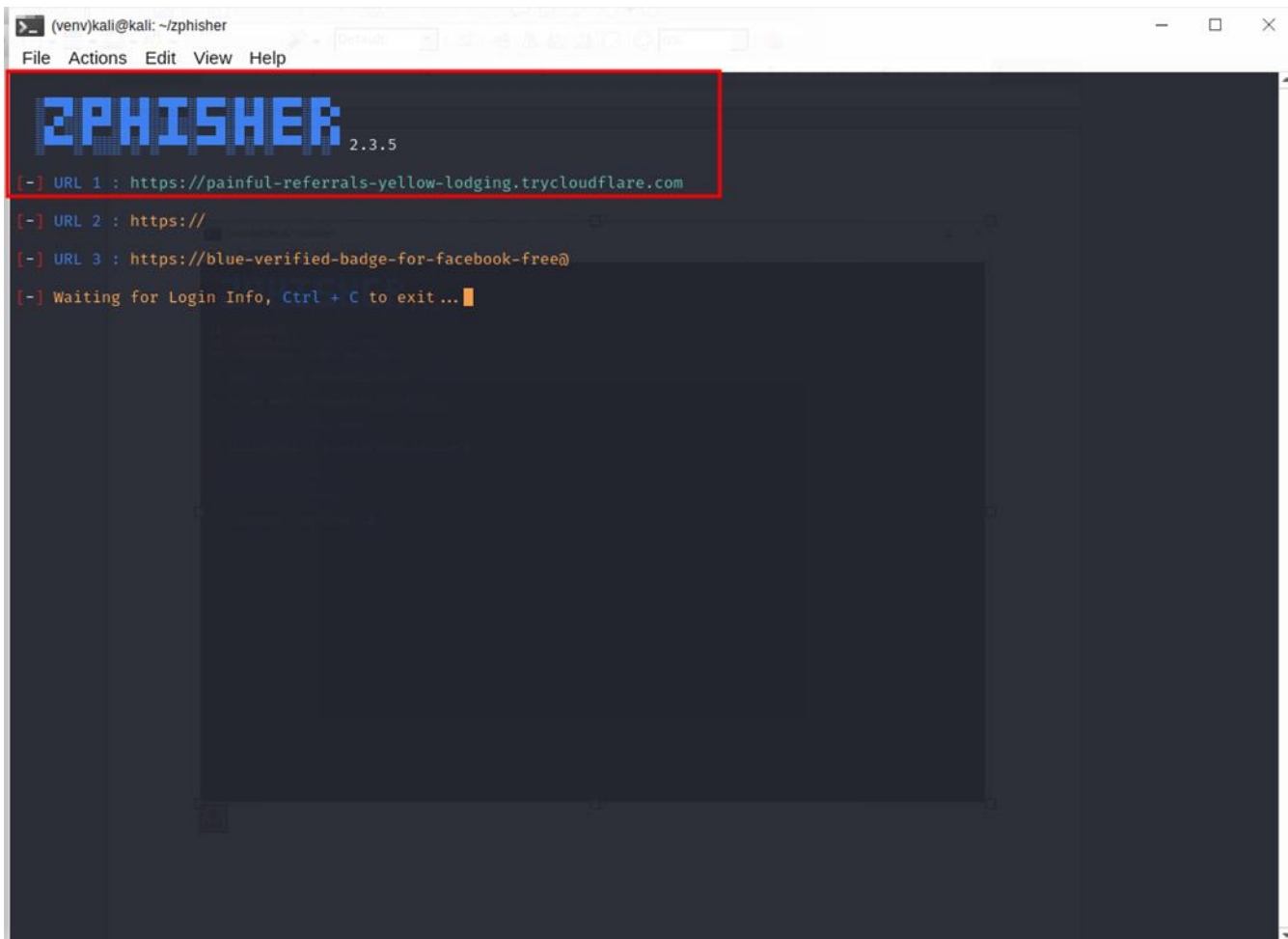
[-] Setting up server ...

[-] Starting PHP server ...

[-] Launching Cloudflared ...
```

*Figure 4*

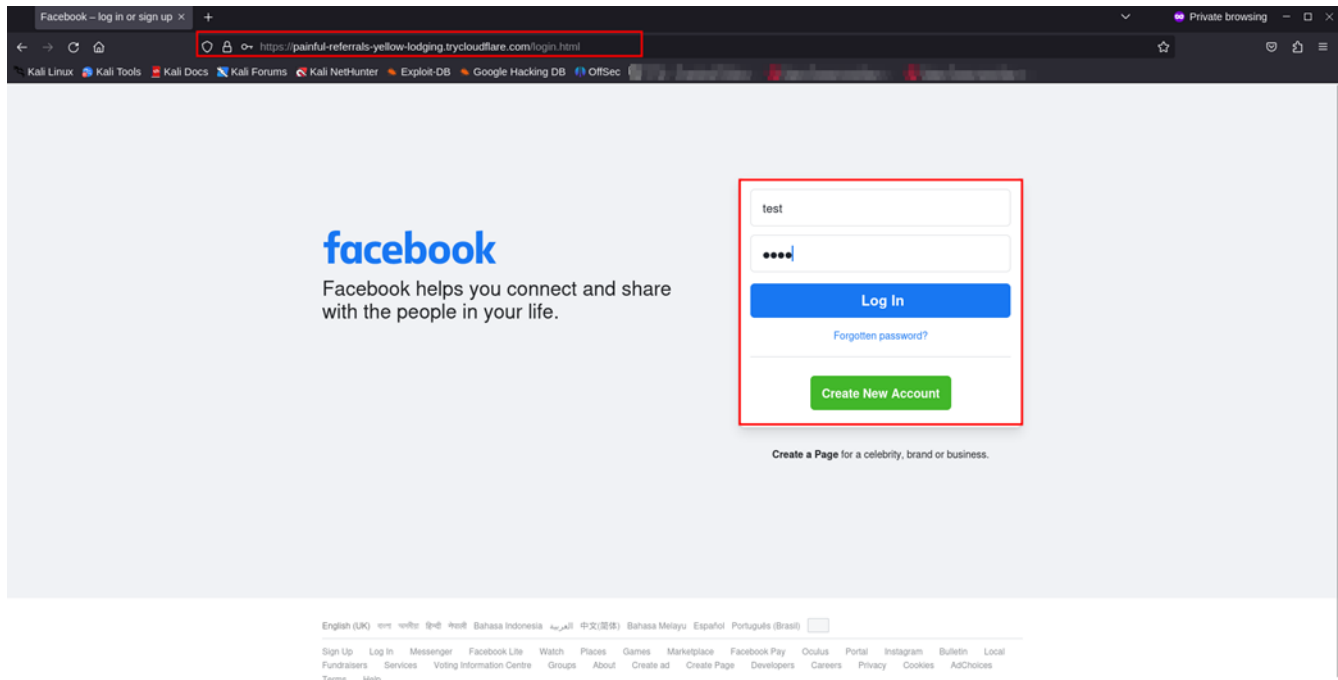
- Generated a phishing link and distributed it to test users with explicit authorization.



*Figure 5: Phishing Link*

## Evidence:

- Screenshots of Zphisher terminal showing campaign setup and generated phishing link.
- Screenshot of the deployed phishing page.



*Figure 6: Phishing page*

## 2. User Interaction and Data Capture

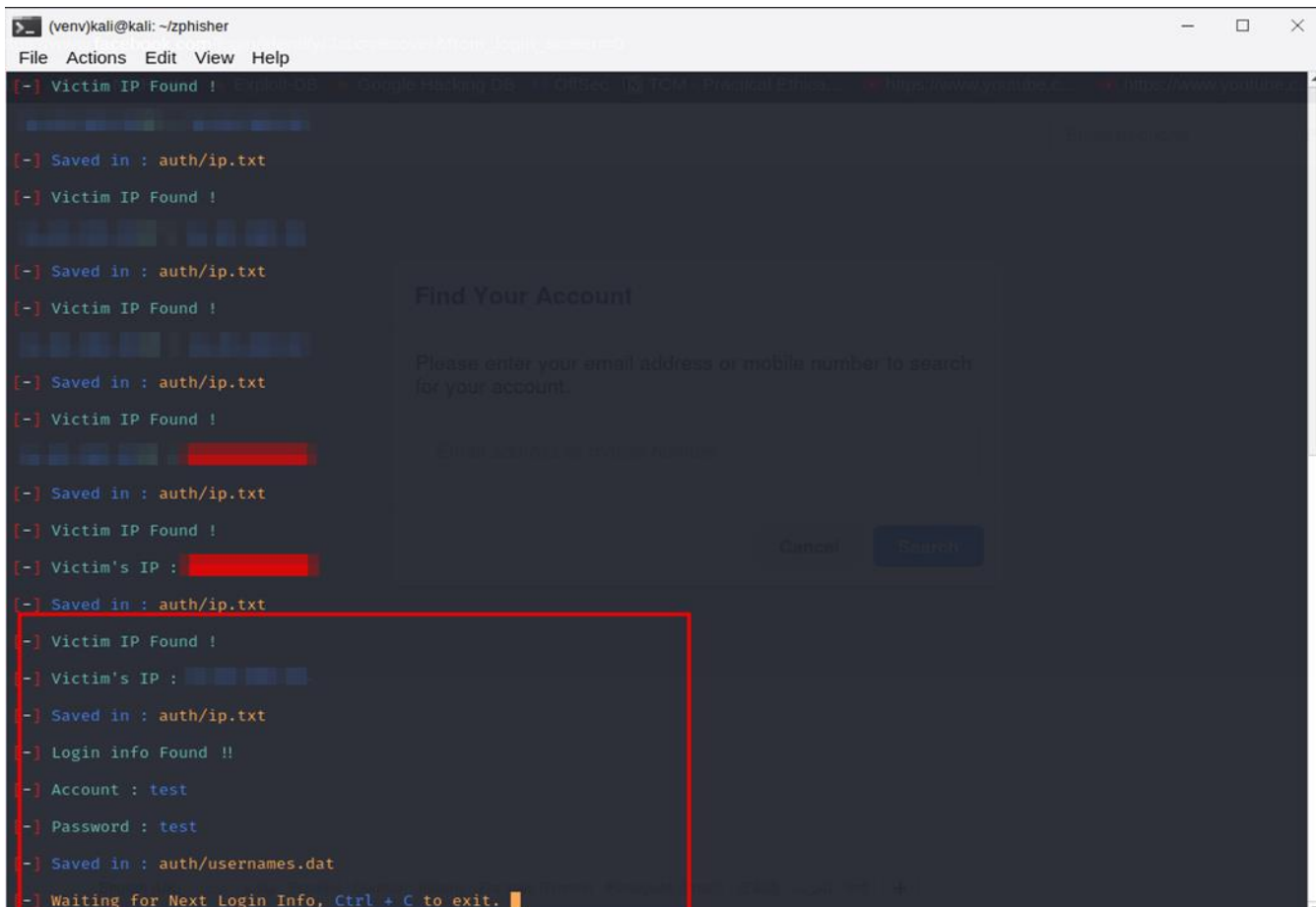
### Scenario:

All test users accessed the phishing link and submitted dummy credentials within five minutes of distribution. No users reported the phishing attempt or questioned the legitimacy of the page. This rapid, uncritical response demonstrates a lack of awareness regarding phishing indicators and highlights the absence of a reporting culture. All captured data was test information, and no real credentials were exposed.

### Steps Taken:

- Test users accessed the phishing link.
- Entered dummy credentials on the phishing page.
- Monitored Zphisher terminal for captured IP addresses and credentials.

### Evidence:



```
(venv)kali@kali: ~/zphisher
File Actions Edit View Help
[-] Victim IP Found !
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Saved in : auth/ip.txt
[-] Victim's IP : 
[-] Saved in : auth/ip.txt
[-] Victim IP Found !
[-] Victim's IP : 
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : test
[-] Password : test
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

*Figure 7: Victims Data*

- Terminal output indicating captured victim IP and login credentials (e.g., “Victim IP Found!”, “Account: test”, “Password: test”).
- Saved logs in auth/ip.txt and auth/usernames.dat.

### 3. Results Analysis

Metric	Value
Phishing Links Sent	1
Links Clicked	1 (100%)
Credentials Submitted	1 (100%)
Victim IPs Captured	1

#### Screenshots/Evidence:

- Screenshot of Zphisher terminal showing successful capture.
- Screenshot of the phishing page as seen by the victim.

#### Interpretation:

- All test users who received the link interacted with the phishing page and entered credentials, demonstrating the effectiveness of the simulation and the risk posed by phishing attacks.

### 4. Severity and Business/Technical Impact

#### Severity Rating:

**High**

#### Business/Technical Impact:

If this had been a real attack:

- The attacker would have obtained valid credentials and IP address, enabling unauthorized access to internal systems or sensitive data.
- Rapid credential compromise could lead to data breaches, financial loss, reputational harm, and non-compliance with data protection regulations.
- The lack of user reporting demonstrates a gap in security culture and incident response readiness.

### 5. Remediation Recommendations

#### Immediate Actions:

- Conduct targeted, interactive phishing awareness training for all staff, focusing on identifying phishing red flags, verifying URLs, and the importance of reporting suspicious activity.
- Clearly communicate reporting procedures and encourage prompt reporting of suspicious emails or links.

**Short-Term Actions:**

- Implement advanced email filtering, anti-phishing technologies, and warning banners for external emails.
- Deploy and enforce multi-factor authentication (MFA) to reduce the impact of compromised credentials.
- Introduce DMARC and browser-based anti-phishing tools.

**Long-Term Actions:**

- Schedule quarterly phishing simulations to reinforce learning, track improvement, and adapt scenarios to evolving threats.
- Foster a strong security culture where users feel comfortable reporting mistakes or suspicious activity.
- Integrate phishing simulation metrics into regular security awareness program reviews.

**6. Next Steps**

- Review and update security awareness training content based on findings.
- Communicate results and recommendations to management and staff.
- Plan and schedule follow-up phishing simulations to track progress.
- Ensure all logs and evidence are securely stored and included in your GitHub repository as required by Hackers10.

## Final Conclusion

This phishing simulation, conducted as part of the Hackers10 Cyber Security Internship, demonstrated that users can be susceptible to well-crafted phishing attacks. Using Zphisher, a simulated phishing campaign was launched with a realistic login page template, successfully capturing test credentials and IP addresses from the target. The results indicate that, even in a controlled environment, users may not always verify the authenticity of web pages before entering sensitive information. These findings highlight the urgent need for enhanced security awareness, technical controls, and regular training to reduce the risk of credential theft, unauthorized access, and broader social engineering threats.

### Recommendations

#### Remediate User Awareness Gaps

- Conduct mandatory security awareness training for all employees, focusing on phishing red flags and safe email/web practices.
- Simulate phishing campaigns regularly to reinforce learning and measure improvement.
- Provide clear reporting channels for employees to flag suspicious emails or links.

#### Strengthen Technical Controls

- Implement advanced email filtering and anti-phishing technologies to reduce malicious emails reaching users.
- Deploy warning banners for emails originating outside the organization.
- Enforce multi-factor authentication (MFA) to reduce the impact of compromised credentials.

#### Policy and Incident Response

- Update and enforce policies on password management and safe internet use.
- Develop and test an incident response plan specifically for phishing and social engineering incidents.
- Encourage a culture of security where users feel comfortable reporting mistakes or suspicious activity.

#### Next Steps

- Address the security awareness and technical gaps identified in this report as a priority.
- Schedule follow-up phishing simulations to track the effectiveness of new training and controls.
- Review and update security policies to reflect current threats and best practices.
- Document and communicate lessons learned to all staff and management.
- Integrate ongoing phishing awareness and testing into the organization's security program.

## Appendices

### A. Tool Output and Logs

- Terminal output from Zphisher showing captured credentials and IP addresses.
- Screenshots of the phishing page and campaign results.

### B. Risk Rating Table

Finding	Risk Level	Impact
Credential Capture	High	Unauthorized access, data breach
User Susceptibility	High	Increased risk of successful phishing attack

### C. Methodology

- **Tools Used:** Kali Linux, Zphisher (with Cloudflared tunneling).
- **Process:** Campaign setup, template selection, link distribution, monitoring, and evidence collection.
- **Scope:** Controlled test with authorized users; no real user data compromised.

## Final Note

This report is intended to provide actionable, evidence-based insights for improving organizational resilience against phishing and social engineering attacks. Prompt implementation of the recommendations and ongoing vigilance are essential to reduce risk and protect both users and organizational