

Phase 3:

Name: Nikhil Kumar

Roll Number: 22BCY10158

Department: SCAI

Course: Computer Science and Engineering

Executive Summary

This project focused on simulating a phishing attack using the Zphisher tool on Kali Linux to understand how attackers steal credentials and how to prevent such threats. A phishing site mimicking Instagram was hosted using LocalXpose for external access. The simulation successfully captured user credentials, highlighting the threat's severity. The project emphasizes the importance of user awareness, secure browsing, and multi-factor authentication in preventing phishing attacks.

Project Overview

Problem Statement

Phishing remains one of the most widespread and dangerous cyber threats. This project demonstrates how attackers create deceptive web pages to steal user credentials and the implications of such attacks.

Objectives

- Understand the inner workings of phishing attacks.
- Simulate a phishing scenario using open-source tools.
- Analyze captured data and recommend countermeasures.

Scope of Work

Included: Phishing simulation, credential capture, tool configuration, and analysis.

Excluded: Real-world exploitation or targeting actual users.

Tools & Lab Setup

Primary Tools Used

- Kali Linux
- Zphisher
- LocalXpose
- Apache Server
- Python

Environment Details

- **Virtual Machine Setup:** VirtualBox
- **Target VM:** Not applicable (external target via phishing link)
- **Network Mode:** NAT with LocalXpose Port Forwarding

Tool Configuration & Commands

- `git clone https://github.com/htr-tech/zphisher.git`
- `cd zphisher`
- `bash zphisher.sh` or `./zphisher.sh`
- LocalXpose login and access token setup

Implementation & Execution Summary

Key Steps Performed:

1. Environment Setup:

- Kali Linux booted on VirtualBox.
- Tools installed and internet connection verified.

2. Traffic Simulation / Attack Execution:

- Instagram page selected via Zphisher.
- Phishing link generated and masked using LocalXpose.

3. Packet Capture / Vulnerability Scanning:

- Victim clicks a link and enters credentials.
- IP address, browser info, and timestamps logged.

4. Packet Analysis & Data Extraction:

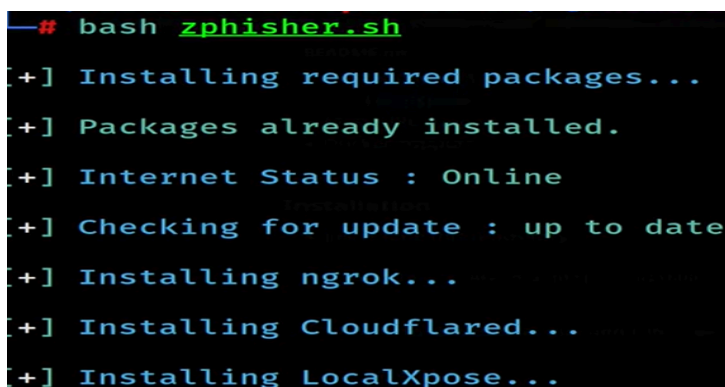
- Data saved in log files by Zphisher.
- Observed user-agent and timestamps.

5. Result Documentation & Mitigation Research:

- Screenshots taken.
- Recommendations drafted.

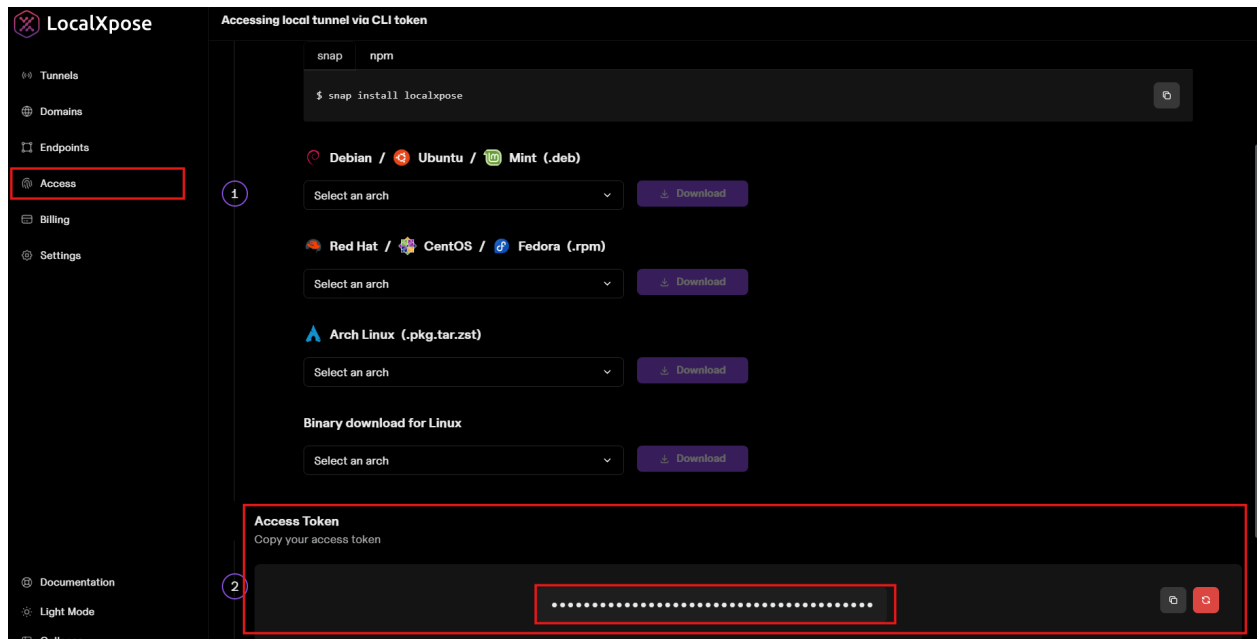
Screenshots / Evidence

- Zphisher launch screen

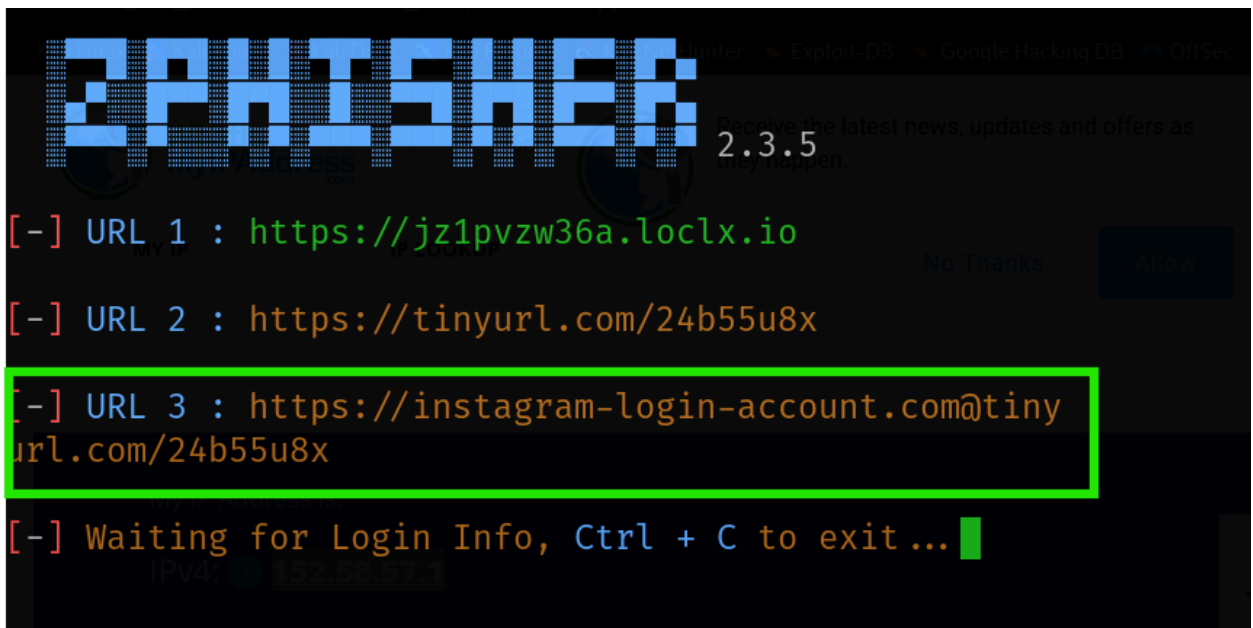


```
# bash zphisher.sh
[+] Installing required packages...
[+] Packages already installed.
[+] Internet Status : Online
[+] Checking for update : up to date
[+] Installing ngrok...
[+] Installing Cloudflared...
[+] Installing LocalXpose...
```

- LocalXpose access setup



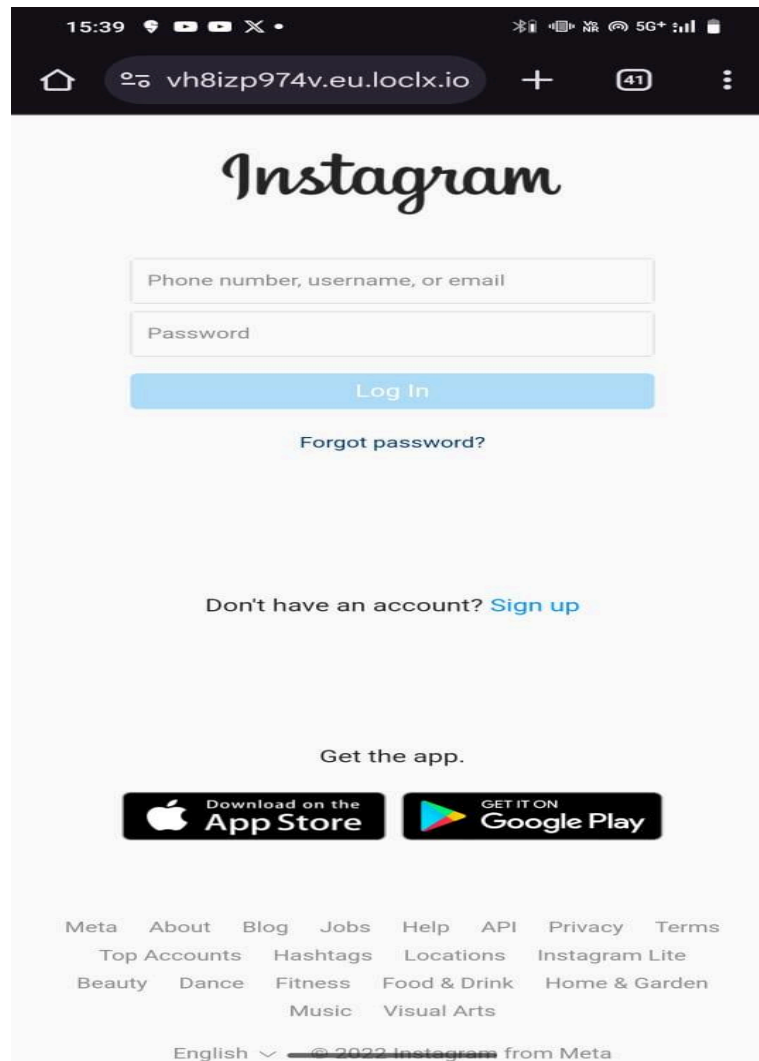
- Phishing URL generated



- Captured credentials log

```
[ - ] Victim IP Found !  
[ - ] Victim's IP : 152.58.57.1  
[ - ] Saved in : auth/ip.txt  
[ - ] Login info Found !!  
[ - ] Account : xyz_123  
[ - ] Password : exposed123
```

- Victim's login screen preview



Findings & Analysis

- Login credentials were successfully captured.
- Zphisher effectively masked the phishing URL.
- Modern browsers did not immediately block LocalXpose links.
- Even a simple phishing tool poses a serious threat to unaware users.

Security Recommendations

- Use encrypted protocols (HTTPS, SSH)
- Enable Two-Factor Authentication (2FA)
- Verify URLs before logging in
- Disable unused ports and services
- Use anti-phishing browser extensions
- Educate users on social engineering

Learning Outcomes

- Learned how phishing tools like Zphisher operate
- Understood port forwarding using LocalXpose
- Gained experience in Linux-based attack simulation
- Understood human vulnerabilities in cybersecurity

Future Scope

- Integrate real-time detection tools to flag phishing links
- Extend simulation to mobile devices and advanced UIs
- Create a phishing awareness training module for users