Simulating an Internal Phishing Attack Using Zphisher Tool

Date: 19.4.2025

Prepared By:

Nelson Mbua Mosisah

Overview

This project demonstrates a phishing attack using the Zphisher tool on Kali Linux. The attack targets a victim by creating a fake login page that mimics a popular website, capturing the user's credentials when they attempt to log in. **This project is intended for educational purposes only. Unauthorized phishing attacks are illegal and unethical. Always obtain proper authorization before conducting any form of penetration testing.**

Tools Used

- **Zphisher**: An automated phishing tool that supports various platforms.
- **Kali Linux**: A Debian-based Linux distribution used for penetration testing and security research.
- **Ngrok/Serveo**: Services to expose the phishing page to the internet.
-

Installation

Prerequisites

- Kali Linux installed on your machine.
- Git installed on Kali Linux.

Steps to Install Zphisher

1. **Update your system**: sudo apt-get update && sudo apt-get upgrade
2. **Clone the Zphisher repository**: git clone https://github.com/htr-tech/zphisher.git

3. **Navigate to the Zphisher directory**: cd zphisher
4. **Give execution permissions**: bash +x zphisher.sh

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$  git clone https://github.com/htr-tech/zphisher.git
```

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$  git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 1801, done.
remote: Counting objects: 100% (336/336), done.
remote: Compressing objects: 100% (85/85), done.
remote: Total 1801 (delta 263), reused 251 (delta 251), pack-reused 1465 (from 1)
Receiving objects: 100% (1801/1801), 28.68 MiB | 2.61 MiB/s, done.
Resolving deltas: 100% (817/817), done.
```

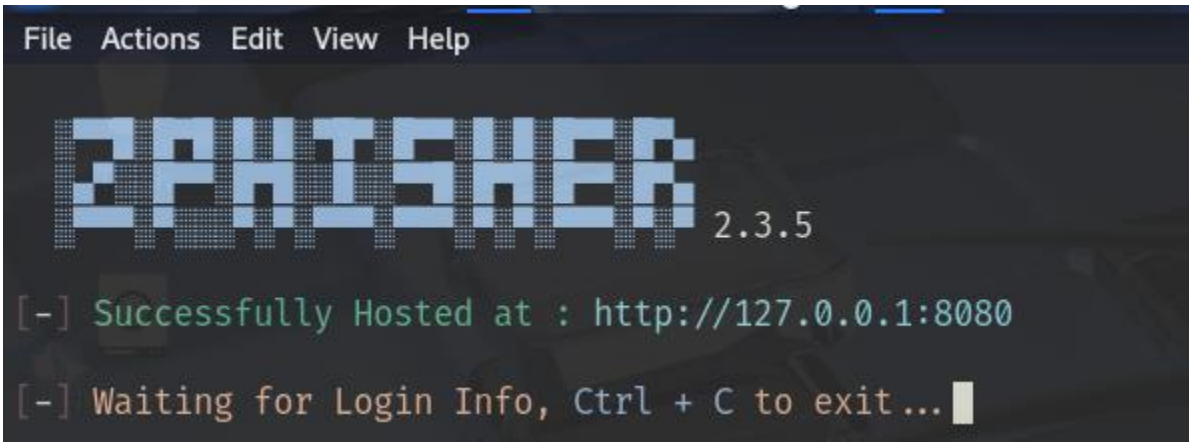
How to Perform the Phishing Attack

Step 1: Run Zphisher

1. **Start Zphisher**: ./zphisher.sh
2. **Select the phishing attack template** (e.g., Facebook, Instagram, Google).
3. **Choose the attack method** (Ngrok is recommended for easy public sharing).

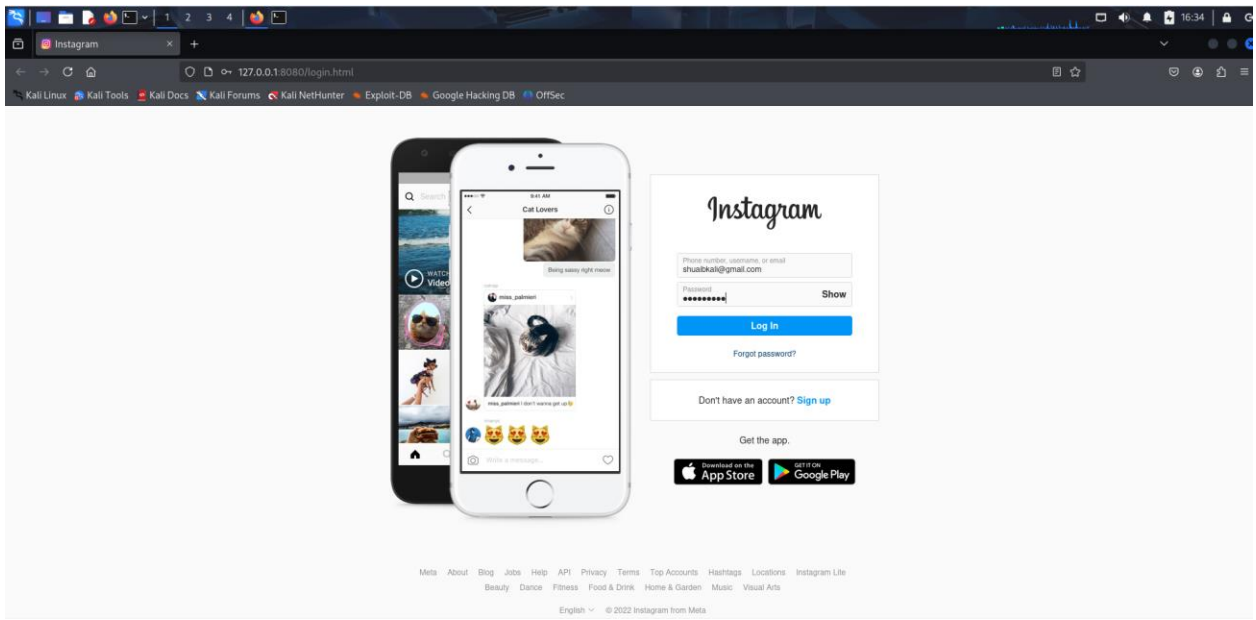
Step 2: Customize the Phishing Page (Optional)

1. **Edit the template** (Optional):
    a. Customize the HTML/CSS files in the `sites` directory to make the phishing page more convincing.
    b. Example: nano sites/instagram/index.html



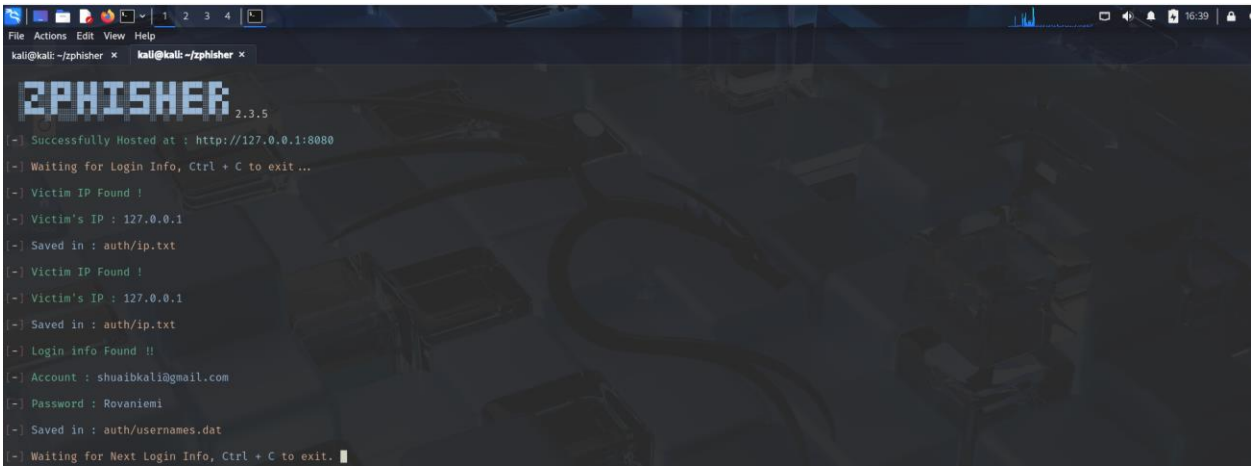
Step 3: Deploy and Monitor

1. **Copy the phishing URL** generated by Ngrok or Serveo.
2. **Distribute the phishing URL** to the target (with permission).
3. **Monitor for login attempts** and view captured credentials in the Zphisher terminal.



Step 4: Stop the Attack

1. **Terminate Zphisher**:
    a. Stop the attack by closing the terminal window or pressing CTRL + C.
2. **Analyze the captured data**.



Ethical Considerations

- **Reflect on the Ethics**: Phishing is a serious security threat, and this knowledge should be used responsibly.
- **Report the Results**: If part of a security assessment, document your findings and provide recommendations to mitigate such attacks.

License

Disclaimer

This project is for educational purposes only. The author does not endorse or condone the use of this tool for illegal or unethical purposes. Use this information responsibly.

Recommendations:

- Reinforce phishing awareness through regular, targeted training.
- Introduce just-in-time learning for users who interacted with the phishing emails.
- Encourage a strong reporting culture with easy-to-use tools.
- Conduct periodic follow-up simulations to track progress.

Outcome: The simulation met its objectives by providing actionable insights into employee behavior and organizational readiness. Next steps include incorporating lessons learned into ongoing training and security policies to enhance the organization's resilience to real-world threats.

Conclusion

The phishing simulation successfully identified both strengths and gaps in employee cybersecurity awareness. While a majority of users did not interact with the phishing content, a notable percentage clicked on links or entered credentials, highlighting the need for continuous education.

Report Prepared By:

Nelson Mbua Mosisah

Cybersecurity Analyst