

Report on Real Simulation Using Zphisher

Date: 2025-10-20

Environment: Kali Linux (local VM), localhost web server

Tool: Zphisher (htr-tech/zphisher) — cloned from GitHub

Purpose: Controlled phishing simulation for learning social-engineering delivery and link generation. No real targets used.

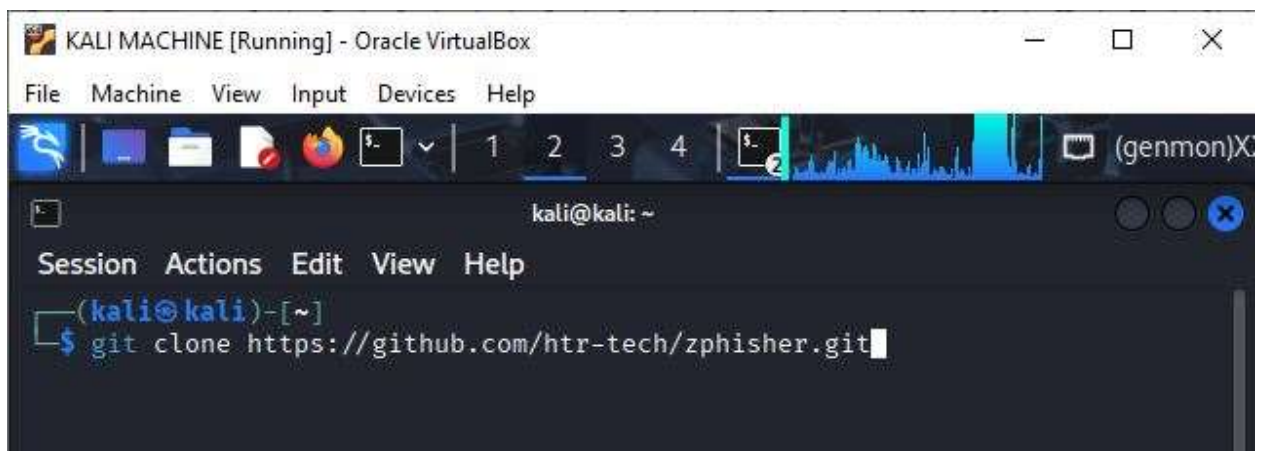
Objective

The objective of this simulation was to understand the process of conducting a phishing attack using **Zphisher**, a popular open-source phishing toolkit. This exercise was performed strictly for educational and research purposes within a controlled environment.

Procedure

1. Cloning the Repository

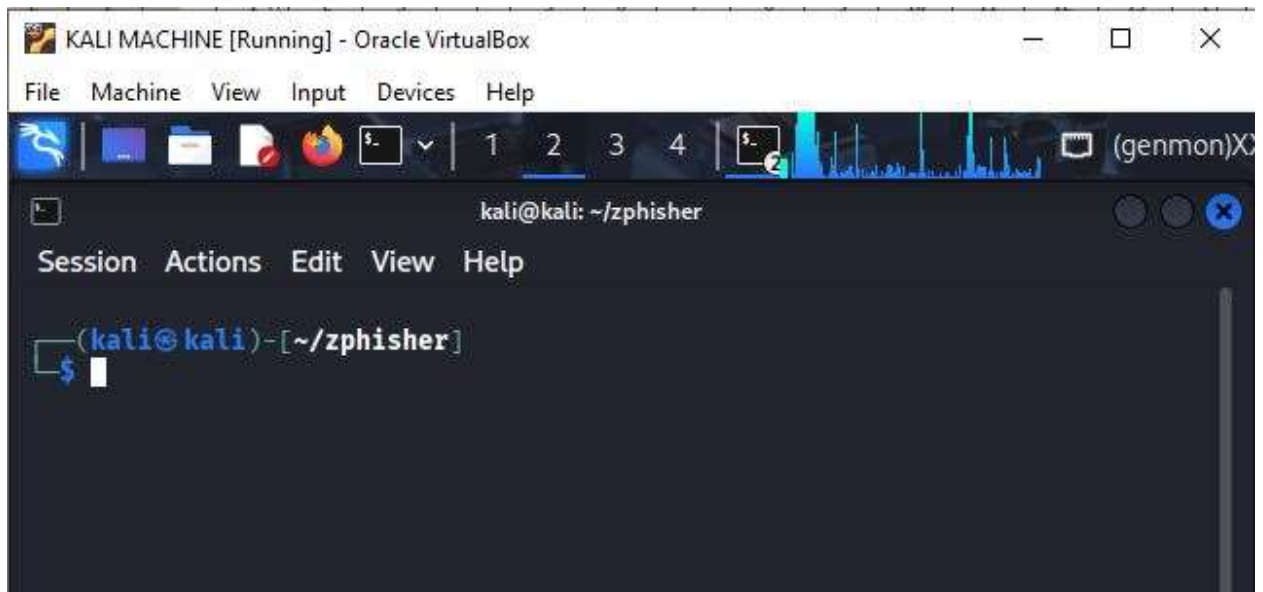
The Zphisher tool was obtained from GitHub by running the following command in the Kali Linux terminal:

A screenshot of a Kali Linux terminal window titled "KALI MACHINE [Running] - Oracle VirtualBox". The terminal shows the command `git clone https://github.com/htr-tech/zphisher.git` being entered. The prompt is `(kali@kali)-[~]`. The terminal window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The status bar at the bottom shows "kali@kali: ~".

```
KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
(kali@kali)-[~]
$ git clone https://github.com/htr-tech/zphisher.git
```

2. Accessing the Directory

The contents of the cloned directory were verified using the command:



3. Executing the Bash Script

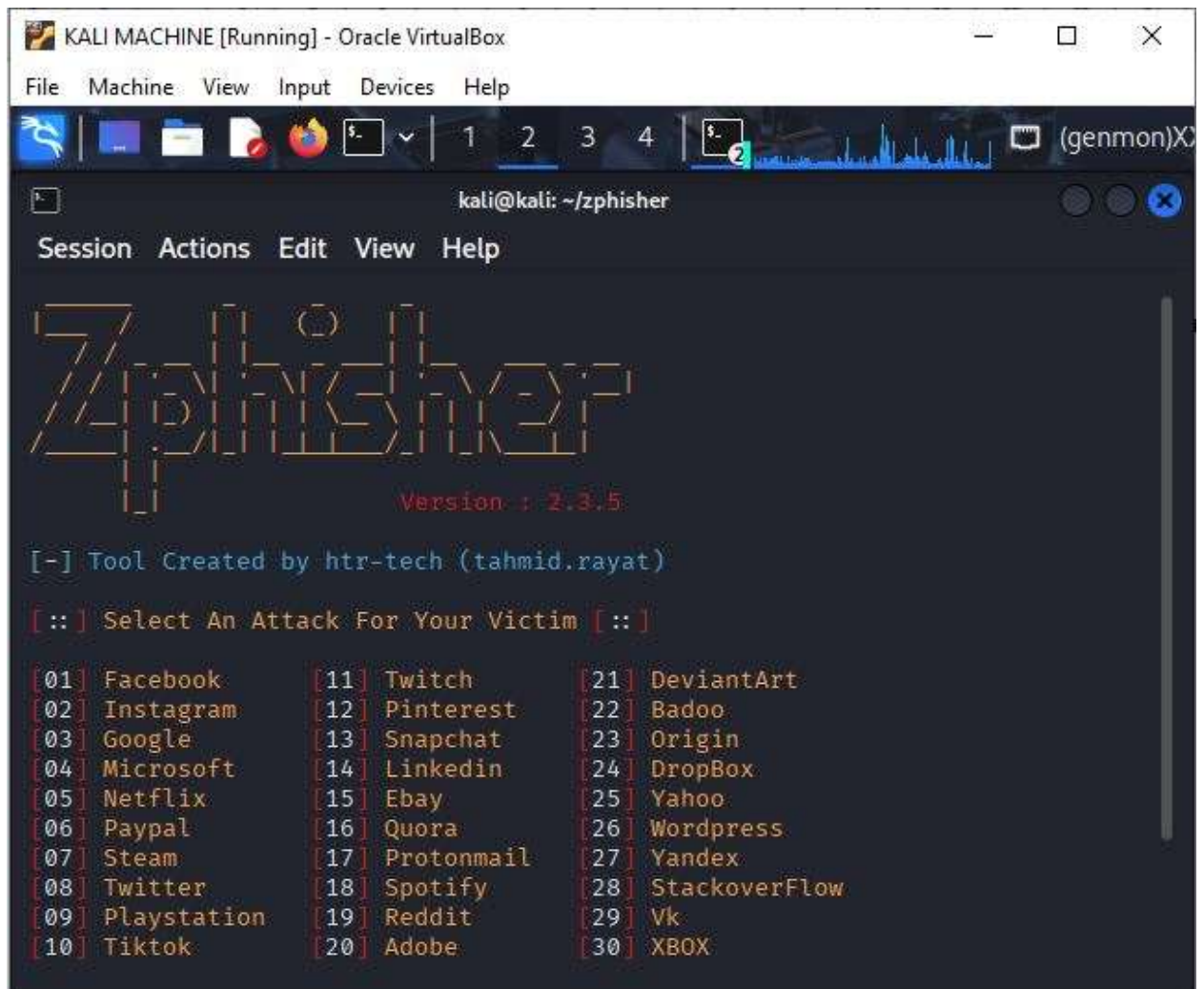
The main script file, `zphisher.sh`, was executed using the command:



```
KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~/zphisher
Session Actions Edit View Help
(kali@kali)-[~/zphisher]
$ ls
auth          LICENSE      README.md   scripts     zphisher.sh
Dockerfile    make-deb.sh run-docker.sh zphisher
(kali@kali)-[~/zphisher]
$ bash zphisher.sh
```

4. Selecting Target Platform

From the list of available platforms, **PayPal (option 6)** was selected as the target for this simulation.



5. Customizing the Link

The tool generated multiple link options. For this controlled project, **localhost** was used to host the phishing page, ensuring that the exercise remained within a safe and legal environment.



The screenshot shows a terminal window titled "KALI MACHINE [Running] - Oracle VirtualBox". The terminal prompt is "kali@kali: ~/zphisher". The menu for "zphisher 2.3.5" is displayed, listing three options: "01] Localhost", "02] Cloudflared [Auto Detects]", and "03] LocalXpose [NEW! Max 15Min]". Below the menu, it says "[-] Select a port forwarding service :".

```
KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~/zphisher
Session Actions Edit View Help
zPHISHER 2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service :
```



The screenshot shows the same terminal window as above, but now it displays the success message: "[-] Successfully Hosted at : http://127.0.0.1:2222". Below this, it says "[-] Waiting for Login Info, Ctrl + C to exit ...".

```
KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~/zphisher
Session Actions Edit View Help
zPHISHER 2.3.5
[-] Successfully Hosted at : http://127.0.0.1:2222
[-] Waiting for Login Info, Ctrl + C to exit ...
```

6. Creating a Legitimate-looking Email

The generated phishing link was embedded within a sample email designed to appear legitimate. This was done to demonstrate how attackers can use social engineering to deceive victims into clicking malicious links.

Update Your PayPal Login Details

Hi John,

We hope you're doing well. This is a quick reminder that your PayPal account login details may need updating to ensure continued access and account security.

To proceed, please log in to your PayPal account directly [here](#) and follow the prompts to update your username and password if necessary.

For your safety, please do not click on any links from unknown sources or share your login credentials via email.

Let us know once you've completed the update or if you run into any issues.

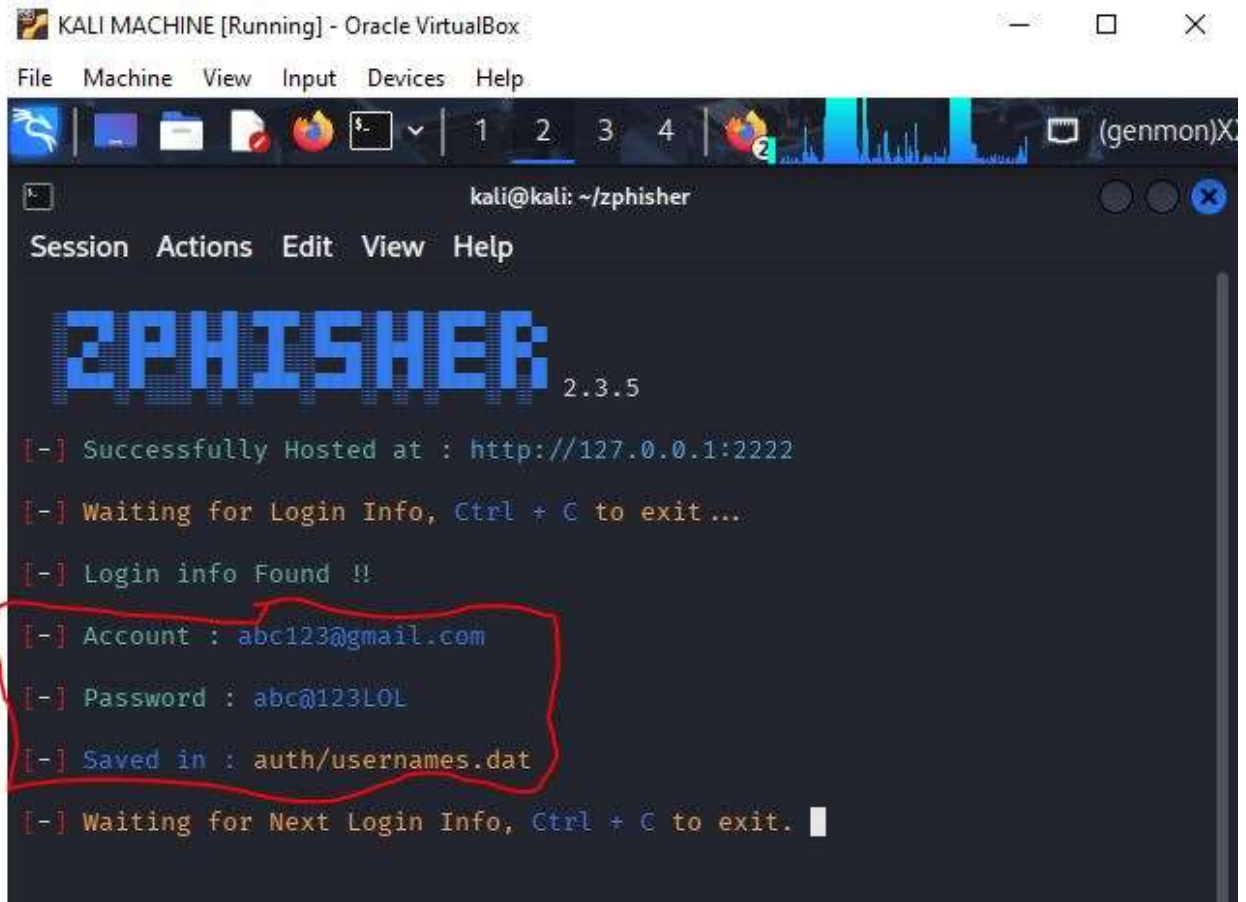
Best regards,
The PayPal Team.



Log In

© 2014 PayPal. All rights reserved.

The image below shows the backend which is the attacker side, it contains the victim's login details supplied in the paypal login space above.



```
KALI MACHINE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~/zphisher
Session Actions Edit View Help
ZPHISHER 2.3.5
[-] Successfully Hosted at : http://127.0.0.1:2222
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Login info Found !!
[-] Account : abc123@gmail.com
[-] Password : abc@123LOL
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

Conclusion

This simulation demonstrated how phishing attacks can be crafted and executed using publicly available tools like Zphisher. It highlights the importance of cybersecurity awareness and vigilance against social engineering attacks.

All activities were performed in a **controlled environment** for **ethical and educational purposes only**, without targeting or compromising any real user data or systems.