



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Academic Year: 2025-26

Semester: V

Class / Branch: TE IT Subject: Security Lab (SL)

Subject Lab Incharge: Prof. Vishal Badgujar

EXPERIMENT NO. 10

Aim: To simulate a phishing attack using Zphisher.

Theory:

Phishing: Phishing is a form of online fraud in which hackers attempt to get your private information such as passwords, credit cards, or bank account data. This is usually done by sending false emails or messages that appear to be from trusted sources like banks or well-known websites.

What is a Phishing Attack?

Phishing is another type of cyber-attack. Phishing got its name from "phish" meaning fish. It's a common phenomenon to put bait for the fish to get trapped. Similarly, phishing works. It is an unethical way to dupe the user or victim to click on harmful sites. The attacker crafts the harmful site in such a way that the victim feels it to be an authentic site, thus falling prey to it. The most common mode of phishing is by sending spam emails that appear to be authentic and thus, taking away all credentials from the victim. The main motive of the attacker behind phishing is to gain confidential information like:

- Password
- Credit card details
- Social security numbers
- Date of birth

The attacker uses this information to further target the user impersonate the user and cause data theft. The most common type of phishing attack happens through email. Phishing victims are tricked into revealing information that they think should be kept private. The original logo of the email is used to make the user believe that it is indeed the original email. But if we carefully look into the details, we will find that the URL or web address is not authentic.

Zphisher - Automated Phishing Tool



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



Zphisher is a powerful open-source tool Phishing Tool. It became very popular nowadays and is used to do phishing attacks on Target. Zphisher is easier than Social Engineering Toolkit. It contains some templates generated by a tool called Zphisher and offers phishing templates webpages for 33 popular sites such as Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Proton mail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc. It also provides an option to use a custom template if someone wants. This tool makes it easy to perform a phishing attack. Using this tool you can perform phishing in (wide area network). This tool can be used to get credentials such as id, password.

Uses and Features of Zphisher:

- Zphisher is open source tool.
- Zphisher is a tool of Kali Linux.
- Zphisher is used in Phishing attacks.
- Zphisher tool is a very simple and easy tool.
- Zphisher tool is a very simple and easy tool.
- Zphisher tool is a lightweight tool. It does not take extra space.
- Zphisher is written in bash language.
- Zphisher creates phishing pages for more than 33 websites.
- Zphisher creates phishing pages of popular sites such as Facebook, Instagram, Google, Snapchat, Github, Yahoo, Protonmail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, etc

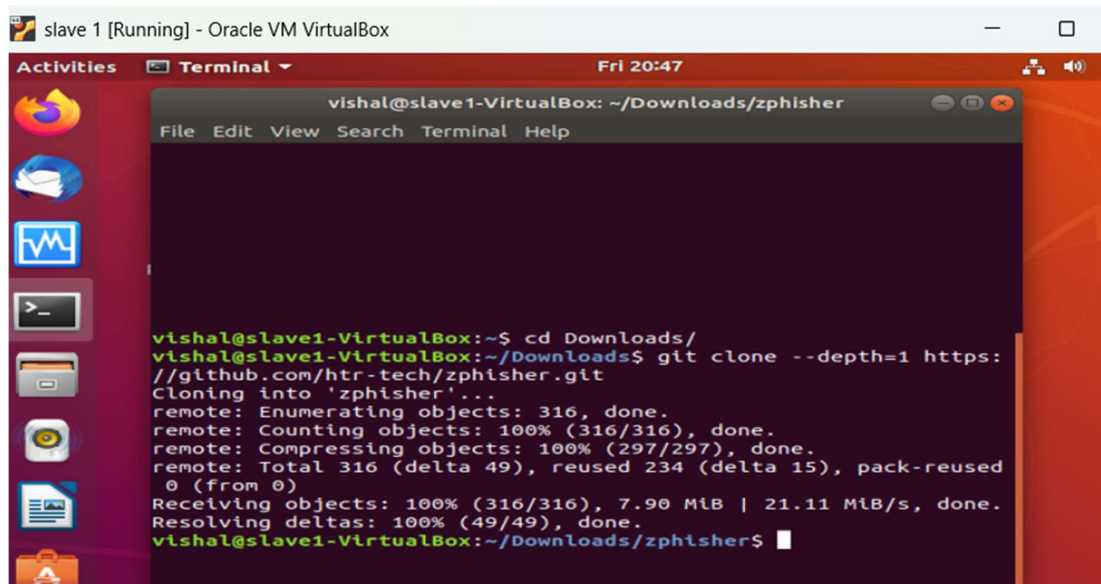
Installation:

Step 1: To install the tool first go to the desktop directory and then install the tool using the following commands.

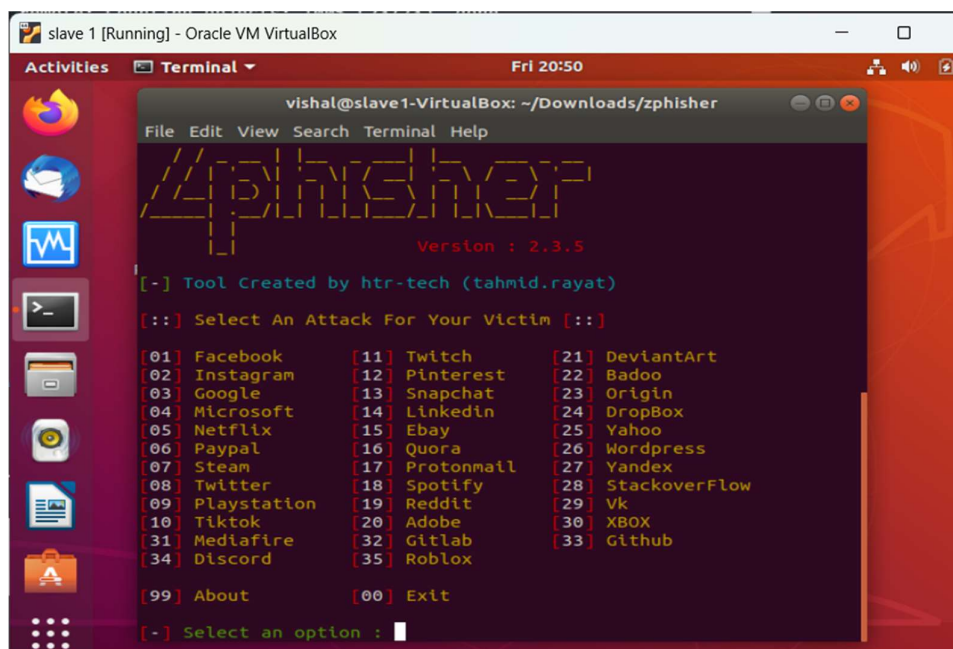
```
cd Downloads
```

```
git clone git://github.com/htr-tech/zphisher.git
```

```
cd zphisher
```



Step 2: Now you are in `zphisher` directory , use the following command to run the tool.
`bash zphisher.sh`



Step 3: The tool has started running successfully. Now you have to choose the options from the tool for which you have to make the phishing page.

Step 4: From these options, you can choose the number for which you have to create a phishing page. Suppose you want to create a phishing page for LinkedIn then choose option 14.



```
slave 1 [Running] - Oracle VM VirtualBox
Fri 20:52
vishal@slave1-VirtualBox: ~/Downloads/zphisher
File Edit View Search Terminal Help
[01] Facebook [11] Twitch [21] DeviantArt
[02] Instagram [12] Pinterest [22] Badoo
[03] Google [13] Snapchat [23] Origin
[04] Microsoft [14] LinkedIn [24] DropBox
[05] Netflix [15] Ebay [25] Yahoo
[06] Paypal [16] Quora [26] Wordpress
[07] Steam [17] Protonmail [27] Yandex
[08] Twitter [18] Spotify [28] Stackoverflow
[09] Playstation [19] Reddit [29] Vk
[10] Tiktok [20] Adobe [30] XBOX
[31] Mediafire [32] Gitlab [33] Github
[34] Discord [35] Roblox

[99] About [00] Exit

[-] Select an option : 14

ZPHISHER 2.3.5

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

[-] Select a port forwarding service : 01
```

Step 5: Suppose you want to host it on localhost then the first option then type 1. And custom port as n for NO

```
vishal@slave1-VirtualBox: ~/Downloads/zphisher
File Edit View Search Terminal Help
[-] Select a port forwarding service : 01
[?] 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...

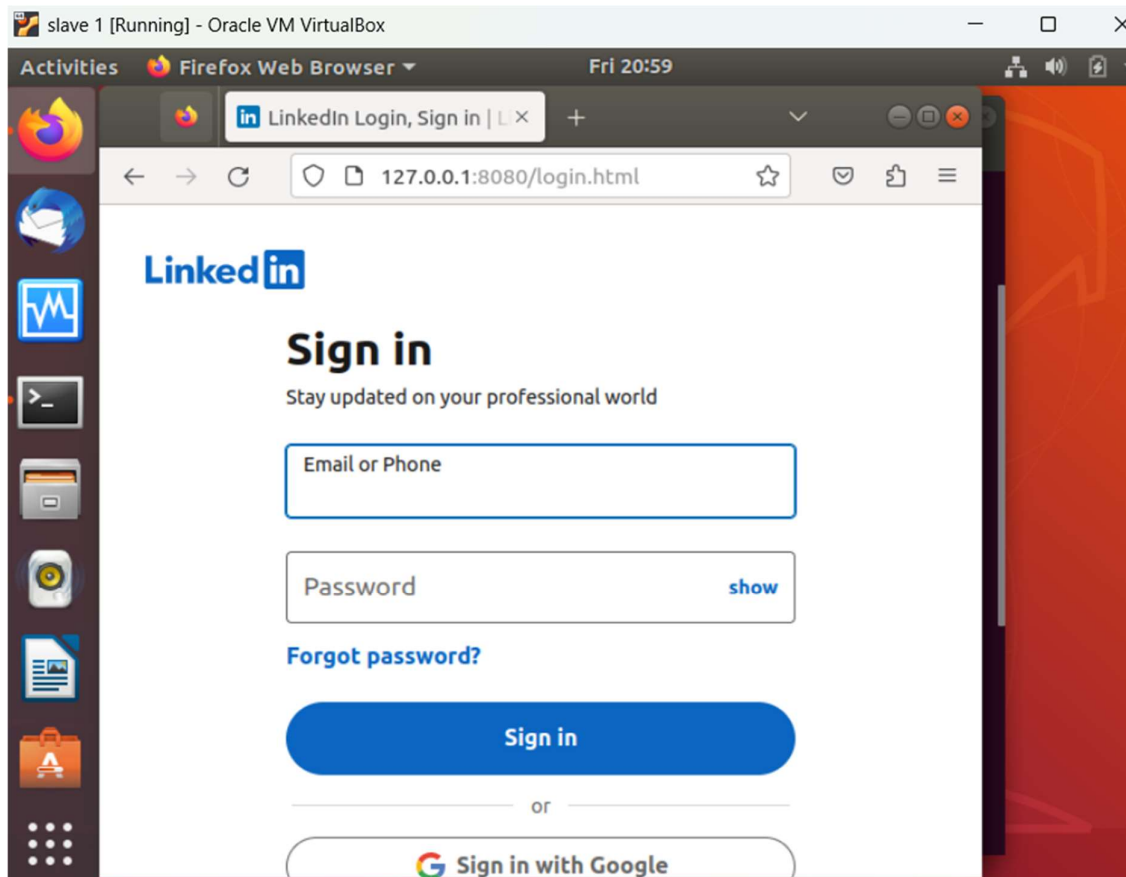
ZPHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C to exit...
```



Step 6: Using Zphisher tool, create a phishing page of Linkdin and get credentials (user id and password) of victim. Now use the browser and open link of localhost as shown in above fig.
<http://127.0.0.1:8080>

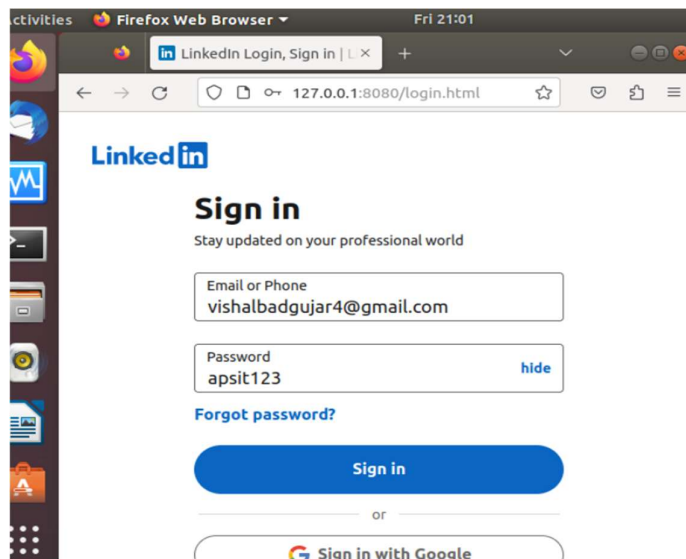
This is the phishing page we have opened. Now the user has to enter his/her id password.



Step 7: put userid and password in authentication page.



PARSHVANATH CHARITABLE TRUST'S
A. P. SHAH INSTITUTE OF TECHNOLOGY
Department of Information Technology
(NBA Accredited)



Step 8: check the terminal to view the recorded victims credentials from phishing website.

```
vishal@slave1-VirtualBox: ~/Downloads/zphisher
File Edit View Search Terminal Help

ZPHISHER 2.3.5

[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP : 127.0.0.1
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : vishalbadgujar4@gmail.com
[-] Password : apsit123
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```



PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)



We got the details of ID and password here. This is how you can perform phishing using zphisher. You can send these links to the victim. Once the victim clicks on the link and types the id password it will be reflected on the terminal itself.

This is how zphisher works. This is one of the best tools that can be used for phishing attacks. You can choose the option as per your requirement. zphisher is a powerful open-source tool Phishing Tool. It became very popular nowadays and is used to do phishing attacks. zphisher is easier than Social Engineering Toolkit.

Conclusion: Write your own findings.