SCENARIO TITLE: **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

☐Advanced

Time Required: 120 minutes

Audience: ☒Instructor-led ☐Self-taught

Scenario Learning Outcomes: Upon completion of this scenario, 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 engage in the development of a simulated deceptive webpage, commonly known as phishing, employing the **Zphisher** tool. Note that Zphisher is a phishing tool created for educational purposes to help people understand how phishing attacks work and to raise awareness about online security. It offers phishing template webpages for numerous popular sites such as Facebook and Instagram. Once the victim clicks on the link and types the id password it will be reflected on the terminal itself.

Additionally, the lab will provide insights into rendering this deceptive page accessible on the internet via **ngrok**. Note that Ngrok provides a convenient and efficient way to share your localhost server with anyone, anywhere without getting filtered by, for example, firewalls. It is commonly used by developers during the development and testing phases of web applications to share their work with others without deploying it on a public server. However, it can also be used by attackers to bypass network security measures and increase the effectiveness of their phishing attacks.

Systems and Tools Used:

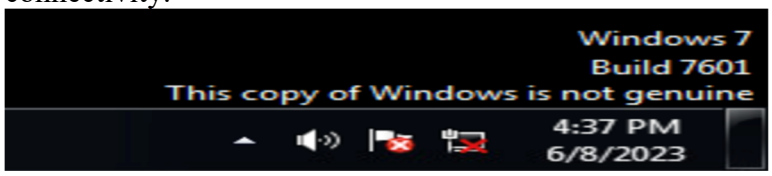
- Kali Linux (u: root, p: toor)
  - Zphisher & ngrok
- Windows 7 (u:administrator, p: Pa$$w0rd)
- Power down all other systems

Environment Setup:

Please refer to the OCRI Sandbox Setup document. In this lab, we will be using Kali Linux and Windows 7 machine instances.

Environment Setup Verification: Before starting this pen test make sure the environment setup is done and deployment is successful.

- Verify that the remote connection to Kali Linux machine is successful and the machine is connected to internet without any error. If there is an error in the Internet Connection that means the deployment is not proper.
- Verify that the remote connection to windows machine is successful and the machine is connected to internet without any error. The image below shows an error with internet connectivity.



- Do not start the pen test if deployment is not successful. Delete the deployment and redeploy it again.

Steps to execute "Phishing Attack" in the Sandbox:

This scenario is executed in 2 parts: firstly, the establishment of the Facebook phishing webpage locally using Zphispher; secondly, the utilization of ngrok to make this fake Facebook page publicly available.

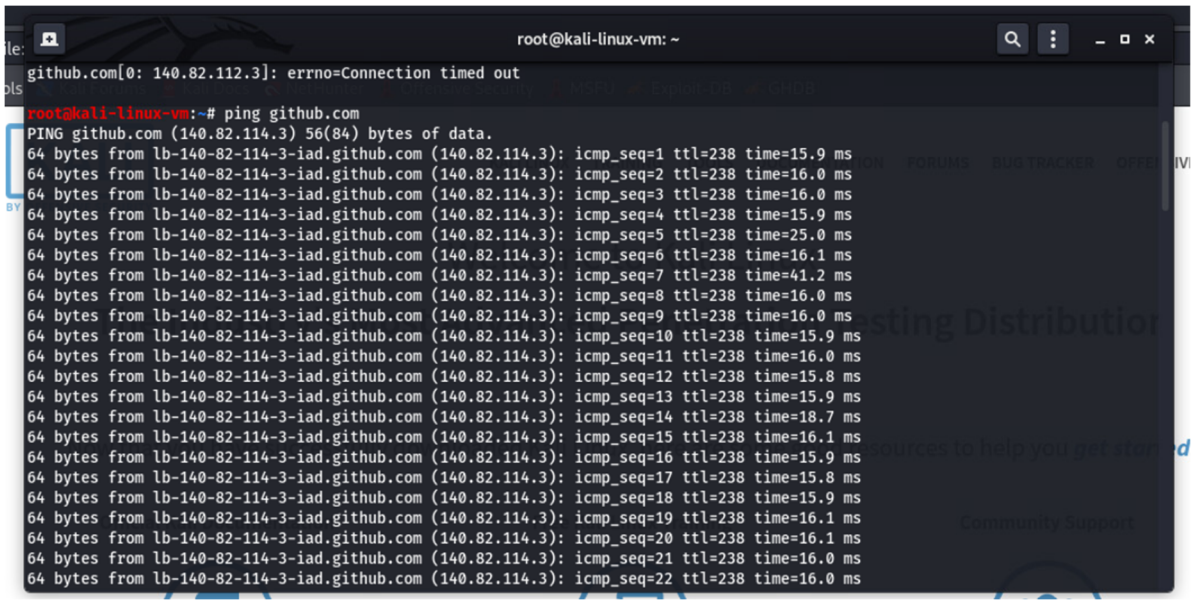
Part One: Setup Phishing page on a local server (Kali Linux)

1. Login to Sandbox using the url: https://sandbox02.cech.uc.edu/ and using the credentials provided to you.
2. Login to Kali Linux machine (username: root , password: toor)
3. Open terminal and clone **Zphispher** using the following command. (***Terminal#1 on Linux***)

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

```
root@kali-linux-vm:~# 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 5 (delta 2), pack-reused 1786
Receiving objects: 100% (1794/1794), 28.69 MiB | 29.67 MiB/s, done.
Resolving deltas: 100% (805/805), done.
root@kali-linux-vm:~#
```

If you encounter any error like shown below, you may be behind a firewall or using a proxy server, which could blocks your connection to GitHub. Check your network settings and ensure that GitHub is not blocked by using the command: "**ping github.com**". And try the **git** command again.

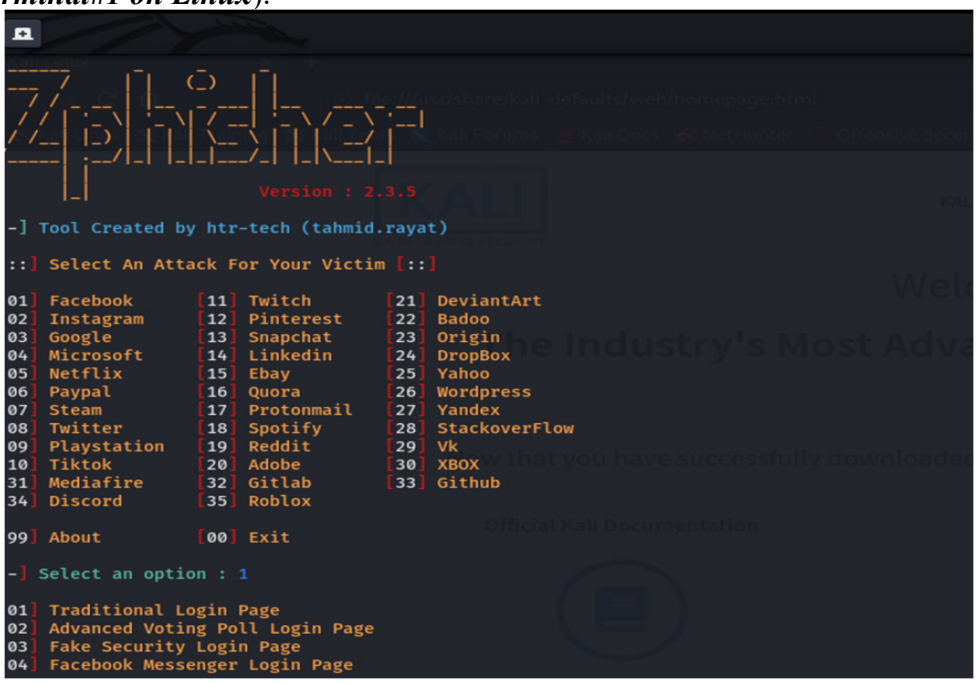


4. Change the directory path to Zphisher and start it using the following commands (***Terminal#1 on Linux***):

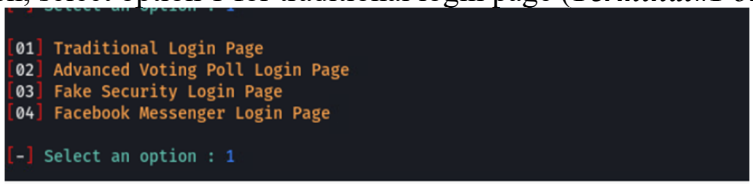
   cd zphisher

   bash zphisher.sh

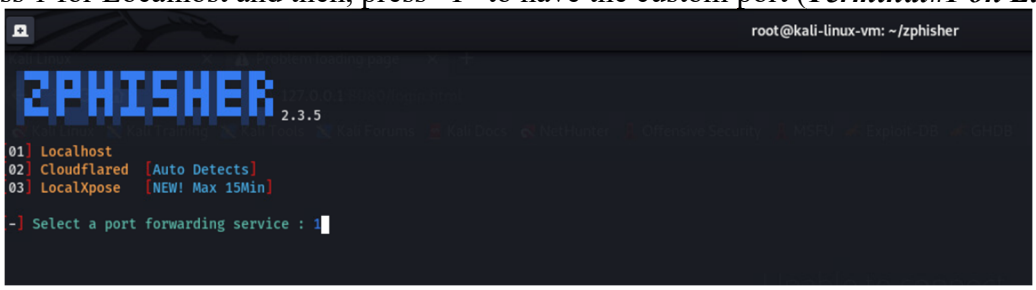
5. Once Zphisher starts the below screen appears. Select option 1 to choose Facebook (***Terminal#1 on Linux***).

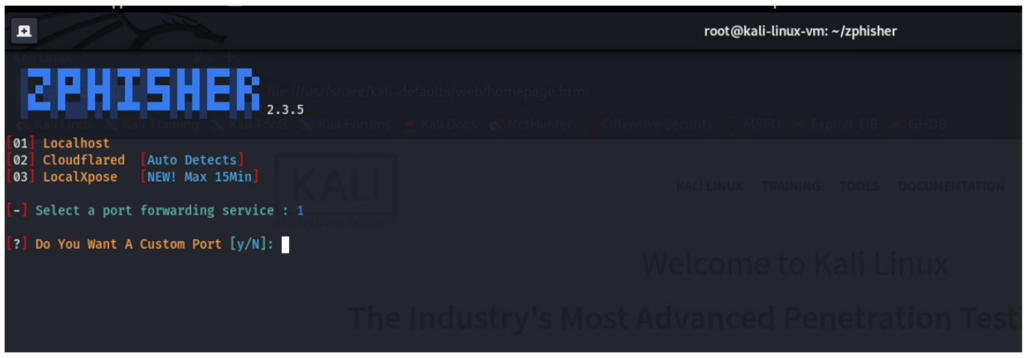


6. Then, select option 1 for traditional login page (***Terminal#1 on Linux***).

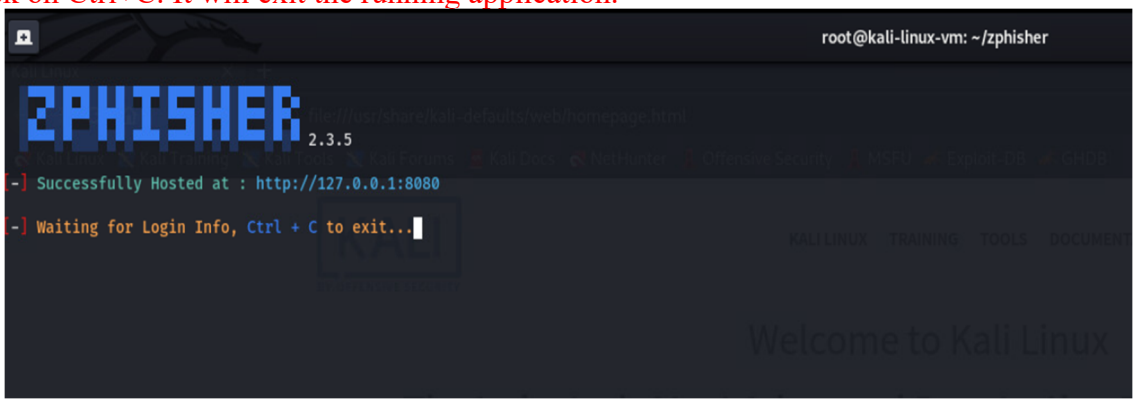


7. Press 1 for Localhost and then, press 'Y' to have the custom port (***Terminal#1 on Linux***).

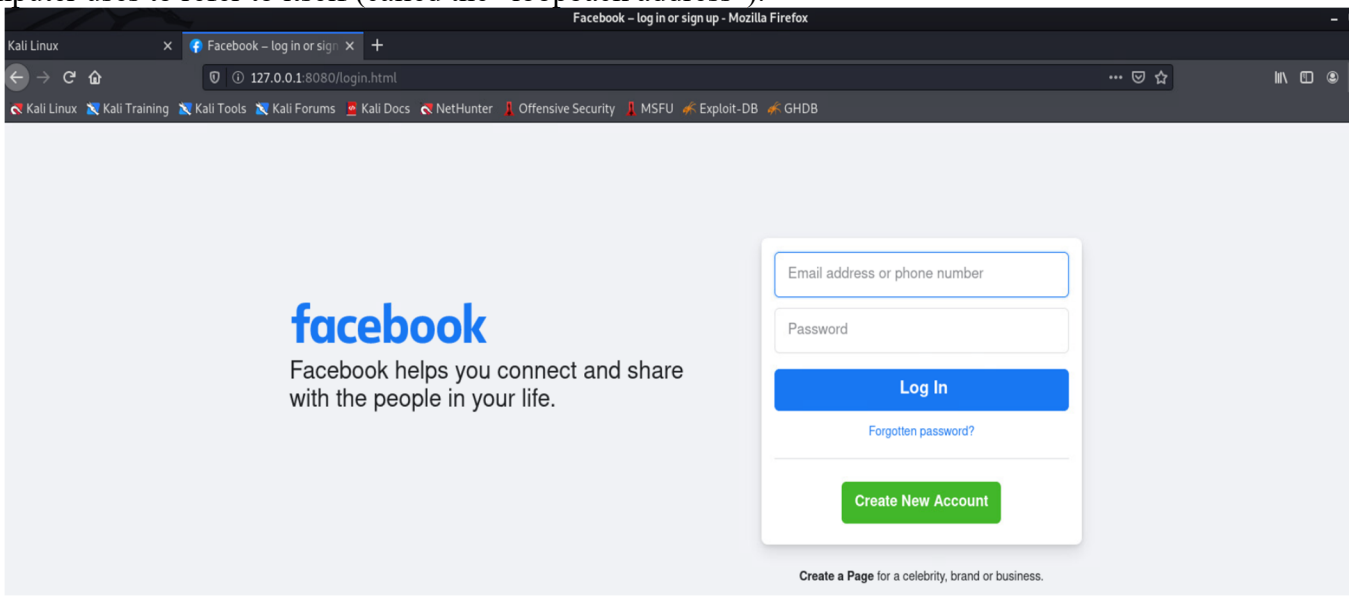




8. Give any port number, for example, 8080. Zphisher hosts the local server on that port. See the successful message as shown in the screenshot below (***Terminal#1 on Linux***). Do not click on Ctrl+C. It will exit the running application.



9. Open the browser and hit the URL taken from the above step (http://127.0.0.1:8080). You'll see the **fake** Facebook page. (***Bowser on Linux***) Note that 127.0.0.1 is the IP address a computer uses to refer to itself (called the "loopback address").



10. Try logging in with any credentials. The IP address of the victim and username and password are stored in "ip.txt" and "username.dat", respectively. (***Browser on Linux***)

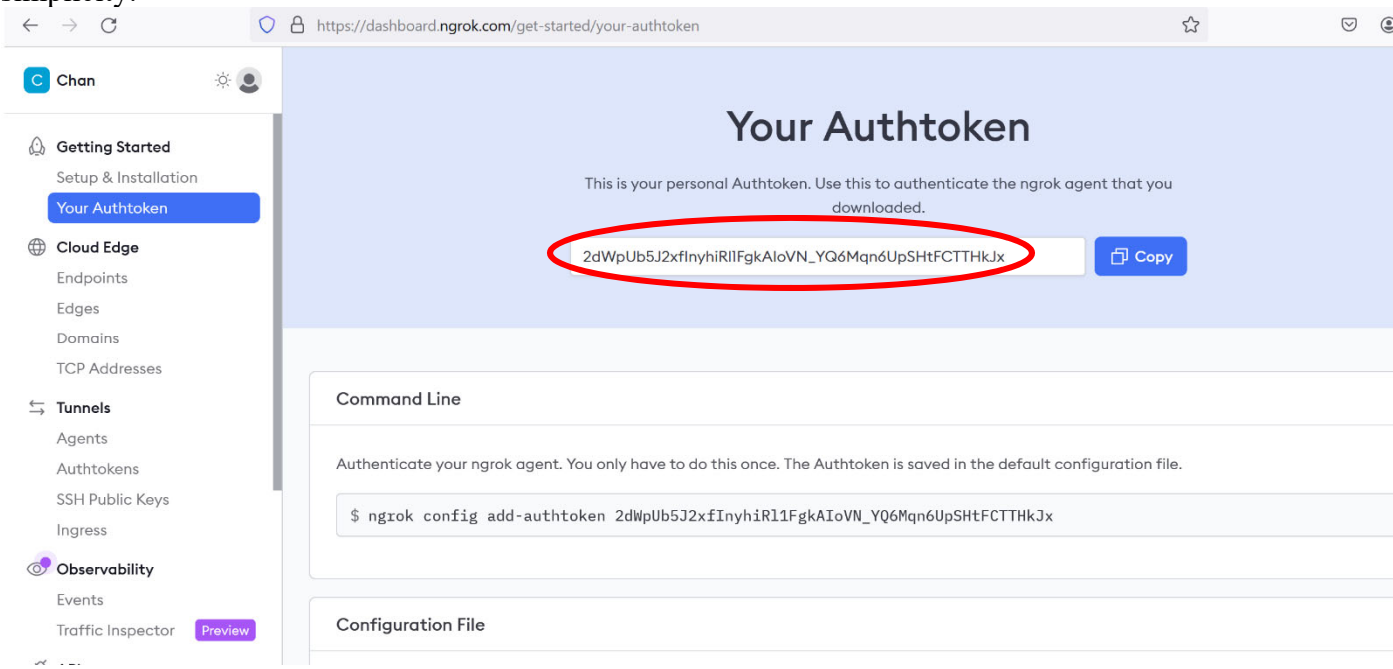
    Note, however, this fake Facebook page is not accessible outside of this computer, Kali Linux. We will see in Part Two how to make this page publicly accessible using ngrok.

Tasks:

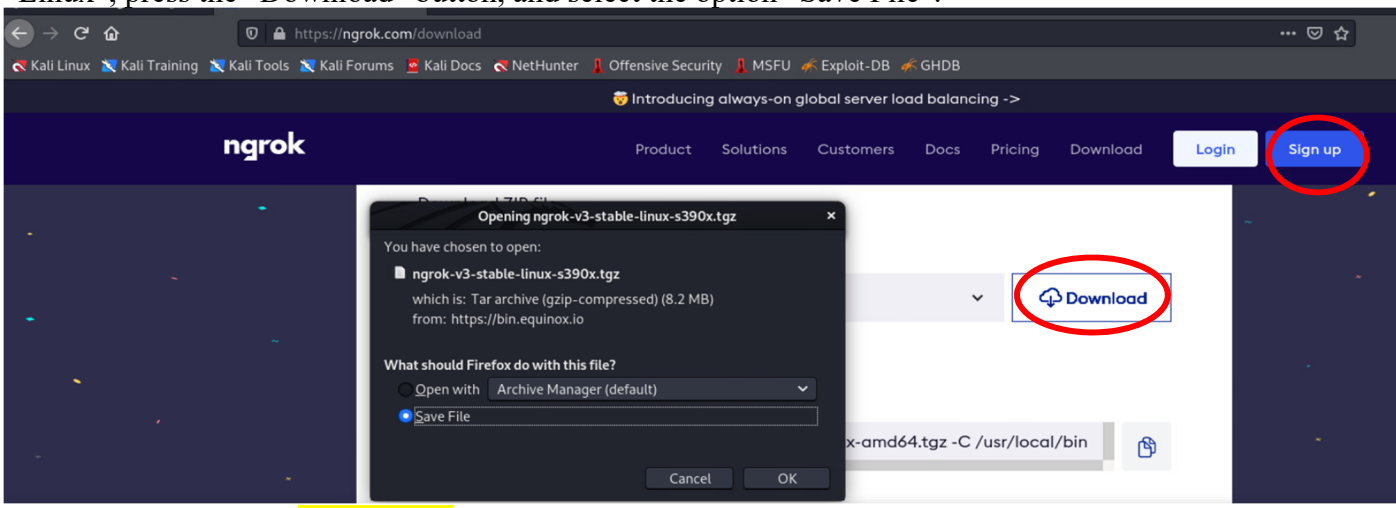
1. Please provide the screenshot showing Zphisher is started at step 5.
2. Please provide the screenshot of the Facebook login page on the local server at step 9.

Part Two: Port Forwarding with ngrok

11. In the Firefox browser, create an account on the ngrok website (click the "Sign up" button) and login to the account. (***Browser on Linux***) Make a record of your authtoken as shown below.
    Note that the signup process takes several steps. You need to provide some information about yourself, e.g., email, for authentication. You may skip Multi-factor authentication for simplicity.



12. Open the Firefox browser. (***Browser on Linux***) Go to ngrok official website and download the ngrok for the Kali Linux machine using the URL: https://ngrok.com/download. Select "Linux", press the "Download" button, and select the option "Save File".

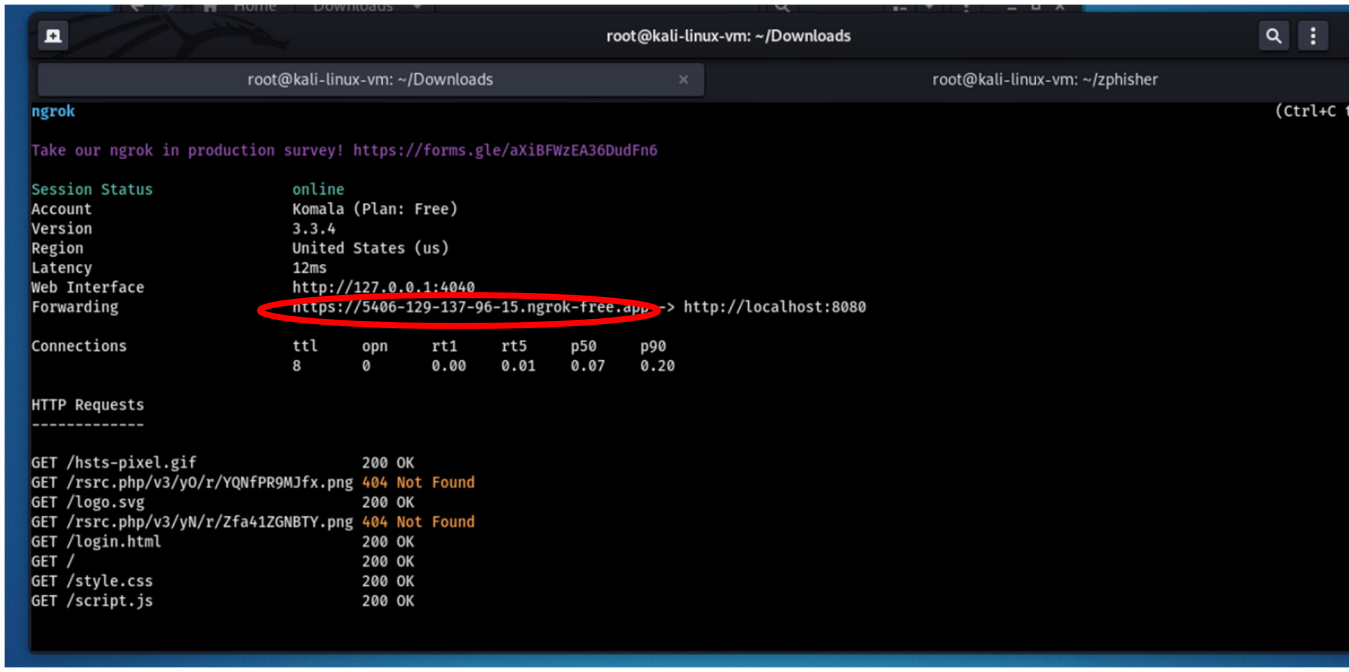


13. Open a new terminal. (***Terminal#2 on Linux***) Unzip ngrok from the terminal using the command.

```
sudo tar xvzf ~/Downloads/ngrok-v3-stable-linux-amd64.tgz -C /usr/local/bin
```

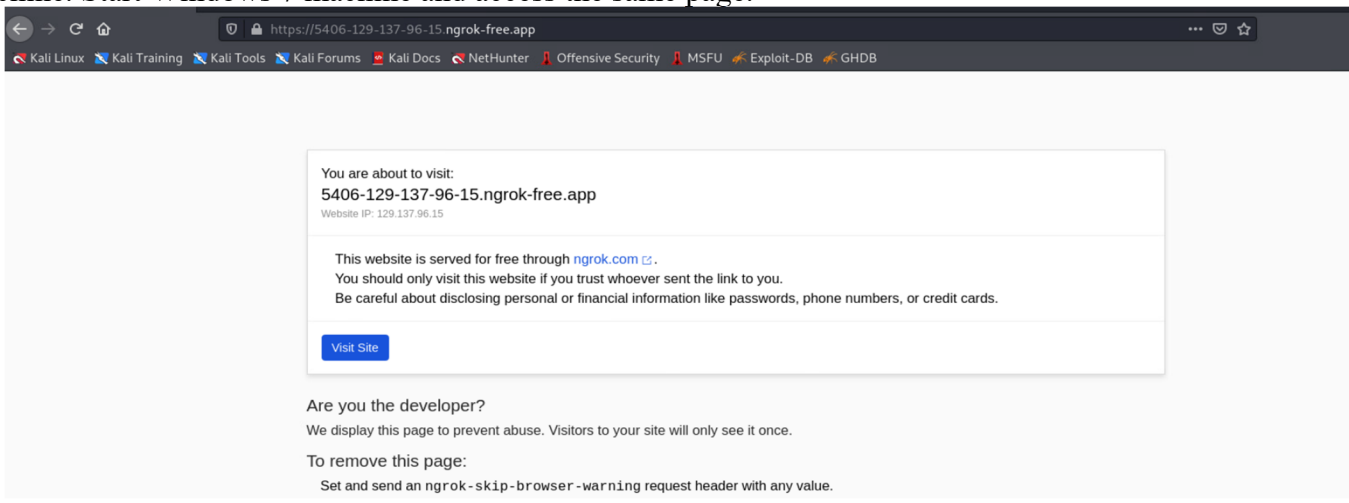
14. In the terminal, add the authtoken using the command shown below. (***Terminal#2 on Linux***)
    ngrok config add-authtoken <token>

15. Start the ngrok tunnel using the following command below, which will create an URL as shown below. (***Terminal#2 on Linux***)
    ngrok http 8080

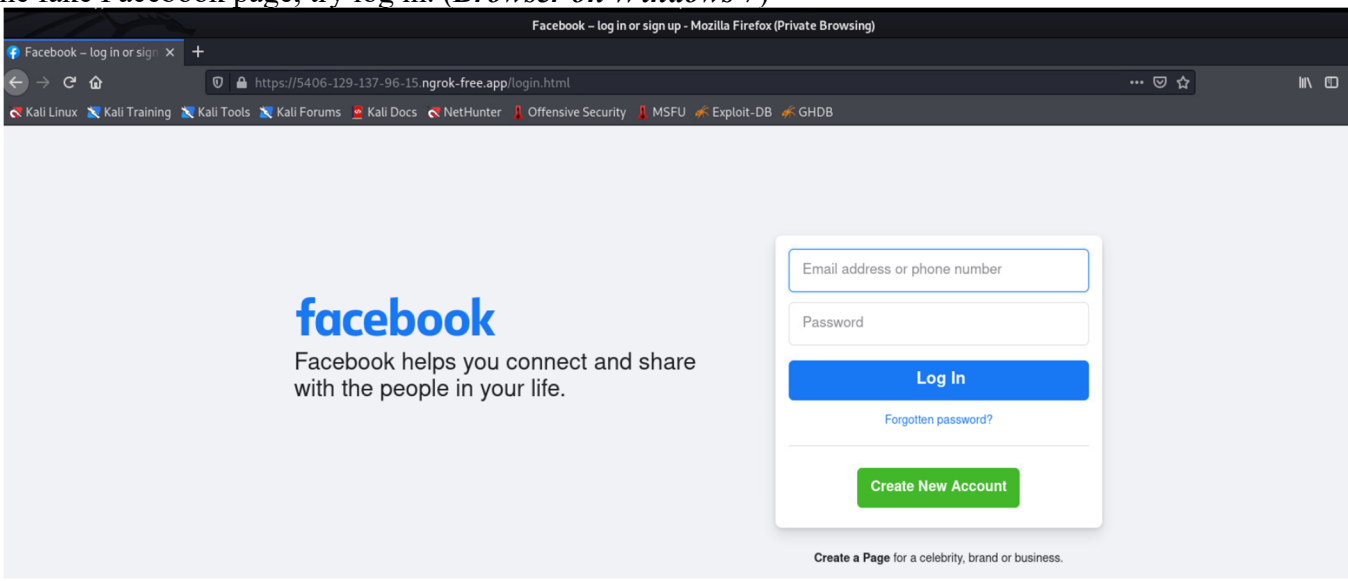


16. Login to Windows 7 machine (u:administrator, p: Pa$$w0rd) and open the Firefox browser in Windows 7. Take the URL from the above and hit this URL. (***Browser on Windows 7***)

    Click on the "Visit Site" button if you encountered the following warning message. As noted in the screen below, this warning message will not appear if you, as an attacker, change the setting. Unlike in Part One, this fake Facebook webpage is accessible from outside of this machine. Start Windows 7 machine and access the same page.

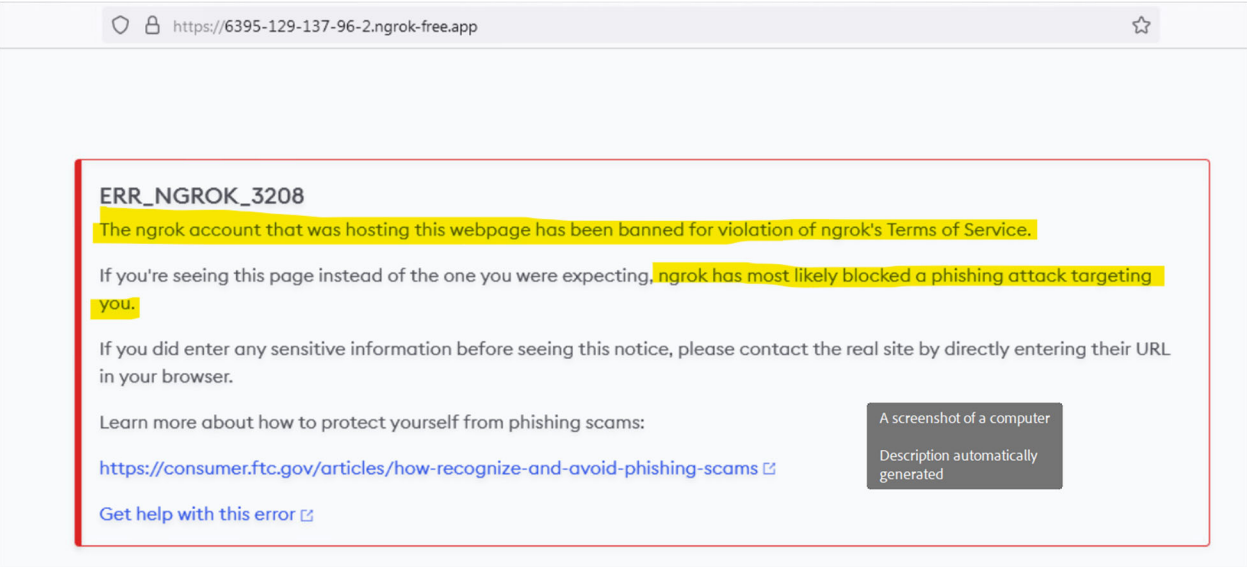


17. In the fake Facebook page, try log in. (***Browser on Windows 7***)



18. You can see the Facebook login credentials present in the terminal Zphisher as shown below. (***Terminal#1 on Linux; I.e., this is a continuation from step 8.***) Make sure to click on Ctrl+C to exit the application.

Warning: ngrok is sophisticated enough to detect if it's being utilized in a phishing attack. If you attempt to access the counterfeit Facebook page again, you may receive the following error message.



Tasks:

3.Please provide the screenshot of the facebook login page as in step 17.

4. Please provide the screenshot of login credentials in Zphisher in terminal as in step 18.

Glossary:

Preliminary Knowledge:

- **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.
- **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.
- **How to 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.

- **Zphisher:** Zphisher is a tool primarily used for phishing attacks. It's designed to automate the process of creating phishing pages for a wide range of online services and websites. Phishing is a malicious activity in which attackers attempt to deceive individuals into revealing sensitive information, such as usernames, passwords, credit card details, or other personal data, by impersonating a legitimate entity. Here are some key characteristics of zphisher:

  Phishing Templates: zphisher provides a collection of phishing page templates for popular websites and online services, including social media platforms, email providers, and banking websites. These templates make it easier for attackers to create convincing fake login pages.

  Automated Page Generation: The tool automates the process of generating phishing pages. Attackers can choose a template, provide some customization options, and then generate a phishing page that closely resembles the target website.

  Credential Harvesting: Once a victim interacts with the phishing page and enters their login credentials, zphisher can capture and store these credentials for later use by the attacker.

  Social Engineering: Phishing attacks often rely on social engineering techniques to trick users into taking specific actions. zphisher's templates are designed to exploit this psychological aspect by making the phishing pages appear legitimate and trustworthy.

  Customization: Users of zphisher can customize the appearance of phishing pages to make them more convincing and tailored to the target audience.

  It's important to note that the use of tools like zphisher for malicious purposes, such as conducting phishing attacks, is illegal and unethical.

- **Ngrok** : Ngrok is a cross-platform, open-source, and secure tunneling service and software that allows you to expose a local development server, service, or web application to the internet. It creates a secure tunnel from a public endpoint to a locally running service on your machine, which is particularly useful during web development and testing. Here are some key features and use cases for Ngrok:

  Tunneling: Ngrok establishes a secure tunnel between a public endpoint and a service running on your local machine. This makes it possible for external users or devices to access your local server or application as if it were hosted on a public server.

  Development and Testing: Developers often use Ngrok to test web applications or APIs on their local development environment. It allows them to share a temporary public URL with clients, team members, or external testers for real-time feedback without the need for deploying the application to a production server.

  Webhooks and Callbacks: Ngrok is commonly used for testing webhooks and callback functionality. It allows developers to receive incoming HTTP requests from third-party services on their local development environment, which is useful for debugging and development.

  Demo and Showcase: When showcasing a project or conducting a demonstration, Ngrok can be used to provide a public URL that allows others to access your local application without needing to deploy it to a production server.

Secure and Authenticated: Ngrok provides options for securing your tunnels with passwords and authentication, ensuring that only authorized individuals can access your local service.
Metrics and Monitoring: Ngrok provides metrics and monitoring capabilities, allowing you to track the usage and performance of your tunnels.
Various Protocols: It supports a variety of protocols, including HTTP, HTTPS, TCP, and more, making it versatile for different use cases.
Public and Private Tunnels: Ngrok offers both public and private tunnel options. Public tunnels are accessible by anyone with the URL, while private tunnels require authentication.
Ngrok comes in both free and paid plans. The free plan provides a limited number of tunnels and connections, while the paid plans offer additional features, such as custom domains, more concurrent connections, and advanced usage analytics.