## 

Disclaimer

*Please note that any material or activity related to cybersecurity or hacking provided here is intended solely for educational purposes. The purpose of this material is to increase awareness and understanding of cybersecurity concepts and principles. The activities described in this material should not be attempted outside of a controlled educational setting. Any attempt to engage in illegal or unethical activities related to cybersecurity could result in serious legal and ethical consequences. It is the responsibility of individuals to use this information in a responsible and ethical manner.*

## What is phishing

## Phishing is a method in which emails are sent to a specific group, designed to appear as authentic messages. The recipient, believing the email to be genuine, may click on a link within the email. However, this link redirects the user to a fraudulent web page that closely resembles an official website. For instance, a user might be directed to a counterfeit banking website that requests sensitive information. Alternatively, clicking the link can result in the download of malicious content onto the user's system, which can then be used to extract information.

## Objective

## The objective for this assignment is to determine how victims are deceived by fake websites. The ultimate phishing tool in Python, PyPhisher, will be utilized for this purpose. It includes popular websites such as Facebook, Twitter, Instagram, GitHub, Reddit, Gmail, and many others.

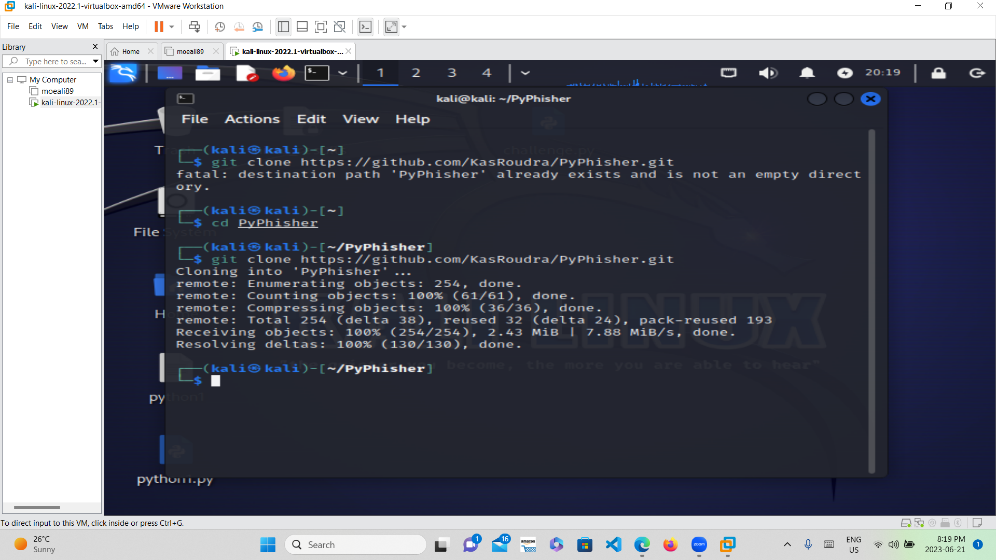
**Steps included (Document the following steps in detail)**

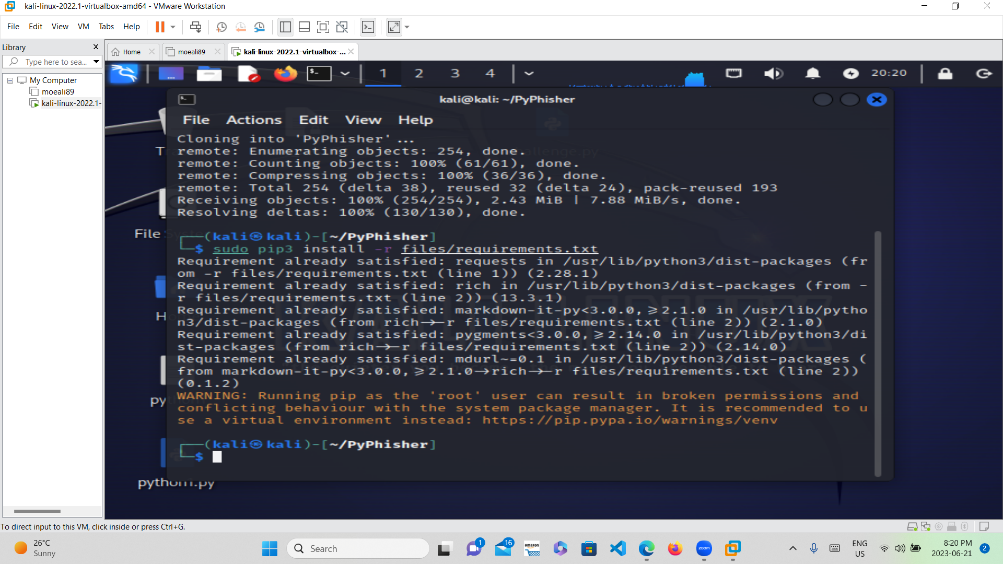
1. Download and install PyPhisher

*git clone* [*https://github.com/KasRoudra/PyPhisher*](https://github.com/KasRoudra/PyPhisher)

*cd PyPhisher*

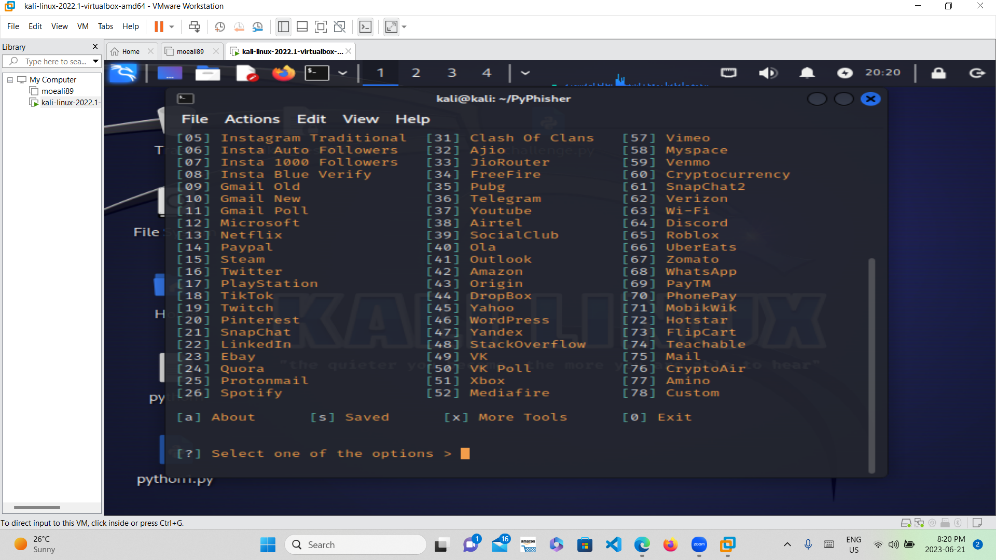
*sudo pip3 install -r files/requirements.txt*

**

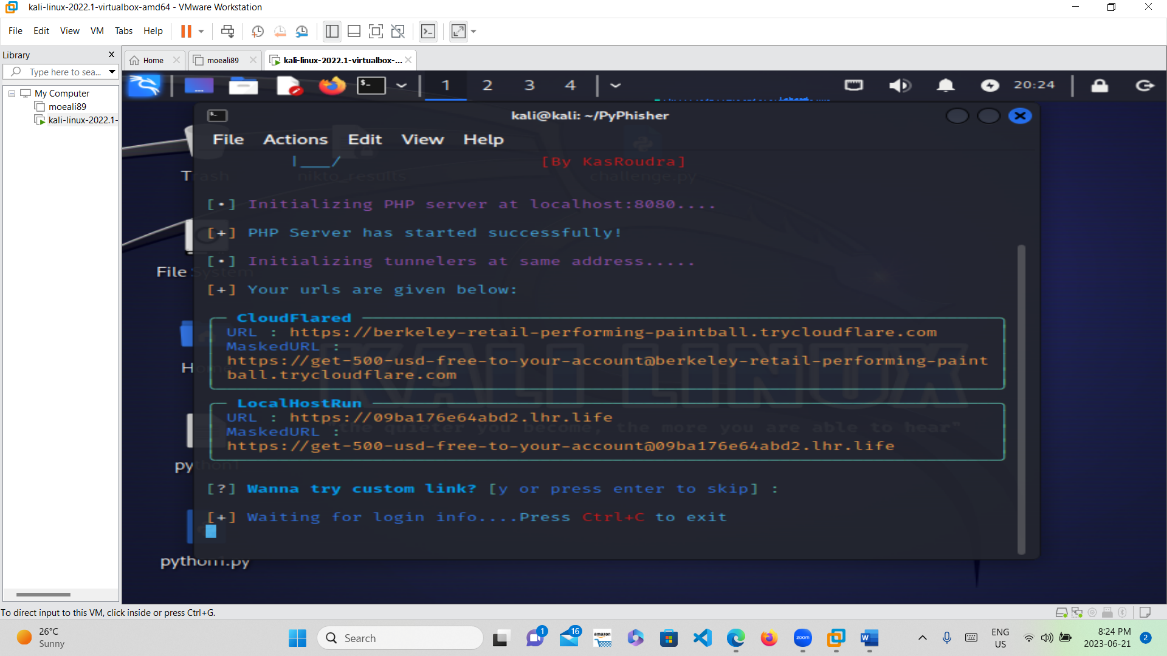
**

1. Run pyphisher after the installation is complete

*sudo python3 pyphisher.py*

**

1. Clone one of the websites such as PAYPAL



## Send a phishing email using the cloned website

Create an email template that includes a hyperlink to the fake website. Here is a Sample

|  |
| --- |
| Subject: Urgent: Claim Your Exclusive Prize Now!  Dear Valued Customer,  Congratulations! You have been selected as the lucky winner of our exclusive prize giveaway. $1000 free twitch gift card. This is a limited-time offer, and you must act quickly to claim your reward.  To receive your prize, please click on the link below Amazone website to login and verify your account:  <https://twitch.com-free-money@is.gd/DiirxN>  Don't miss out on this amazing opportunity! |
|  |

Send the phishing email to at least two classmates who know that you are using it for educational purposes and attempt to capture their credentials by monitoring the program.

Challenge task (optional)

Find a tool in Kali to clone a website which is not include in Pyphisher

# Blackphish – Phishing tool in Kali Linux

**Blackphish** is a powerful open-source Phishing Tool. Blackphish is becoming very popular nowadays , that is used to do phishing attacks on Target. Blackphish is easier than Social Engineering Toolkit.  Blackphish contains some templates generated by another tool. Blackphish offers phishing templates web pages for 6 popular sites such as **Facebook, Instagram,** **Google, Snapchat etc.** This tool is very helpful for performing phishing attacks. blackphish Included twitter not found in Pyphish

