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
```

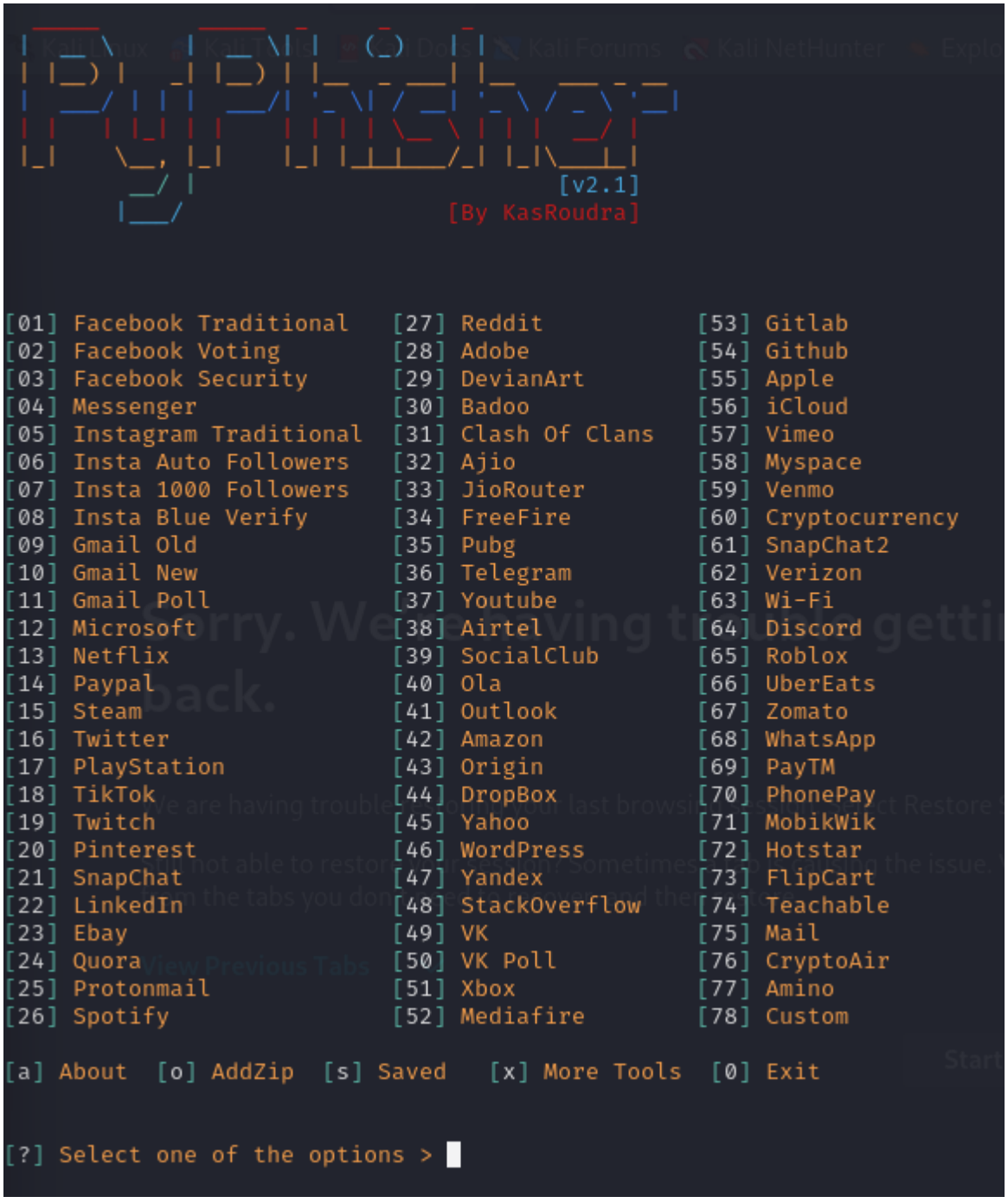
```
Ls
```


```
Chmod +x *
```

Lancer le script

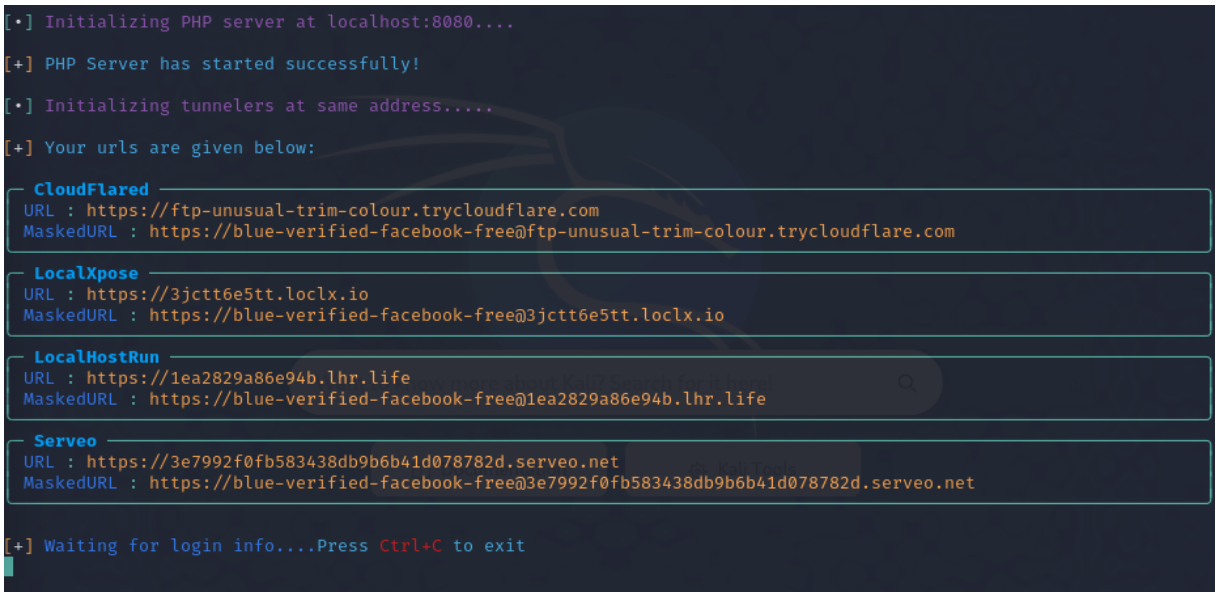
```
Python3 pyphisher.py
```

Choisir le site que nous voulons simuler :

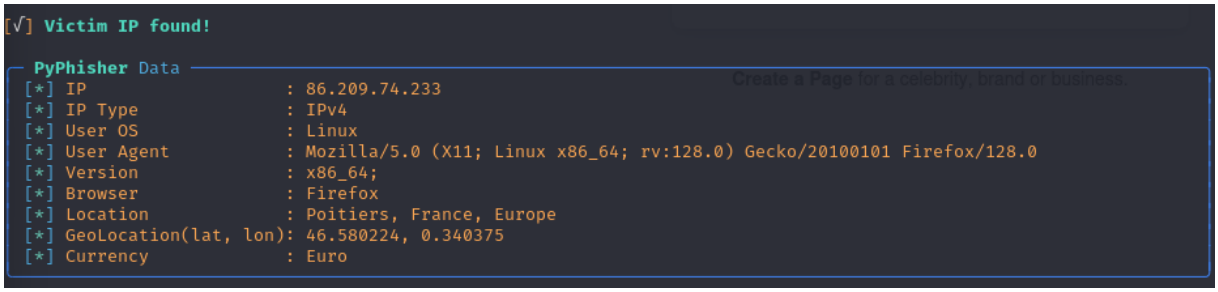


Entrez une URL de redirection pour simuler un site, comme par exemple facebook.com pour Facebook. Cela permet de rediriger la victime vers le véritable site après l'envoi des informations, augmentant ainsi les chances de ne pas être détecté :

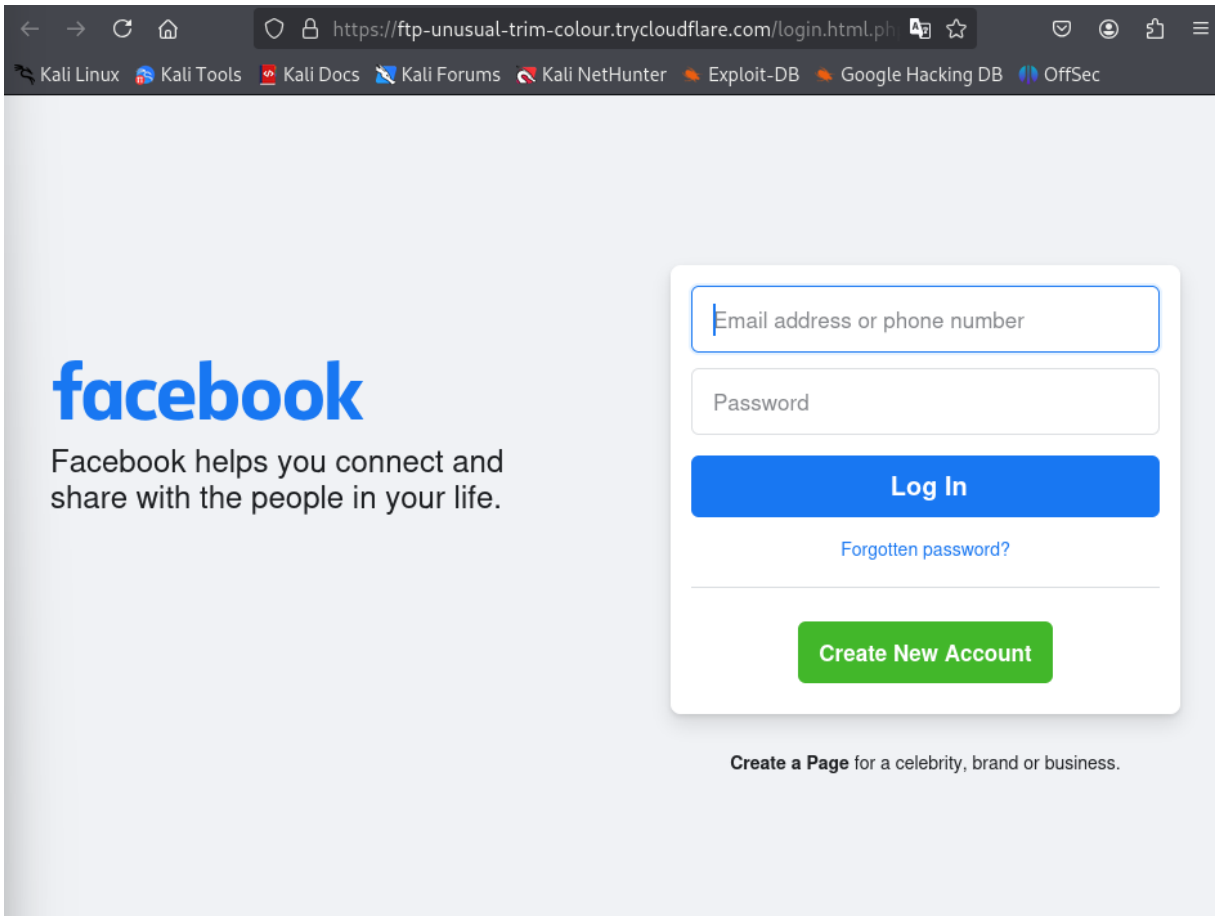
Choisir le lien crée



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



La victime elle ne voit que ça :



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