Simulation de phishing en local avec Zphisher

1. Contexte et objectif

Zphisher est un outil open source permettant de générer rapidement des pages de connexion factices imitant des services populaires (Facebook, Google, Instagram, etc.).

L'objectif de cette documentation est de présenter le déploiement de Zphisher via Docker, en environnement strictement local et isolé, afin de démontrer le fonctionnement d'une attaque de phishing basique.

2. Installation et lancement via Docker

Le code source est récupéré depuis le dépôt officiel GitHub, puis une image Docker est construite et exécutée localement :

```
git clone https://github.com/htr-tech/zphisher.git
cd zphisher
docker build -t zphisher .
docker run -it --name zphisher -p 8080:8080 zphisher
```

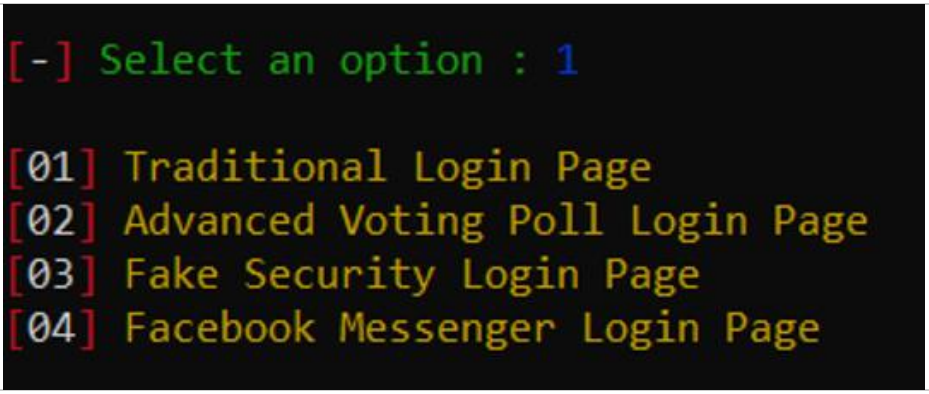
3. Configuration de la campagne dans Zphisher

3.1 Sélection du service à imiter

Au lancement, Zphisher affiche un menu listant les services pouvant être imités (Facebook, Instagram, Google, Netflix, PayPal, etc.). Pour cette démonstration, le service Facebook (option 01) a été sélectionné.

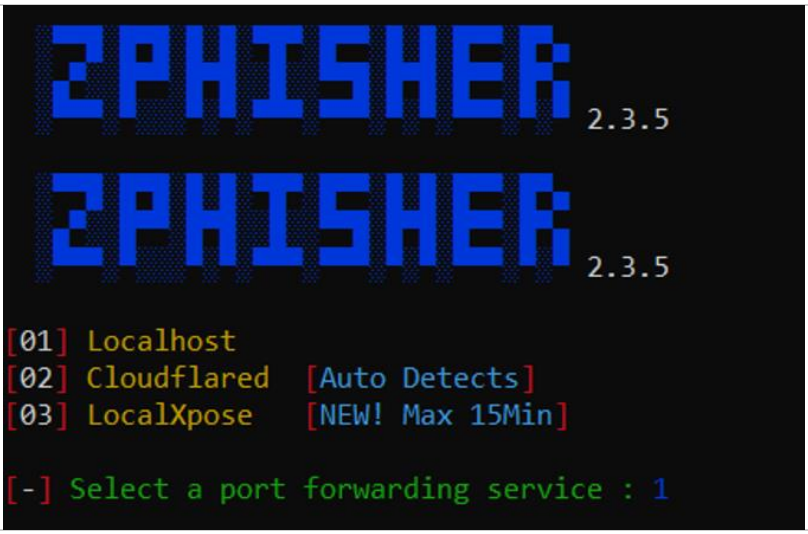
3.2 Choix du type de page piégée

Une fois le service choisi, Zphisher propose plusieurs variantes de pages : ici, la page de connexion classique "Traditional Login Page" a été retenue, reproduisant fidèlement l'interface de connexion Facebook.



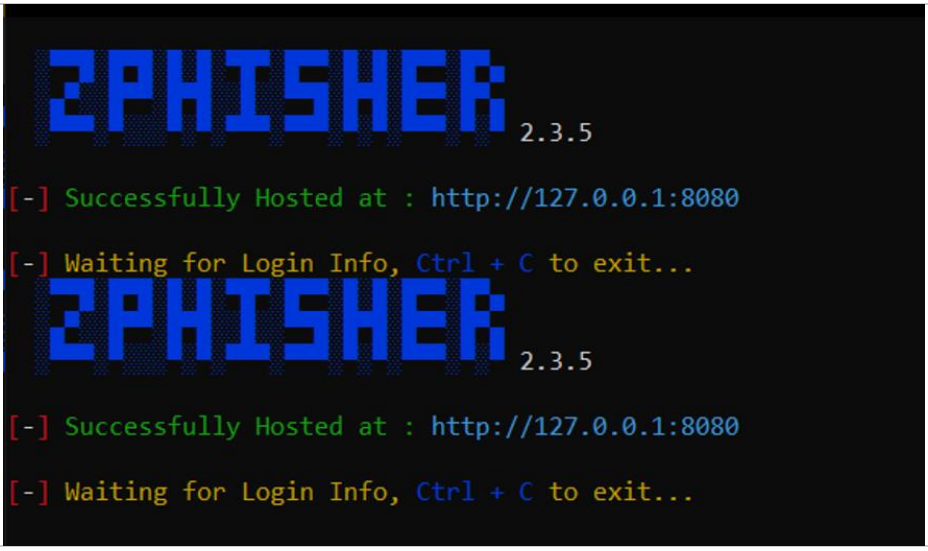
3.3 Choix du service de redirection de port

Zphisher doit ensuite rendre la page accessible : trois options sont proposées (Localhost, Cloudflared, LocalXpose). Pour rester dans un cadre strictement local et sans exposition sur Internet, l'option "Localhost" a été choisie.



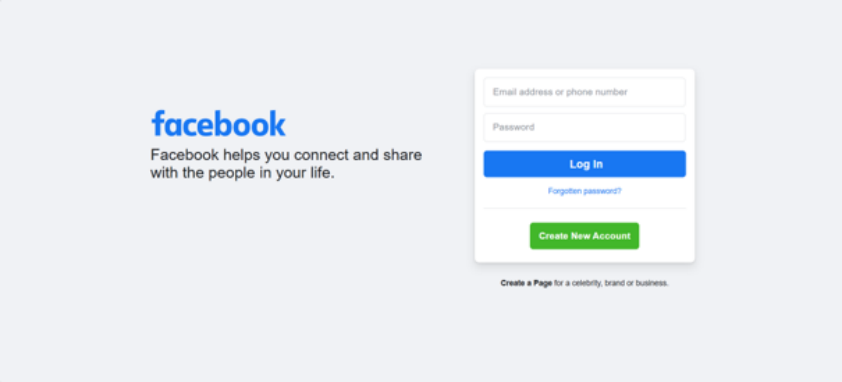
3.4 Hébergement de la page piégée

La page factice est alors générée et rendue disponible à l'adresse http://127.0.0.1:8080. Zphisher se met en attente de connexion et affiche un message indiquant qu'il attend la saisie d'informations de connexion par une victime.

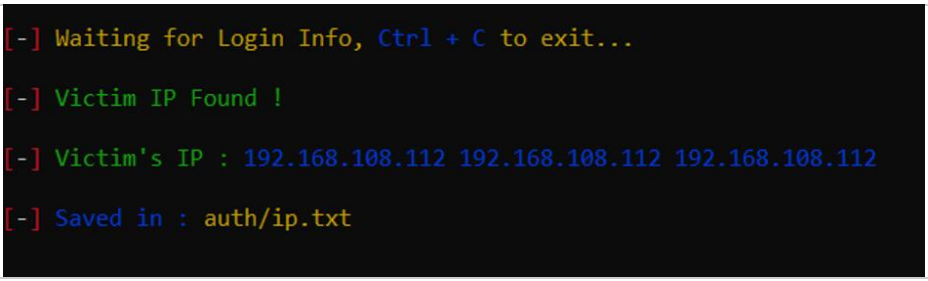


4. Déroulement de la simulation côté victime

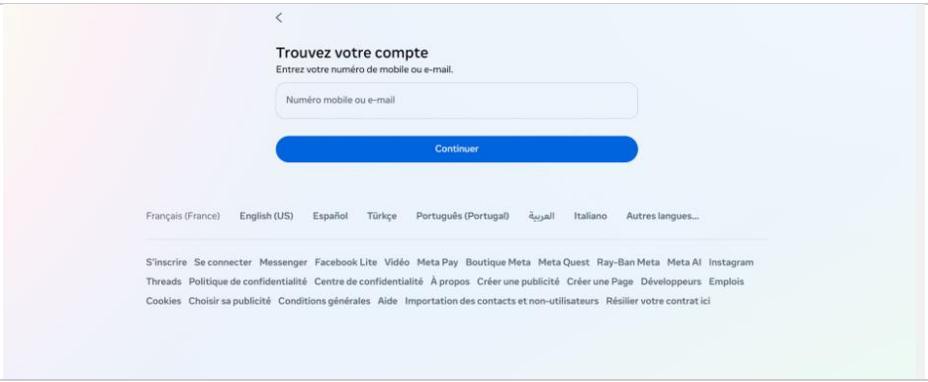
En se rendant sur l'adresse locale, la victime (dans ce cas un poste de test) accède à une page visuellement identique à la page de connexion Facebook, sans pouvoir distinguer qu'il s'agit d'une copie.



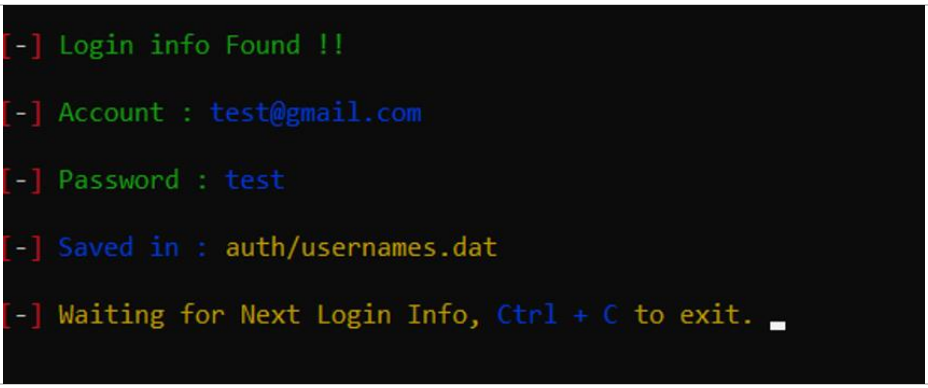
Dès l'accès à la page, Zphisher détecte et enregistre l'adresse IP de la victime dans le fichier auth/ip.txt, permettant d'identifier la machine ayant consulté le lien piégé.



Si la victime poursuit la saisie, elle est ensuite redirigée vers la véritable page Facebook, ce qui renforce la crédibilité de l'attaque en masquant la supercherie une fois les identifiants transmis.



Pendant ce temps, les identifiants saisis par la victime (adresse e-mail et mot de passe) sont interceptés et affichés dans le terminal de Zphisher, puis sauvegardés dans le fichier auth/usernames.dat.



5. Conclusion

Cette mise en pratique illustre, dans un environnement Docker isolé, le déroulement complet d'une attaque de phishing basée sur une page de connexion factice : génération, hébergement local, capture de l'IP puis des identifiants de la victime. Elle met en évidence la simplicité de mise en œuvre de ce type d'attaque et l'importance de sensibiliser les utilisateurs à vérifier systématiquement l'URL et l'authenticité d'une page avant d'y saisir leurs identifiants.