TAKENINT Mouloud
MUNIR Mohammed
ROJAS Luis

Fiche Technique - BTS SIO 2023/2024

Phishing

Sommaire

1.Introduction

Le phishing est une technique de cybercriminalité dans laquelle des attaquants tentent de tromper des individus pour obtenir des informations sensibles telles que des noms d'utilisateur, des mots de passe, des numéros de carte bancaire ou d'autres informations personnelles. Cela se fait généralement en se faisant passer pour une entité de confiance dans une communication électronique, comme un email, un appel téléphonique ou un message texte.
Les attaques de phishing impliquent souvent des sites web ou des emails frauduleux qui semblent provenir de sources légitimes, comme des banques, des agences gouvernementales ou des entreprises bien connues. L'objectif est de tromper les victimes pour qu'elles cliquent sur des liens malveillants ou des pièces jointes qui peuvent installer des logiciels malveillants sur leurs appareils ou les rediriger vers de faux sites web conçus pour recueillir leurs données personnelles.
Types principaux de phishing :

1. Phishing par email : La forme la plus courante, où des emails frauduleux semblent provenir d'organisations légitimes.
2. Spear phishing : Une forme de phishing plus ciblée où les messages sont personnalisés pour des individus ou des organisations spécifiques.
3. Whaling : Un type de spear phishing visant des cibles de haut niveau, comme des dirigeants d'entreprises ou des responsables gouvernementaux.
4. Smishing : Phishing effectué par SMS (message texte).
5. Vishing : Phishing réalisé par téléphone, où les attaquants se font passer pour des figures de confiance afin d'obtenir des informations personnelles.

Le phishing peut entraîner de graves conséquences, comme le vol d'identité, des pertes financières ou l'accès non autorisé à des informations confidentielles. Il est donc essentiel de rester vigilant et de ne jamais fournir d'informations personnelles par le biais de canaux non sécurisés.

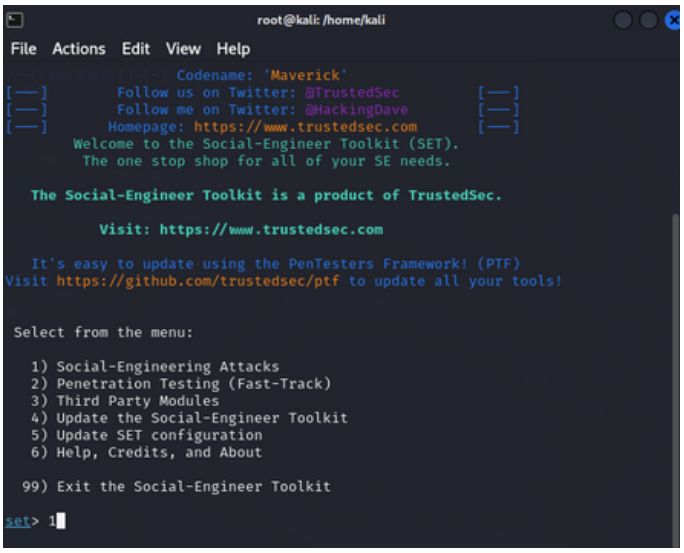
2. Clonage Website

SET (Social Engineering Toolkit) :
Le Social Engineering Toolkit (SET) est un ensemble d'outils préinstallé sur Kali Linux, conçu pour effectuer des attaques d'ingénierie sociale. Il permet aux professionnels de la cybersécurité de tester la vulnérabilité des utilisateurs en simulant des attaques comme le phishing, le clonage de sites web et la récolte d'informations sensibles (mots de passe, identifiants). SET est largement utilisé pour évaluer la résilience des systèmes humains face à des attaques de manipulation.
Il est destiné à des fins de tests de sécurité légaux uniquement.

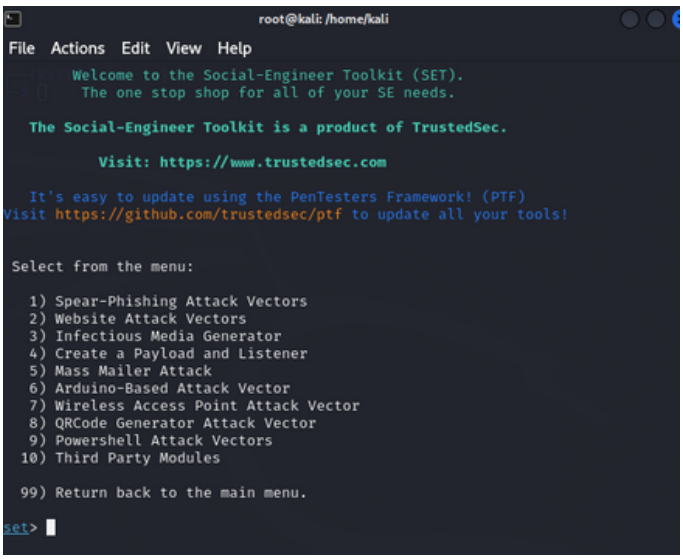
Tapez la commande suivante pour lancer SET en tant qu'administrateur :

```
┌──(root㉿kali)-[/home/kali]
└─# setoolkit
[-] New set.config.py file generated on: 2024-11-24 18:14:16.676009
```

Choisir la premier option social-engineering attacks : qui va permetre de choisir une attaque basée sur l'ingénierie sociale (par exemple, création d'un site de phishing, attaques par courriels malveillants, etc.).

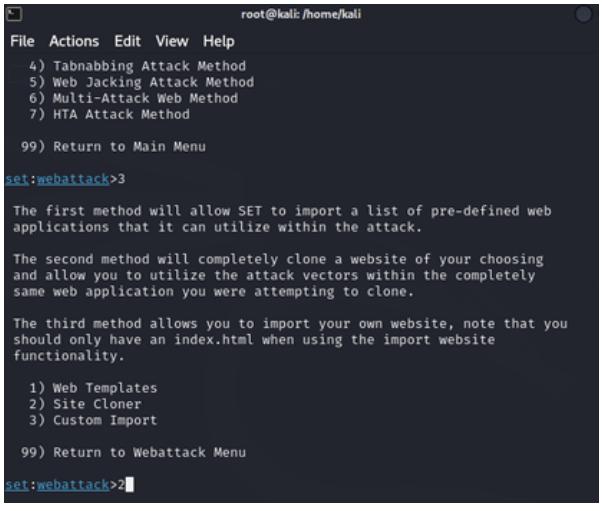


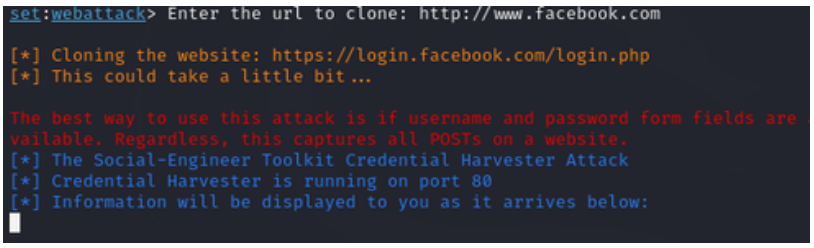
Choisir la deuxième option Website Attack Vectors (pour cloner des sites Web ou insérer des scripts malveillants).



Ensuite, choisissez l'option 3 (Credential Harvester) pour collecter des informations d'identification.

Clonage d'un site web :
Choisissez l'option 2 (Site Cloner).
Fournissez une adresse IP locale pour héberger le site de phishing. Utilisez ifconfig pour obtenir votre IP.
Indiquez l'URL du site à cloner (dans cet exemple, www.facebook.com) puis va mettre en écoute .





3. Résultat + Test

Maintenant je vais envoyer un mail à la victime

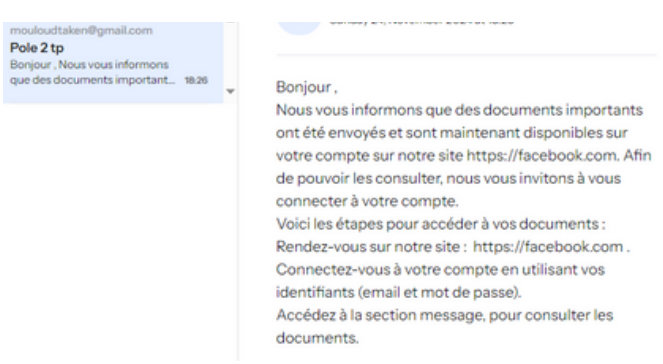
Bonjour ,

Nous vous informons que des documents importants ont été envoyés et sont maintenant disponibles sur votre compte sur notre site https://facebook.com. Afin de pouvoir les consulter, nous vous invitons à vous connecter à votre compte.

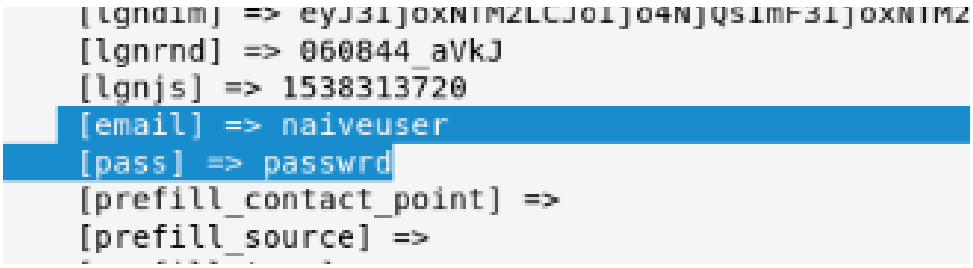
Voici les étapes pour accéder à vos documents :

1. Rendez-vous sur notre site : https://facebook.com .
2. Connectez-vous à votre compte en utilisant vos identifiants (email et mot de passe).
3. Accédez à la section message, pour consulter les documents.

La victime va recevoir un mail de l'attaquant puis entrer dans le lien qui va faire apparaitre un faux site de facebook que on a cloné



- Enfin, récoltez les bénéfices. Allez sur /var/www/html et vous pouvez voir le fichier ou il ya le mail et le mot de passe



Conclusion

Le phishing est une des méthodes les plus répandues en ingénierie sociale, exploitant la confiance et l'inattention des utilisateurs pour obtenir des informations sensibles. Avec des outils comme le Social-Engineer Toolkit (SET) sous Kali Linux, il est possible de simuler des attaques sophistiquées pour évaluer la sécurité d'un réseau ou sensibiliser les utilisateurs.
Cependant, il est essentiel de respecter des principes éthiques et légaux lors de l'utilisation de ces outils. Les simulations de phishing doivent toujours être réalisées dans un cadre contrôlé, avec l'accord explicite des parties concernées. L'objectif principal doit être l'apprentissage, la formation, et le renforcement des défenses contre ce type d'attaques.
En sensibilisant les utilisateurs aux risques de phishing, en adoptant de bonnes pratiques de cybersécurité (comme la vérification des URL et des expéditeurs) et en renforçant les mécanismes techniques de protection, il est possible de réduire considérablement les risques associés à ces attaques.