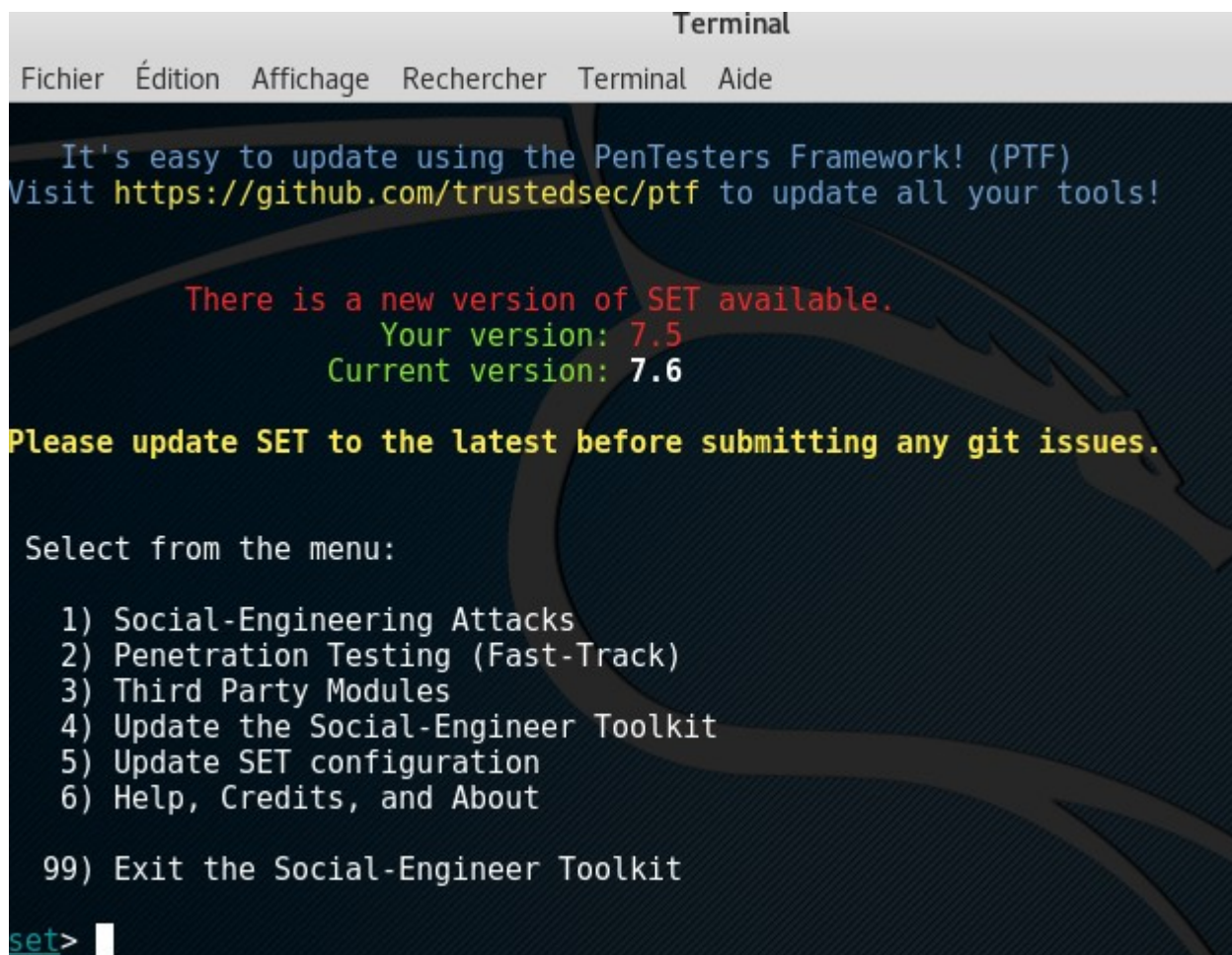


Utilisation basique du SET (Social Engineer Toolkit)

SET est un outil permettant d'automatiser des techniques d'ingénierie sociale. Nous allons voir comment l'utiliser.

Tout d'abord, vous pouvez le lancer en vous rendant dans Kali, dans le menu « Applications -> Outils Exploitation -> social engineer toolkit ».



```
Terminal
Fichier  Édition  Affichage  Rechercher  Terminal  Aide

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.5
Current version: 7.6

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 
```

il vous suffit de taper le numéro en question pour accéder à un menu, ou « 99 » pour en sortir.

Vous pouvez par exemple sélectionner « 1 » pour vous rendre dans « Social-Engineering Attacks » puis « 2 » pour sélectionner « Website Attack Vectors ».

Vous y retrouverez plusieurs attaques que nous avons vu dans les vidéos :

```
Terminal
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inj
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

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) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>
```

En sélectionnant par exemple « 1 » (« Java Applet Attack Method »), SET va créer un site (soit une copie d'un site existant, soit un modèle prédéfini) et y ajouter l'applet malveillant pour prendre le contrôle de la cible.

Le site se trouvera dans le dossier `~.set/web_clone`, et l'avertissement Java se lancera lors du lancement du site :

VulneWeb by LeBlogDuH... x file:///root/...ne/index.html x +

file:///root/.set/web_clone/index.html Search ☆ 📁 ✓ ↓

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-n

facebook
You must log in first.

Email or Phone Password


Log In

[Create New Account](#)

- [Forgot Password?](#) · [Help Center](#)
-

English (US) · [Español](#) · [Português \(Brasil\)](#) · [Mo](#)
Facebook ©2014

Security V

 The application's digital signature cannot be verified. Do you want to run the application? It will be granted full permissions on your computer.

Name: applet
Publisher: Verified Secure
From:

☐ Always trust content from this publisher

The digital signature could not be verified by a trusted source. You can still run if you trust the origin of the application. This may be given full permissions, ignoring any Java policy.

Bien entendu, il vous faudra ensuite configurer divers paramètres, comme l'adresse IP qui recevra les connexions (handler)...etc.

L'idée étant ici d'observer qu'il est **facile de créer des attaques sur mesure**. Raison de plus de **se protéger des attaques par ingénierie sociale**, car le pirate n'aura pas forcément besoin d'être un expert technique.