Tabnabbing Attack Method

pentestlab.blog/category/social-engineering/page/8

March 20, 2012

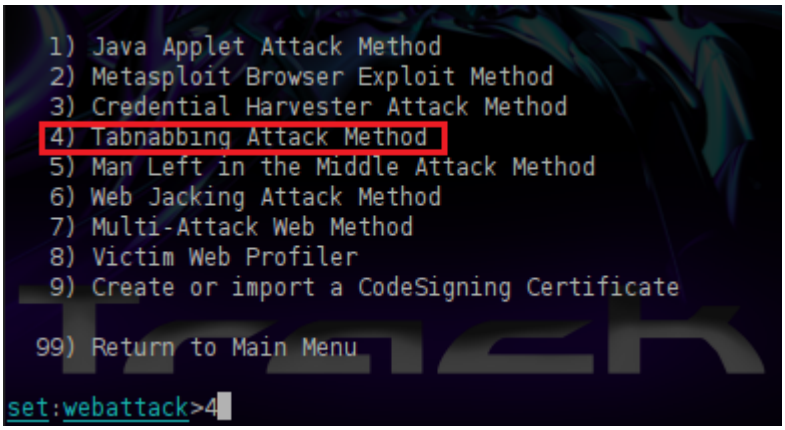
Another method that you can use when you conduct a social engineering attack is the Tabnabbing attack.The only thing that it requires from the user is to switch tabs in his browser in order to load the fake website and then if he inserts his credentials it harvest them.

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.

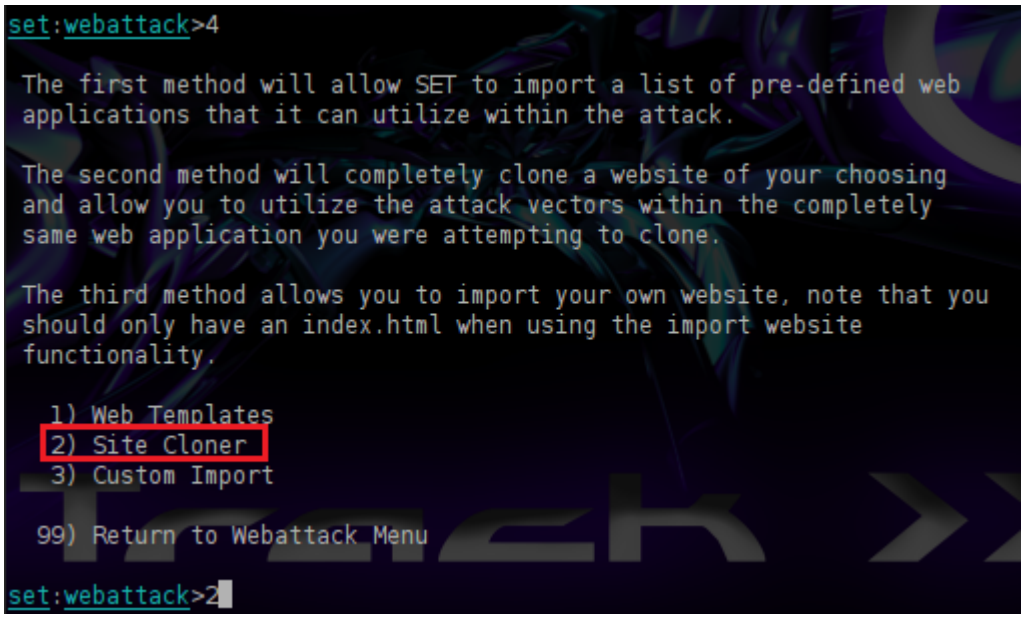
Website Attack Vector

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.



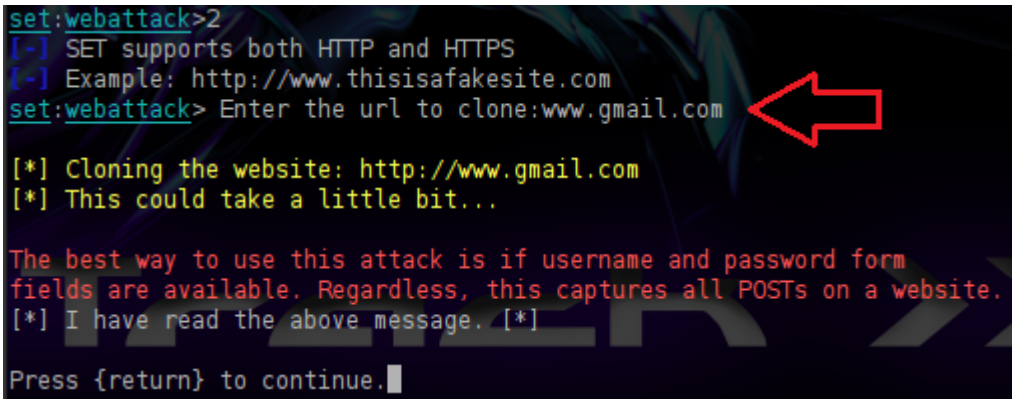
Selecting the Tabnabbing Attack

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.



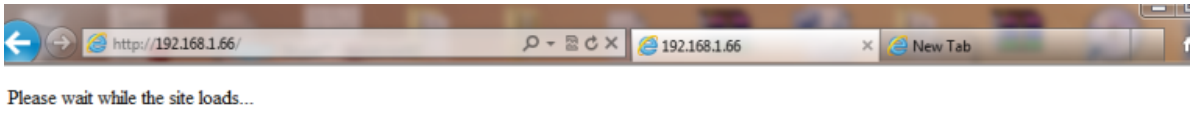
Selecting the Site Cloner

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



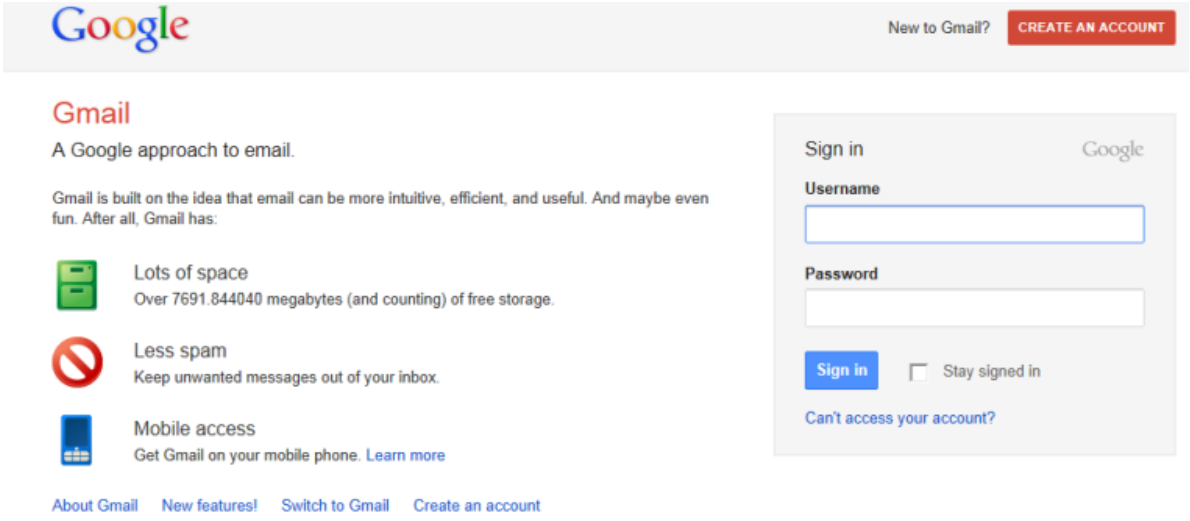
Enter the Fake Website for Cloning

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:



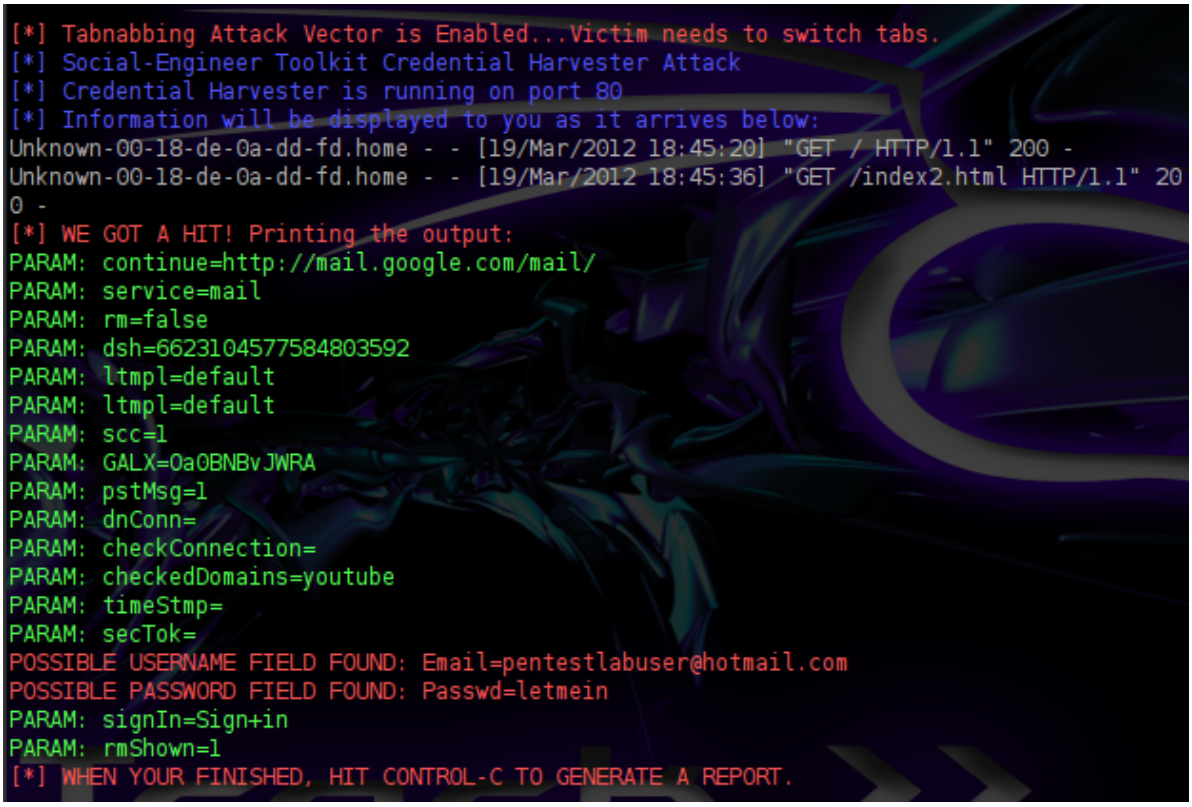
Opening the webpage

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.



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 unexperienced users will probably become victims so these type of users they need to have extra awareness.