PRACTICAL 05

Problem Statement: ` of Kali Linux.

Lab Environment

To carry out this lab, you will require the following:
Kali Linux as virtual machine

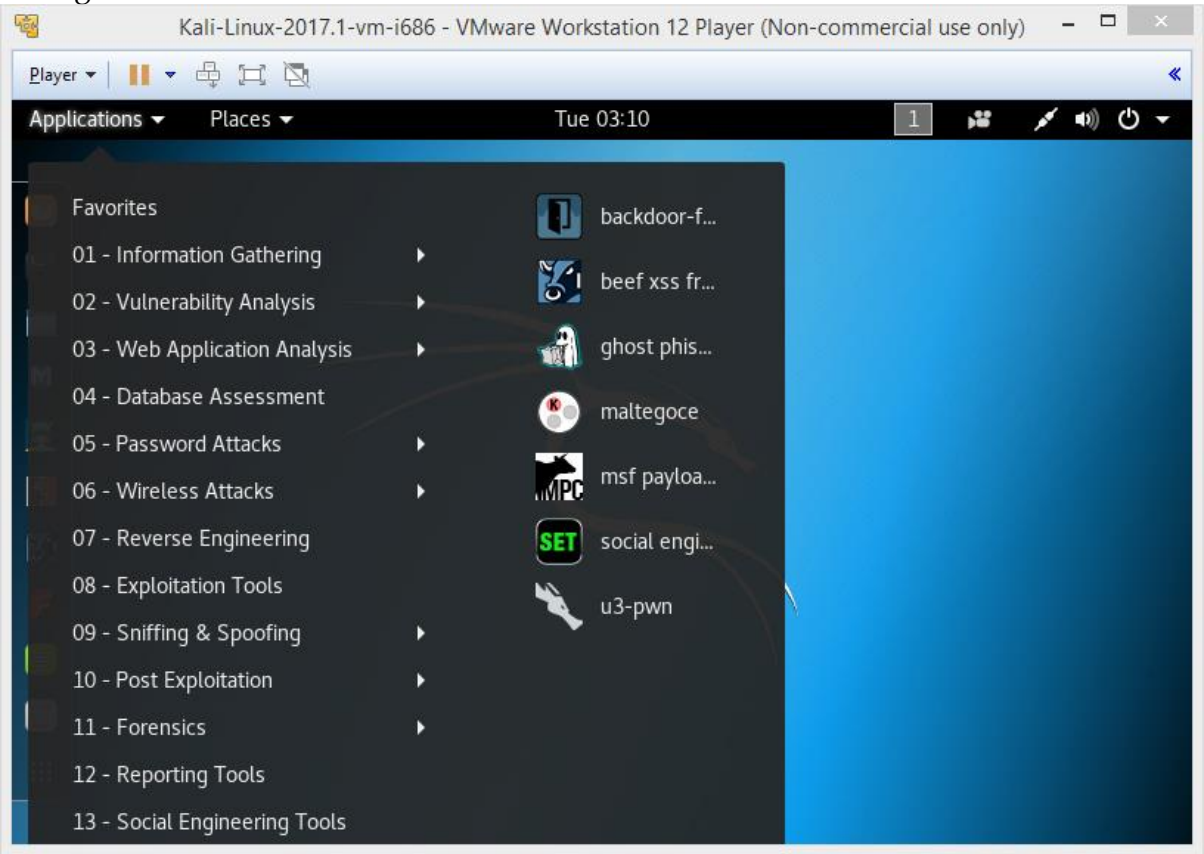
Web browser with Internet connection

Administrative privileges

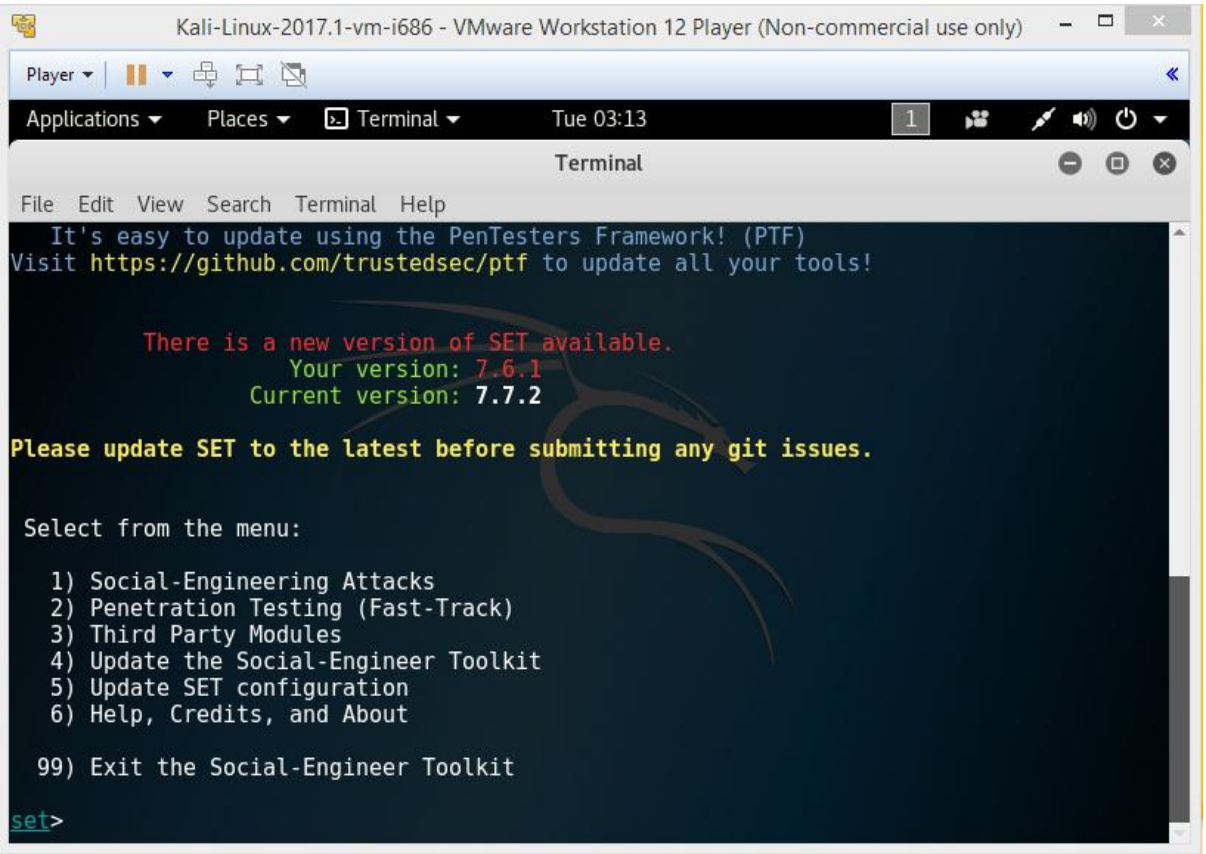
Lab Tasks

To perform social engineering and obtain the credentials of the target user, perform the following steps:

1. Log in to Kali Linux as a Virtual Machine.
2. Go to Applications > Exploitation Tools > SET Social Engineering Tool, as shown in Figure 1.

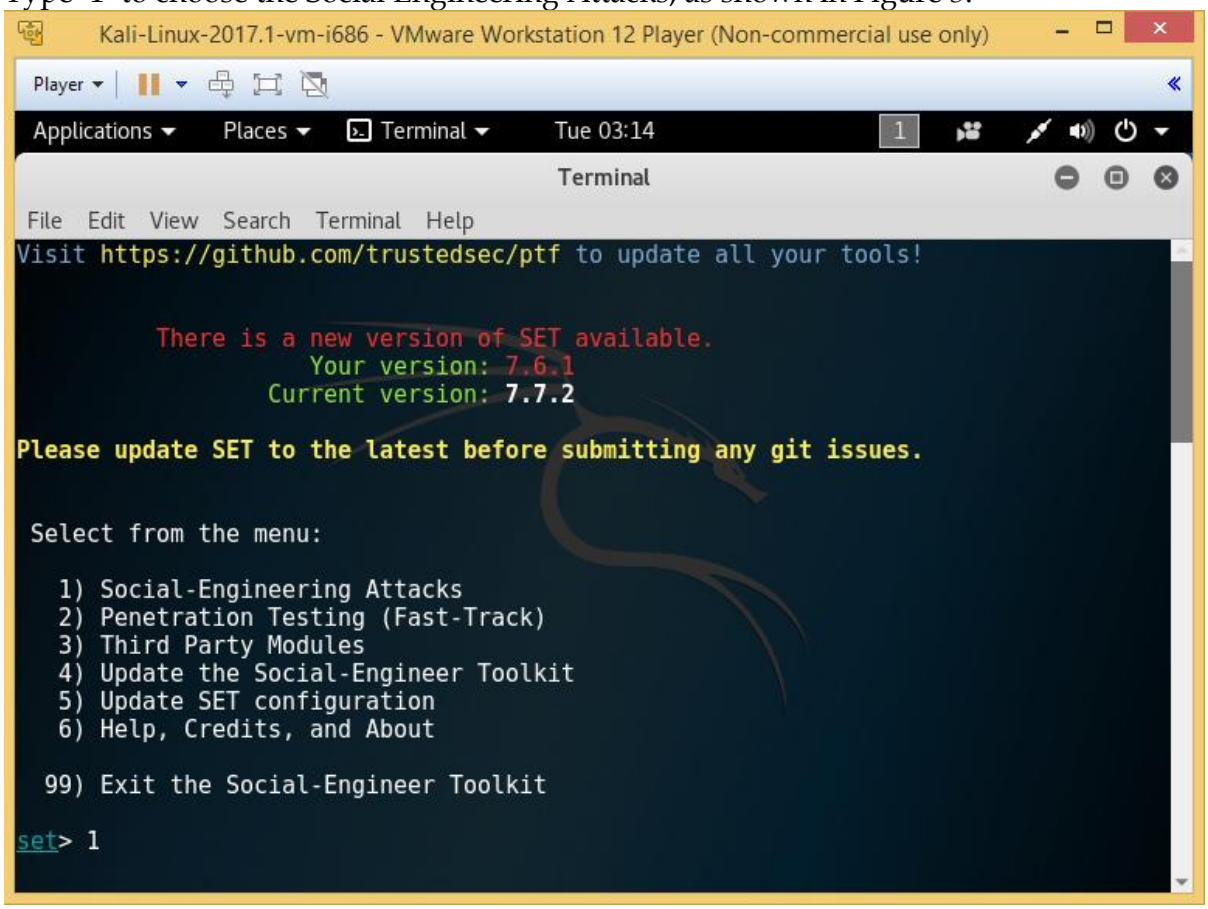


Then you will get the Set menu, as shown in Figure 2.



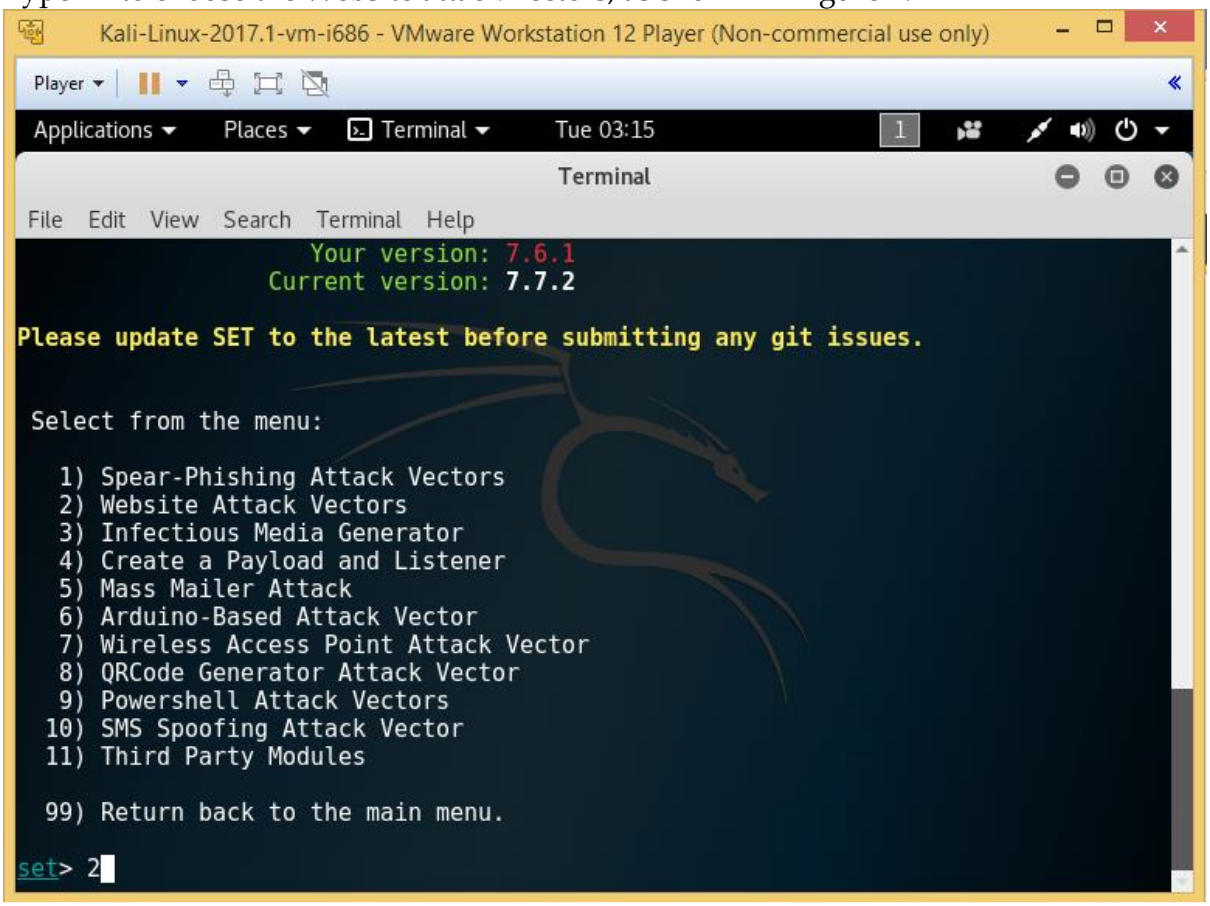
Now the list of social engineering methods will appear, as shown in Figure 3.

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

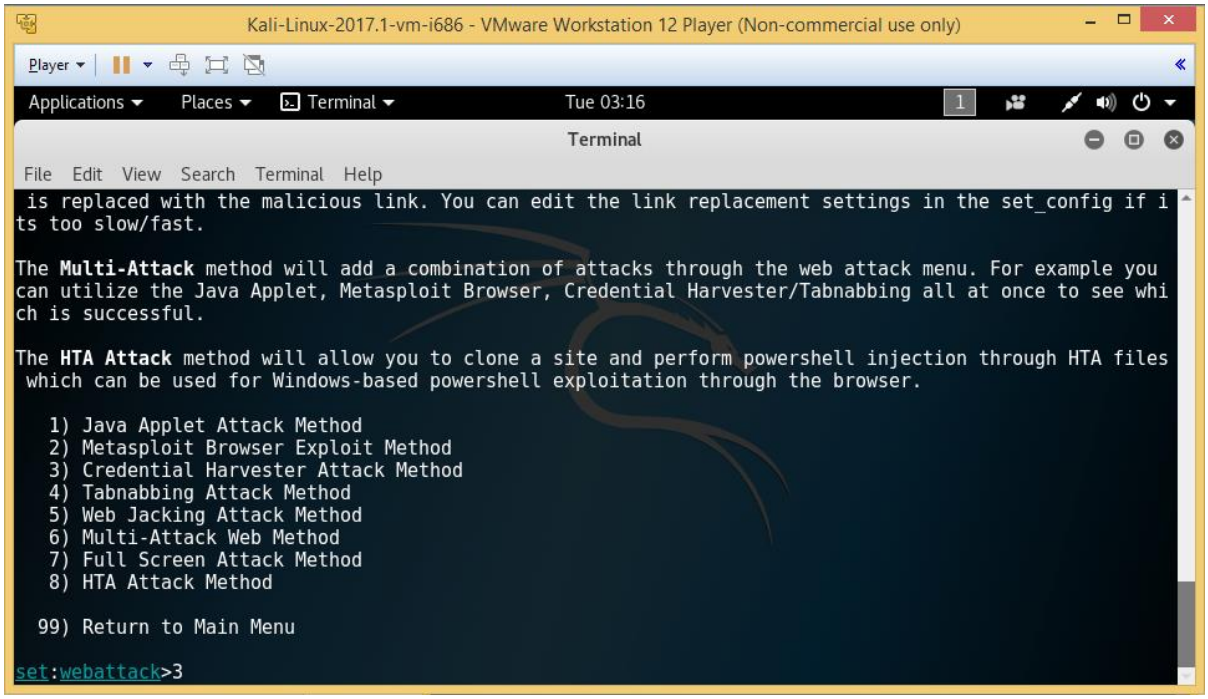


Then the list of menus in the social engineering attacks will appear, as shown in Figure 4.

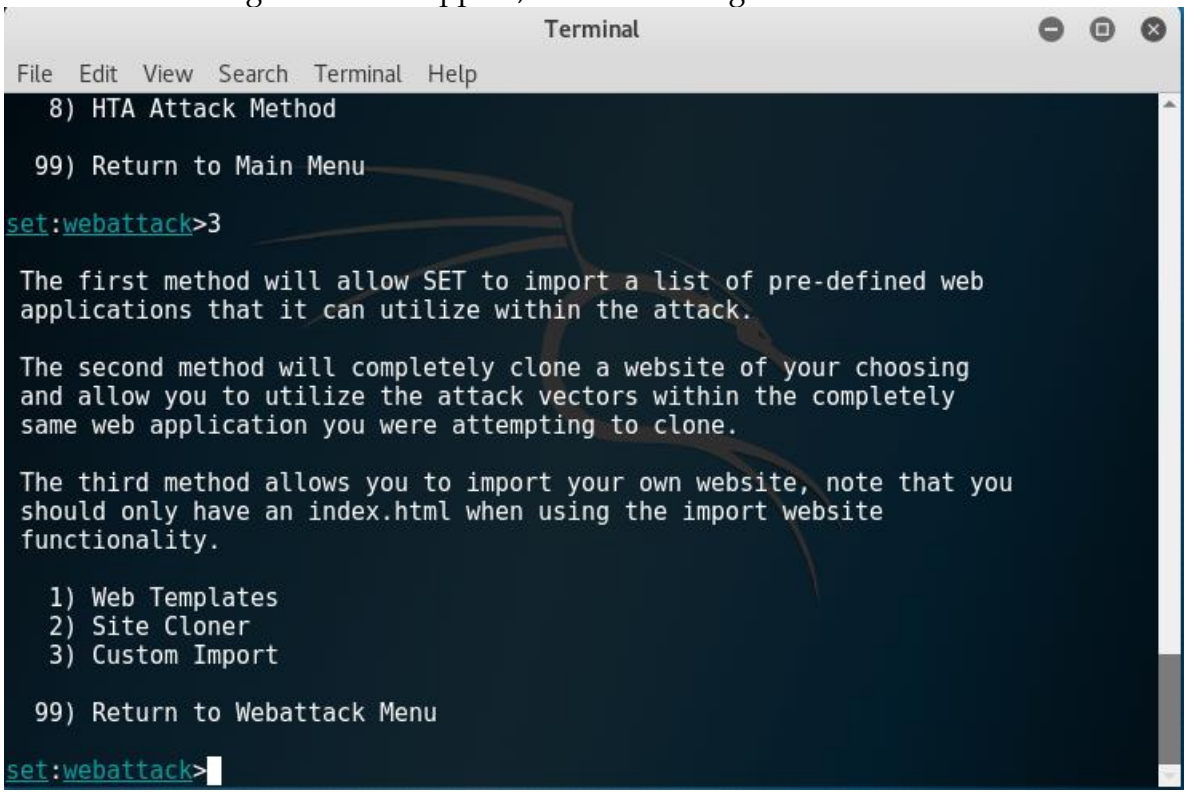
4. Type '2' to choose the Website attack vectors, as shown in Figure 4.



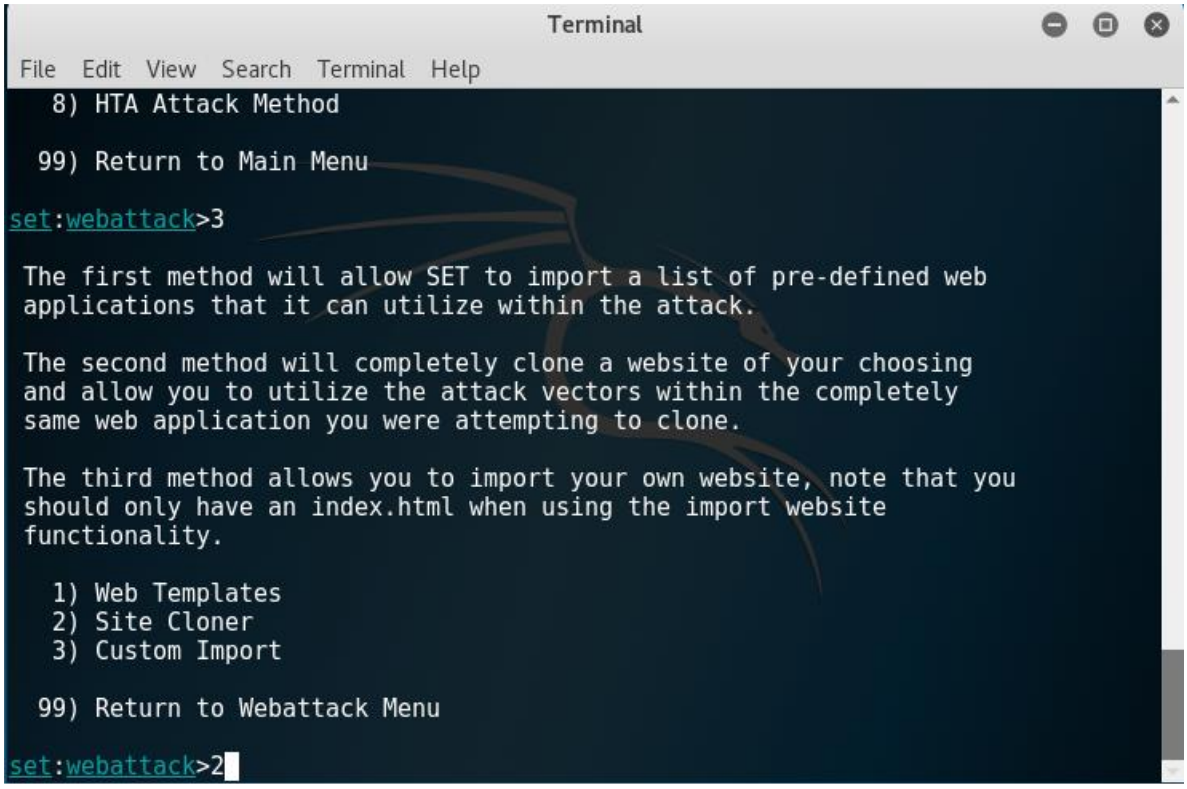
5. In the next screen that appears, type '3' to choose the credential harvester attack method, as shown in Figure 5.



Then the following screen will appear, as shown in Figure 6.

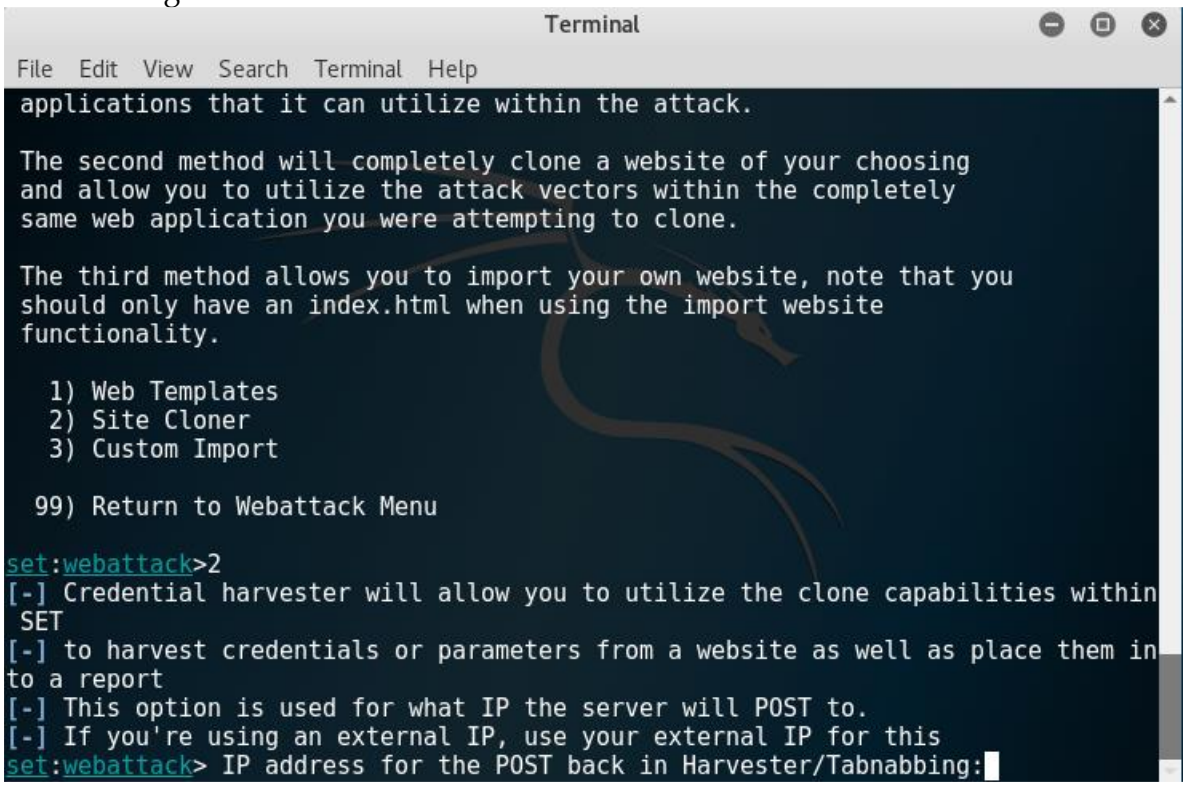


6. Type '2' to choose Site Cloner, as shown in Figure 7.

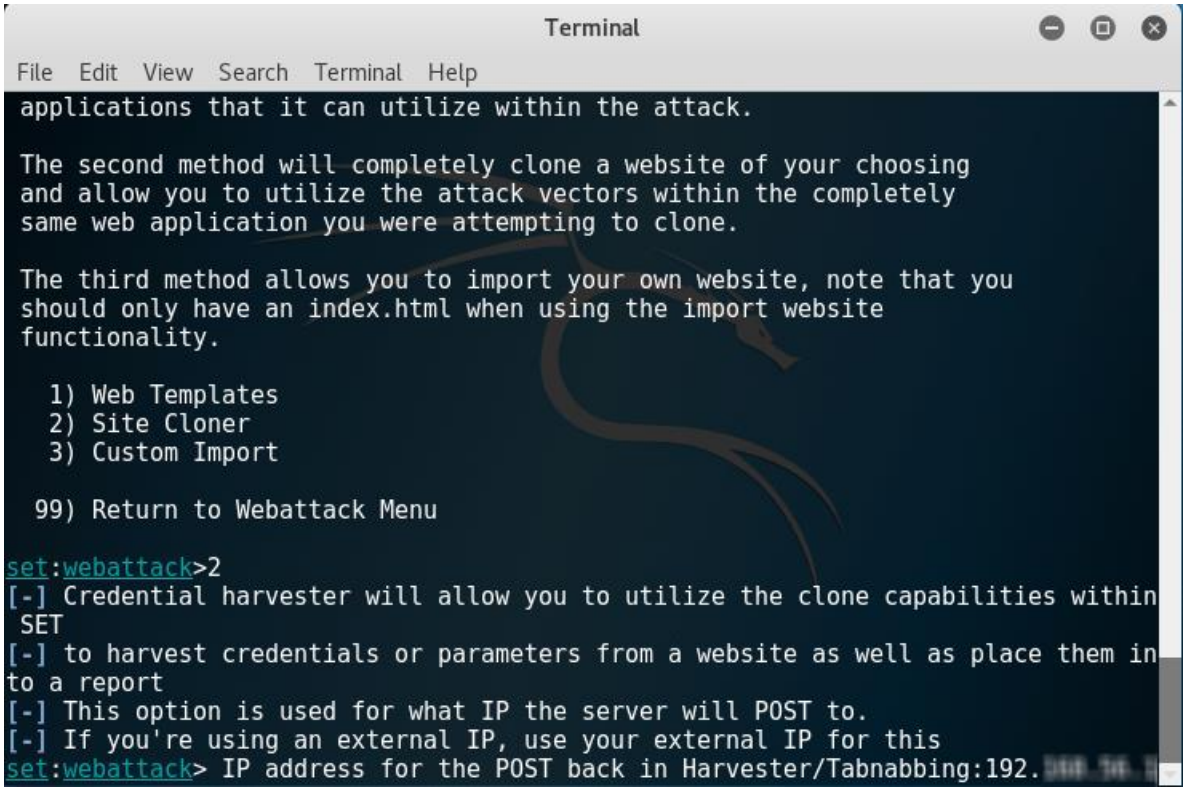


Then the following screen will appear, as shown in Figure 8.

Now it will prompt for IP address for the PostBack in Harvester/Tabnabbing, as shown in Figure 8.

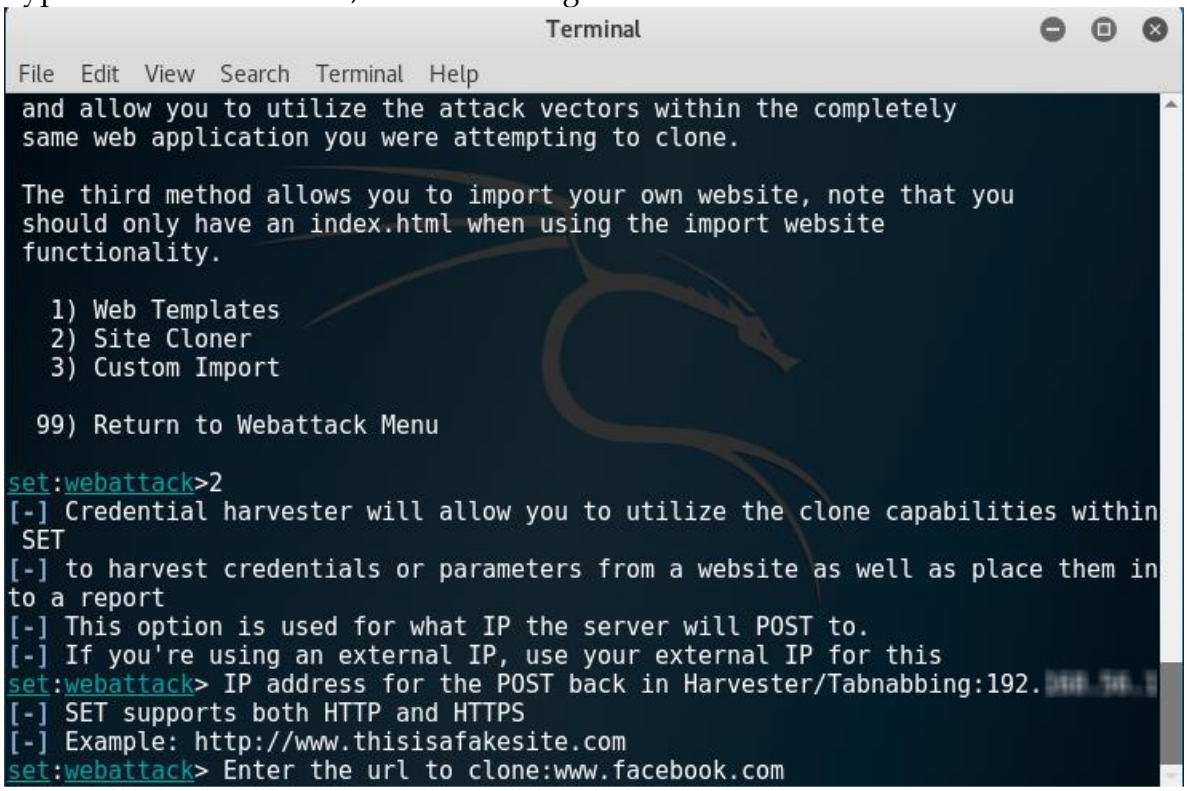


7. Type the IP address of the Kali Linux of VM. Here, we have used 192.XX.XX.XX as the IP address, as shown in Figure 9.

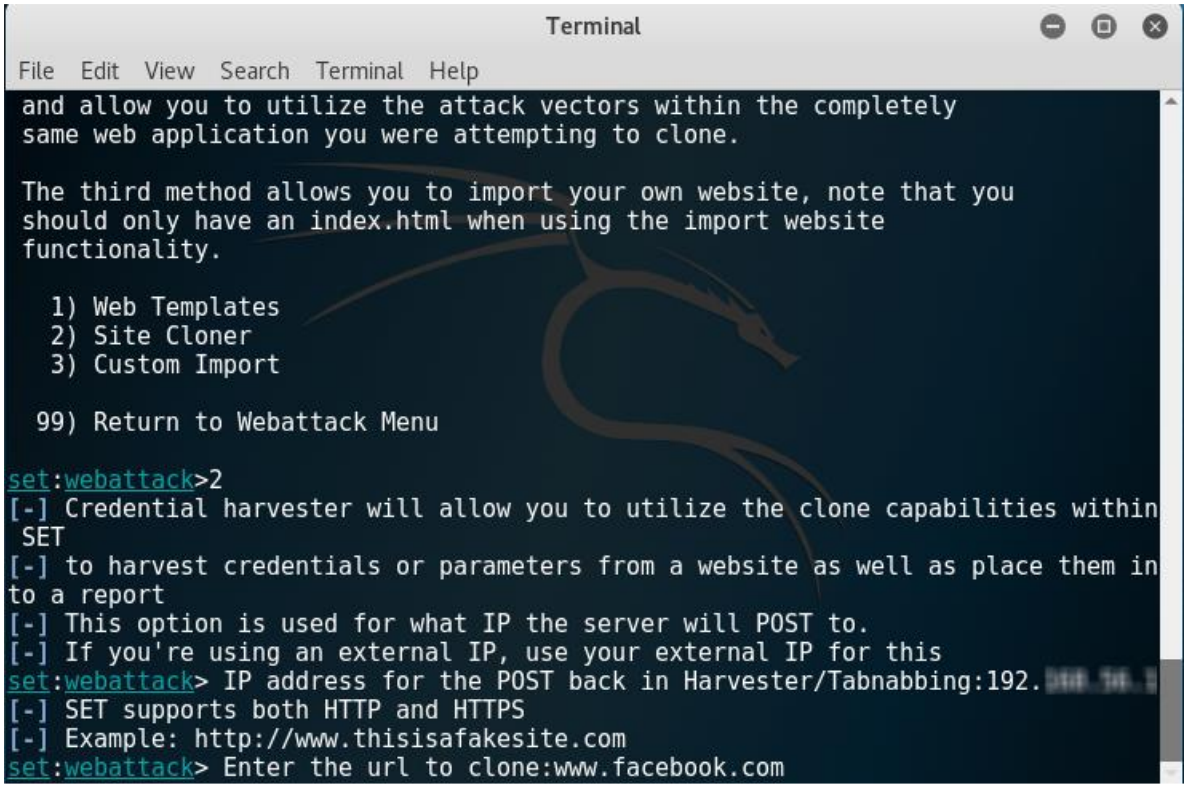


Then it will prompt to enter the URL of the website which is required to be cloned.

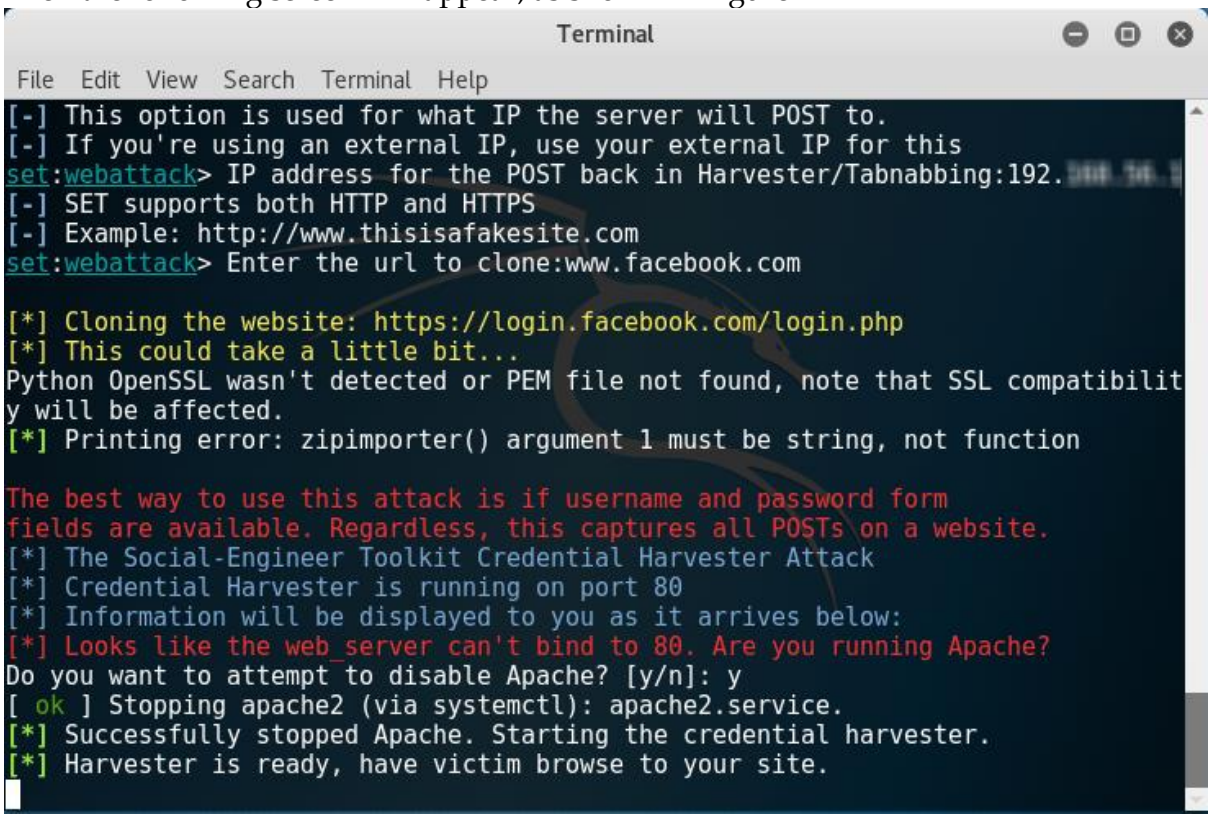
8. Type www.facebook.com, as shown in Figure 10.



9. Type www.facebook.com, as shown in Figure 10.

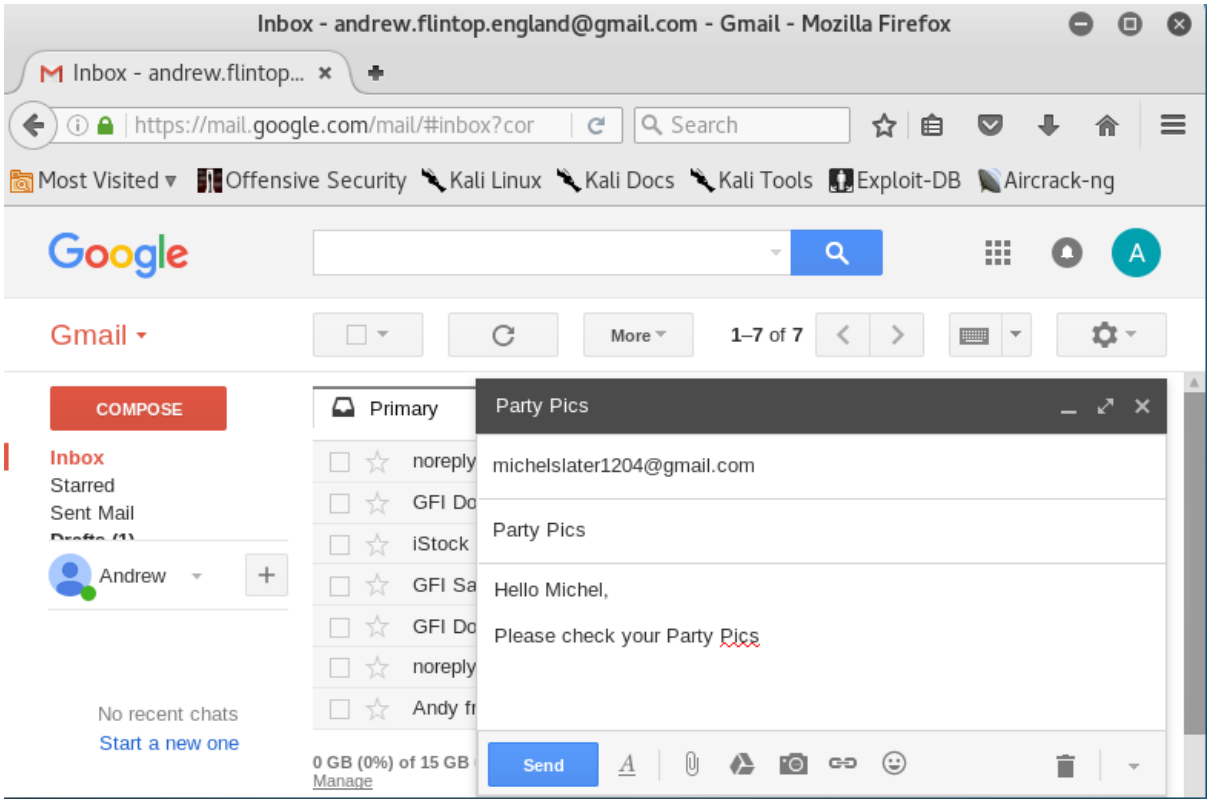


Then the following screen will appear, as shown in Figure 11



10. Launch a web browser in Kali Linux and open an email service, as shown in Figure 12.

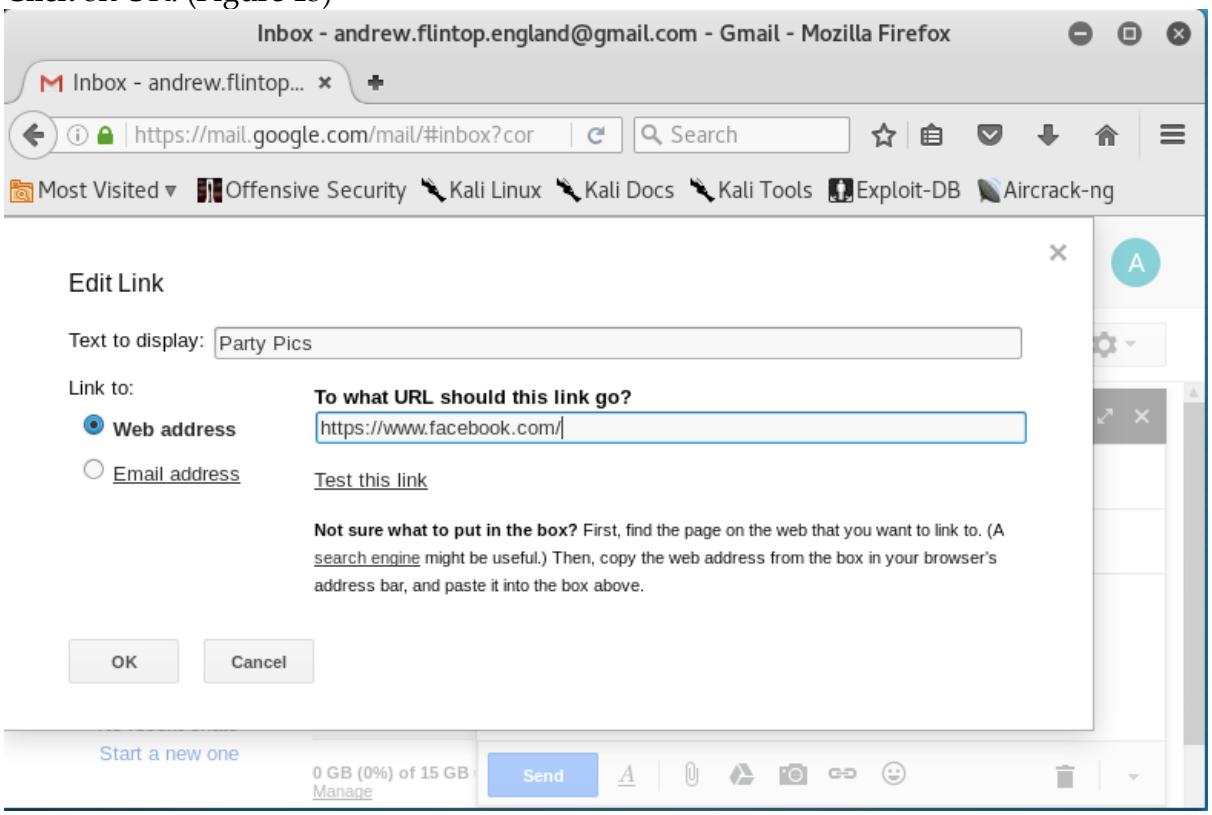
11. Compose an email and provide the target users email id in the To textbox, as shown in Figure 12.



12. Click on the link icon.

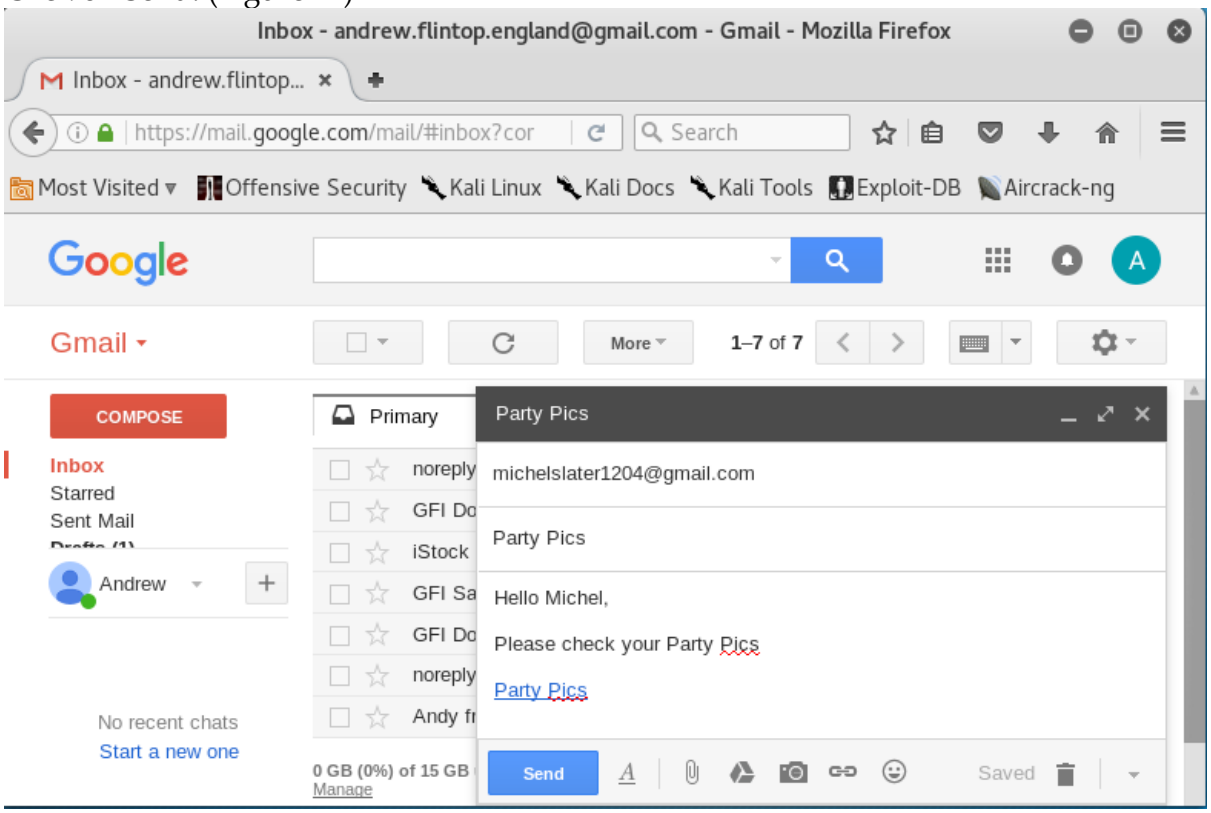
The following window will appear, as shown in Figure 13.

13. Type a text in the Text to display textbox. (Figure 13)
14. Click on the radio button Web address. (Figure 13)
15. Type the fake URL https://facebook.com/ in the Web address text box. (Figure 13).
16. Click on OK. (Figure 13)

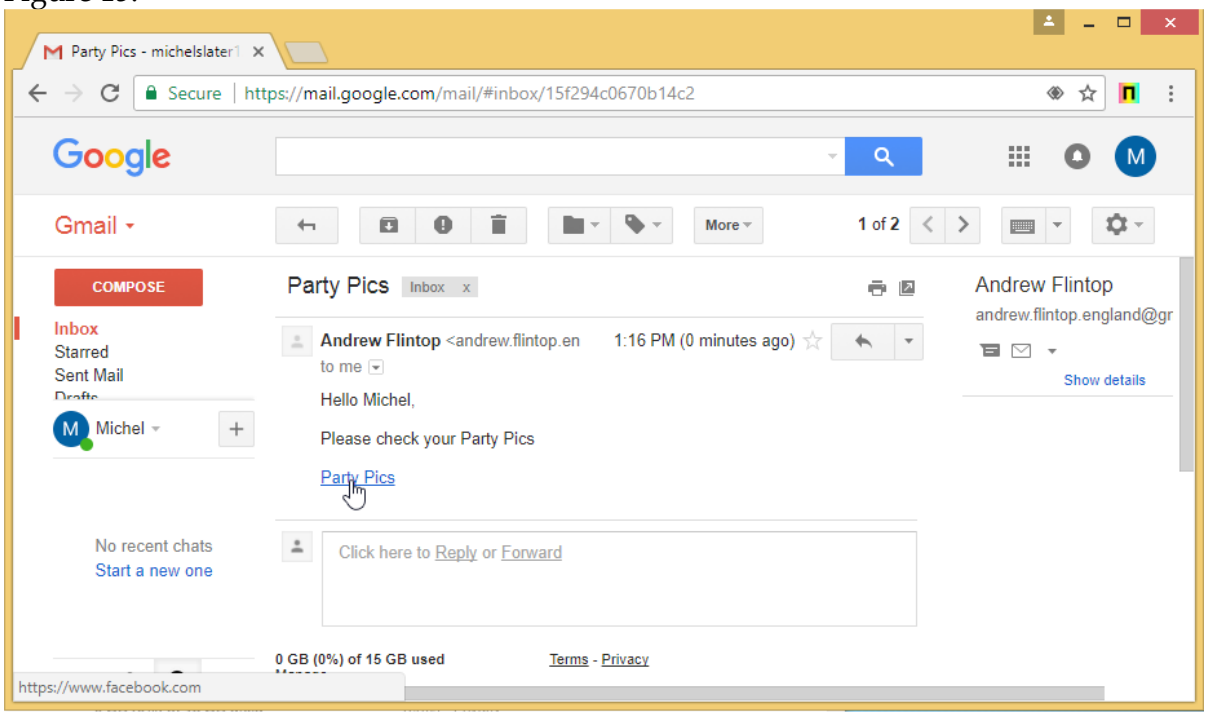


Now the text that you have typed will appear in the email body as a link, as shown in Figure 14.

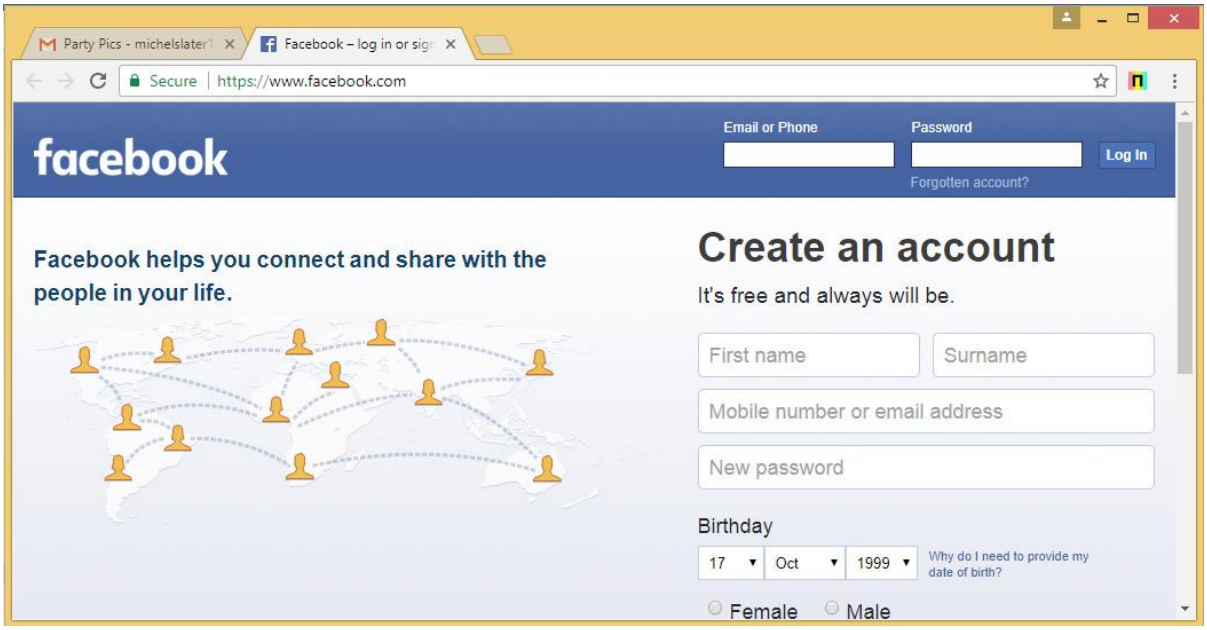
17. Click on Send. (Figure 14)



Now when the target user will open his email, he will find the link, as shown in Figure 15.



When the target user will click on the link, he/she will be presented with a replica of Facebook.com, as shown in Figure 16.



The fake Facebook.com page will ask the target user to enter the email and password tor view the pictures. When the target user enters the credentials, the SET terminal of Kali Linux will fetch the email id and password