Information System Security - IS2109

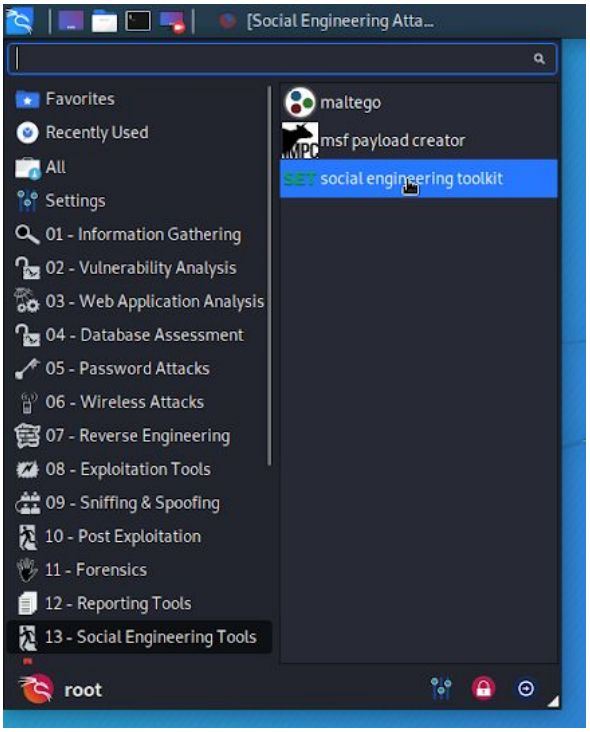
Social Engineering attack

Group 2

University of Colombo

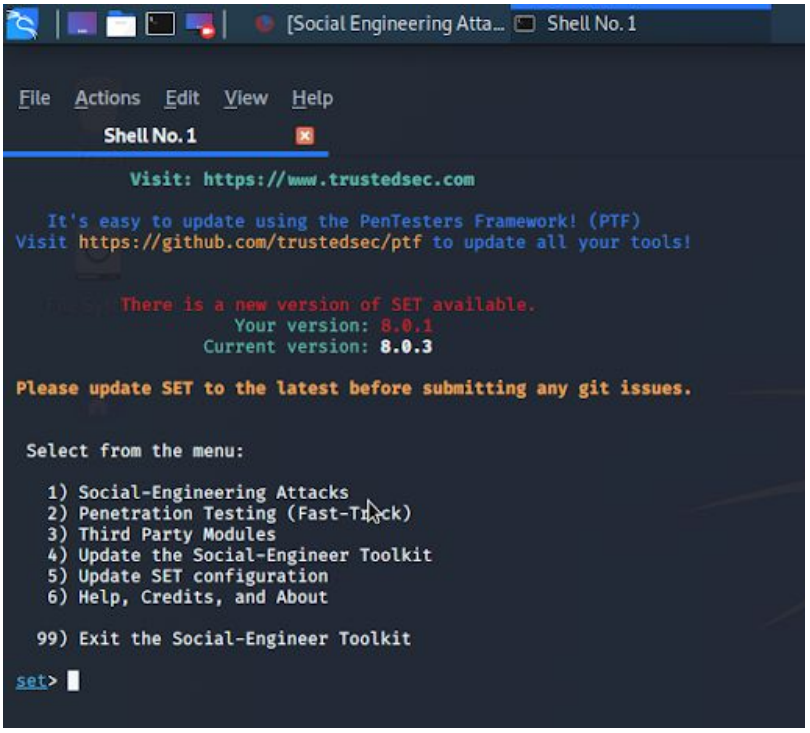
School of Computing

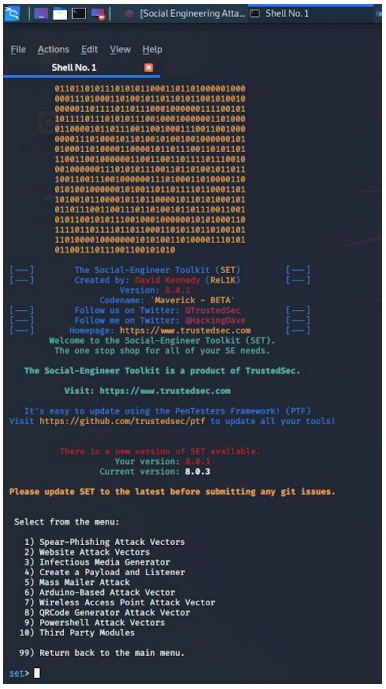
Kali Linux is a debian based Linux distribution which is aimed at advanced penetration testing and security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Our aim was to create a phishing attack on a selected group of students and to study the responses and behaviours of victims in a statistical manner.

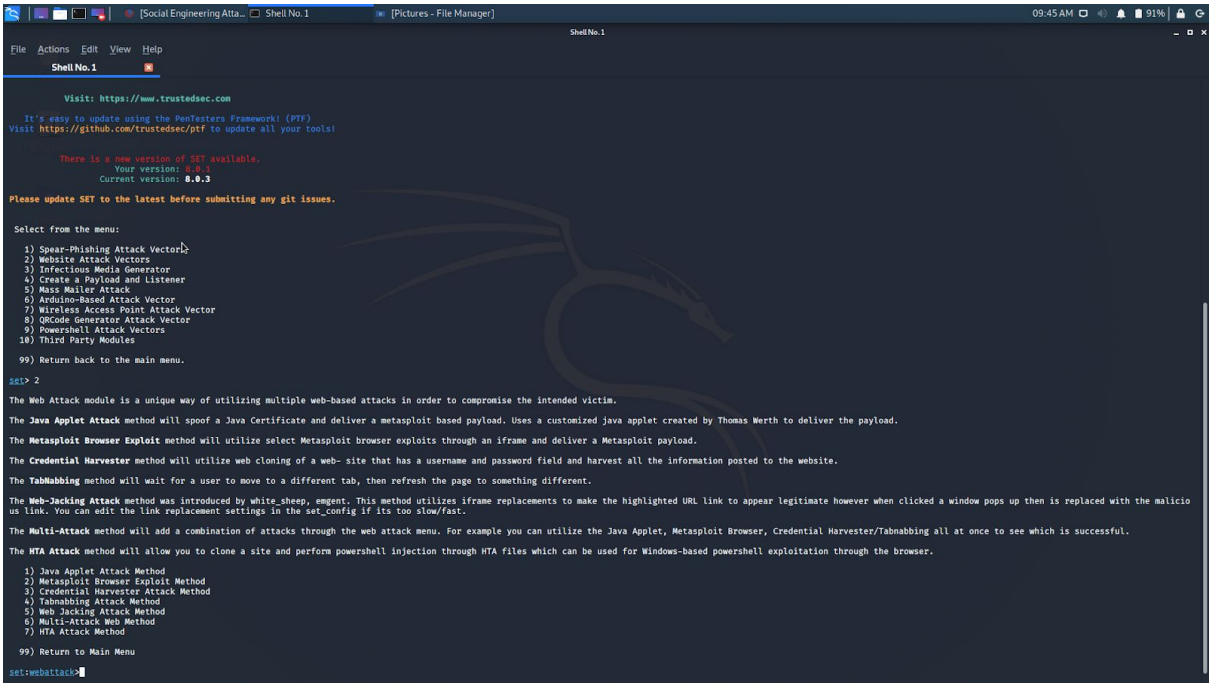


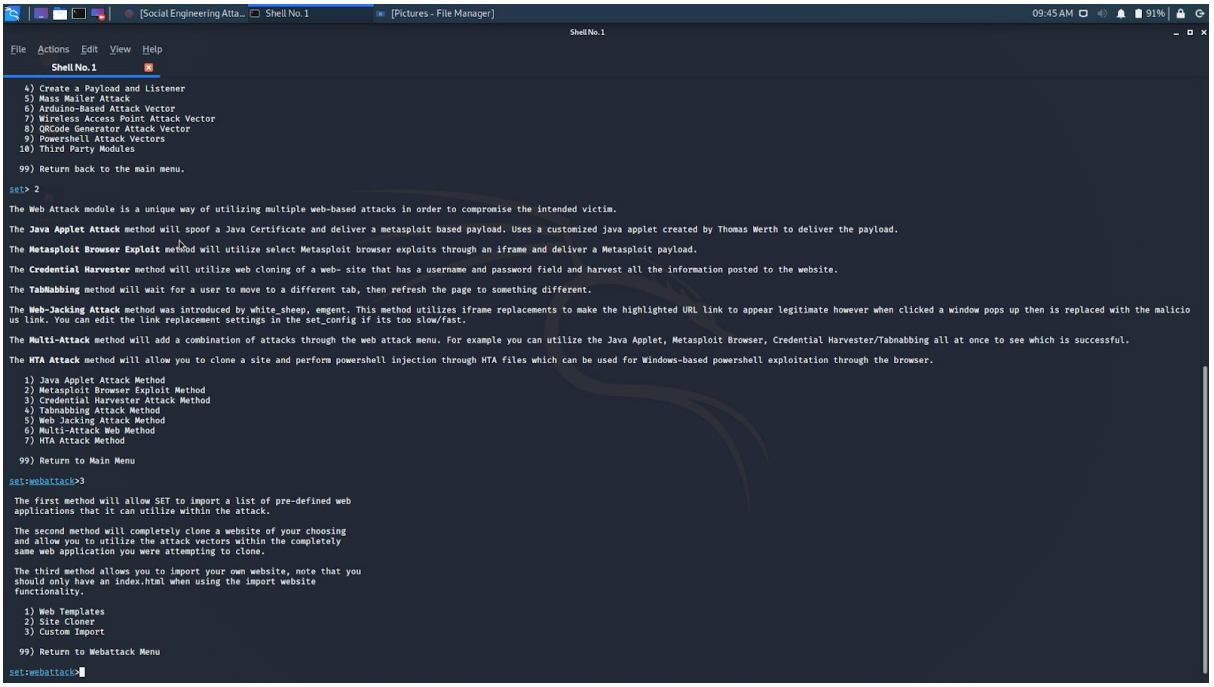
Since Kali is geared specifically towards System penetration testing and SET (Social Engineering Toolkit) is pre-installed on it with already being configured, It was chosen for conducting our project.

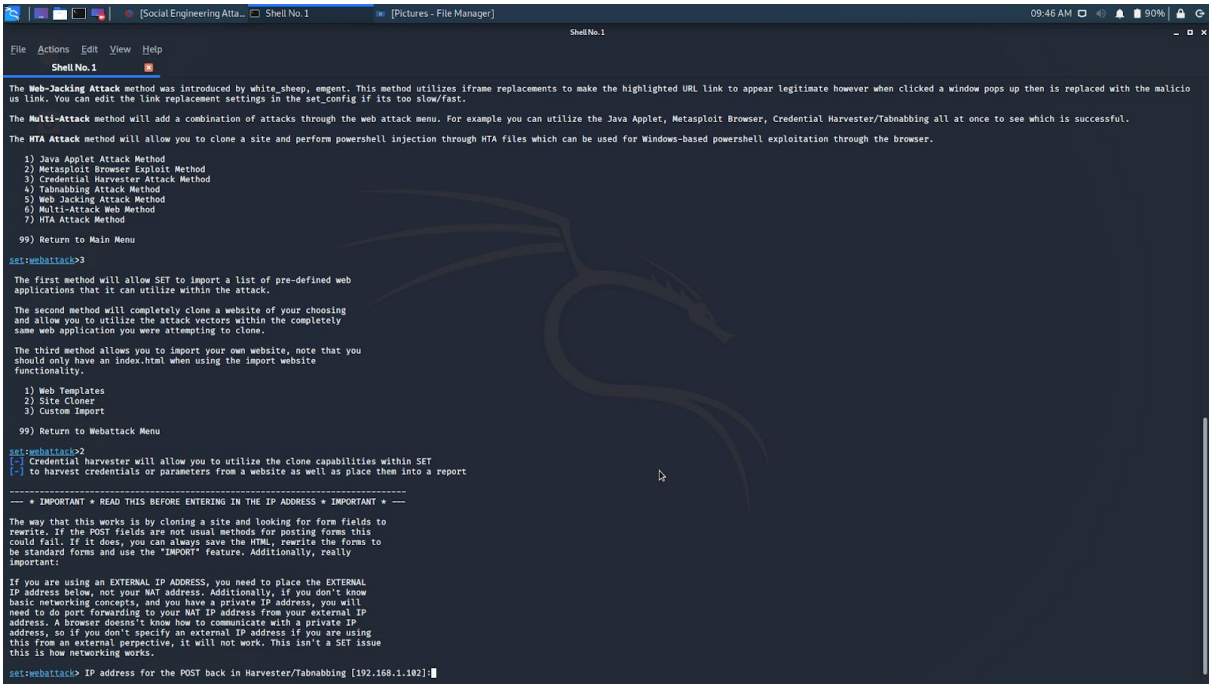
From the given menu in the terminal, we did the attack which came under the Social Engineering Attack and website attack vectors. The Website Attack vector was selected and it contains multiple web attacks. Then the credential harvester method was selected. This method primarily aimed at the phishing credentials of users using web attacks. From the given options as site cloner, custom import, web templates the site cloner was selected since it clone a known site of preferred and allows to utilize attack vectors within it.



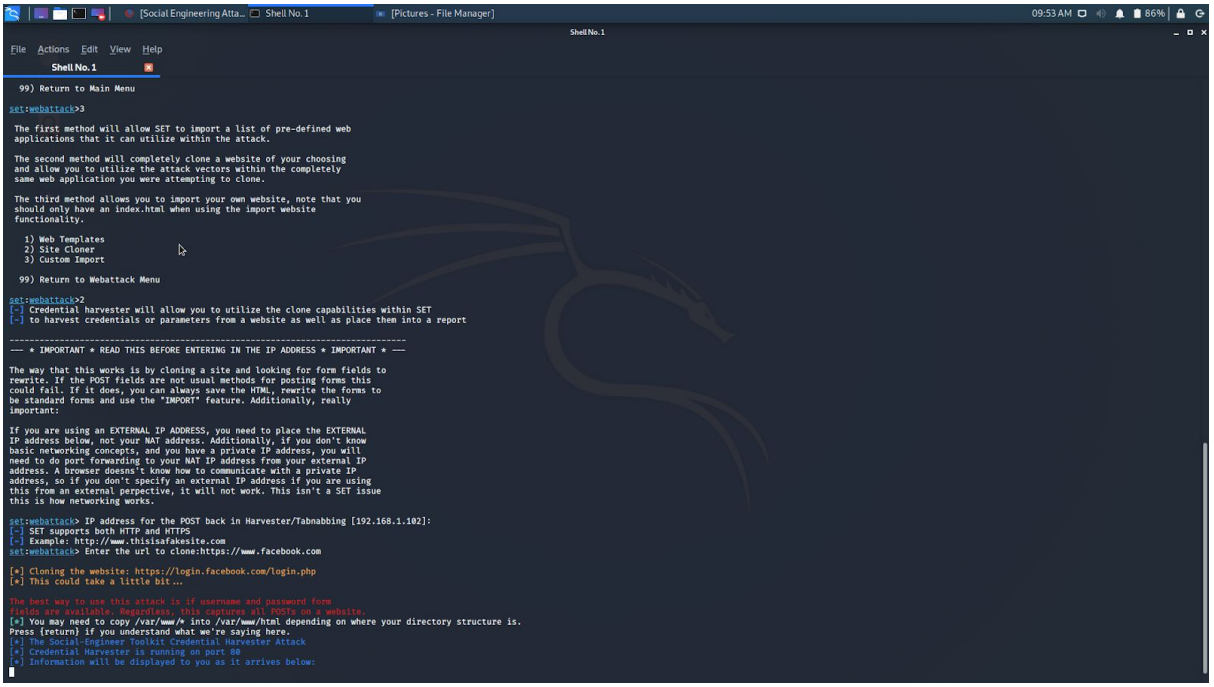





[Social Engineering Atta...
Shell No. 1
[Pictures - File Manager]
09:45 AM
91%
Shell No. 1
File Actions Edit View Help
Shell No. 1
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 2
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 malicio
us 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>

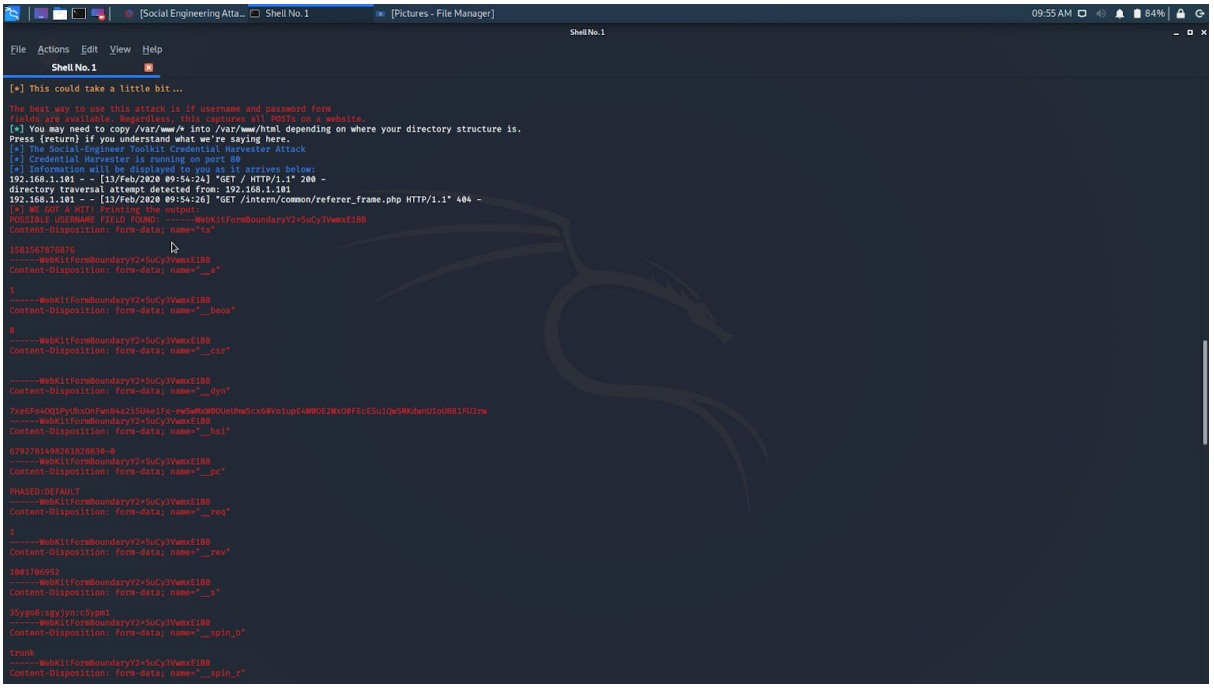

[Social Engineering Atta...
Shell No. 1
[Pictures - File Manager]
09:46 AM
90%
Shell No. 1
File Actions Edit View Help
Shell No. 1
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicio
us 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>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 [192.168.1.102]:

192.168.1.102



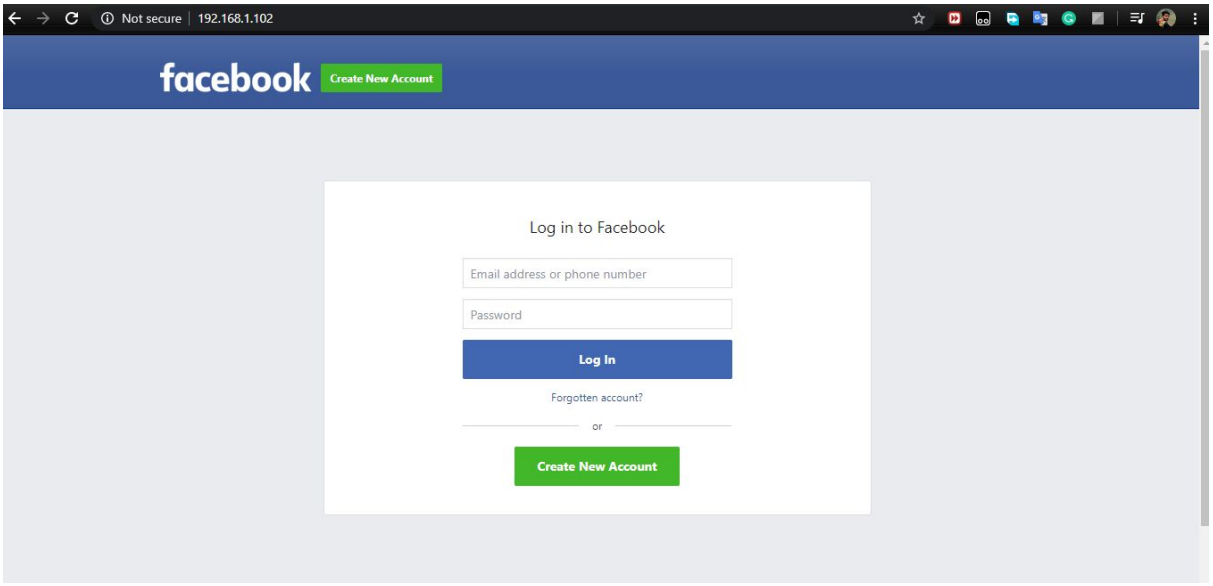
Since SET supports both http and https here https://www.facebook.com was given as the site to clone. And the IP address to it is 192.168.1.102. If someone access it fill out the login page credential harvester will automatically send the data to the attacker. And in this case credential harvester ran on port 80.

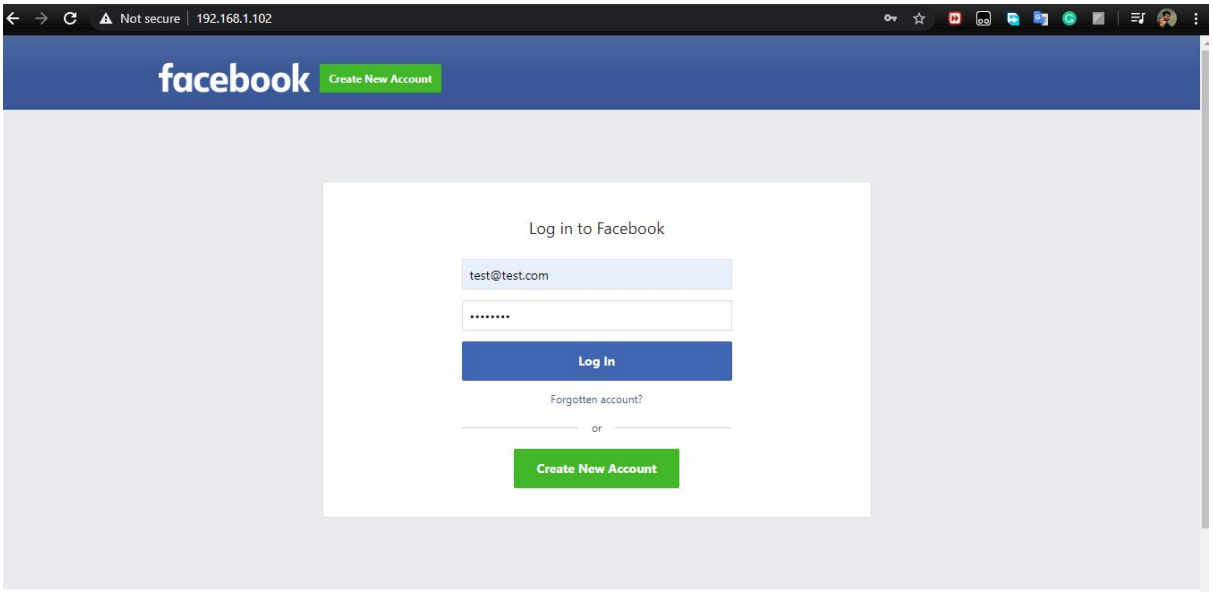
We can save all the data posted by the user in .xml format on our machine.



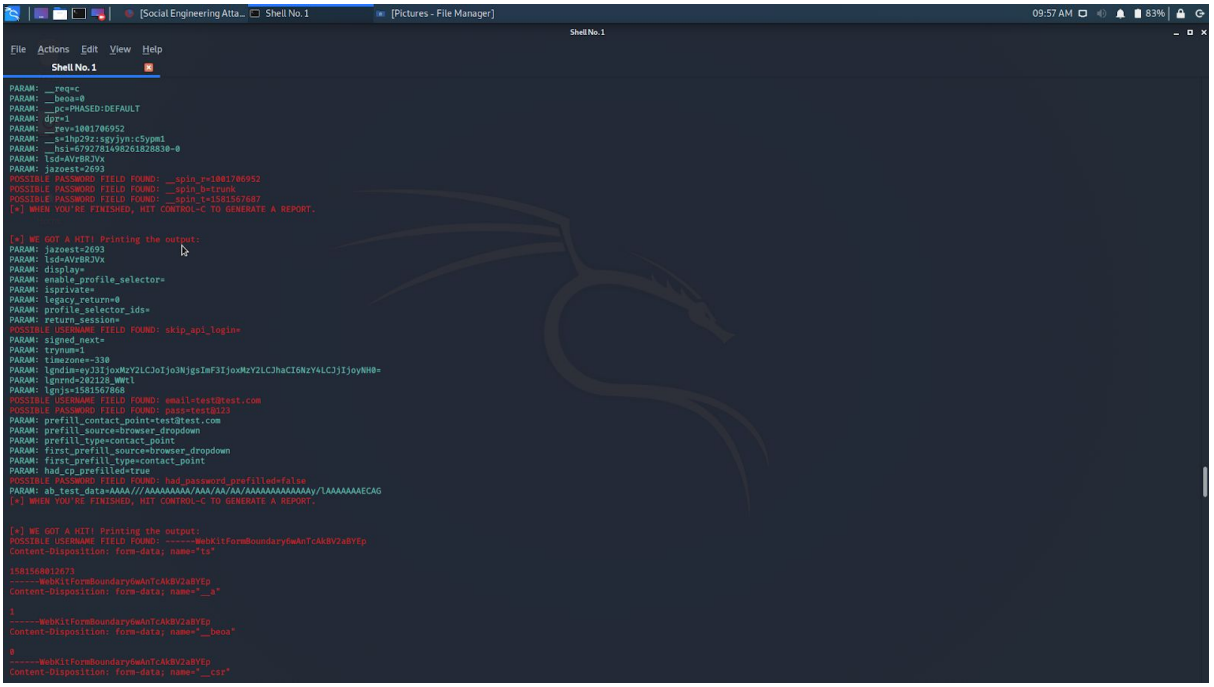
When someone tries to visit the above IP 192.168.1.102

Visitor IP = 192.168.1.101



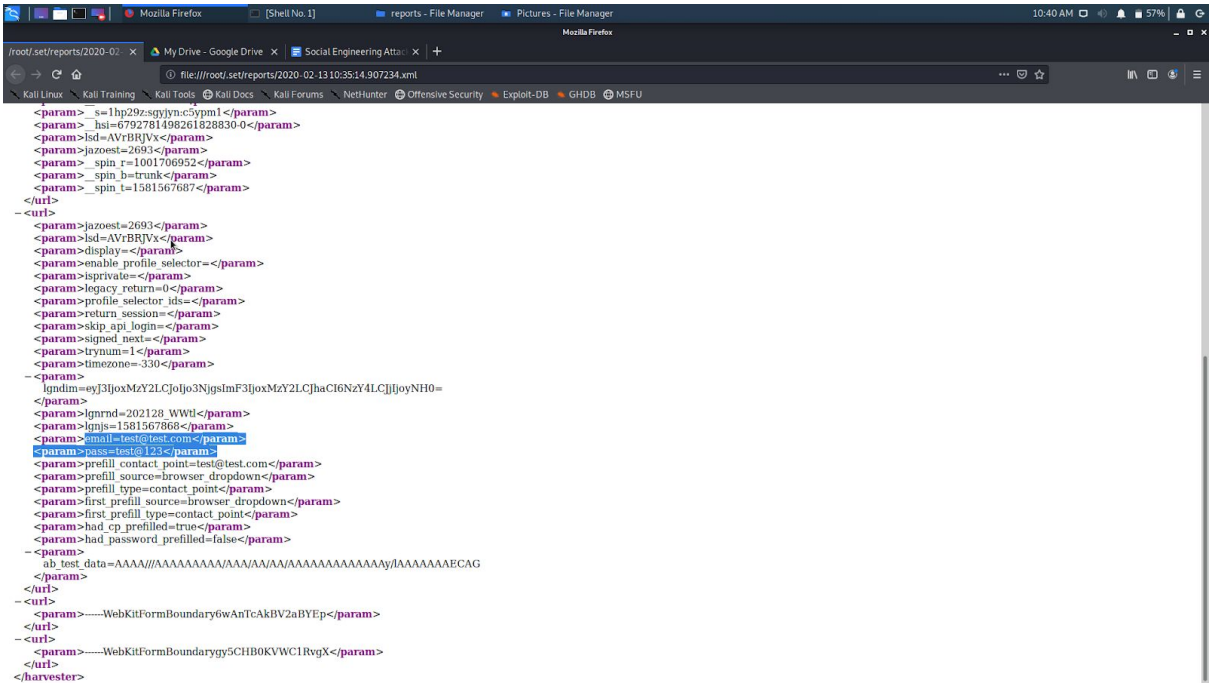


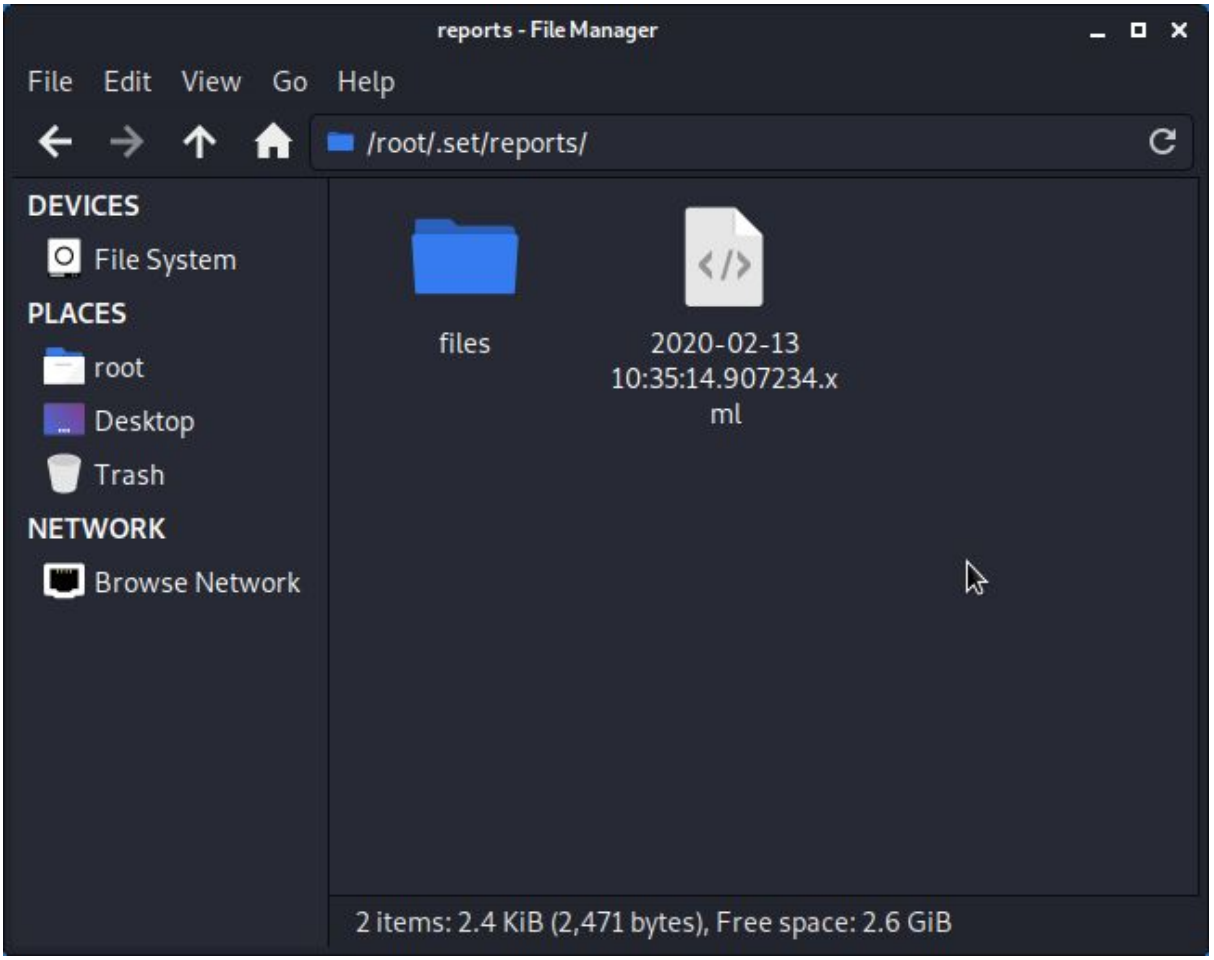
Visitor put email and password and click login



We can see the username and password he put.

Tool save all the data in .xml file


Mozilla Firefox
[Shell No. 1]
reports - File Manager
Pictures - File Manager
10:40 AM
57%
Mozilla Firefox
/root/.set/reports/2020-02-
My Drive - Google Drive
Social Engineering Attac
file:///root/.set/reports/2020-02-13 10:35:14.907234.xml
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
<param>__s=1hp29z:sgyjyn:c5ypm1</param>
<param>__hsi=6792781498261828830-0</param>
<param>lsd=AVrBRJVx</param>
<param>jazoest=2693</param>
<param>__spin_r=1001706952</param>
<param>__spin_b=trunk</param>
<param>__spin_t=1581567687</param>
</url>
<url>
<param>jazoest=2693</param>
<param>lsd=AVrBRJVx</param>
<param>display=</param>
<param>enable_profile_selector=</param>
<param>isprivate=</param>
<param>legacy_return=0</param>
<param>profile_selector_ids=</param>
<param>return_session=</param>
<param>skip_api_login=</param>
<param>signed_next=</param>
<param>trynum=1</param>
<param>timezone=-330</param>
<param>
lgndim=eyJ3IjoxMzY2LCJoIjo3NjgsImF3IjoxMzY2LCJhaCI6NzY4LCJjIjoyNH0=
</param>
<param>lgnrnd=202128_WWtl</param>
<param>lgnjs=1581567868</param>
<param>email=test@test.com</param>
<param>pass=test@123</param>
<param>prefill_contact_point=test@test.com</param>
<param>prefill_source=browser_dropdown</param>
<param>prefill_type=contact_point</param>
<param>first_prefill_source=browser_dropdown</param>
<param>first_prefill_type=contact_point</param>
<param>had_cp_prefilled=true</param>
<param>had_password_prefilled=false</param>
<param>
ab_test_data=AAAA///AAAAAAAAA/AAA/AA/AA/AAAAAAAAAAAAAy/lAAAAAAAECAG
</param>
</url>
<url>
<param>------WebKitFormBoundary6wAnTcAkBV2aBYEp</param>
</url>
<url>
<param>------WebKitFormBoundarygy5CHB0KVWC1RvgX</param>
</url>
</harvester>


reports - File Manager
File Edit View Go Help
/root/.set/reports/
DEVICES
File System
PLACES
root
Desktop
Trash
NETWORK
Browse Network
files
2020-02-13
10:35:14.907234.x
ml
2 items: 2.4 KiB (2,471 bytes), Free space: 2.6 GiB

Group Members

Name	Index number	Registration number
W.M.D.T.Andradi	17020107	2017/IS/010
P.B.K.T.Gunarathne	17020271	2017/IS/027
S.A.Abesiriwardhana	17020018	2017/IS/001
T. A. Delpachithra	17020204	2017/IS/020