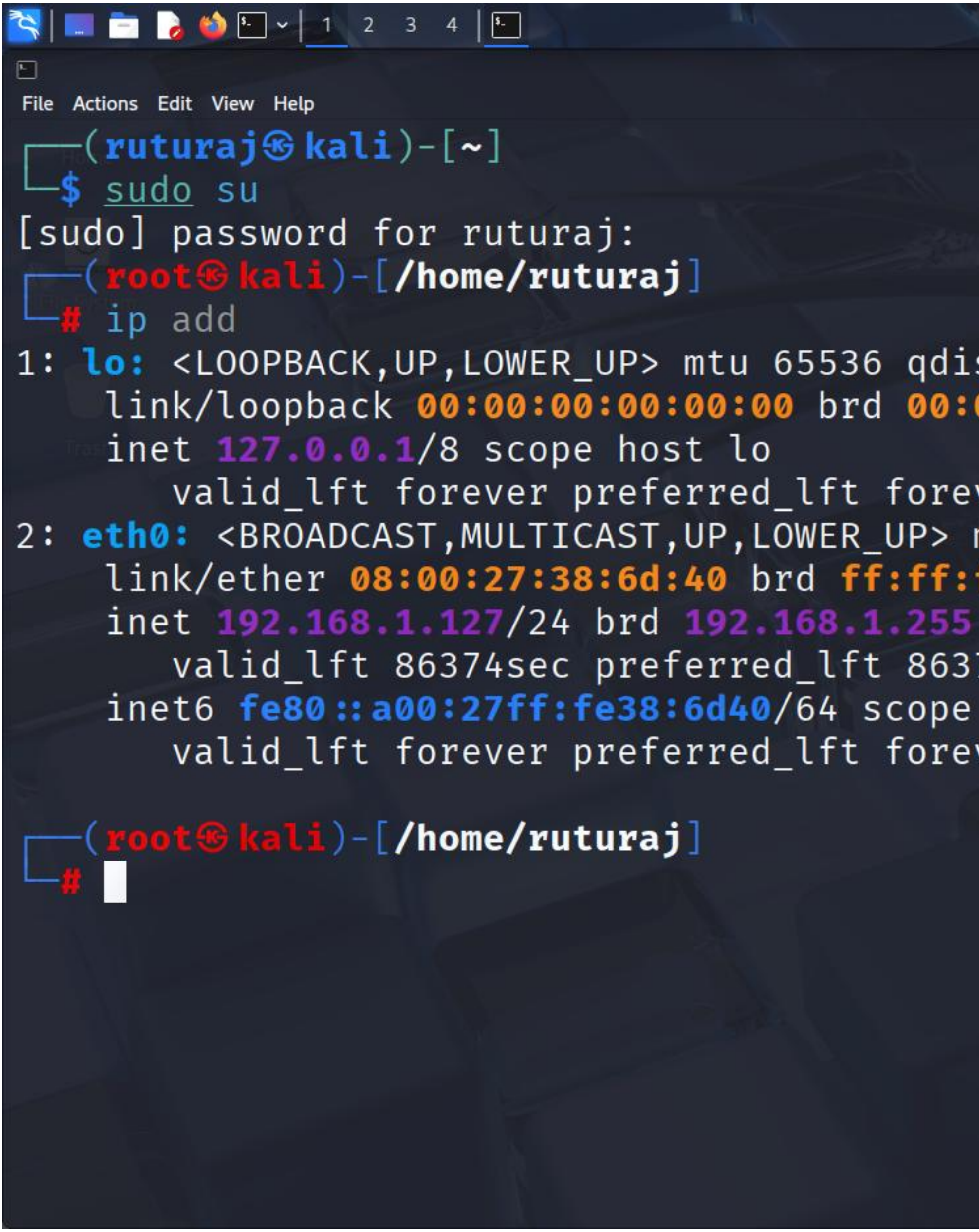
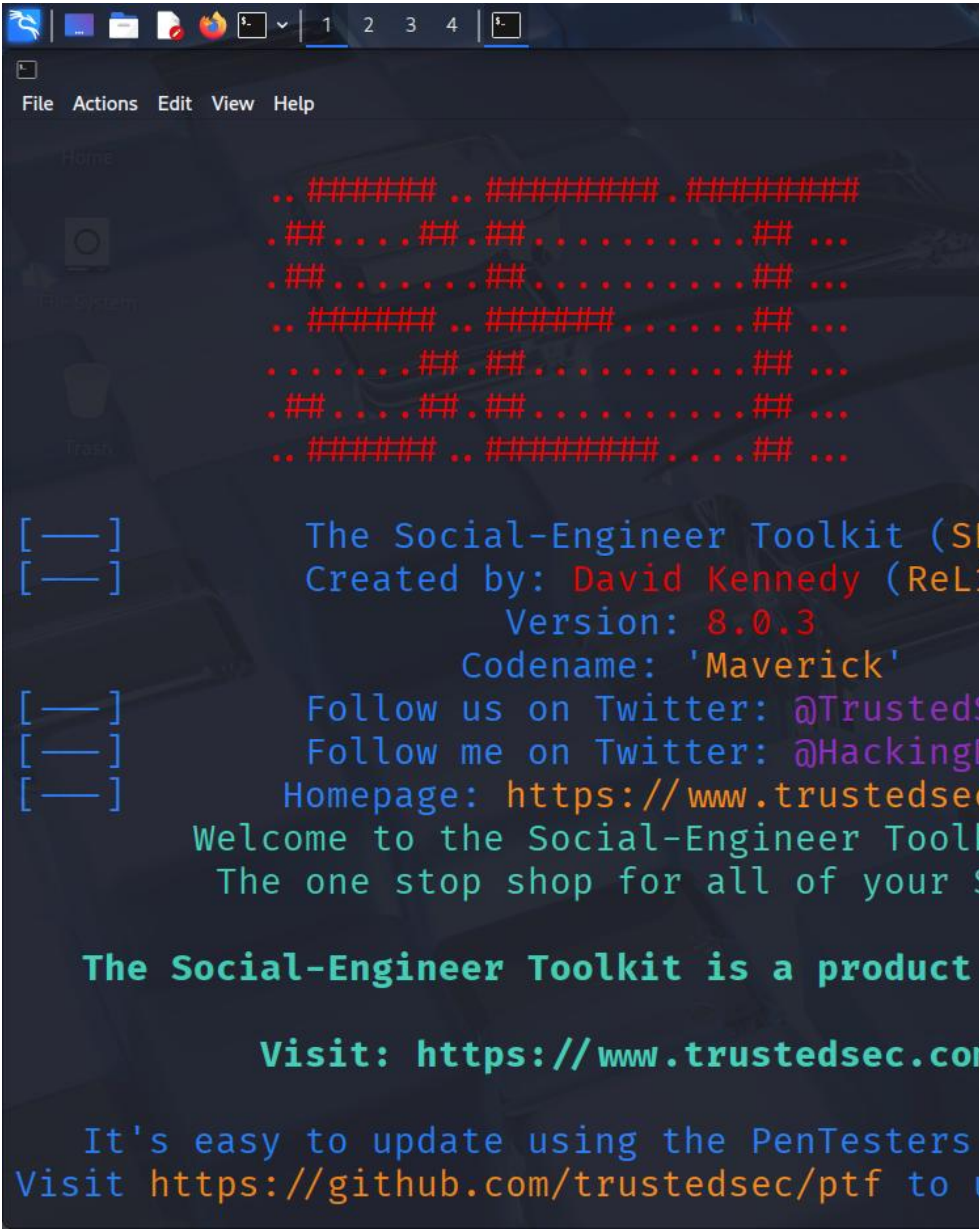
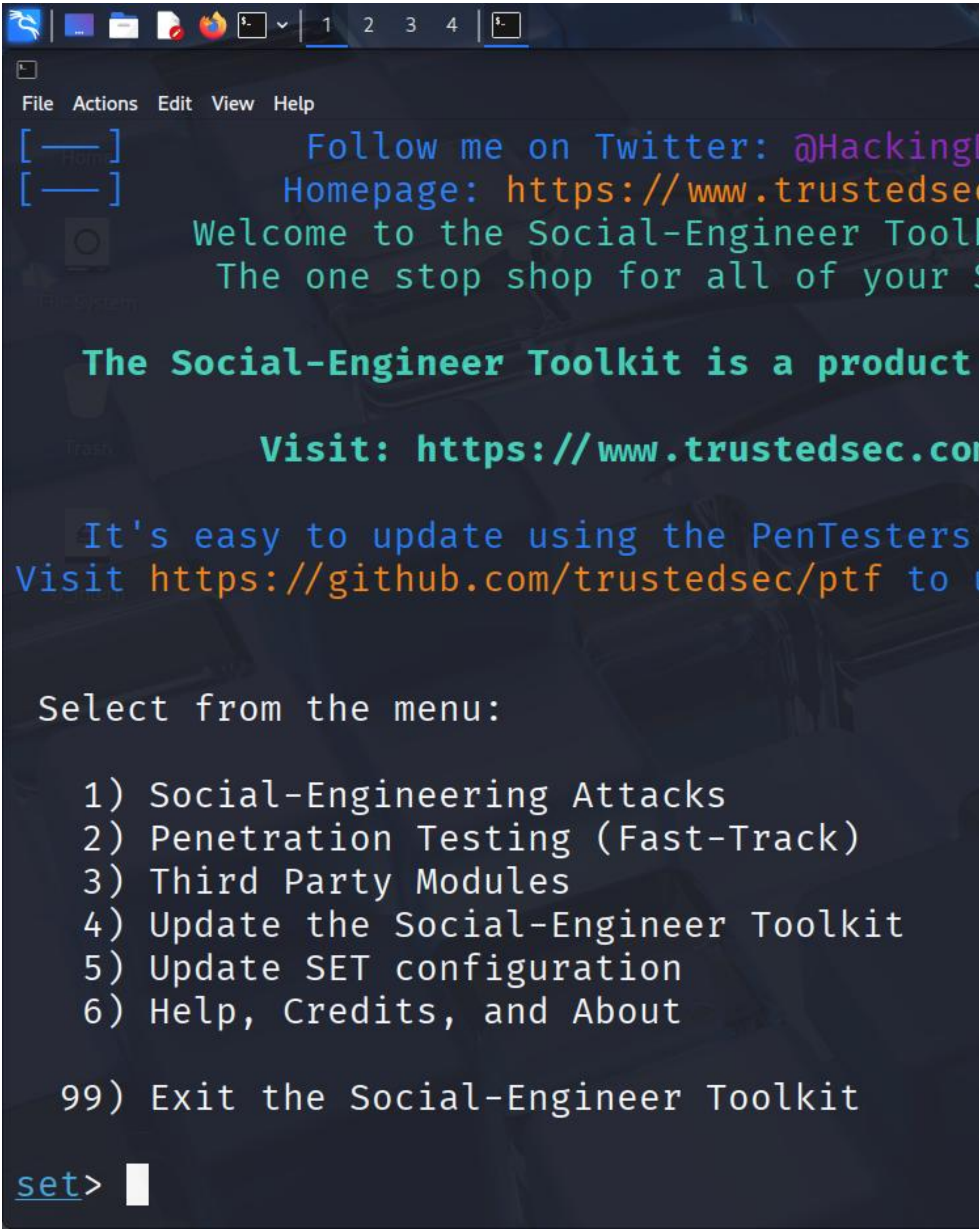


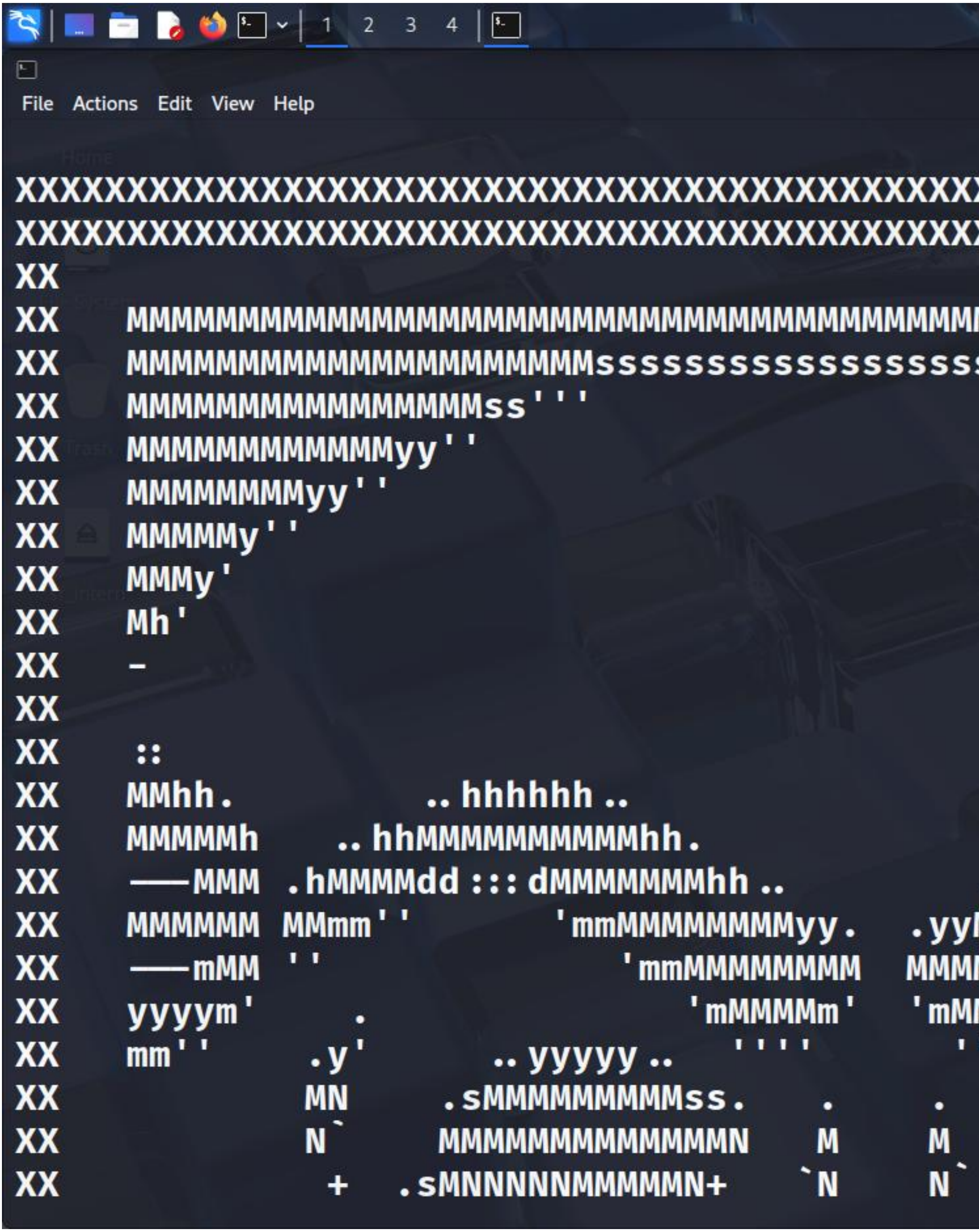
```
┌──(ruturaj㉿kali)-[~]
└─$ sudo su
[sudo] password for ruturaj:
┌──(root㉿kali)-[/home/ruturaj]
└─# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdis
    link/loopback 00:00:00:00:00:00 brd 00:0
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forev
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> m
    link/ether 08:00:27:38:6d:40 brd ff:ff:f
    inet 192.168.1.127/24 brd 192.168.1.255
       valid_lft 86374sec preferred_lft 8637
    inet6 fe80::a00:27ff:fe38:6d40/64 scope
       valid_lft forever preferred_lft forev

┌──(root㉿kali)-[/home/ruturaj]
└─#
```



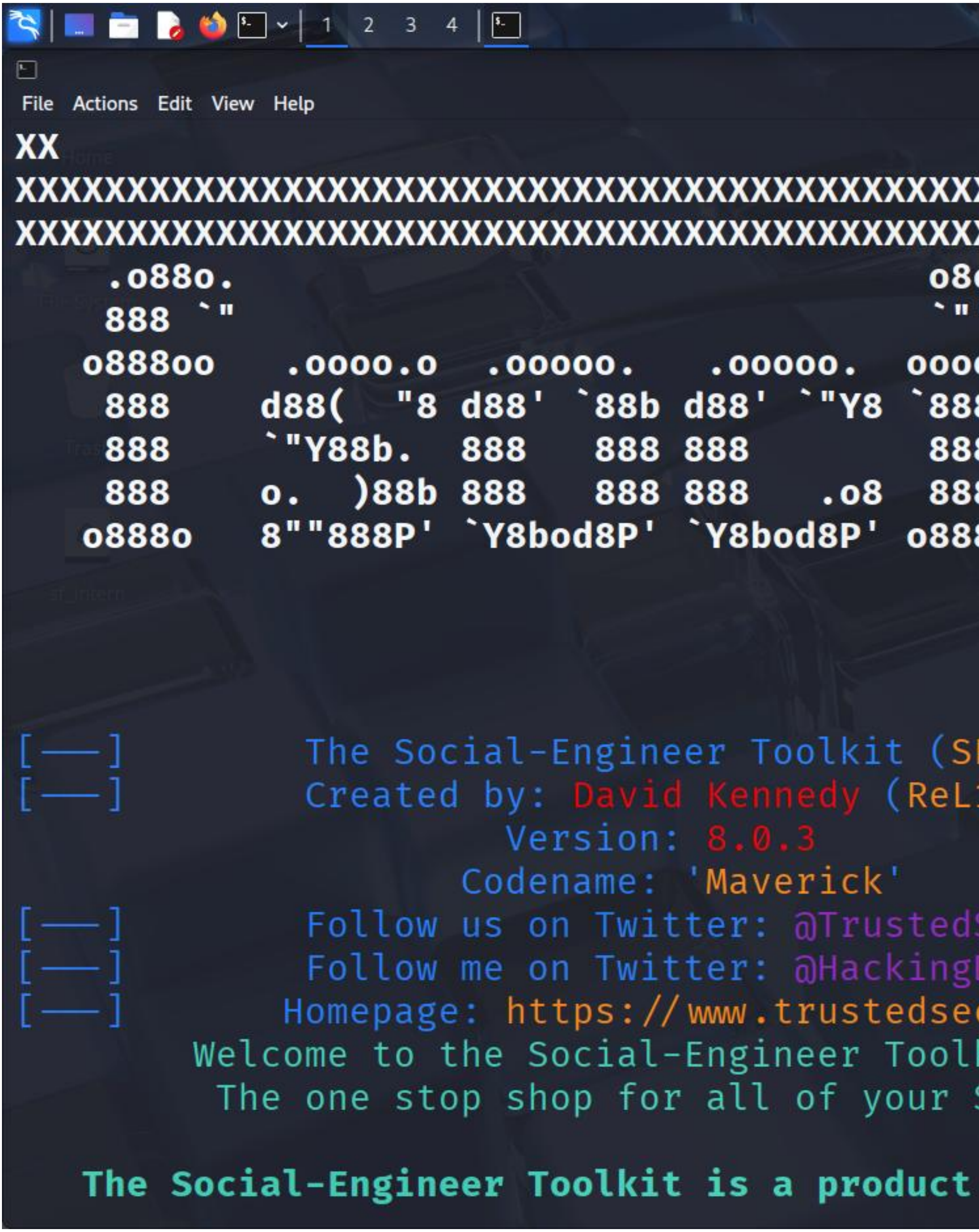
```
               ..######..########.########
               .##....##.##..........##...
               .##.......##..........##...
               ..######..######......##...
               .......##.##..........##...
               .##....##.##..........##...
               ..######..########....##...

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

   The Social-Engineer Toolkit is a product

             Visit: https://www.trustedsec.co

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



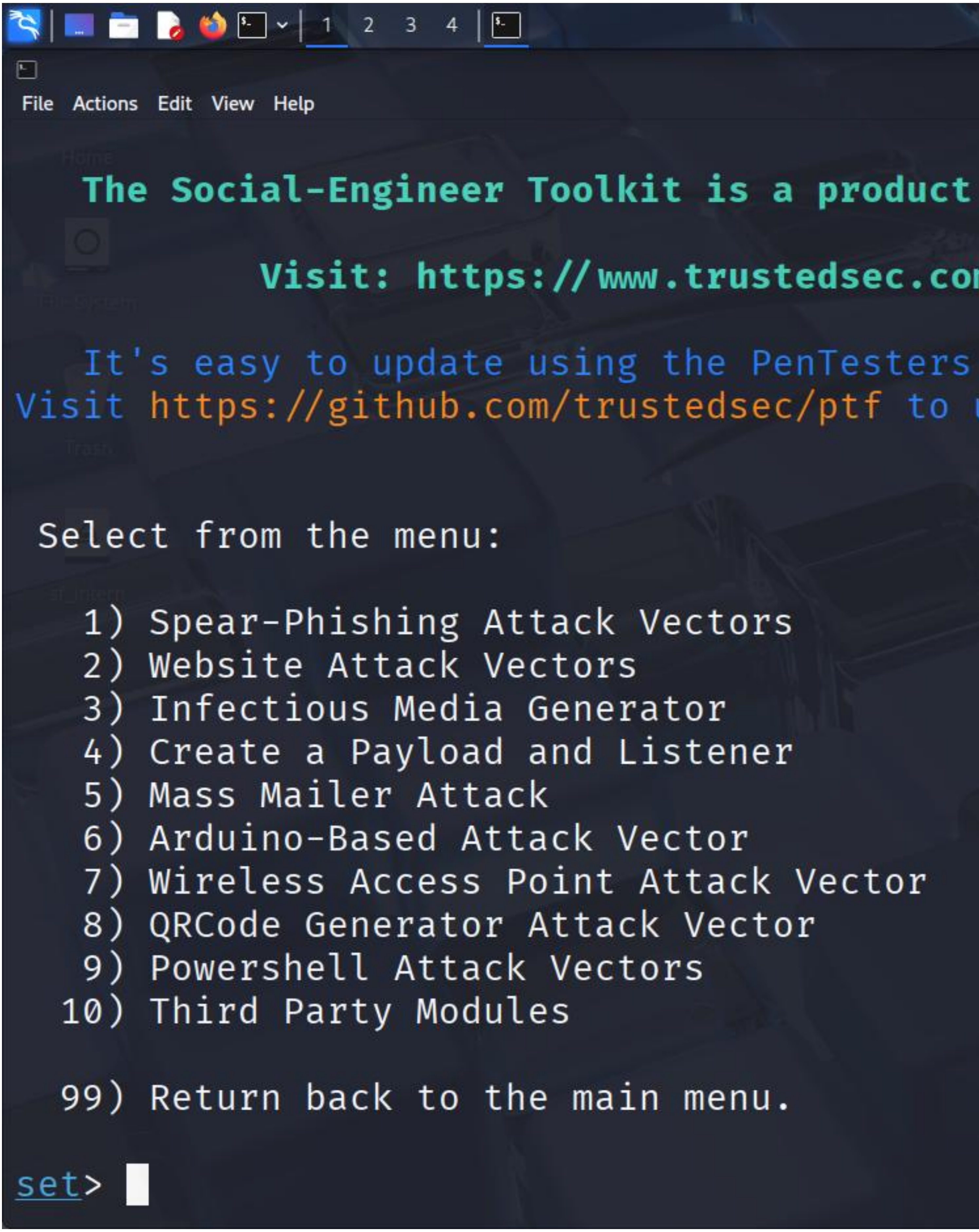
```
[—]         Follow me on Twitter: @Hacking
[—]        Homepage: https://www.trustedse
       Welcome to the Social-Engineer Tool
        The one stop shop for all of your 

   The Social-Engineer Toolkit is a product

           Visit: https://www.trustedsec.co

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


 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> 
```



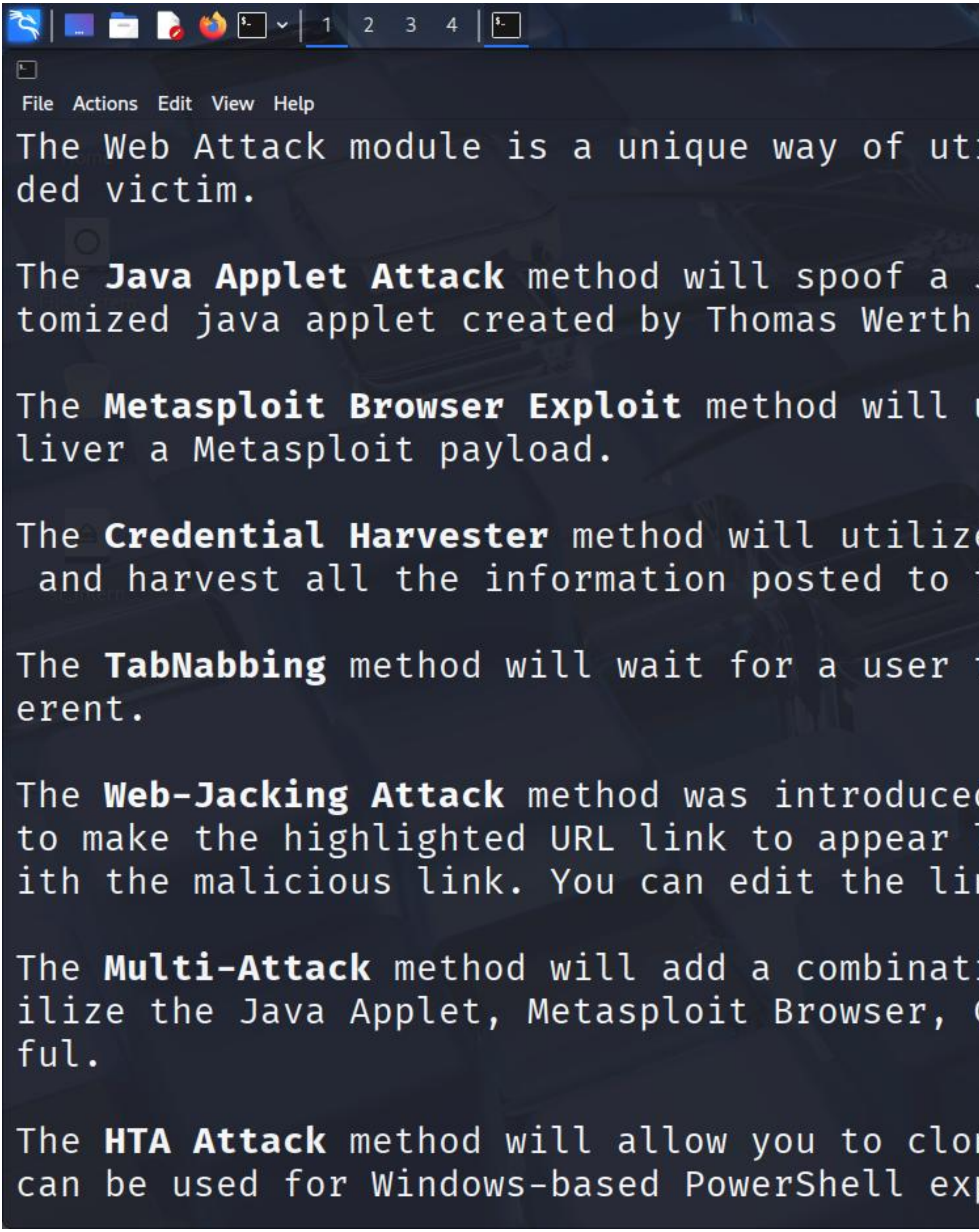
```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XX
XX   MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
XX   MMMMMMMMMMMMMMMMMMMMMssssssssssssssssss
XX   MMMMMMMMMMMMMMMMss'''
XX   MMMMMMMMMMMMyy''
XX   MMMMMMMMyy''
XX   MMMMMy''
XX   MMMy'
XX   Mh'
XX   -
XX
XX   ::
XX   MMhh.        ..hhhhhh..
XX   MMMMMh   ..hhMMMMMMMMMMhh.
XX   ---MMM .hMMMMdd:::dMMMMMMMhh..
XX   MMMMMM MMmm''      'mmMMMMMMMMyy.  .yy
XX   ---mMM ''             'mmMMMMMMMM  MMM
XX   yyyym'    .              'mMMMMm'  'mM
XX   mm''    .y'     ..yyyyy..  ''''      '
XX           MN    .sMMMMMMMMMss.   .    .
XX           N`    MMMMMMMMMMMMMN   M    M
XX            +  .sMNNNNNMMMMMN+   `N    N`
```



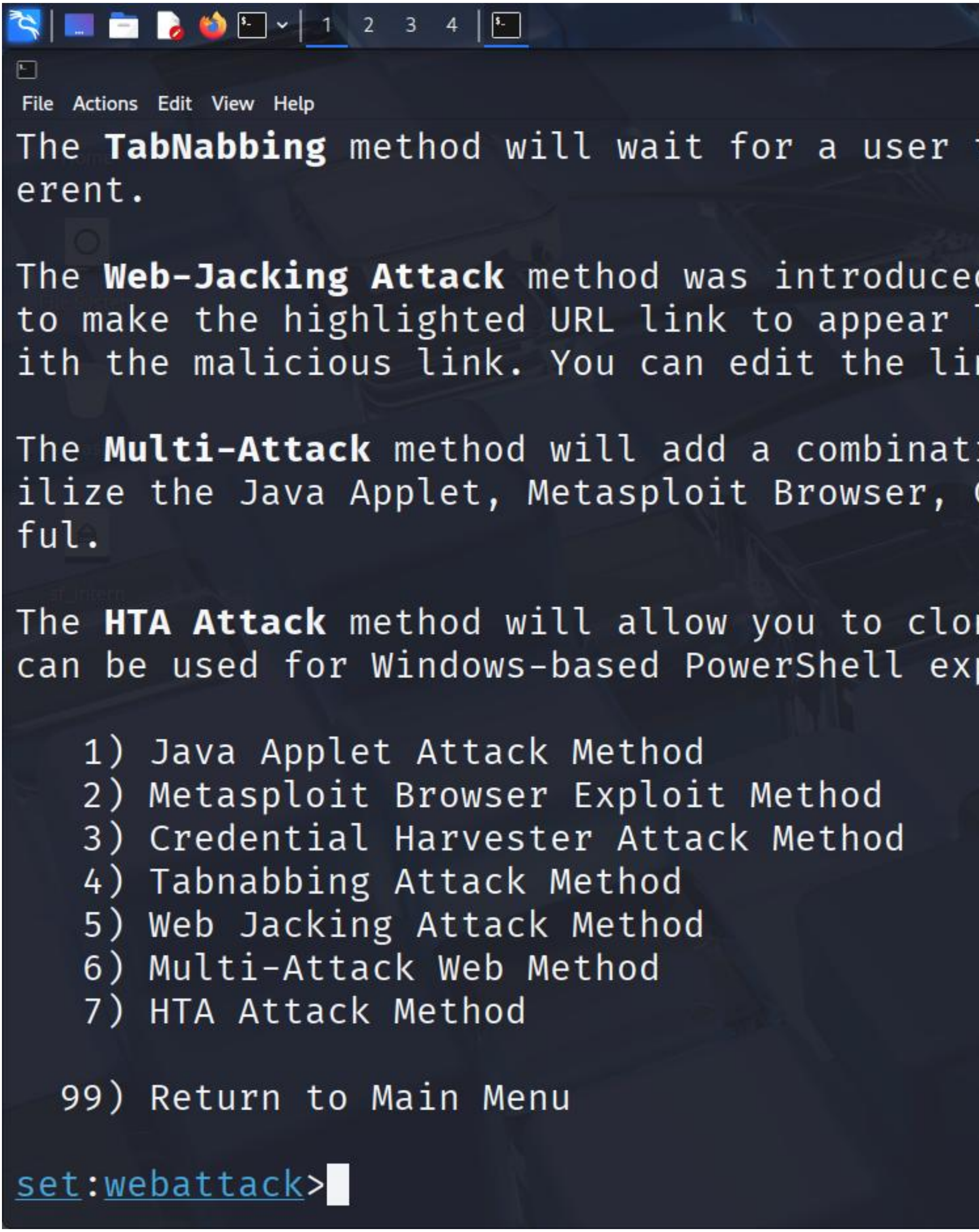
```
XX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
    .o88o.                                o8
    888 `"                                `"
   o888oo   .oooo.o  .ooooo.   .ooooo.  oooo
    888    d88(  "8 d88' `88b d88' `"Y8 `888
    888    `"Y88b.  888   888 888        888
    888    o.  )88b 888   888 888   .o8  888
   o888o   8""888P' `Y8bod8P' `Y8bod8P' o888



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

   The Social-Engineer Toolkit is a product
```



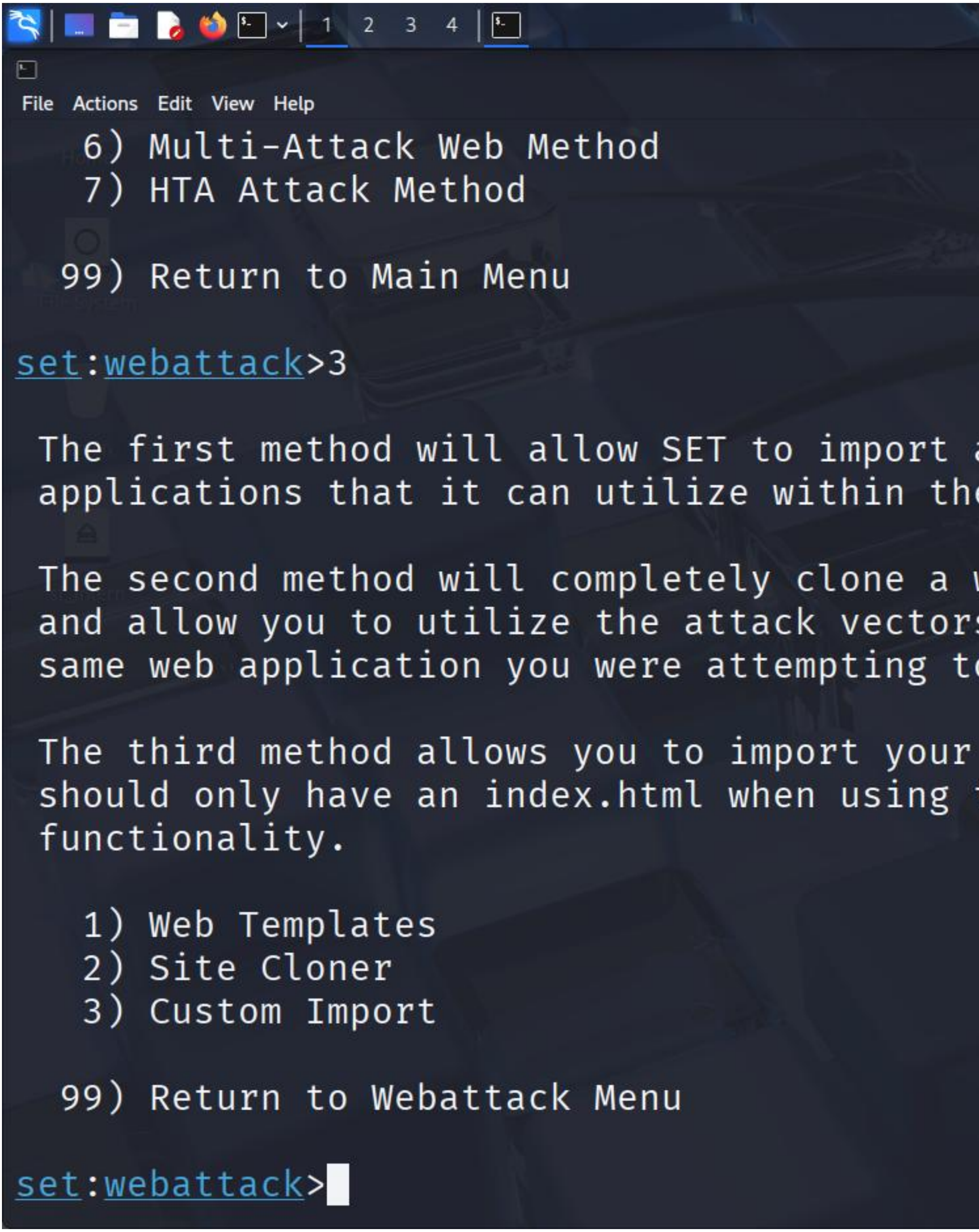
```
   The Social-Engineer Toolkit is a product

           Visit: https://www.trustedsec.co

   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> 
```



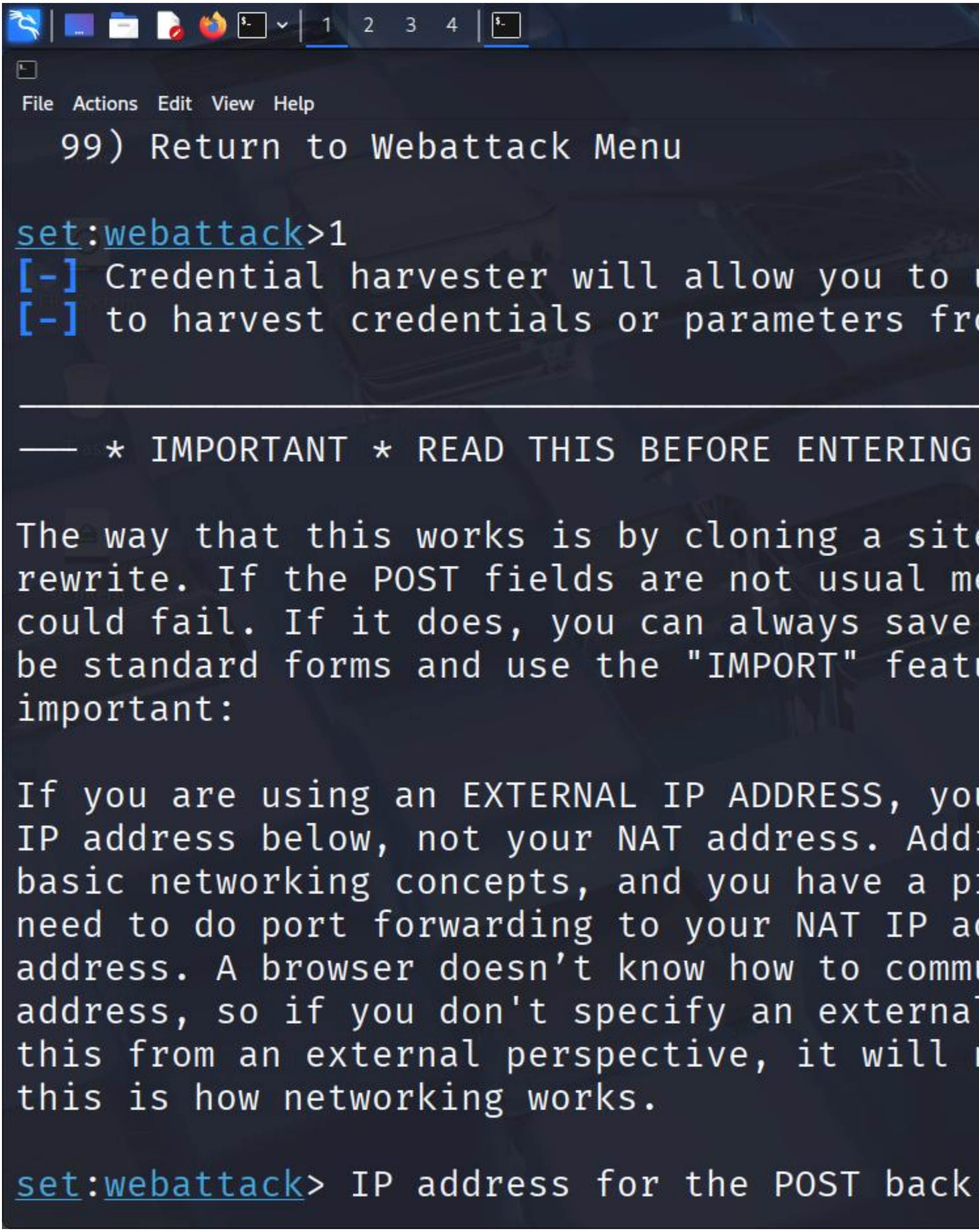
```
The Web Attack module is a unique way of uti
ded victim.

The Java Applet Attack method will spoof a
tomized java applet created by Thomas Werth

The Metasploit Browser Exploit method will
liver a Metasploit payload.

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

The TabNabbing method will wait for a user
erent.

The Web-Jacking Attack method was introduce
to make the highlighted URL link to appear
ith the malicious link. You can edit the li

The Multi-Attack method will add a combinat
ilize the Java Applet, Metasploit Browser,
ful.

The HTA Attack method will allow you to clo
can be used for Windows-based PowerShell ex
```



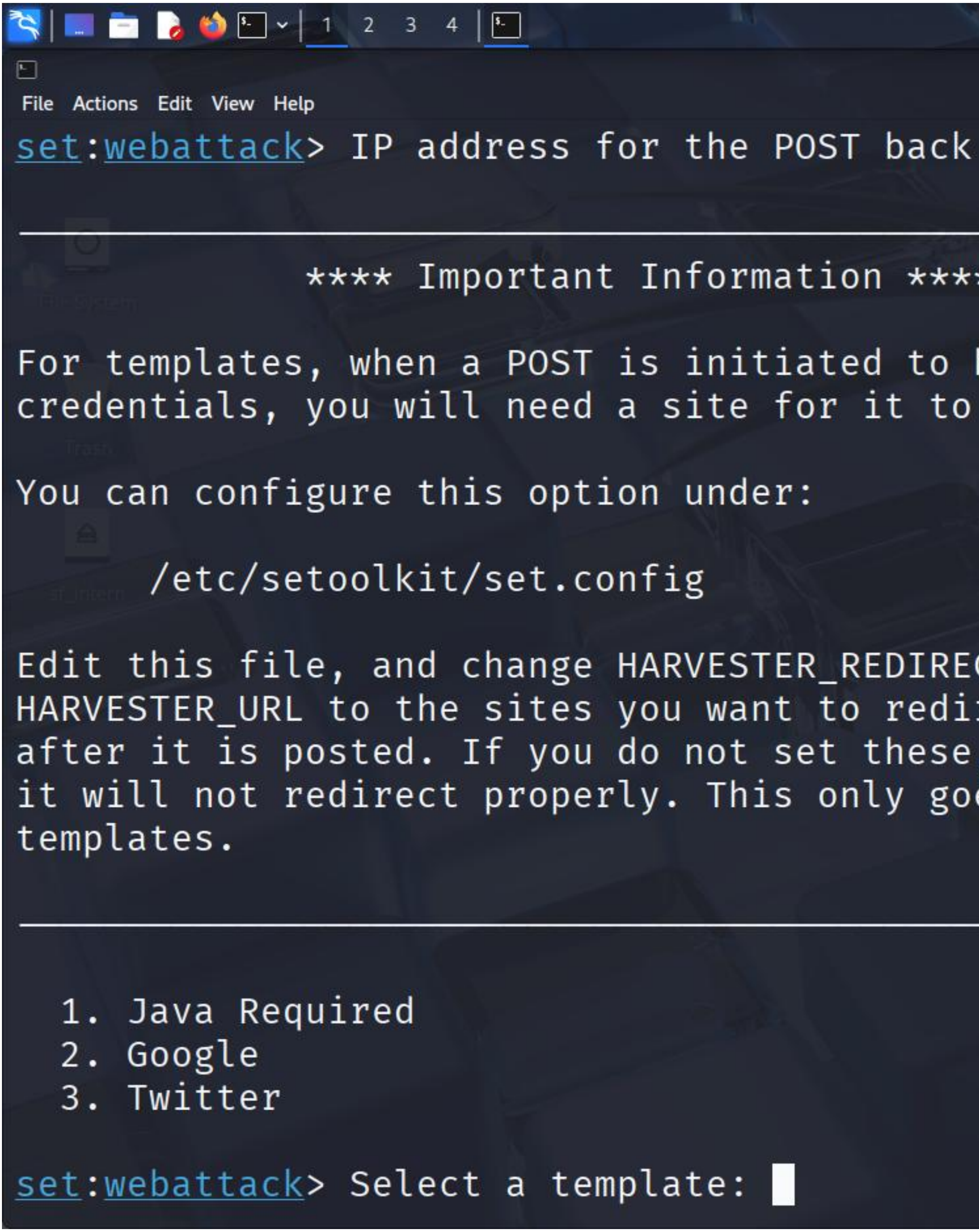
```
The TabNabbing method will wait for a user 
erent.

The Web-Jacking Attack method was introduce
to make the highlighted URL link to appear 
ith the malicious link. You can edit the li

The Multi-Attack method will add a combinat
ilize the Java Applet, Metasploit Browser, 
ful.

The HTA Attack method will allow you to clo
can be used for Windows-based PowerShell ex

   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>
```



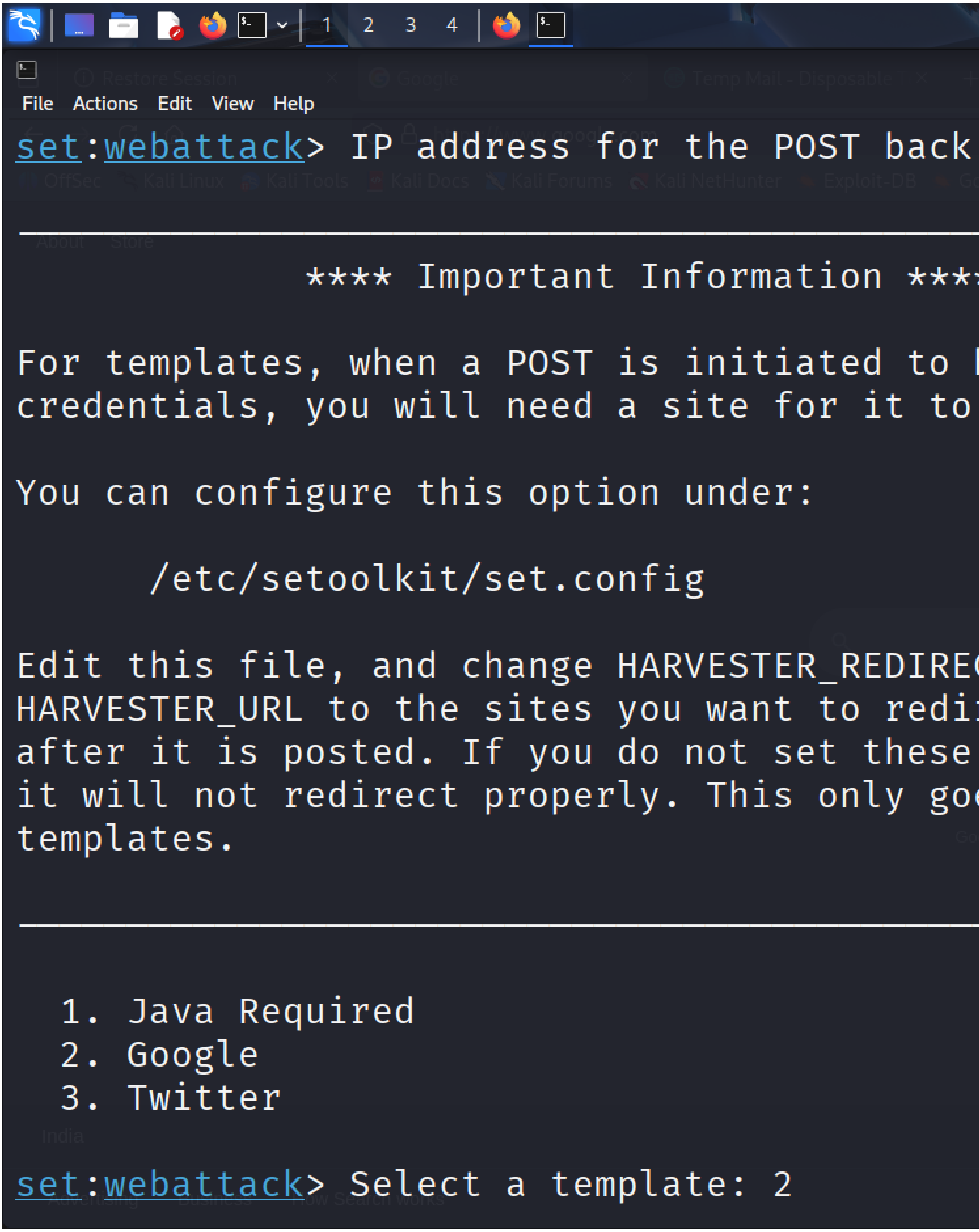
```
    6) Multi-Attack Web Method
    7) HTA Attack Method

   99) Return to Main Menu

set:webattack>3

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

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

 The third method allows you to import your
 should only have an index.html when using t
 functionality.

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

   99) Return to Webattack Menu

set:webattack>
```



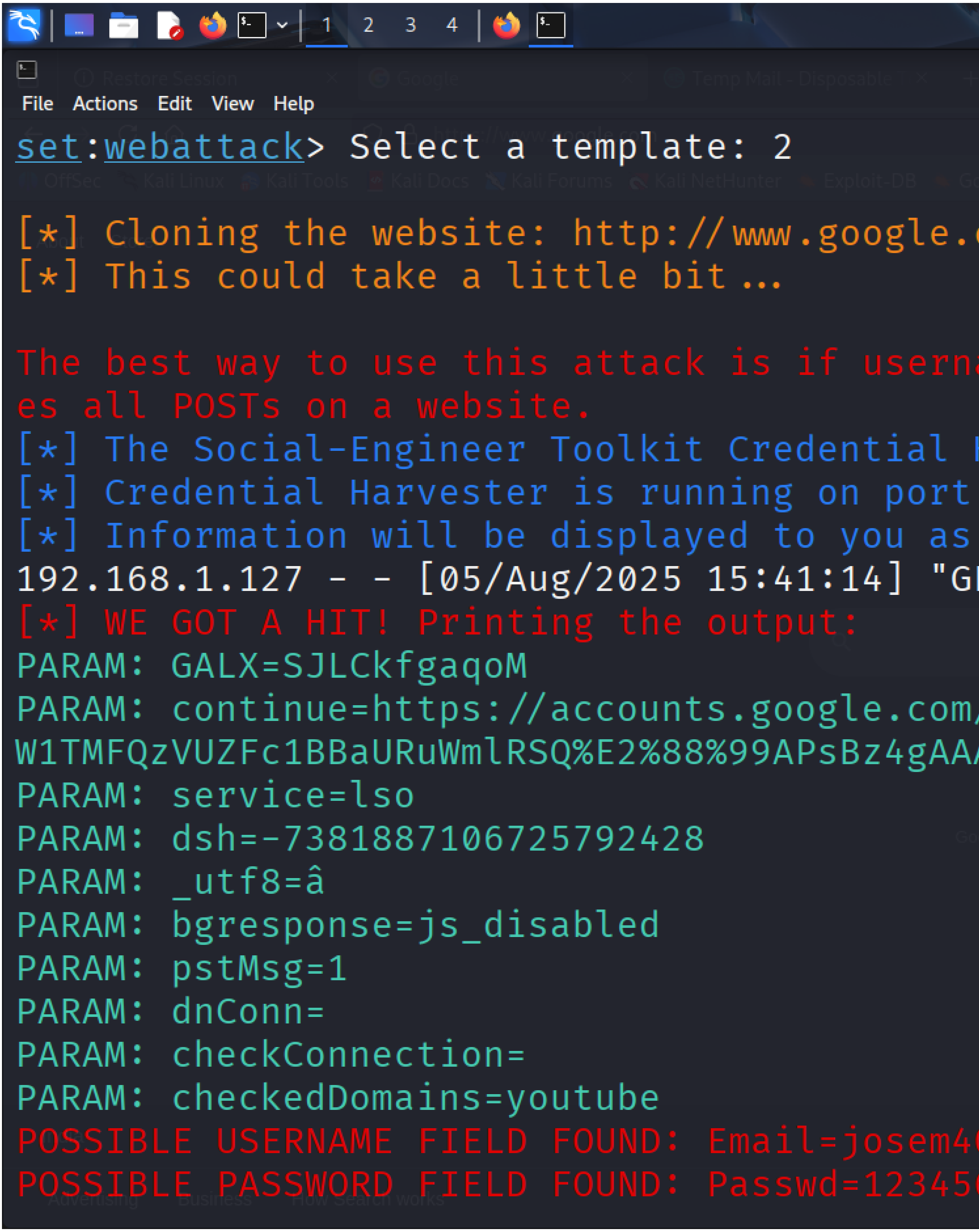
```
  99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to 
[-] to harvest credentials or parameters fr


───────────────────────────────────────────
─── * IMPORTANT * READ THIS BEFORE ENTERING

The way that this works is by cloning a sit
rewrite. If the POST fields are not usual m
could fail. If it does, you can always save
be standard forms and use the "IMPORT" feat
important:

If you are using an EXTERNAL IP ADDRESS, yo
IP address below, not your NAT address. Add
basic networking concepts, and you have a p
need to do port forwarding to your NAT IP a
address. A browser doesn’t know how to comm
address, so if you don't specify an externa
this from an external perspective, it will 
this is how networking works.

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



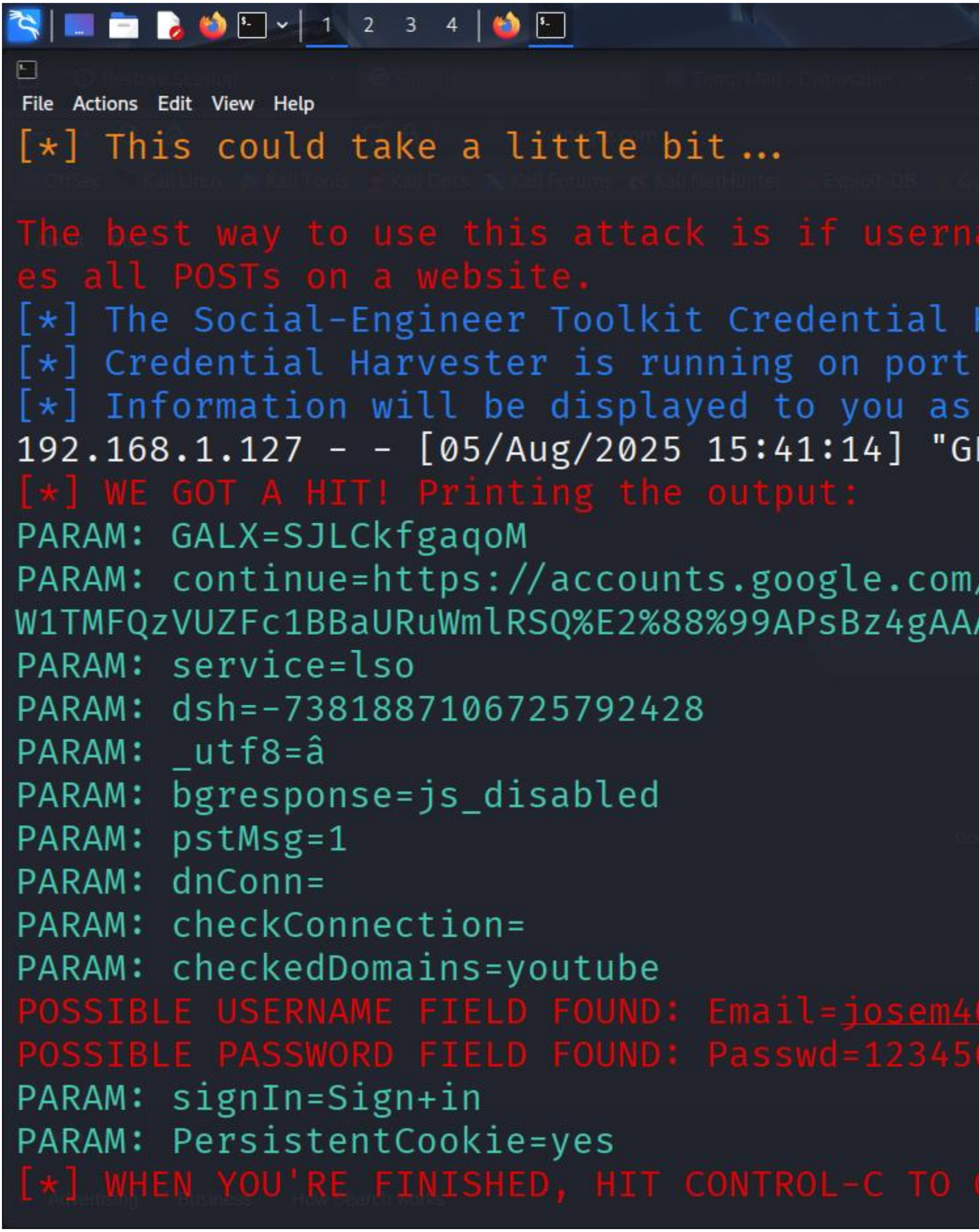
```
set:webattack> IP address for the POST back

                    **** 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_REDIRE
HARVESTER_URL to the sites you want to redi
after it is posted. If you do not set these
it will not redirect properly. This only go
templates.


  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template: 
```



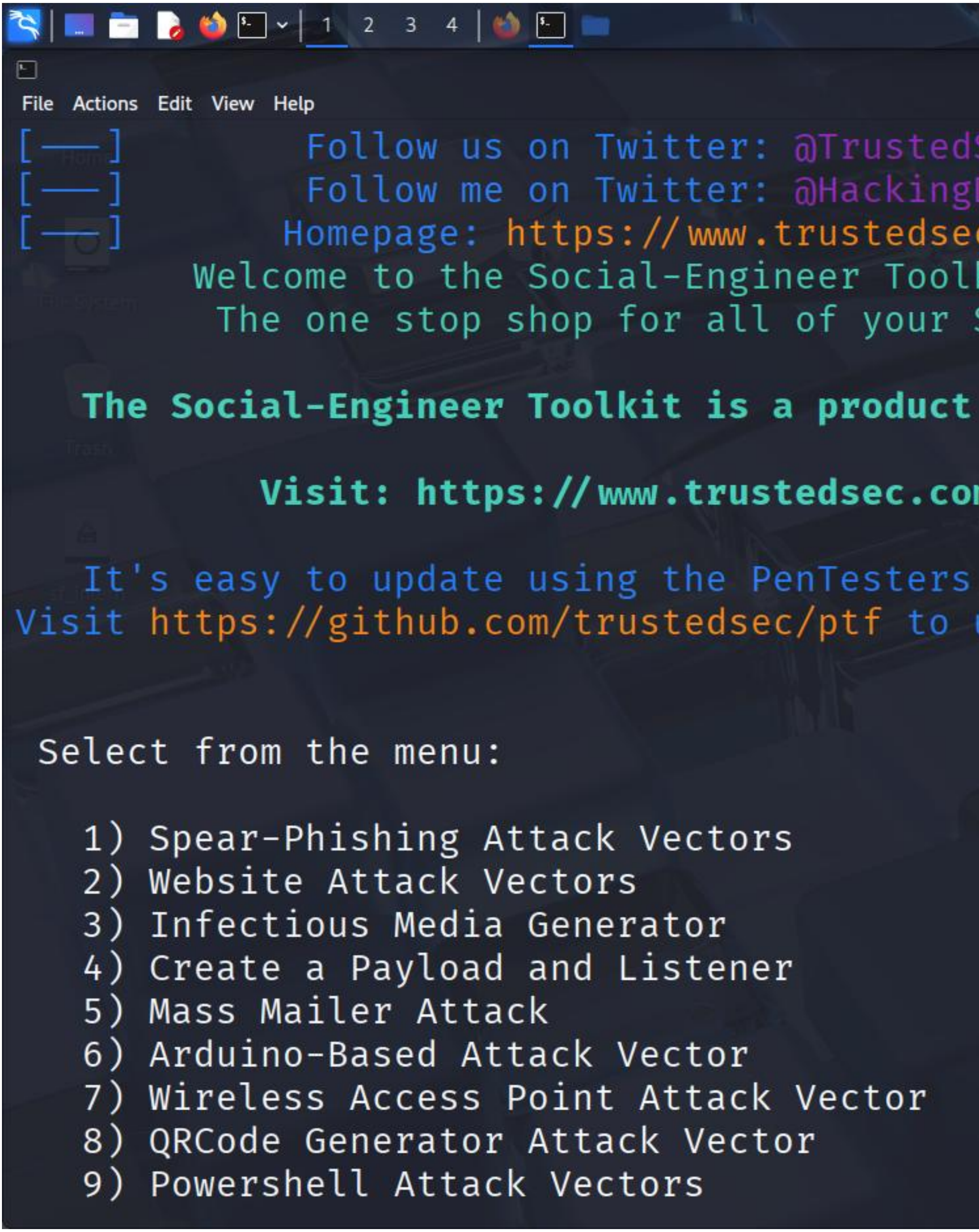
```
set:webattack> IP address for the POST back

______________________________________________________________

                 **** Important Information ****

For templates, when a POST is initiated to h
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_REDIREC
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 goe
templates.

______________________________________________________________


  1. Java Required
  2. Google
  3. Twitter

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



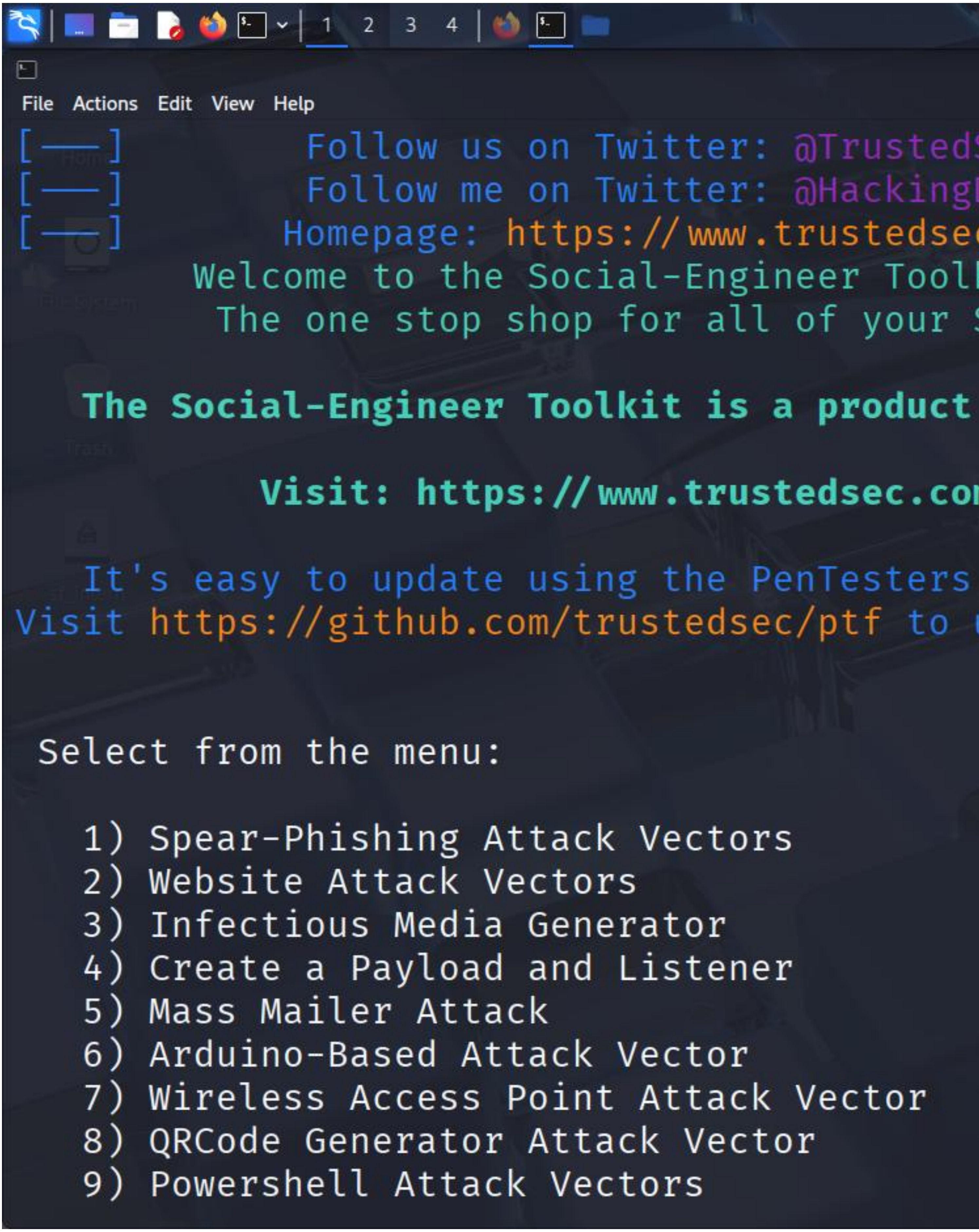
```
set:webattack> Select a template: 2

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

The best way to use this attack is if userna
es all POSTs on a website.
[*] The Social-Engineer Toolkit Credential H
[*] Credential Harvester is running on port
[*] Information will be displayed to you as
192.168.1.127 - - [05/Aug/2025 15:41:14] "GE
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/
W1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAA
PARAM: service=lso
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
```



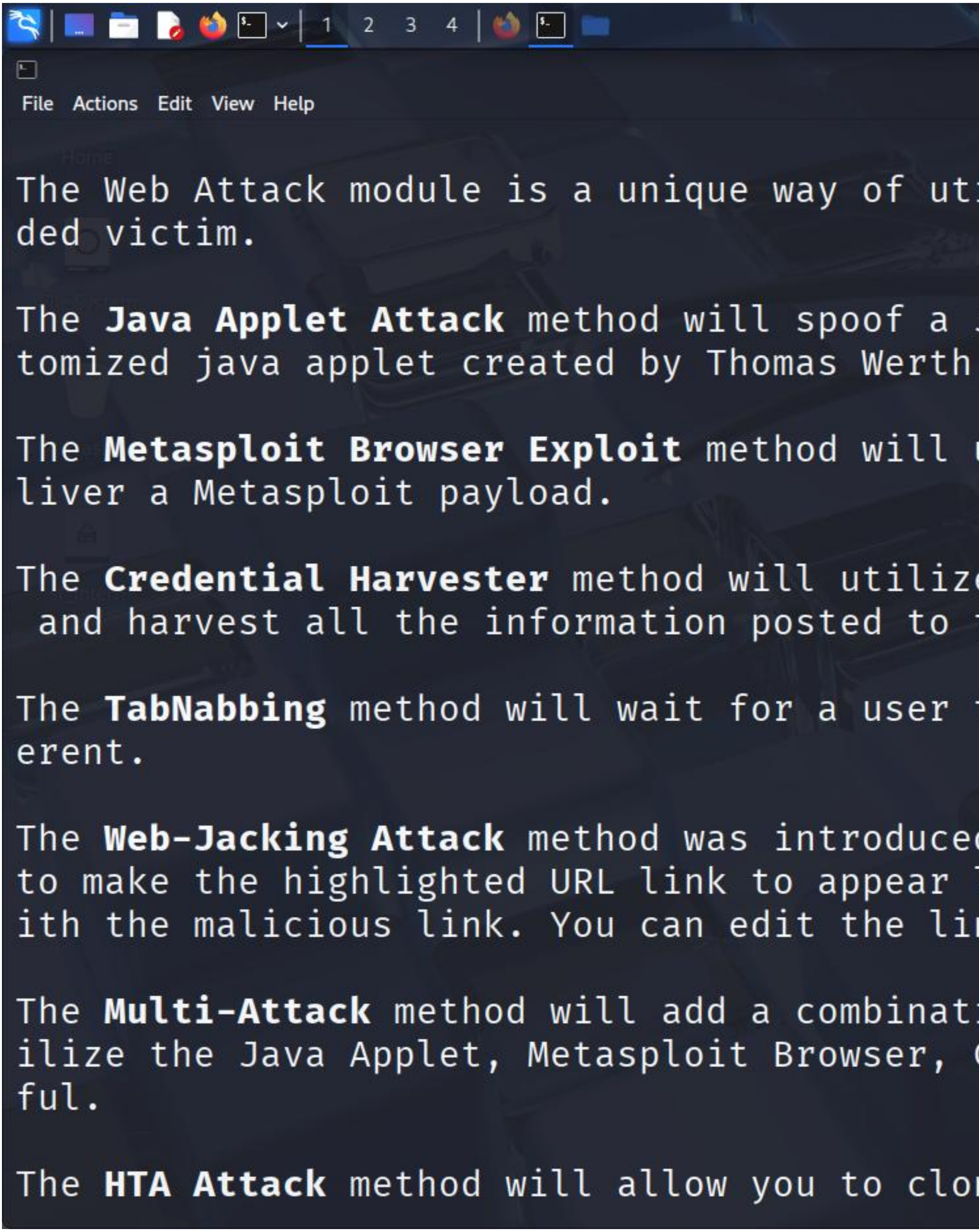
```
[*] This could take a little bit...

The best way to use this attack is if userna
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
W1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAA
PARAM: service=lso
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
```



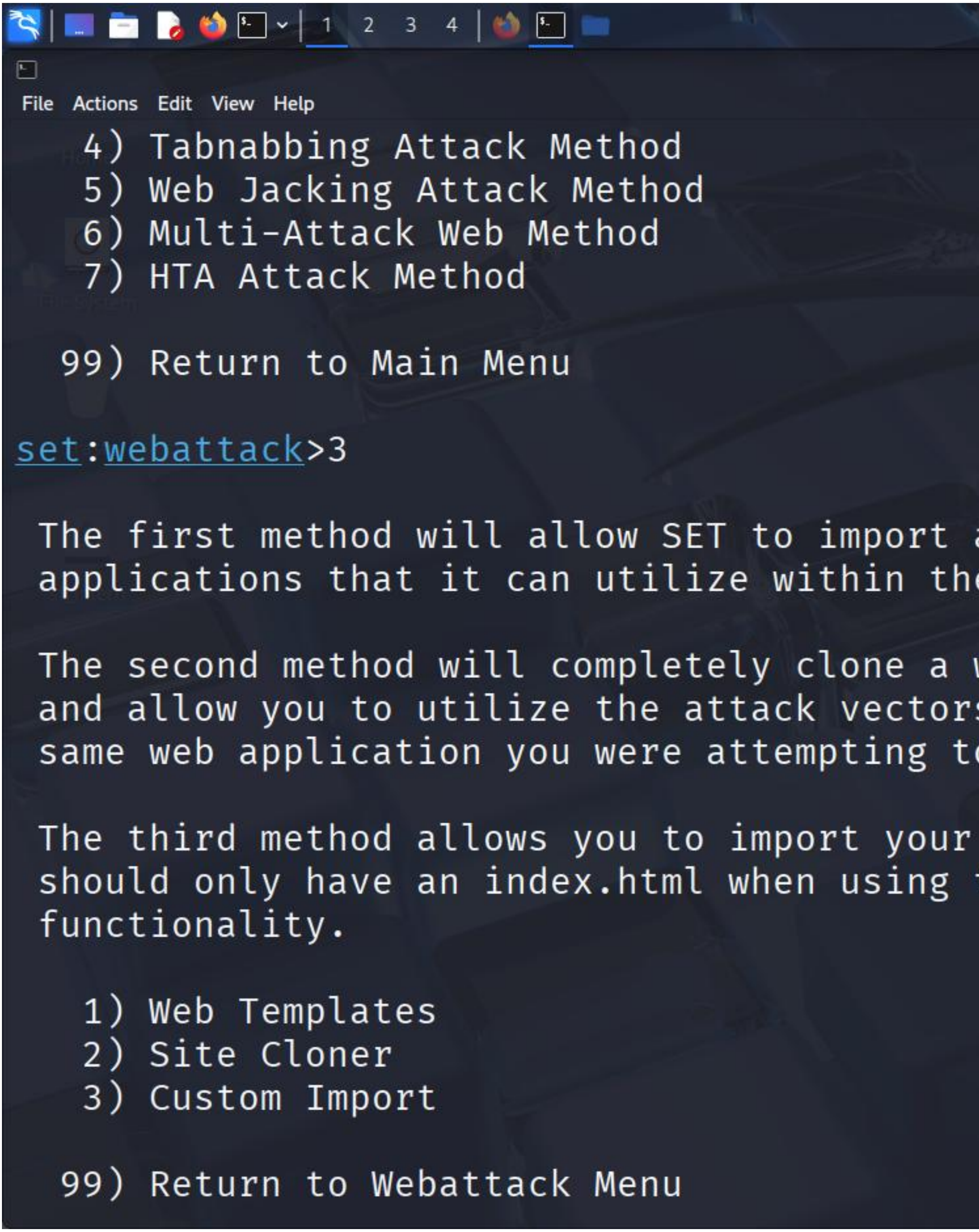
```
[---]           Follow us on Twitter: @Trusted
[---]           Follow me on Twitter: @Hacking
[---]          Homepage: https://www.trustedse
          Welcome to the Social-Engineer Tool
           The one stop shop for all of your 

   The Social-Engineer Toolkit is a product

           Visit: https://www.trustedsec.co

   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
```



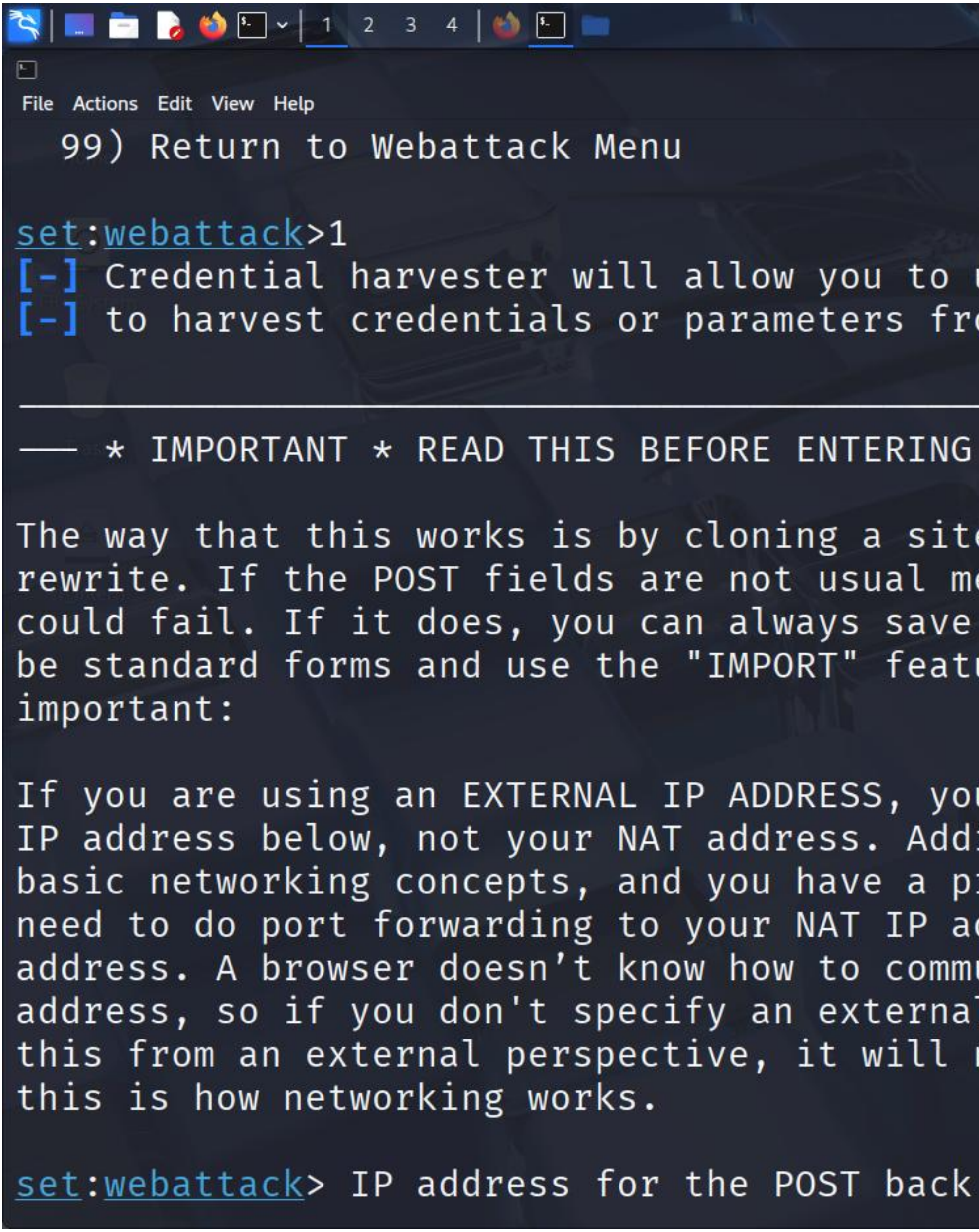
```
[---]        Follow us on Twitter: @TrustedS
[---]        Follow me on Twitter: @HackingD
[---]       Homepage: https://www.trustedsec
          Welcome to the Social-Engineer Toolk
           The one stop shop for all of your S

   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 u


 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
```



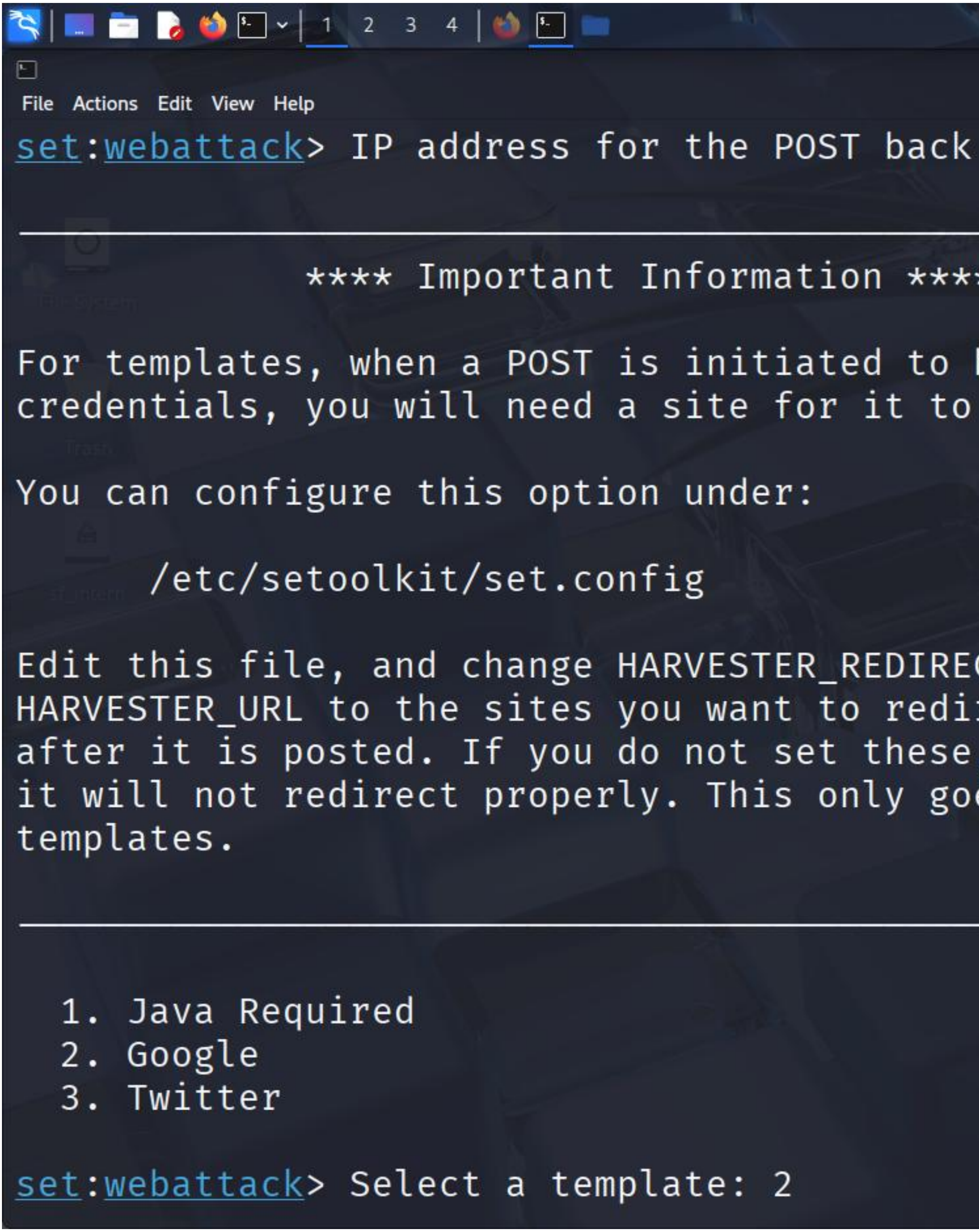
```
The Web Attack module is a unique way of uti
ded victim.

The Java Applet Attack method will spoof a
tomized java applet created by Thomas Werth

The Metasploit Browser Exploit method will
liver a Metasploit payload.

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

The TabNabbing method will wait for a user
erent.

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

The Multi-Attack method will add a combinati
ilize the Java Applet, Metasploit Browser,
ful.

The HTA Attack method will allow you to clon
```



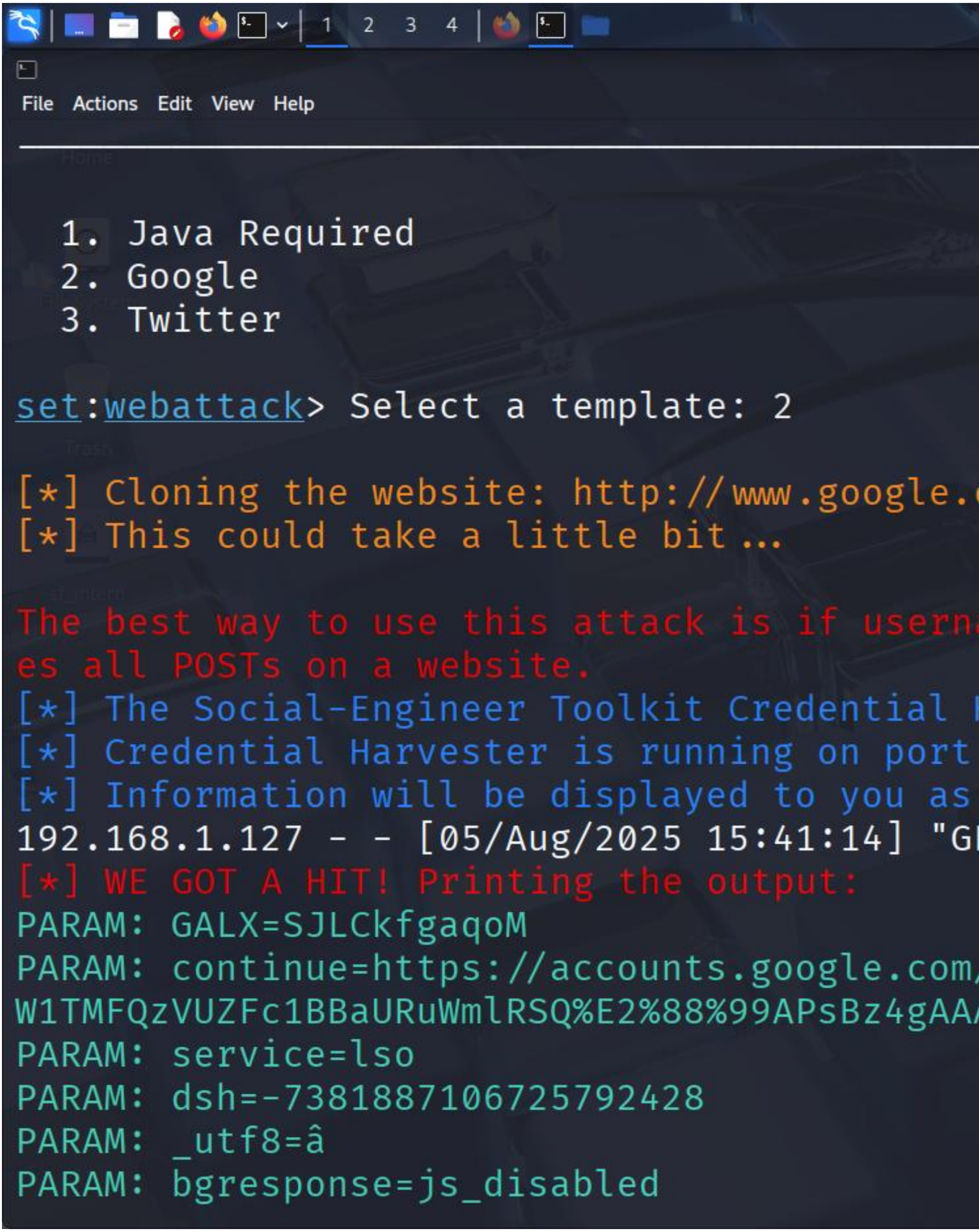
```
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

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

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

 The third method allows you to import your
 should only have an index.html when using t
 functionality.

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

  99) Return to Webattack Menu
```



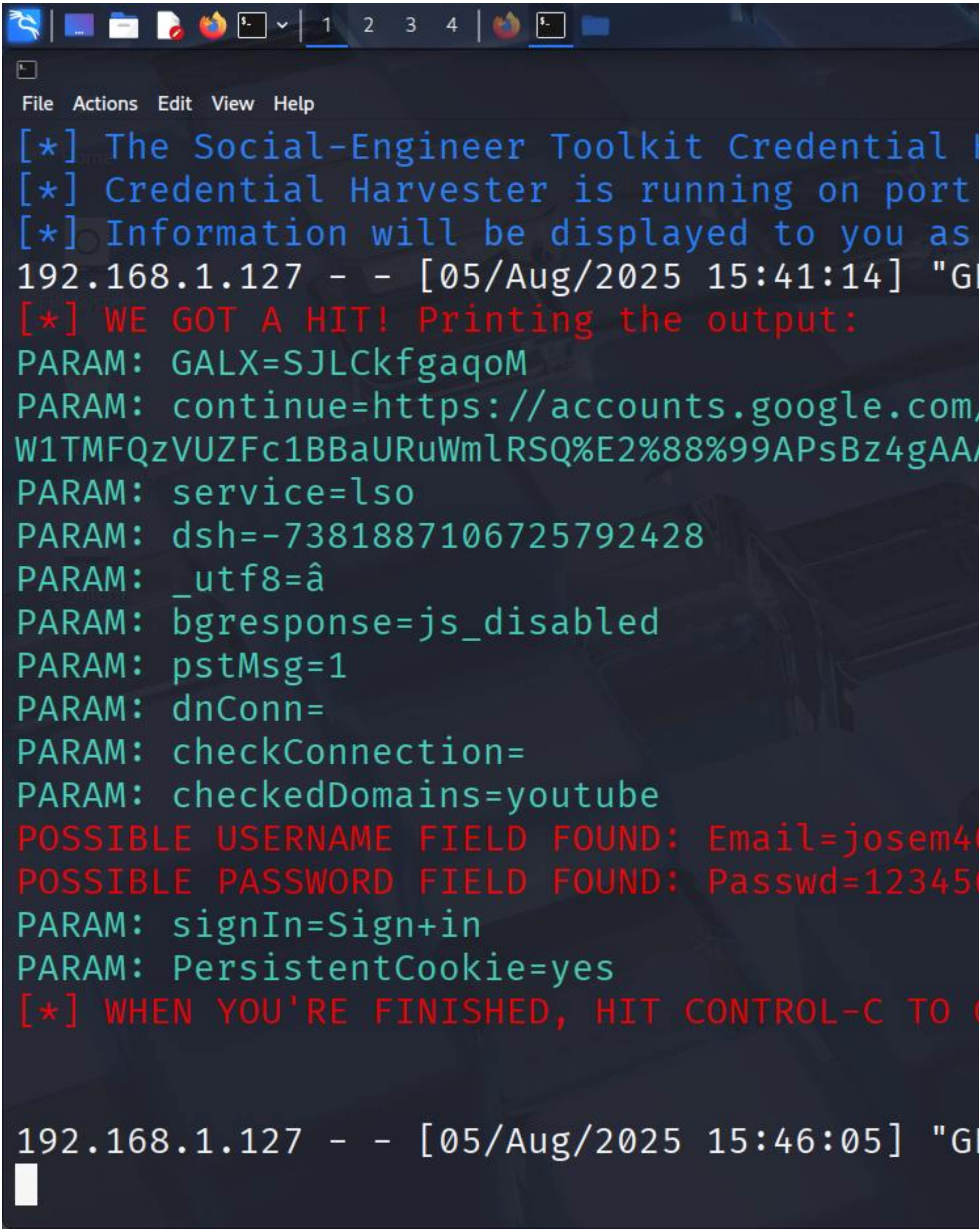
```
  99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to
[-] to harvest credentials or parameters fr

────────────────────────────────────────────────
─── * IMPORTANT * READ THIS BEFORE ENTERING

The way that this works is by cloning a sit
rewrite. If the POST fields are not usual m
could fail. If it does, you can always save
be standard forms and use the "IMPORT" feat
important:

If you are using an EXTERNAL IP ADDRESS, yo
IP address below, not your NAT address. Add
basic networking concepts, and you have a p
need to do port forwarding to your NAT IP a
address. A browser doesn’t know how to comm
address, so if you don't specify an externa
this from an external perspective, it will
this is how networking works.

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



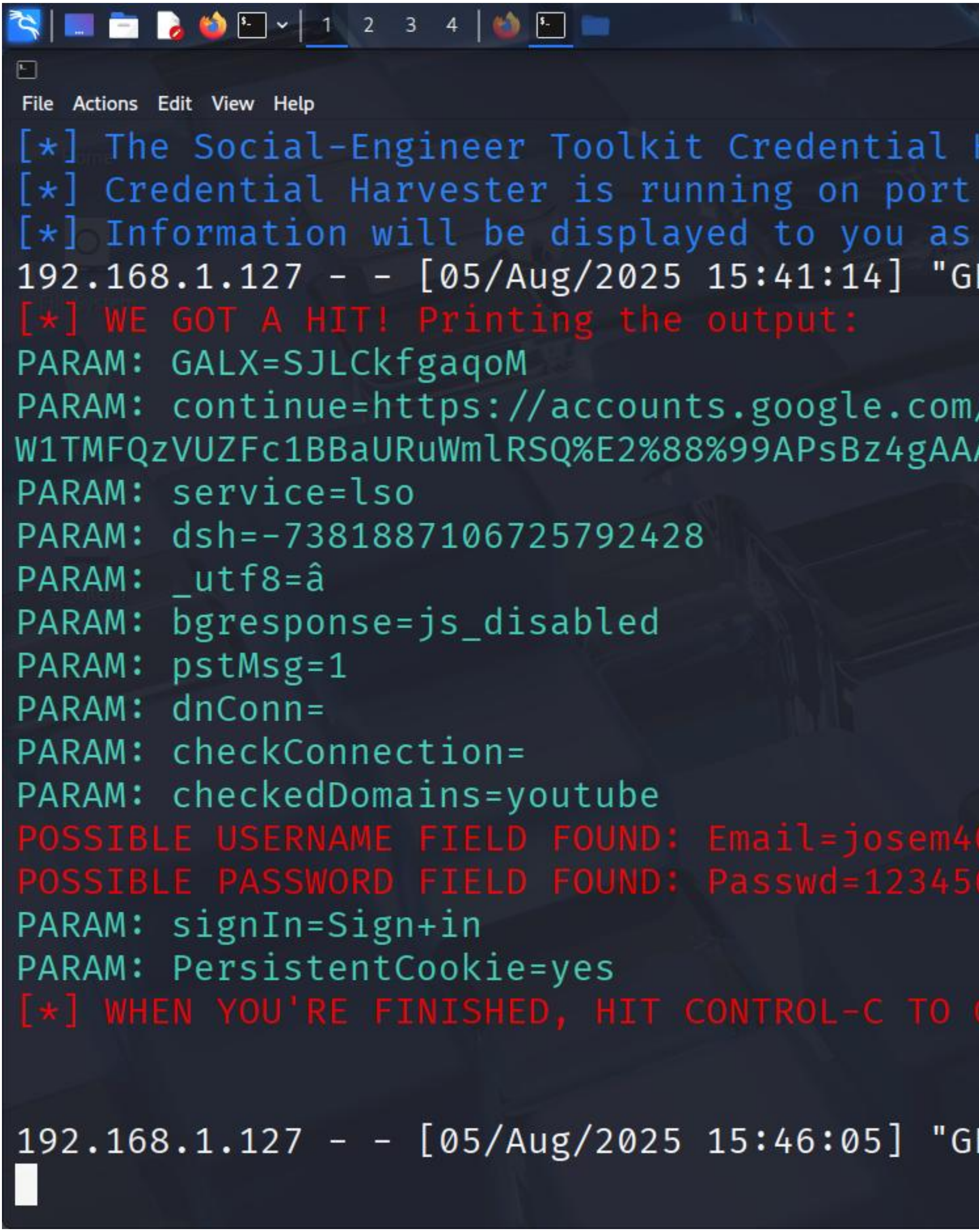
```
set:webattack> IP address for the POST back

                 **** 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_REDIRE
HARVESTER_URL to the sites you want to redi
after it is posted. If you do not set these
it will not redirect properly. This only goe
templates.


  1. Java Required
  2. Google
  3. Twitter

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



```
  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 userna
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
W1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAA
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
```



```
[*] 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
W1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAA
PARAM: service=lso
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 


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



```
[*] 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
W1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAA
PARAM: service=lso
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 


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