CYSE 450 Ethical Hacking and Penetration Testing

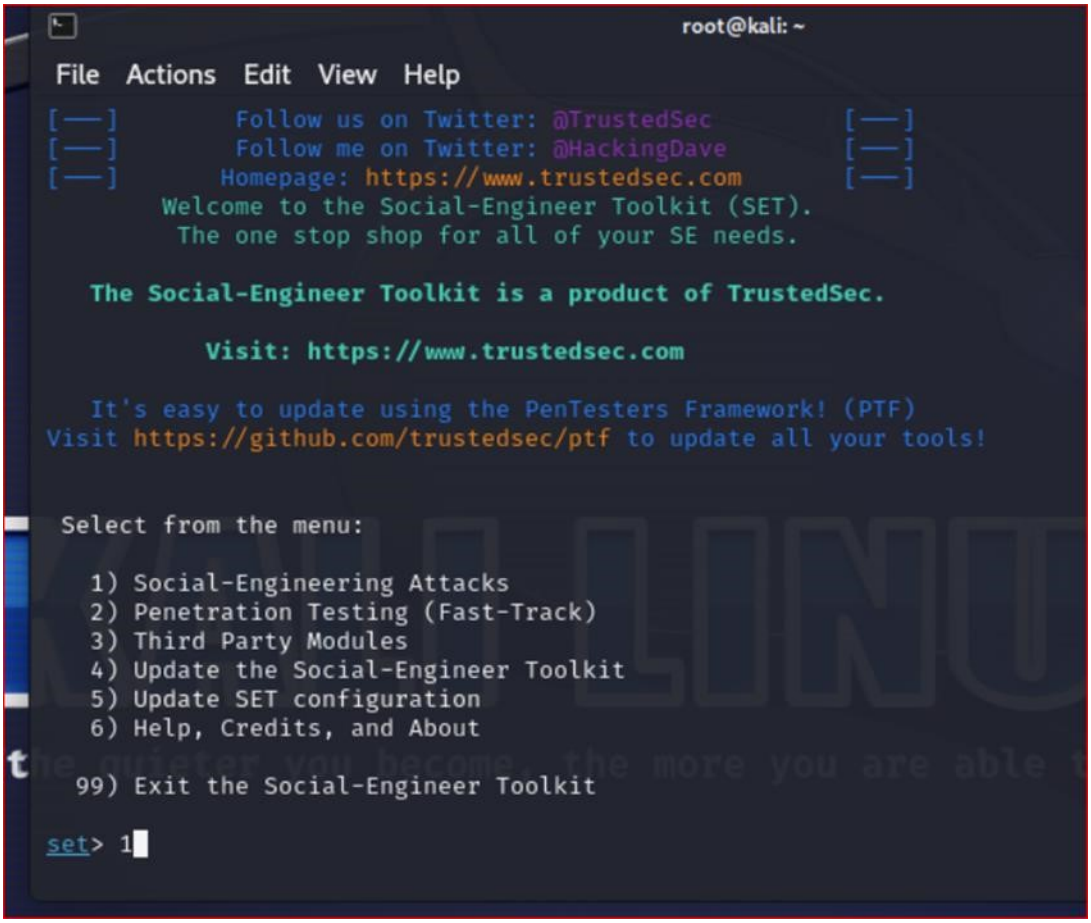
Assignment 10.1 - Using the Social Engineering Toolkit (set) to Harvest Credentials

(50 Points)

Complete all the steps and **submit the screenshot for the contents of the XML file** with login credentials for**, johnsmith@test.com**.

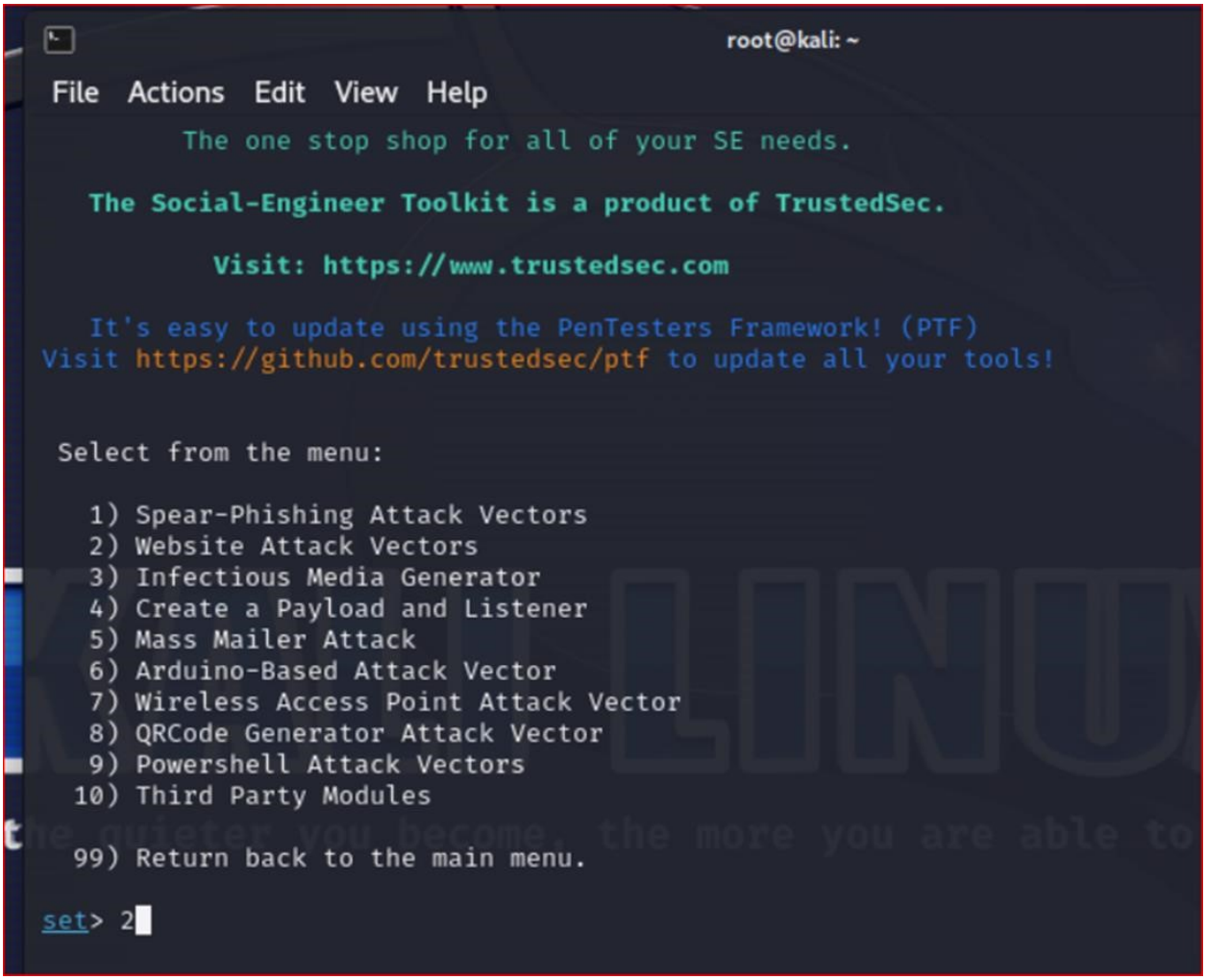
1. Open the **root** terminal in Kali.
2. Type the command **setoolkit** to open the social engineering toolkit.
3. On the SET main page, select **1.) Social Engineering Attack** menu item by pressing **1**, followed by pressing the "Enter" key.

4.



On the social Engineering Attacks page, select the **2.) Website Attack Vectors** menu item by pressing **2**, followed by pressing the "**Enter**" key.

5.



On the Website Attack Vectors page, select **3.) Credential Harvester Attack** Method menu item by pressing **3**, followed by pressing the “Enter” key.

6.

```
root@kali: ~
File  Actions  Edit  View  Help
The TabNabbing method will wait for a user to move to a different tab, then refresh the page t
thing different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes ifra
lacements to make the highlighted URL link to appear legitimate however when clicked a window
p then is replaced with the malicious link. You can edit the link replacement settings in the
nfig if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For exa
ou can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at onc
ee which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through
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>3
```

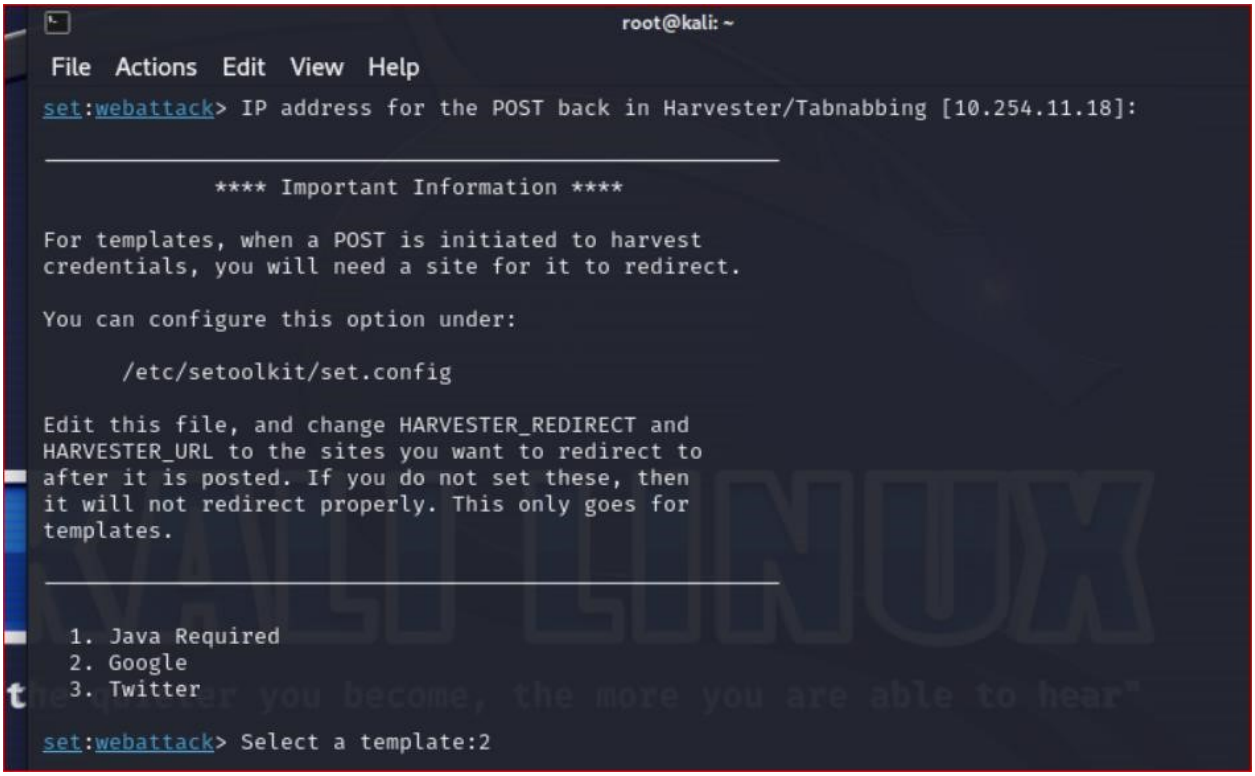
On the Credential Harvester Attack Method page, select **1.) Web Templates** menu item by pressing **1**, followed by pressing the “Enter” key.

7.

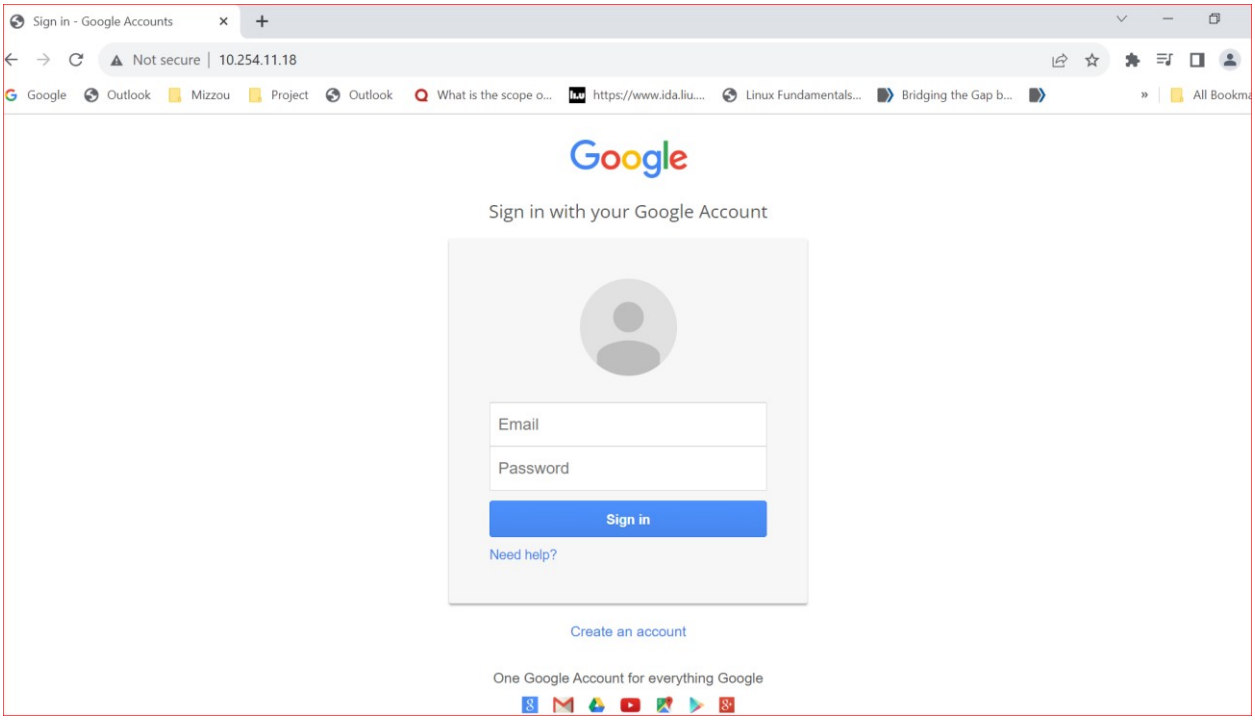
```
root@kali: ~
File  Actions  Edit  View  Help

  99) Return to Webattack Menu

set:webattack>1
[-] 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 repor

──────────────────────────────────────────────────────────────────────────────
── * 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 [10.254.11.18]:
```

7. When prompted for an IP address for the POST back, just hit “Enter” key to keep your kali machine IP address as the default one.

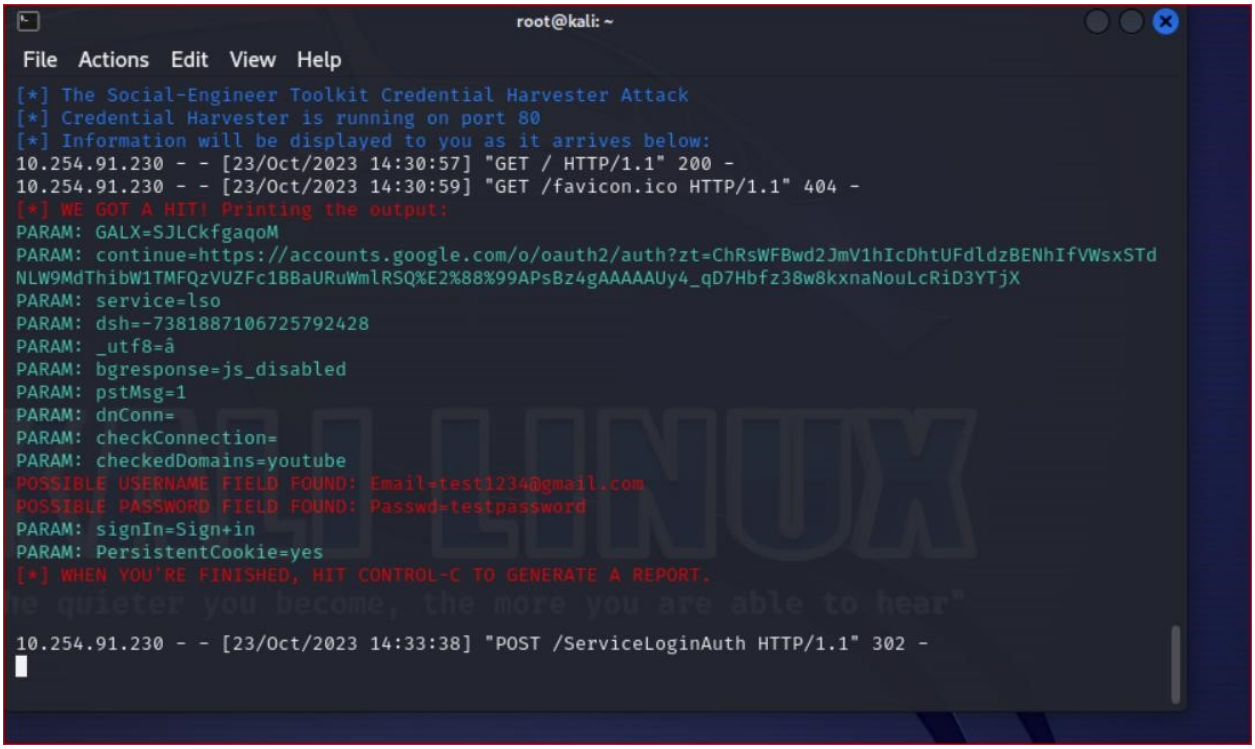
8. On the Select a template prompt, select the **2. Google** menu item



9. Open a tab in the browser of your Windows VM or your local computer.
10. Type the address of the Kali Linux in the address bar and press “Enter”



11. In the email field, type any fake email for example**,** **johnsmith@test.com** and for password, type **letMEin@2023** and press “sign in”
12. Go back to Kali root terminal, where it was listening for harvesting the credentials. You should be able to see the login and password now like, as shown in the following screenshot:



13. Press **CONTROL+c** key to copy.
14. Type **99**, when prompted to return.
15. Again, keep typing 99 until you exit

```
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> 99

Thank you for shopping with the Social-Engineer Toolkit.

Hack the Gibson ... and remember ... hugs are worth more than handshakes.
```

16. Open a new **root** terminal in Kali and type the following to view your report.

```
┌──(root㉿kali)-[~]
└─# cd /root/.set/reports

┌──(root㉿kali)-[~/.set/reports]
└─# ls
'2023-11-04 16:12:52.278295.xml'   files
```

17. To view/ generate the report in the XML file (the report generated after completing the social engineering attack), use **cat** command and type only 2023, then hit the tab key (to fill the rest of the characters in the file name). Highlight the login and password in the

report.

```
root@jgibs016: ~/.set/reports
File  Actions  Edit  View  Help
 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> 99


 Thank you for shopping with the Social-Engineer Toolkit.

 Hack the Gibson ... and remember ... hugs are worth more than handshakes.


┌──(root㉿jgibs016)-[~]
└─# cd /root/.set/reports

┌──(root㉿jgibs016)-[~/.set/reports]
└─# ls
'2023-11-20 22:16:03.427657.xml'   files

┌──(root㉿jgibs016)-[~/.set/reports]
└─# cat 2023-11-20\ 22:16:03.427657.xml
<?xml version="1.0" encoding='UTF-8'?>
<harvester>
   URL=http://www.google.com
   <url>      <param>GALX=SJLCkfgaqoM</param>
      <param>continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThi
bW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX</param>
      <param>service=lso</param>
      <param>dsh=-7381887106725792428</param>
      <param>_utf8=â</param>
      <param>bgresponse=js_disabled</param>
      <param>pstMsg=1</param>
      <param>dnConn=</param>
      <param>checkConnection=</param>
      <param>checkedDomains=youtube</param>
      <param>Email=johnsmith@test.com</param>
      <param>Passwd=letMEin@20223</param>
      <param>signIn=Sign+in</param>
      <param>PersistentCookie=yes</param>
   </url>
</harvester>

┌──(root㉿jgibs016)-[~/.set/reports]
└─#
```