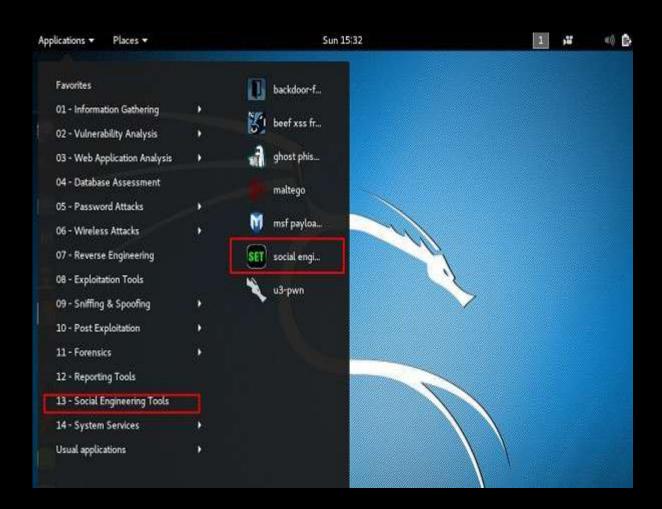
Social Engineering Toolkit Usage

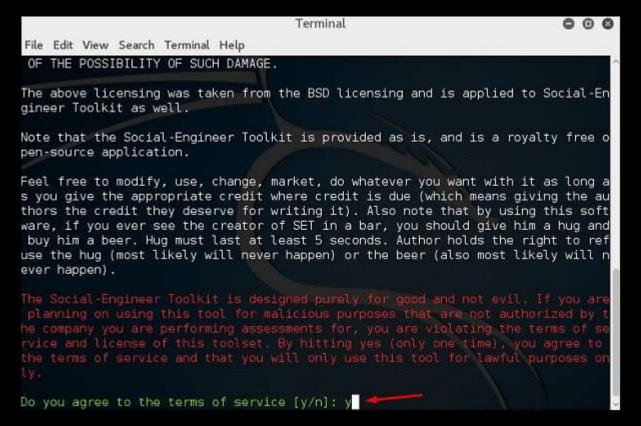
The **Social-Engineer Toolkit** (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them to the attack vectors.

Let's learn how to use the Social Engineer Toolkit.

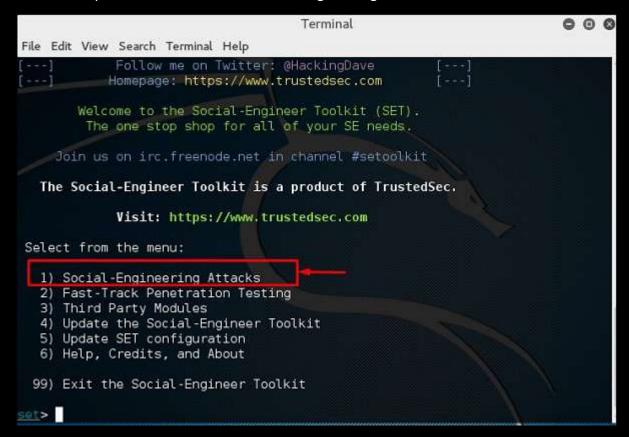
Step 1 – To open SET, go to Applications \rightarrow Social Engineering Tools \rightarrow Click "SET" Social Engineering Tool.



Step 2 – It will ask if you agree with the terms of usage. Type "y" as shown in the following screenshot.



Step 3 – Most of the menus shown in the following screenshot are self-explained and among them the most important is the number 1 "Social Engineering Attacks".



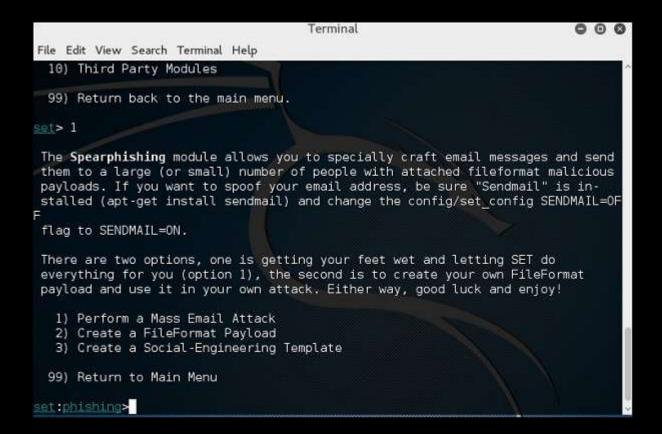
Step 4 – Type "1" \rightarrow Enter. A submenu will open. If you press the **Enter** button again, you will see the explanations for each submenu.

The Spear-phishing module allows you to specially craft email messages and send them to your targeted victims with attached **FileFormatmalicious** payloads. For example, sending malicious PDF document which if the victim opens, it will compromise the system. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set config SENDMAIL=OFF flag to SENDMAIL=ON.

There are two options for the spear phishing attack –

- •Perform a Mass Email Attack
- •Create a FileFormat Payload and a Social-Engineering Template

The first one is letting SET do everything for you (option 1), the second one is to create your own FileFormat payload and use it in your own attack.



Type "99" to go back to the main menu and then type "2" to go to "The web attack vectors".

The web attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim. This module is used by performing phishing attacks against the victim if they click the link. There is a wide variety of attacks that can occur once they click a link.



Type "99" to return to the main menu and then type "3".

The infectious USB/CD/DVD module will create an autorun.inf file and a Metasploit payload. The payload and autorun file is burned or copied on a USB. When DVD/USB/CD is inserted in the victim's machine, it will trigger an autorun feature (if autorun is enabled) and hopefully compromise the system. You can pick the attack vector you wish to use: fileformat bugs or a straight executable.

Following are the options for Infectious Media Generator.

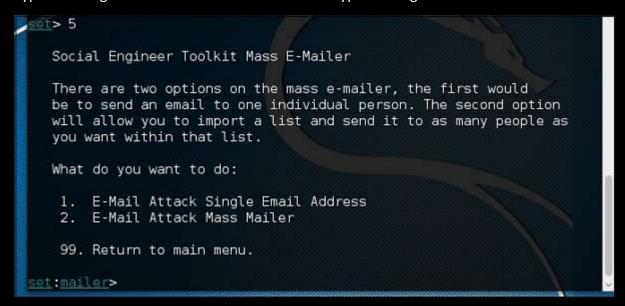


Type "99" to go back to the main menu. Then, type "4" to go to "The web attack vectors".

The create payload and listener is a simple way to create a Metasploit payload. It will export the exe file for you and generate a listener. You would need to convince the victim to download the exe file and execute it to get the shell.



Type "99" to go back to the main menu and then type "5" to go to "The web attack vectors".



The mass mailer attack will allow you to send multiple emails to victims and customize the messages. There are two options on the mass e-mailer; the first is to send an email to a single email address. The second option allows you to import a list that has all recipient emails and it will send your message to as many people as you want within that list.

- •E-Mail Attack Single Email Address
- •E-Mail Attack Mass Mailer

Type "99" to go back to the main menu and then type "9" to go to "Powershell Attack Vector".

set> 9

The **Powershell Attack Vector** module allows you to create PowerShell specific att acks. These attacks will allow you to use PowerShell which is available by defau it in all operating systems Windows Vista and above. PowerShell provides a fruit ful landscape for deploying payloads and performing functions that do not get triggered by preventative technologies.

- 1) Powershell Alphanumeric Shellcode Injector
- 2) Powershell Reverse Shell
- 3) Powershell Bind Shell
- 4) Powershell Dump SAM Database
- 99) Return to Main Menu

The Powershell Attack Vector module allows you to create PowerShell specific attacks. These attacks allow you to use PowerShell, which is available by default in all operating systems Windows Vista and above. PowerShell provides a fruitful landscape for deploying payloads and performing functions that do not get triggered by preventive technologies.

- •Powershell Alphanumeric Shellcode Injector
- Powershell Reverse Shell
- Powershell Bind Shell
- Powershell Dump SAM Database