

Kali Linux - Social Engineering

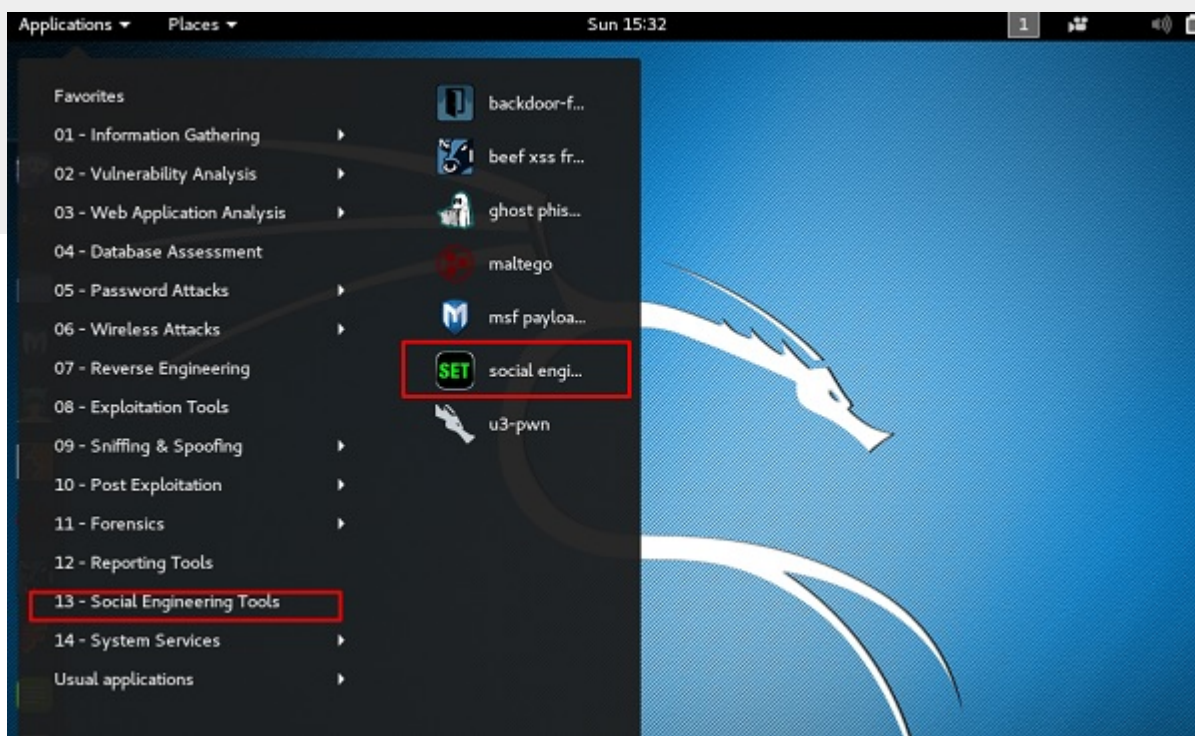
In this chapter, we will learn about the social engineering tools used in Kali Linux.

Social Engineering Toolkit Usage

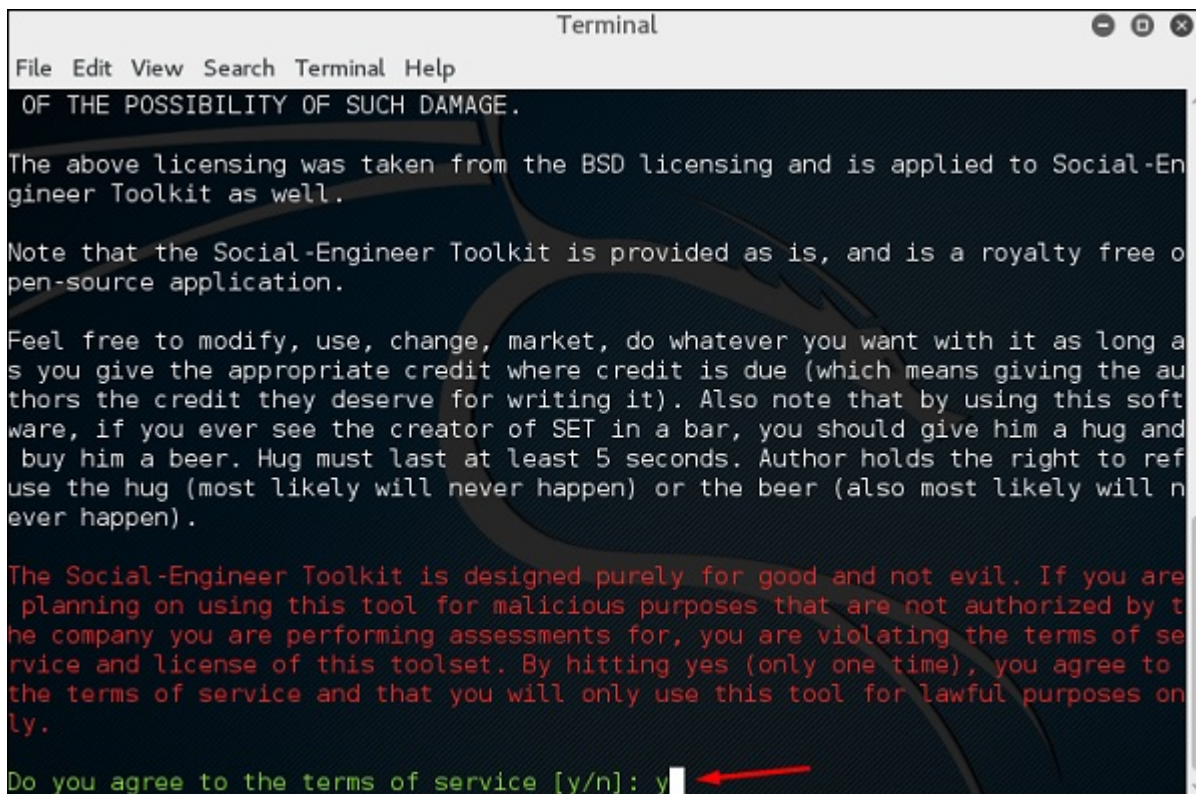
The **Social-Engineer Toolkit** (SET) is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of time. These kind of tools use human behaviors to trick them to the attack vectors.

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

Step 1 – To open SET, go to Applications → Social Engineering Tools → 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.



```
Terminal
File Edit View Search Terminal Help
OF THE POSSIBILITY OF SUCH DAMAGE.

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

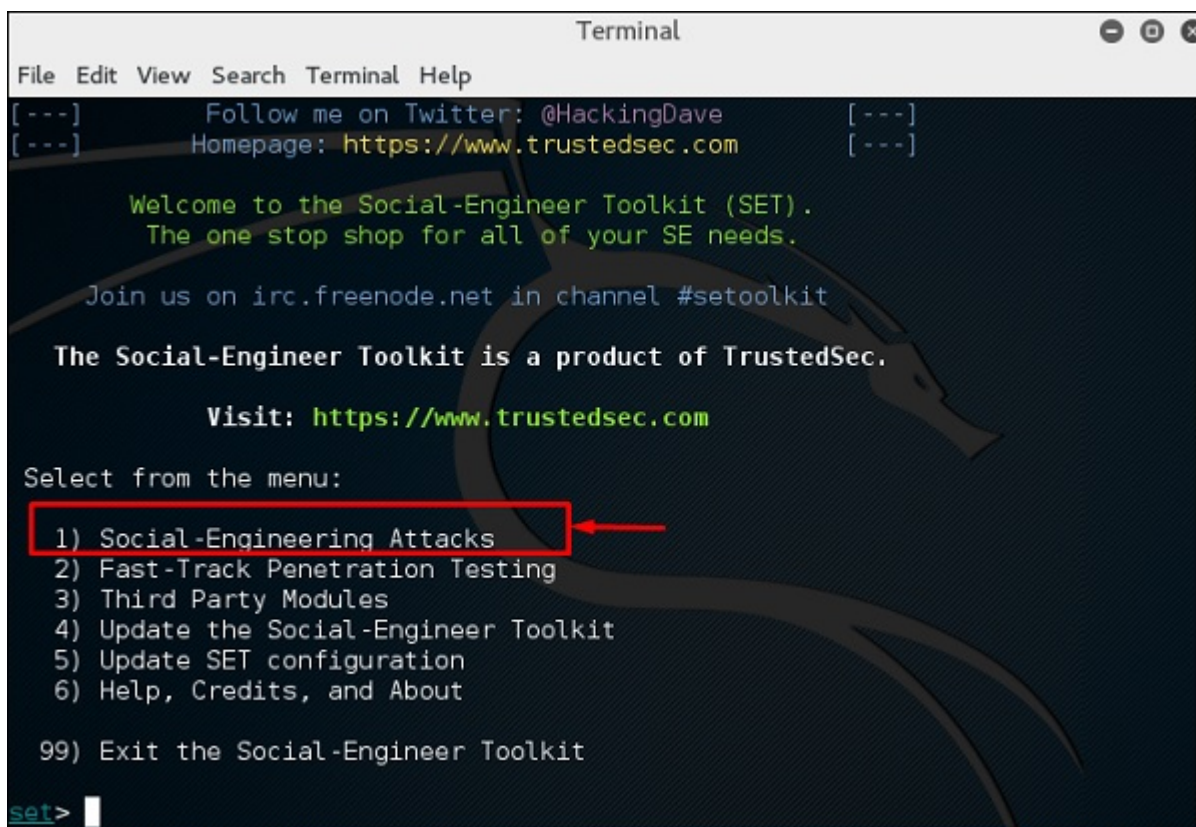
Note that the Social-Engineer Toolkit is provided as is, and is a royalty free open-source application.

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 give him a hug and buy him a beer. Hug must last at least 5 seconds. Author holds the right to refuse the hug (most likely will never happen) or the beer (also most likely will never happen).

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
```

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”.



```
Terminal
File Edit View Search Terminal Help
[---] 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>
```

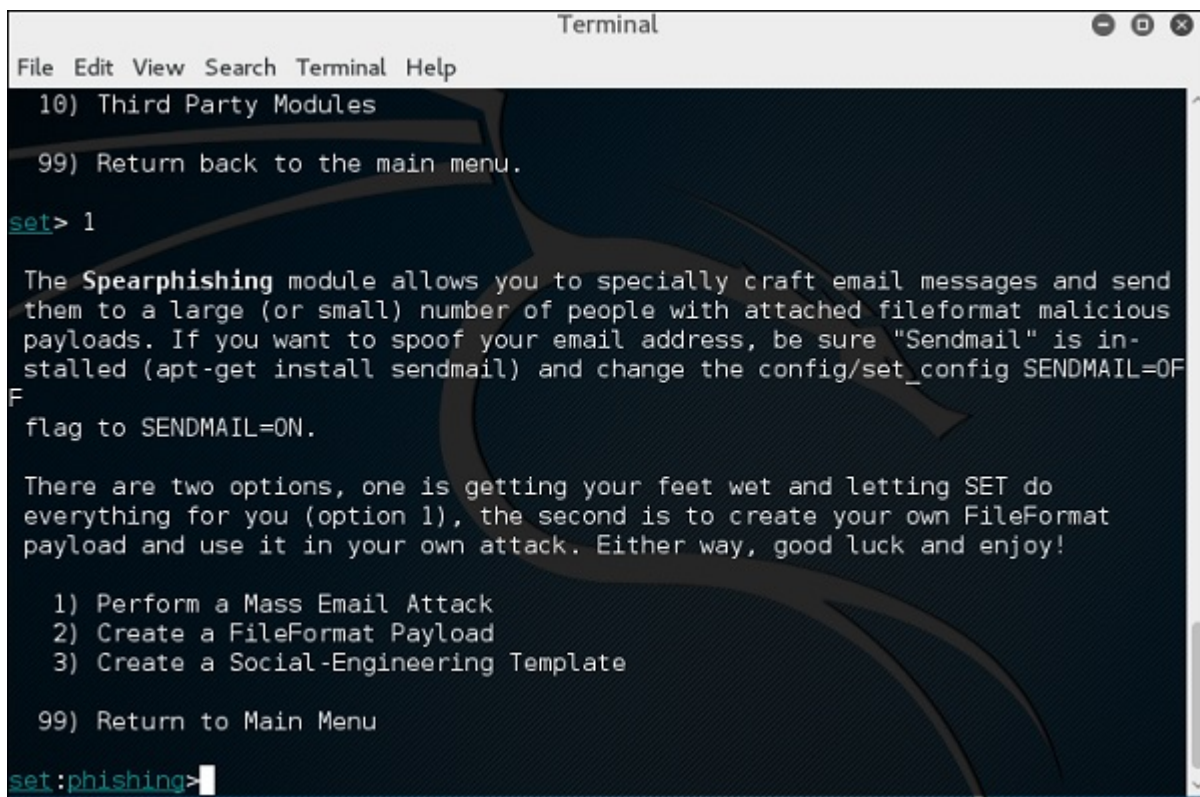
Step 4 – Type “1” → Enter. A submenu will open. If you press the **Enter** button again, you will see the explanations for each submenu.

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.



```
Terminal
File Edit View Search Terminal Help
10) Third Party Modules
99) Return back to the main menu.
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=OF
F
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>
```

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.

```

Terminal
File Edit View Search Terminal Help
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injec
tion through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

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>

```

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.

- ☐ File-Format Exploits
- ☐ Standard Metasploit Executable

```

set> 3

The Infectious USB/CD/DVD module will create an autorun.inf file and a
Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executabl
e.

1) File-Format Exploits
2) Standard Metasploit Executable

99) Return to Main Menu

set:infectious>

```

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.


```

set> 4

1) Windows Shell Reverse_TCP          Spawn a command shell on victim and
d send back to attacker
2) Windows Reverse_TCP Meterpreter    Spawn a meterpreter shell on victi
m and send back to attacker
3) Windows Reverse_TCP VNC DLL        Spawn a VNC server on victim and s
end back to attacker
4) Windows Shell Reverse_TCP X64      Windows X64 Command Shell, Reverse
TCP Inline
5) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Wind
ows x64), Meterpreter
6) Windows Meterpreter Egress Buster  Spawn a meterpreter shell and find
a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS  Tunnel communication over HTTP usi
ng SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS    Use a hostname instead of an IP ad
dress and use Reverse Meterpreter
9) Download/Run your Own Executable   Downloads an executable and runs i
t

set:payloads>

```

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

```

set> 5

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:mailer>

```

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 attacks. These attacks will 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 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