In this homework, I choose Social Engineers and Social-Engineer Toolkit (SET) to dig because of this lab. When I do the lab to clone Chase Bank’s website, I am very interesting in the SET. This is my first time to use this tool. After I use it, I want to know more details about the tricks of Social Engineers.

Social Engineers are the people who can manipulate others to gain access to systems, unauthorized areas or confidential information. They try to get the information from authorized users which include username/password, credit card information, name and address, procedural information and the method use to discover PIN (Personal Identification Number) codes used with bank cards. According different deception method, there are two categories for Social Engineers. One is human based deceptions and the other one is computer or technology based deception.

The human approach is done through deceptions have exit for thousand years. In this method, a person is the key point. Generally, Social Engineers will interact with the users face to face or voice to voice.

The technology-based approach is Social Engineers use some software to set up some masquerading and let the users believe that they are interacting with the ‘real’ computer system. Then, the users can provide confidential information automatically.

These both approaches have the same cycle. Social Engineers usually collect authorized users’ information at the beginning. Then, they try to build some trust with the users. Next step is using deception and trickery to convince people to give them password. Finally, they use this password to get what they want1.

There are six common techniques used in Social Engineering2. The first one is direct approach. It means Social Engineers gain the information directly form the users. The second one is dumpster diving. As we know, a huge amount of information can be collected through company dumpsters, such as company phone books, organizational charts, memos, and so on. Hackers can get some useful information from these trash or junk mails. The third method is spying and eavesdropping. In this case, if the users are careless, the Social Engineers can gain the information through observing users typing keyboard, listening the conversation which involve the confidential information or find the notes where uses write down the passwords. The forth one is IT experts. In this method, some Social Engineer will pretend as a technical expert and try to help users. Then, after gaining users’ trust, get some useful information. The fifth method is the voice of authority. For example, some people pretend he is a company’s department manager. He give a call to this company’s help desk and said to them that he forget the password and need to reset right now. After the help desk give him new password, he can log in this company’s system and do what he wants to. The last one is on-line Social Engineering. This happens on the computer world. Hackers may obtain information on-line. They can pretend as the network administrator and send e-mail to the users to ask for their password. Furthermore, they may use pop-up windows which look like part of the website and request users to reenter their username and password to fix some sort of problems. Or, they can use phishing. This practice is Social Engineers attempt to obtain users’ information using spoofed e-mail addresses and URLs which include various viruses or a link to a cracker-owned Web site.

There are many security polices to prevent it happen, such as monitoring the computer, keeping confidential information in safe place or cleaning the viruses. However, I think these approaches are used after Social Engineers success to get the information. The most important thing is we need to prevent it to happen. The best way is educating the people to know all kinds of tricks from Social Engineers. The SET is this kind of tools for aimed at penetration testing around on-line Social Engineering3.

The SET was created and written by David Kennedy. It originally released in 2009 to coincide with the launch of social-engineer.org and updated on April 1st, 2014. The SET is an open-source Python-driven tool. There are three main functions in SET. Firstly, it can create malicious websites through site cloning or templates that launch Metasploit or Java applet attacks at users. Secondly, it can create and send phishing emails. Finally, it can create malicious files, such as PDFs, MS Office docs, EXEx, etc.

SET’s installation is very simple. Firstly, you need download python and PyCrypto library. Next, in the Linux environment, you just need run the command, svn *co http://svn.secmaniac.com/social\_engineering\_toolkit set/.* In Windows environment, you can download SET in the website, such as *https://github.com/trustedsec/social-engineer-toolkit/*.

Another interesting thing is the SET uses menu, not commands to run the program. The lists in this menu present different Social-Engineer attacks in the real world. Option 1, Spear-Phishing Attack is a more targeted version of phishing attacks that combines tactics. In a typical spear-phishing attack, a forged email is sent to specific individuals from a target organization. The recipients are convinced through clever and relevant social engineering tactics to either download a malicious file attachment or to click a link to a malware- or an exploit-laden site, starting a compromise. Option 2, Website Attack clones websites using Metasploit or Java applet attacks at users. Option 3, Infectious Media Generator creates an autorun.inf file. When you burned a DVD or placed on a USB, it will trigger an auto-run feature and compromise your system. Option 4, Create a Payload and Listener can create a payload, export the exe for you and generate a listener. Option 5, Mass Mailer Attack will let you send tons of emails to victims and you can customize these emails. Option 6, Arduino-Based Attack let you use the Arduin-based device to remote the victims’ physical parts. Now, I just list some attacks of them. You can go through the menu and try one by one to get more details.

Bibliography:

1. Malcolm Allen, “Social Engineering: A Means To Violate A Computer System”, <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>
2. Radha Gulati , “The Threat of Social Engineering and Your Defense Against It”, <https://www.sans.org/reading-room/whitepapers/engineering/threat-social-engineering-defense-1232>
3. <http://www.social-engineer.org/>
4. <http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/>