
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.