
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.