3.1.2 Social Engineering Overview Facts

Social engineering refers to enticing or manipulating people to perform tasks or relay information that benefits an attacker. Social engineering tries to get a person to do something the person wouldn't do under normal circumstances.

This lesson covers the following topics:

- Manipulation tactics
- Social engineering process

Manipulation Tactics

Social engineers are master manipulators. The following table describes some of the most popular tactics they use on targets.

Manipulation Type	Description
Moral obligation	An attacker uses moral obligation to exploit the target’s willingness to be helpful and assist them out of a sense of responsibility.
Innate human trust	Attackers often exploit a target’s natural tendency to trust others. The attacker wears the right clothes, has the right demeanor, and speaks words and terms the target is familiar with so that the target will comply with requests out of trust.
Threatening	An attacker threatens when they intimidate a target with threats convincing enough to make them comply with the attacker’s request.
Offering something for very little to nothing	Offering something for very little to nothing refers to an attacker promising huge rewards if the target is willing to do a very small favor or share what the target thinks is a very trivial piece of information.
Ignorance	Ignorance means the target is not educated in social engineering tactics and prevention, so the target can’t recognize social engineering when it is happening. The attacker knows this and exploits the ignorance to his or her advantage.

Social Engineering Process

The social engineering process can be divided into three main phases: research, development, and exploitation. The following table describes each phase.

Phase	Description
Research	In the research phase, the attacker gathers information about the target organization. Attackers use a process called footprinting, which is using all resources available to gain information, including going through the target organization’s official websites and social media; performing dumpster diving; searching sources for employees’ names, email addresses, and IDs; going through a organization tour; and other kinds of onsite observation. Research may provide information for pretexting. Pretexting is using a fictitious scenario to persuade someone to perform an unauthorized action such as providing server names and login information. Pretexting usually requires the attacker to perform research to create a believable scenario. The more the attacker knows about the organization and the target, the more believable a scenario the attacker can come up with.
Development	The development phase involves two parts: selecting individual targets within the organization being attacked and forming a relationship with the selected targets. Usually, attackers select people who not only will have access to the information or object they desire, but that also show signs of being frustrated, overconfident, arrogant, or somehow easy to extract information from. Once the targets are selected, the attacker will start forming a relationship with them through conversations, emails, shared interests, and so on. The relationship helps build the targets’ trust in the attacker, allowing the target to be comfortable, relaxed, and more willing to help.
Exploitation	In the exploitation phase, the attacker takes advantage of the relationship with the target and uses the target to extract information, obtain access, or accomplish the attacker’s purposes in some way. Some examples include disclosing password and username; introducing the attacker to other personnel, providing social credibility for the attacker; inserting a USB flash drive with a malicious payload into a organization's computer; opening an infected email attachment; and exposing trade secrets in a discussion. If the exploitation is successful, the only thing left to do is to wrap things up without raising suspicion. Most attackers tie up loose ends, such as erasing digital footprints and ensuring no items or information are left behind for the target to determine that an attack has taken place or identify the attacker. A well-planned and smooth exit strategy is the attacker's goal and final act in the exploitation phase.