Social Engineering

Introduction

Social Engineering is an attack against a user, and typically involves some form of social interaction.

The best defence against social engineering attacks is a comprehensive training and awareness program that includes social engineering.

Impersonation

Impersonation is a common social engineering technique and can be employed in many ways. It can occur in person, over a phone, or online.

In the case of an impersonation attack, the attacker assumes a role that is recognized by the person being attacked.

Types/Ways

Third-Party Authorization

Using previously obtained information, the attacker arrives with something the victim is expecting.

Uses the guise of a project in trouble or some other situation where the attacker will be viewed as helpful.

Name-drops the contact "Mr. Big," who happens to be out of the office and unreachable at the moment, thus avoiding the reference check.

The attacker seldom asks for anything that seems unreasonable or is unlikely to be shared based on the circumstances.

Contractors/Outside Parties

It is common in many organizations to have outside contractors clean the building, water the plants, and perform other routine chores.

An attacker can simply put on clothing that matches a contractor's uniform, show up to do the job at a slightly different time than it's usually done, and, if challenged, play on the sympathy of the workers by saying they are filling in for X or covering for Y.

The attacker then roams the halls unnoticed because they blend in, all the while photographing desks and papers and looking for information.

Online Attacks

Impersonation can be employed in online attacks as well.

In these cases, technology plays an intermediary role in the communication chain.

Some older forms, such as pop-up windows, tend to be less effective today because users are wary of them. Yet phishing attempts via e-mail and social media scams abound.

Defenses

The best defense is simple—have processes in place that require employees to ask to see a person's ID before engaging with them if the employees do not personally know them.

That includes challenging people such as delivery drivers and contract workers.

Don't let people in through the door, piggybacking, without checking their ID.

Reconnaissance

An adversary will examine the systems they intend to attack, using a wide range of methods to gain information.

Although most reconnaissance is accepted as inevitable, some of it is helped via press releases telling the world who your security partners are, what products you are employing, and so on.

Exam Tips

The key in all social engineering attacks is that you are manipulating a person and their actions by manipulating their perception of a situation. A social engineer preys on people's beliefs, biases, and stereotypes—to the victim's detriment. This is hacking the human side of a system.

For the exam, be familiar with all of the various social engineering attacks and the associated effectiveness of each attack.

A training and awareness program is still the best defense against social engineering attacks.

Defenses

Stopping social engineering begins with policies and procedures that eliminate the pathways used by these attacks.

Once you have layered policies and procedures to avoid these issues, or their outcomes, the critical element is employee training.

Lastly, have multiple layers of defenses, including approvals and related safeguards so that a single mistake from an employee will not give away the keys to the kingdom.

Principles (Reasons for Effectiveness)

Social engineering is very successful for two general reasons.

The first is the basic desire of most people to be helpful.

The second reason that social engineering is successful is that individuals normally seek to avoid confrontation and trouble.

Principles

Authority

The use of authority in social situations can lead to an environment where one party feels at risk in challenging another over an issue.

Intimidation

Intimidation can be either subtle, through perceived power, or more direct, through the use of communications that build an expectation of superiority.

Consensus

Consensus is a group-wide decision. It frequently comes not from a champion, but rather through rounds of group negotiation.

Scarcity

If something is in short supply and is valued, then arriving with what is needed can bring rewards and acceptance

Familiarity

People do things for people they like or feel connected to. Building this sense of familiarity and appeal can lead to misplaced trust.

Trust

Trust is defined as having an understanding of how something will act under specific conditions.

Urgency

Time can be manipulated to drive a sense of urgency and prompt shortcuts that can lead to opportunities for interjection into processes.

Hoax

Hoax can be very damaging if it causes users to take some sort of action that weakens security.

Example:
Described a new, highly destructive piece of malicious software. It instructed users to check for the existence of a certain file and to delete it if the file was found. In reality, the file mentioned was an important file used by the operating system, and deleting it caused problems the next time the system was booted.

As with other forms of social engineering, training and awareness are the best and first line of defense for both users and administrators.

A hoax often also advises the user to send it to their friends so that they know about the issue as well—and by doing so, the user helps spread the hoax.

Users need to be suspicious of any e-mail telling them to "spread the word."