Social Engineering

LECTURE 8

What is Social Engineering

includes type of attack that is nontechnical in nature and that involves some type of human interaction with the goal of trying to trick or coerce a victim into revealing information or violate normal security practices.

- Scams may include trying to make a victim believe the attacker is technical support or someone in authority.
- An attacker may dress a certain way with the intent of fooling the victim into thinking the person has authority.

The end goal of each approach is for the victim to drop their guard or for the attacker to gain enough information to better coordinate and plan a later attack.

Social engineers as same in context as con artists

Moral Obligation An attacker may prey on a victim's desire to provide assistance because they feel compelled to do so out of a sense of duty.

Trust Human beings have an inherent tendency to trust others. Social engineers exploit a human's tendency to trust by using buzzwords or other means. In the case of buzzwords, for example, use of familiar terms may lead a victim to believe that an attacker has insider knowledge of a project or place.

Threats A social engineer may threaten a victim if they do not comply with a request.

Something for Nothing The attacker may promise a victim that for little or no work, they will reap tremendous rewards.

Ignorance The reality is that many people do not realize the dangers associated with social engineering and don't recognize it as a threat.

Why Does Social Engineering Work?

Lack of a Technological Fix : One thing that technology has little or no impact on is blunting the effectiveness of social engineering.

Insufficient Security Policies The policies that state how information, resources, and other related items should be handled are often incomplete or insufficient at best.

Difficult Detection Social engineering by its very nature can be hard to detect. Think about it: An attack against technology may leave tracks in a log file or trip an intrusion detection system (IDS), but social engineering probably won't.

Lack of Training Lack of training or insufficient training about social engineering and how to recognize it can be a big source of problems.

The Power of Social Engineering

Trust Human beings are a trusting lot. It's built into the species. When you see someone dressed a certain way (such as wearing a uniform) or hear them say the right words, you trust them more than you normally would. For example, if you see someone dressed in a set of scrubs and carrying a stethoscope, you tend to trust them. This tendency to trust is a weakness that can be exploited.

Human Habit and Nature Human beings tend to follow certain default habits and actions without thinking. People take the same route to work, say the same things, and take the same actions without thought. In many cases, people have to consciously attempt to act differently from the norm in order to break from their learned habits. A good social engineer can observe these habits and use them to track people or follow the actions of groups and gain entry to buildings or access to information.

Social-Engineering Phases

1. Use footprinting and gather details about a target through research and observation. Sources of information can include dumpster diving, phishing, websites, employees, company tours, or other interactions.

2. Select a specific individual or group who may have the access or information you need to get closer to the desired target. Look for sources such as people who are frustrated, overconfident, or arrogant and willing to provide information readily. In fact, the presence of this type of person can take the form of an insider threat.

3. Forge a relationship with the intended victim through conversations, discussions, emails, or other means.

4. Exploit the relationship with the victim, and extract the desired information.

Social Engineering Process

- Research (step 1)
- Develop (steps 2 and 3)
- Exploit (step 4)

Common Targets of Social Engineering

Receptionists: They see many people go in and out of an office, and they hear a lot of things. In addition, receptionists are meant to be helpful and therefore are not security focused.

Help desk personnel: Filing fake support requests or asking these personnel leading questions can yield valuable information.

System administrators: The typical administrator can be counted on to have very highlevel knowledge of infrastructure and applications as well as future development plans.

Also, some system admins possess far-reaching knowledge about the entire company's network and infrastructure.

Techniques I have used in the past include asking questions about their experience, career path, and such, and then using that to learn more about what they currently do.

Cont.

Executives: because individuals in these types of positions are not focused on security. In fact, many of the people in these positions focus on business processes, sales, finance, and other areas.

Users: one of the biggest sources of leaks because they are the ones who handle, process, and manage information day to day. Couple this with the fact that many of these individuals may be less than prepared for dealing with this information safely.

Example, for reading:

Many times over the years I have noticed the tendency for system administrators to leave themselves shortcuts to get their jobs done. Although I am not going to bash the idea of shortcuts—I use them myself and fully endorse their usage—it's the incorrect usage of shortcuts that I want to address. One of the applications that I find most problematic is the use of backdoor accounts. I have performed many system audits in which I found these accounts, put there to allow an administrator to quickly and easily log in and/or perform certain tasks without having to go through safer or permitted methods. In many of my audits, these accounts were unmonitored—or even forgotten when the original owner left the organization. In the latter case, the accounts remained and were unsecured; no one knew they existed except their original creator, who had long since moved on. Knowing that some administrators have this tendency, a good social engineer can look for clues as to the existence of such accounts.

So why do system administrators and the like place backdoors that may circumvent security on a system? Well, I have found in some cases that they have been put there to provide an alternative means to enter the system in the event their primary accounts are unavailable. In other words, they are put there in case they lose access or their primary accounts are locked out.

Social Networking to Gather Information

The rapid growth of these technologies lets millions of users each day post on Facebook, Twitter, and many other networks. What type of information are they posting?

- Personal information
- Photos
- Location information
- Friend information
- Business information
- Likes and dislikes

Before you post any type of information on these networks, ask yourself a few questions:

- Have you thought about what to share?
- How sensitive is the information being posted, and could it be used negatively?
- Is this information that you would freely share offline?
- Is this information that you wish to make available for a long time, if not forever?

Cont.

Social networking has made the attacker's job much easier based on the sheer volume of data and personal information available. In the past, this information may not have been as easy to get, but now, with a few button clicks, it can be had with little time investment. With little effort is it possible for an attacker to gather the following:

- Location information
- Personal data
- Company information
- Photos of private or secure facilities
- Information on coworkers
- Event or vacation information

scams can ensnare users by preying on an aspect of human nature

Secret Details about Some Celebrity's Death This type of post feeds on people's insatiable desire for information regarding celebrities or public figures.

I'm Stranded in a Foreign Country—Please Send Money. These types of scams target users by claiming that the message is from someone the user knows who is trapped without money in a foreign country or bad situation.

Did You See This Picture of J-Lo? Both Facebook and Twitter have been plagued by phishing scams that involve a question that piques your interest and then directs you to a fake login screen, where you inadvertently reveal your Facebook or Twitter password.

Test Your IQ. This type of scam attracts you with a quiz. Everybody loves quizzes. After you take the quiz, you are encouraged to enter your information into a form to get the results.

Countermeasures for Social Networking

As an ethical hacker and security professional, consider recommending and training users on the following practices:

- Discourage the practice of mixing personal and professional information in social networking situations
- Always verify contacts, and don't connect to just anyone online.
- Avoid reusing passwords across multiple social-networking sites
- Don't post just anything online; remember that anything you post can be found, sometimes years later.
- Avoid posting personal information that can be used to determine more about you, impersonate you, or coax someone to reveal additional information about you.