Social Engineering Fundamentals

Critical Mass – Phantasm - 404
http://th3untouchables.org – http://textbox.net
Part of Textbox Networks

What Is Social Engineering All About?

How It Used To Be Defined?

Most articles I've read on the topic of social engineering begin with some sort of definition like "the art and science of getting people to comply to your wishes an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system", or "getting needed information (for example, a password) from a person rather than breaking into a system". In reality, social engineering can be any and all of these things, depending upon where you sit. The one thing that everyone seems to agree upon is that social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.

Security is all about trust. Trust in protection. Generally agreed upon as the weakest link in the security chain, the natural human willingness to accept someone at his or her word leaves many of us vulnerable to attack. Many experienced security experts emphasize this fact. No matter how many articles are published about network holes, patches, and firewalls, we can only reduce the threat so much... and then it's up to Maggie in accounting or her friend across the hall from her, dialing in from a remote site, to keep the corporate network secured. They will never knew what hit them until the attack is over and maybe even then they still don't have any clue that is going on.

Targeting and Attacking Your Host

Playing That Mind Game

The common goal of social engineering is to gain information. The specific motives of a social engineer may be a hard item to determine, he could be looking for information for personal gain of knowledge or in the most extreme cases, corporate espionage. Most companies do not like to disclose the fact they were a victim of a security compromise, this is something an attacker would like to gladly exploit.

The goals of a social engineer can range from gaining unauthorized access to systems and information either to satisfy personal curiosity or even to commit fraud, network intrusion, industrial espionage, identity theft or even just to disrupt network services. In all aspects of social engineering, the attacks are done against the weakest links of an organization, the people. Typical targets for attack include telephone companies and answering services, internet service providers, software companies, financial institutions, military and government agencies, and hospitals.

Although the internet boom had its share of attacks on small start-up companies, general focus is placed on larger corporations. The bigger the company, the easier it is masquerade as someone in another office of the corporation. Utilizing large corporations and attacking a busy department could yield small treasures of information that could not only further information gathering, but may provide you with the exact information you are looking for. Asking questions to a busy department can provide answers, especially when they want to get off the phone and get back to an important project they are working on, or even if they just trying to clear the lines so they can step out for a cigarette break.

Attacking from a phone near you

Hello, Operator

Choosing your victim over a phone can be easy but then again it may be hard at times if they do not like talking to another person on the phone. Women make good social engineers in cases such as this. Most people do not have a problem talking to a sweet seductive voice. If you are going to do something like this, try to find a female friend that you can trust and get her to help you out with your calls.

Some other methods for this is to call the place that you are trying to get information from a few times a week, get to know the people you are calling, who they are and when they work. If you can find out this information most likely it will lead to a great attack. There are a few things that you have to remember about talking on a phone, you can masquerade as almost anyone you want, or even be from any company you want.

If you are going to be calling a place you may not want to call them from a friend's and pay phones are not an option there is too much background noise. You want a place that is nice, not a lot of noise, and a place that you can think without people running around. If there is a lot of noise and people running around they can tell you aren't in a office. A car is a good place to make a call from because a lot of people have cell phones. A good tool to have is a TracPhone or other prepaid cellular phone service. Most of the pre-paid cell phones are cheap and disposable, this helps you dump evidence and change the phone number you are attacking from often.

If you can find out a number of a person that works there, such as a direct line, call that instead of a general access 1-800 number. If you call from an 800 number they have the ease of using the ANI display to find your phone number.

Social Engineering takes a lot of practice and patience. Some people just do not have the patience to sit on a phone and try to get information out of random people. The best time of day to call your victim is at the end of the day. A lot of companies are busy in the day. The end of the day is when you are most likely going to get a person in a rush and too pre-occupied to validate who is calling for what specific information.

I.T. staff are always told to make sure to look for these type of attacks, but sometimes they just don't catch the rouse. A long day of work can make you tired, can slow down your thinking and can cause you to miss anything that would identify an attack from a social stand point.

Attacker: Hello my name is James & I am from Tri Star Computers, do you mind if I ask you a

few questions?
Target: Sure
Attacker: Ok thanks.
Target: How may I help you?

Right here is the best place to start your attack, inform them that you are with a company and that you are starting up and you are trying to see what kind of network and what not is hooked up if you do this you will know what they are running, and how everything is working there. Tell them that you will have a employee or some one get back to them. What you are trying to do is get as much information as you can out of them without seeming like you are poking around in the wrong areas. When you get off the phone with them make sure that you took notes of what was going on and don't forget the important things about the conversation. Everything they said can be lead in the attack. A few days later get another person to call them and see what is going on over there.

Tell them you are having a major problem close to the information that you are trying to get from the other person. This will make it easier for you. If you are very successful you will have most of the information that you want. Ok here is the second to last thing that you would want to do. Call the company again and tell them that your problem has not gone away and you are wondering if you could come down and see how they are set up. Most companies wont just let anyone into there computer area unless if they work there, but you would be a exception to the rule. If this works you and a friend can go down there.

Bring a tape recorder these are great for remembering the important things that you won't remember most of the time. When you are there if you see in the trash go for it, this would be a open opportunity to get what you are looking for. After this is all over you want to leave like you would any other place. And remember to be nice to the people, this will get you farther then it would be any other way.

A lot of people when they do this to other computer companies have to make up a name of a company that they work for and what they are doing this can be a pain in the ass if you are lacking imagination skills. It is kind of like playing a role playing game without the playing part it just does not happen you have to be ready for anything that they are going to through in your face. There is a famous quote that says "If I don't know the answer, I will make something up." That is a great quote for this kind of job. Because once you enter into there world the ball is then in there hands and you have to use your know how against there knowledge. This can be hard for people that think they know everything and this can also break a person down into being busted and I am sure you do not want the FBI come knocking at your door in the middle of the night.

Networking Your Attack

When I say networking your attack I mean just that, networking your resources. The more people you have focused on the target the better, it help compromise the target faster. Using multiple attackers will help gain both acceptance of your main attacker's story (IE why they are there, what they "need" to do) and can also be used to monitor suspicion.

A caller can say he is from ABC computing and he is sending in a repair technician to install a firmware update or that he is from XYZ company and they are sending a courier over to pick up some packages, when inside the building the courier can call the target to confirm whatever as so can the target - helping give your story authenticity.

Examples of various attacks

Target: Hello?
Attacker: Hi this is Jack in HR. Whom am I speaking with?
Target: This is Jane in Accounting
Attacker: Hi Jane, we have been having some issues connecting to the Accounting database to pull a few user files, have you been experiencing any connectivity issues over there?
Target: No, everything has been running smoothly
Attacker: Ok well we have been fighting this thing tooth and nail, I was wondering if I could have you forward me the files for _____ or I could have someone come in and pick it up – whatever works for you guys over there.
Target: Sure, I can get that out to you. Where did you want me to send the files to?
Attacker: You can email them to me at _____

Target: Human Resources, this is Christy.
Attacker: Hi, Christy. This is Greg, in the parking garage. You know the access cards you use to get into the parking garage and elevators? Well, we had a problem and we are reprogramming the cards for all the new hires from the last fifteen days.
Target: So you need their names?
Attacker: And their phone numbers.
Target: I can check our new hire list and call you back. What's your number?
Attacker: I'm at 87... Uh, I'm going on break, how about if I call you back in about an hour?
Target: Oh, that's fine with me.

After giving the needed time & calling back:

Target: Oh, yes. Well, there's just two. Sammy Self, in Finance, she's a secretary. And that new VP, Mr. Tanner.
Attacker: And there phone numbers?
Target: Right……. Ok, Mr. Tanner's is 3423. Sammy Self is 2432.
Attacker: You have been a big help. Thanks.

Sammy's call:
Target: "Finance, Sammy speaking.
Attacker: I'm glad I found somebody working this late. Listen, this is Robert Walls, I'm publisher of the business division. I don't think we've been introduced. Welcome to the company.
Target: Oh, thank you.
Attacker: Sammy, I'm in Nashville and I've got a crisis on my hands. This will only take about ten minutes of your time.
Target: Of course what do you need?
Attacker: Go up to my office. Do you know where that is?
Target: No.
Attacker: Okay, it's the corner office on the thirteenth floor—room 1337. I'll call you that in a few minutes. When you get to the offices, you'll need to press the forward button on the phone so my call won't go directly to my voice mail.
Target: Okay, I'm on my way now.

About ten minutes later she was in the office looking around. As she went to go do what he asked her to do the phone rang. It was the attacker on the other side. He told her to sit down at his desk and launch Internet Explorer. When she did that the attacker asked her to type in a web address that was a location of a remote access trojen the attacker had waiting.

Once she went to the site a box popped up asking her if she wanted to download a program and she clicked yes. The attacker told Sammy to click yes before she even asked about it. So she did like she was told. When she did this the backdoor had downloaded and when she clicked to open the program, nothing had happened, the screen just went white. She told the attacker what had happened.
When she did this, it let the attacker have full access to the system. The backdoor was in place and nobody would know about what was going on. Most backdoors won't work when you are on a

LAN, so you will need something that will work such as *Assassin By Evileye Software.* Once he got her to execute the program he talked her into restarting the computer for him, telling her it had been on for a very long time and need to be rebooted. When the computer was up and running again, Robert thanked her for all the hard work and then hung up the phone. Now Robert is in charge of a computer in the finance department of a company and all the credit goes to Sammy for being a great pawn.

This is how most attacks happen and there is nothing they can do about them. When a backdoored application is released into a computer the hacker on the other side has 100% control of the computer and everything that goes in and out of it. This will let our friend Robert do whatever he would like to the computer system and their LAN as well. Most of these attacks will not be reported or you would not hear about it due to them never figuring out what is going on.

Resources:

The Art of Deception by Mitnick & Simon
You and the Law by Unknown