

Forum:[Hack Forums](#)

Thread: [Social Engineering Tutorial](#)

ReaperX - March 11, 2011, 6:35 pm

Social Engineering

Why use Social Engineering?

The reasons for using social engineering to gain access are simple: once mastered, social engineering can be used on a system despite the platform or the quality of the hardware and software present. Social engineering comes in many forms, but they are all based on the principle of disguising oneself as a non-hacker who needs or deserves the information to gain access to the system. Aside from user larger security systems, another tactic that security professionals employ is 'security through obscurity,' which is providing little or no information to a user, assuming that legitimate users have already been trained, and that the hackers would be discouraged by having to guess different commands or procedures. Security through obscurity methods can also be accomplished by hiding certain files or information systems or having confusing login prompts. This method of security is completely undermined when social engineering is involved. With a legitimate human user providing information, all the information that allowed for security through obscurity would also be divulged to the hacker.

Methods of Attack

Although the methods used by social engineers rely on the same principle, the disguises of the hackers may vary greatly, depending on the hacker's level of skill and the type of information he or she is after. One common method used is for the attacker to pretend he is new to the system and needs assistance with gaining access. The role as a new person (or 'newbie' or 'neophyte') is easy for a potential hacker to pull off. The hacker can easily pretend to not know much about a system and still retrieve information. This ruse is commonly used when the attacker is unable to research enough about the company or find enough information to get a foot in the door. A simple method of this technique is for the hacker to call a secretary for the company and pretend that he is a new temp agent and is having trouble gaining access into the system. The secretary (or other legitimate user) may be inclined and proud to be able to offer help to the new person on the job. The user may simply give out the guest account name and password, or may even go into detailed instructions on login procedures for different departments. Once the intruder is in a guest account however, he may be able to access other (more important) accounts from there. He may also be able to find out enough information about the company to use a similar tactic: reverse social engineering, which is covered in the next section.

Other guises used by social engineers are to pose as a computer aide or helper, and try to gain information as you fix the computer. This technique, however, relies on the assumption that there is something wrong with the computer system. By posing as a helper, the legitimate user will be less suspicious and more willing to answer your inquisitive questions. Another form for the attacker to take is that of a system operator for the network itself. The potential hacker will pretend that an error in all the accounts has been made, and that he needs to reset the accounts. In order to do that, he needs the old passwords of the users. If the employee is naive enough, he or she will divulge the information, thinking that they are doing their company a service. Although there are many other methods and techniques, these previous examples account for most recorded incidents of social

engineers.

The disguises and tricks that the hackers use to social engineer legitimate users do have limits, however. During a social engineering attack, the hacker assumes a great deal and also relies on luck to pull off a successful hack. The above examples usually only work on employees who are not aware of the different forms of social engineering, or that they don't care about the company's security. Even if an employee is not aware of social engineering, he or she may not trust who the hacker is without proper identification. The employee may also be aware that temp agents usually have contact managers or other people within their own office to assist them, and would be suspicious when the call comes to their desk. These problems are a constant danger to the potential hacker, which has called for a new type of social engineering- called reverse social engineering.

Reverse Social Engineering

Reverse social engineering is a superior form of social engineering that deals with the common difficulties that come with normal social engineering. This form can be described as a legitimate user of a system asking the hacker questions for information. In reverse social engineering (RSE), the hacker is thought to be a higher-level than the legitimate user, who is actually a target. In order to pull off an RSE attack, however, the attacker must be knowledgeable of the system and usually must also have previous access granted to him, usually through normal social engineering. A quick glance of the some pros and cons of SE and RSE are given here:

Social Engineering: The hacker places the calls and is dependent on the user

Reverse Social Engineering: The user places the calls and are dependent the hacker

Social Engineering: The user feels that the hacker is indebted to them.

Reverse Social Engineering: The user feels indebted to the hacker.

Social Engineering: Questions often remain unresolved to the victim.

Reverse Social Engineering: All the problems are corrected, no suspicious loose ends

Social Engineering: The user has control by providing information.

Reverse Social Engineering: The hacker has complete control.

Social Engineering: Little or no preparation required.

Reverse Social Engineering: Lots of planning and previous access usually needed

The typical RSE attack consists of three major parts: sabotage, advertising, and assisting. After gaining simple access through other means, the hacker sabotages a workstation by either corrupting the station, or giving the appearance that it is corrupted. An abundance of error messages, switched parameters/options, or simulation programs such as fake prompts can accomplish this type of sabotage. The user of the system sees the malfunctions, and then tries to seek help. In order to be the one that the users call, the attacker must advertise that he or she is capable of fixing the problem. Advertising may include placing fake business cards around the office or even providing the number to call in the error message itself. A sample error message might be:

ERROR 03 - Restricted Access Denied - File access not allowed by user. Consult with Mr. Crack at () 595-1474 for file permission information.

In this case, the user would call 'Mr. Downs' for help, and divulge account information without being suspicious of the legitimacy of 'Mr. Downs.' Another method of advertisement can actually involve social engineering. An example of this is for the hacker to call the target and inform them that the new technical support number has changed, and then the hacker would give them their own

number. The third (and easiest) part of an RSE attack is for the hacker to assist with the problem. Since the hacker is the instigator of the sabotage, the problem is easily fixed, and the target is not suspicious of the helper since he or she appears to be a knowledgeable user of the system. The duty of the hacker is only to get account information out of the target while he is helping them. After the information is attained, the hacker solves the problem and then ends the conversation, eager to use his newfound knowledge.

Why Social Engineering Works

The use of social engineering and reverse social engineering are common because they often work under good conditions and take less time (and sometimes less knowledge) to pull off than brute-force attacks. They work because all humans have certain psychiatric characteristics that can be taken advantage of. Such characteristics are diffusion of responsibility, ingratiation opportunities, and moral duty. Diffusion of responsibility is used when the legitimate user feels that he or she is not solely responsible for their actions, which allows them to give up information more easily. A user may also divulge information if they feel that are doing something that will help them in the future, such as getting their boss out of a jam. Moral duty is played on when the target believes that they are helping the company with a problem, and they are often glad to help. There are other factors that allow social engineers to be successful, such as the use of guilt and personal persuasion.

Methods of Prevention

As social engineering and reverse social engineering become more prevalent, companies and network managers are trying to stop the attacks from being successful. Companies concerned with security realize that the great amounts of money spent on upgrades and security kits are being wasted if they can't prevent SE and RSE attacks. The simple answer to preventing these attacks is education. A knowledgeable user of a system can easily be told to never give out account information without permission of a supervisor. The users should be aware of the common methods of SE attacks, and should always report suspicious behavior. While catching on to RSE attacks is much harder, the users should still be aware of who to trust when a problem occurs. Since social engineers can attack any employee for information, all employees should be concerned with methods of attacks. Hackers know that low-level employees and users with low company morale are easy targets for giving up information without much thought. These employees must team to care about computer and company security as a whole.

Conclusion

All computer systems in the world must rely on human operators that have vulnerable characteristics. No matter how secure the equipment is from electronic invasion, the knowledge extracted from a legitimate user may render a computer network inoperable if used in an unauthorized manner. Hackers try to learn how to manipulate legitimate users into providing valuable network information. Once in, they may even use reverse social engineering to gain further access to the system- this golden method of hacking is easily prevented by education the users to be aware of such attacks, and to use wise judgment when providing others with company information.

Credits to : H0AX