Global Information Assurance Certification Paper

Social Engineering: A Backdoor to the Vault
Chris Orr
September 5, 2000

Protecting a network is supposed to be like building a vault around your computers and servers. Unfortunately no matter how much money and hardware is thrown at trying to make a network secure there is always one element that is neglected: The human element. Many attackers who have mediocre programming skills can often defeat or bypass even the most stringent defenses by employing a tactic known as social engineering. Social Engineering can be likened to building your vault but adding a backdoor and then giving everyone a key.

From numerous Internet sources, Social Engineering is defined as a:

> *Term used among crackers and samurai for cracking techniques that rely on weaknesses in wetware rather than in software; the aim is to trick people into revealing passwords or other information that compromises a target system's security.*
>
> Bernz "Bernz' Social Engineering Webpage"
> URL: http://members.tripod.com/~bernz/soceng.html.

Common ploys by Social Engineers to crack a network may involve someone pretending to be a new user, calling a help desk. Others may impersonate delivery boys or computer technicians, wandering around the premises until they find a user name and password conveniently posted on a monitor. Dumpster diving is another tried and true method of getting the information that an attacker needs to crack any network.

Social engineering hackers and their prey are made for each other. Social Engineers often don't want to take the time to perform more elegant hacks involving *IP crafting* or *spoofing*. At the same time, the average end-user doesn't want to memorize complex passwords or have to authenticate every time they step away from their desk.

Some potential security breaches are so mundane that they hardly seem noticeable. With the rush to install the latest and greatest firewalls, encryption software and keys, administrators often neglect the most obvious factors.

1. **Passwords**-One of the weakest areas of security. Many network administrators believe that having incredibly long and complex passwords will protect them from hackers. In fact, it is the very use of complex passwords and password schemes that can lead to the weakness. Imagine a firm with a password protection scheme that requires the use of a 17 digit alphanumeric code with mixed characters. Now give that password to the receptionist or the mailroom clerk and expect them to use it on a daily basis. Now tell them that this password will change every two weeks. What is the first thing that this employee will do with a complex password that is not even worth memorizing due to the frequency of change? There are tens of thousands of monitors, keyboards, drawers, and lamps across the country with little yellow stickies, declaring open access to any and all attackers who happen to wander through the room. Even the process of distributing passwords is perilous at best. An engineer who had just setup a new network was about to take the system online and was distributing passwords to the users and instructing them how to log on to the network. He was about to turn around and instruct the users to destroy the slips he had given them when he noticed that just about all of the employees were comparing passwords.
2. **Modems**-Every company has one, two, or thirty of them lying around connected to computers. Usually these are the remnants of the "old days" of the Internet when using dial-up Internet accounts was the only way to surf the web or check e-mail. Some consulting firms even require the use of a modem with *pcAnywhere* or other remote access software for support purposes. War dialing (if you remember the movie "Wargames" with Matthew Broderick) consists of figuring out what the number exchange is for any given company and then dialing the range of numbers until something answers. A computer left on with pcAnywhere services running in the background ensures that the attacker does not even have to bother with passwords to gain access to the network.
3. **Help Desks**-Are there for just that, helping. For an attacker, this is prime ground for gaining system

access, especially in large companies where there are thousands of end-users and usually only a few help desk technicians who are overworked. An attacker who strikes on a particularly bad day for the help desk simply implies that he is "user so and so" and had forgotten his password. If the company's policies on this matter are weak, then the attacker will hang up with the user name and password they need to attack the system.

4. **Websites**-The social engineer can target user names, passwords, and IP addresses through something as mundane as a website. With sweepstake sites running rampant, imagine a site that requires users to enter e-mail addresses as user names and then passwords to register to win prizes. The problem with many networks with their own e-mail server is that the e-mail address is usually derived from the user's own logon name. Now, the attacker has two critical components of the network, the domain name and a user name. The last element comes from the fact that users will often register the same password on a website that they use to logon to their own network. To them, it is a password they already know and one that they are less likely to forget. With the domain information, the user name, and password, the social engineer does not even have to look for a sticky note. The users will key all of this information into the site in the hopes of winning a prize.

In an article for Network World Security and Bug Patch Newsletter, Jason Meserve writes,

> *Instead of using technical skills to break into computers, hackers often use the weakness of the human mind to gain access to corporations. Hackers befriend users and trick them into giving away sensitive information that can be used to gain access to systems. These hackers also use trickery pretending to be from tech support to get unsuspecting users to give up their user names and password information*.
>
> Meserve, Jason "Social Engineering" 24 April 2000. URL: http://www.nwfusion.com/newsletters/bug/0424bug1.html.

As an engineer working for a consulting firm, we have many clients who outsource their IT functions to us. With 15 technicians who are constantly out in the field being assigned to various troubleshooting jobs, some companies have become used to a random selection of engineers plopping themselves in front of a terminal and working there. This begins to work against the company we work for and ourselves.

A social engineer may quite simply walk in and behave like one of our employees. Within minutes, they can have a full run of the company. This was illustrated in a recent event when I was sent to troubleshoot a network for a client I had never serviced. I found myself walking into their supposedly secure back office, sat at a terminal, and began plugging away. Not one person ever asked me who I was, or what I was doing there.

So what are the lessons to be learned at this point? Human nature, being what it is, will always be susceptible to social engineering. The level of protection against such attackers depends upon the amount of education that employees have about the subject. There are a surprising number of firms, even high tech ones that have no one trained in the field of Information Security.

Many of these companies rely on perimeter defenses such as firewalls and proxy servers. As a result, these companies become highly suspect over basic security policies. Hiring a consulting firm with no security policy would be like hiring a bank robber to guard the vault.

Listed below are some common defenses against social engineering from an article posted at netsecurity.tqn.com.

1. Require anyone who claims they are there to service the computers to show ID.
2. Make a policy that passwords are never to be spoken over the phone. A network administrator does not need a user's password to diagnose problems.
3. Make a policy that passwords are not to be left lying around near the computers.
4. Implement caller ID technology. Make a list of all employee phone numbers. When someone dials into the modem bank, hang up and compare the number that called in with the list of "good" numbers. If the number is on the list, call it back and establish a connection.
5. Invest in a paper shredder to prevent snooping through the garbage.

Author Unknown. "Crime, Security, and Privacy" URL:

http://netsecurity.tqn.com/compute/netsecurity/gi/msub27.htm.

Very few people would think of tip #5 as an issue. Even Microsoft found out recently how detrimental this could be when Oracle was accused of hiring a private investigation firm for attempting to purchase trash from the janitors. When someone wants your secret, they will go to any lengths to get it.

All of the issues above also point to one very basic fact. Every company should have a security policy in place. If the firm cannot afford to hire someone specifically trained in security matters, then they should immediately address this oversight.

Adhere to the policies and make sure that all employees are well versed with the contents. Furthermore, if a company's IT functions are outsourced, then make sure they have a security policy in place and have a list of all of their employees. Non-disclosure agreements would also protect any firm from their employees in the event that the employee may work for a competitor.

Social Engineering is not going to go away. Security policies need to be enforced at every level. It is no good driving the point home to the average worker if the CEO of the company leaves his laptop lying around in the airport. At the same time, the policies cannot be so complex and intrusive that they interfere with the company's efficiency and workflow, resulting in the unacceptable display of password-laden stickies.

Education about socially engineered attacks coupled with a solid, well written security policy, and well maintained internal and perimeter defenses may not prevent the most tenacious hacker from getting in, but it will certainly help keep the lazy or unskilled ones from having a free ride into your network.

References for Social Engineering Paper

Author Anonymous, "Crime, Security, and Privacy", Netsecurity.tqn.com,
Url: http://netsecurity.tqn.com/compute/netsecurity/gi/msub27.htm

Bernz, "The Complete Social Engineering FAQ", Bernz's Social Engineering Homepage,
Url: http://members.tripod.com/~bernz/soceng.html

Meserve, Jason, "Social Engineering", NetworkWorldFusion,
Url: http://www.nwfusion.com/newsletters/bug/0424bug1

to top of page | to Reading Room Home