Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Enemy Within: A System Administrator's Look at Network Security

Network security has always been a key player in the system administrator's day-to-day duties and must conform to the environment that it commands. In order to combat the continued risk from intrusion, we need to define the enemy, determine what the enemy wants and how to keep them from reaching it.

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

The Enemy Within: A System Administrator's Look at Network security
By Lawrence Dubin
01/07/2002 - Version 2.0

Network security has always been a key player in the system administrator's day-to-day duties: however, since the onset of the new self-propagating virus infections and the terrorist attacks of late the need and calling for more security has escalated beyond reason. Everyone is sending his or her administrators for training. Some long lost specializations have now found a new lease on life, such as the study and understanding of Steganography. In case you are new to the field, Steganography in it most simplistic form is data hiding. Network security takes on many shapes and forms; it must conform to the environment that it commands. One often-overlooked method of breaching your network is the concept of SEPS. SEPS is an acronym for Social Engineering Psychological Subversion. This concept is not new and along with technology continues to evolve into a powerful enemy that attacks from within our networks. In order to face an enemy on the battlefield, we must look at the world through the eyes of the enemy. In order to define the enemy, we must determine what the enemy wants and how to keep them from reaching it.

Nowadays, more companies are hiring outside consultants to perform a security analysis of their organizations. They want to know what the security holes are within their business and they want to know what the costs involved with plugging those hole's will be? There is a common denominator in the business world when deciphering risk. If the cost of minimizing the risk is more than the value of the risk then maybe we can live with the risk. It sounds insane but if you look at securing your network as a guarantee against a breach than you are not only fooling yourself but you are also throwing away valuable funds.

To combat the continued risk from intrusion we must go back to the basics that any administrator will learn especially those that will attend an Eric Cole SANS course. Follow these basic rules and most of your worries will be addressed. Following the methods of defense in depth and the principle of least access we can safely protect our systems from the most common vulnerabilities. I can go on for pages and pages on the various theories associated with total network security, but from my years of experience in System Administration as well as providing the security infrastructure for many Microsoft/ Novell networks, I have found that the there are certain uncontrollable aspects of security that will most likely be the demise of your network security plan. I will now give you a scenario that will open your minds to the demon that lurks within our realm.

By following the principles of defense in depth I have setup my network in a multi-layered fashion. From the Internet into my network I have a Router set with Ingress and Egress filtering on. From there the data must travel through a stateless firewall and pass through a proxy firewall. If you have the access and capability of passing these barriers as well as bypassing the multiple network and hardware IDS's (Intrusion Detection Systems) set up on the system you have entered the land of OZ. We have also employed the principles of least access by only giving users rights to those areas deemed necessary for them to complete their daily tasks. We have applied a very strong password policy requiring 8 characters, at least one capital and at least one alphanumeric or symbol. The policy is set to require password change every 90 days with a memory of 5 passwords with a minimum password life of 1 week. Basically we have covered a

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

lot of the major network no no's needed to secure the data. At least you would expect that as being so. To add to that we do multiple port scans and network analysis, as well a biweekly password-cracking algorithm to check on the password strengths and adherence. We also have antivirus software running on both the servers as well a the desktops with automatic push updating of new dats and software upgrades and we are running scanmail (A program that scans Outlook folders for malicious code and attachments) on each exchange server to add an additional layer of protection. We do not allow through any executables or registry files as well as block excel and PowerPoint attachments from entering from the outside world. In a nutshell we have taken a very strong look at our network and attempted to provide as many possible layers to secure the data as we have capability as well as funding.

Enter the demon, as history shows from the cure arises a new disease. This parable holds true even when dealing with computers, as quickly as we find a way to block an attack the hackers figure out a new way to enter. Network security is a full time job and it's a job that needs to be taken seriously. The one thing we must learn is no matter how protected we are from intrusion we are completely vulnerable to a professional who wants access. The most difficult security breach that we need protection from is right in front of our eyes. They are sitting right next to us; they are eating lunch with us at the corner deli. That's right! The most dangerous factor within our entire security structure is our USERS. It will become clear that the one resource that most security experts failed to address was right under their noses.

Enter the role of Social Engineering as the culprit most used by intruders to gain access to your network. Social engineering is not a new subject it has been around since the dawn of time. There have been people through the centuries that have had that certain gift, the ability to convince people to do what ever they wanted. The definition of Social Engineering as explained on Searchsecurity.com (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html):
"In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures. A social engineer runs what used to be called a "con game". For example, a person using social engineering to break into a computer network would try to gain the confidence of someone who is authorized to access the network in order to get them to reveal information that compromises the network's security. They might call the authorized employee with some kind of urgent problem; social engineers often rely on the natural helpfulness of people as well as on their weaknesses. Appeal to vanity, appeal to authority, and old-fashioned eavesdropping are typical social engineering techniques."

When a system administrator thinks his network is secure and lets his users become aware of that fact, they become complacent. Users and administrators will let their guard down. As quoted from a speech by an experienced hacker Susan Thunder "Increased security measures make psychological attacks easier because users think their data is safe". She has coined the term "Psychological subversion as using social engineering over an extended period of time to maintain a continuous stream of information and help from unsuspecting users". http://www.defcon.org/html/defcon-3.html

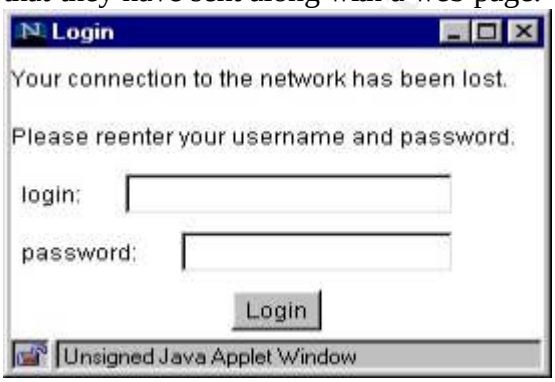
© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A well schooled hacker will be able to convince a naïve user that what they are doing is either for the benefit of the company or will help the user get ahead.

http://nativeintelligence.com/awareness/pw-soci.asp - Picture

Ask yourself this simple question. How many of you're users when called by the help desk will require proof of who is on the other end of the phone? An even more intense question: How many of your help desk staff will question the Vice president of the company who has forgotten his password and is demanding that it be reset in time to close a multi-million dollar deal? If you were within the norm, most of you would have answered a small percentage to both questions. There are other methods that the Intruder will use to gain access to your data, from posing as repairmen, to even impersonating your LAN Administrator.

The intruders will use whatever tools at their disposal to get the information they seek. They will use the naiveté of a user to get them to input their user name and password into a Java Applet that they have sent along with a web page.



http://nativeintelligence.com/awareness/pw-soci.asp - Picture

Our business networks are not unique, even the Government has been defiled by this new wave of security breach. In a statement from Senator Daniel Akaka in support of S. 1993 the Government Security Act on March 23 2000: The General Accounting Office has been conducting security audits and controlled penetration tests of various government networks.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

They found that even the poor social engineering tactics that they used as compared to the profession hacker allowed them to gain easy nearly undetectable access to some of the governments most sensitive systems. All in all 22 federal agencies were cited with computer security deficiencies and were ordered to take sufficient steps to ensure infrastructure protection was brought up to par.

Now, the question arises, how do we protect ourselves from this invisible intruder? How do we put up walls to stop this Psychological invasion from happening under our own noses? The answers to those questions are not simple, but if you follow some careful guidelines you will at least stand a fighting chance.
First, we need to identify who it is we are protecting ourselves from. I logged onto the Internet and brought up a basic search window, you can use Yahoo or Google or any other flavor of search engine that you choose. I typed in a simple request "Social Engineering Tips" and then clicked on the enter key. To my amazement hundreds of sites popped up onto my desktop. One of the first sites that I entered was a hacker's web site, who goes by the name of "Bernz". On his site he listed a series of statements one must follow to master the art of Social Engineering.

1. Be Professional: You don't want someone to not buy what you're doing. You're trying to create an illusion. You're trying to be believable.
2. Be Calm: Make them believe you belong there.
3. Know your mark: Know your enemy. Know exactly how they will react before they do.
4. Do not fool a superior scammer: trying to out scam an observant or smarter person will end in disaster.
5. Plan your escape from your scam: Don't burn your bridges. Save the source.
6. Be a Woman. It is proven that women are more trusted than men over the phone. Use that to an advantage.
7. Watermarks: Learn to make them. They are invaluable in a mail scam.
8. Business cards and fake names: Use them for professional things.
9. Manipulate the less fortunate.
10. Use a team if you have to: Don't be arrogant and overly proud. If you need help, get it.

Right before our very eyes are the instructions for anyone who is willing to put in the time. This very successful method of network intrusion has cost companies around the world Billions of dollars, and will continue until we stop them in their tracks.

As we continue to strive for improved security and conquer the enemy on their own turf we find that they adapt as quickly as we conquer. As we develop methods to battle the effects of social engineering the intruders have already traversed onto new territory. Enter the world of "Reverse Social Engineering" It requires that the hacker do more homework than before but it will in the long run lead to then same end product. This form of attack still requires the intruder to have some sort of low-level access prior to the attack. The attack is broken down to three parts. Sabotage, Advertising and Assisting. Basically in this for of attack it is the user who will be asking the intruder the questions for information. The scenario breaks down like this: the intruder sabotages a workstation that he had prior access to, either causing corruption or switched parameters or any other method to cause the appearance of system failure. The intruder must then advertise; either by placing a phony business card or by customizing an error message with his name and number to call for assistance. When the unsuspecting user calls for assistance the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

intruder will easily be able to repair the problem, thus gaining trust of the caller. Once this trust is gained the information that is required will more easily be attained from the user.

Enough discussion on the attacker let us now consider the defense.
The first line of defense is not allowing the attacker to gain valuable information about your company and its employees. **Protect your trash**!!!!!!!!!:

1. Shred all paper refuse to prevent someone from going through your trash searching for info.
2. Make sure all of your magnetic media (hard drives, floppy disks etc.) is bulk erased. To stop someone from attempting to retrieve data from them.
3. Lock your dumpsters.

The next line of defense is inside of your company's facility:

1. Require all visitors to be escorted at all times within your facility.
2. Instruct your employees not to grant access to repairmen until their identities can be verified.
3. Keep all server rooms, wiring closets and telecom closets securely locked at all times.
4. Keep accurate inventory.

And the final piece of the puzzle, the single most important remaining factor within the security framework of you company is the users. What can you do to protect them from themselves?

1. The most important piece of the pie is Training!!!!!!! – You must develop a comprehensive program involving both computer based and classroom instruction. You must teach your users the "Whys" and "Hows" of security. Employees are much more likely to follow security rules if they understand the consequences of not following them. Instruct user's to logoff of their PC's when they are leaving the area. Show them how to set password protected screen savers that initiate after a few of minutes of idle activity. Make sure that there are no post-it notes with user names and passwords attached to workstations or monitors. Initially this will be the most difficult stage to develop. However, once the users get used to the security frame of mind, they will find it actually isn't so difficult to follow.
2. Create a company security policy. A standard set of rules and regulations that the users can rely on as the framework of what they can and cannot do. Include Internet and email guidelines, as well as what is considered acceptable practice. (Remember to make your guidelines achievable, do not set your standards so high that users cannot comply) Along with this policy you should include what the consequences are for not following the procedures. You must make the users aware of the need to keep the companies business private and that there is a zero tolerance factor involved with protecting the assets of both physical as well as intellectual property.
3. Enforce a strong password policy and continually check for adherence. (Minimum of eight characters including upper and lower case letters mixed with numbers and symbols. Require frequent password changes with a password memory of 5 passwords and a minimum password age of 1 week)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

4. Require your help desk to verify all users prior to assisting and visa versa require each user to verify that it is in fact the help desk on the phone. Either by calling the user or the help desk back or by enforcing a Pin (personal Identification Number) policy that can be verified.
5. Use your company's intranet or bulletin board to post statistics of losses due to network intrusion. Allow your users to read about when a bad guy gets caught. Let them know that the law is on their side.
6. Recognize those that have followed the rules and those that have stopped an intruder in their tracks.
7. Put a plan of action together on how to respond to an attack or intrusion.
8. Test your readiness
9. Use new technology to its fullest. Most PBX systems allow for call initiated outside the facility to ring differently than those call from inside. Use this to identify whether a call originates from within your facility or not.
10. Teach your users to recognize the signs. You cannot emphasize enough how important it is to ask questions, get information and do not ever give your password to anyone.

These are just a few principles that if properly put into place and acted upon will add another very powerful barrier to invasion. One more note to keep in your mind, technology is in a constant state of change. The more we advance our security the powers that be increase the possibilities of intrusion. Case in point, a new web site promises to give users remote access to their desktops from anywhere in the world for less than one hundred dollars a year. I said it couldn't be true; my network is so secure that it would be impossible to traverse all of the levels of protection from the outside. So, I called my wife at home, I told her to surf to www.gotomypc.com and download a trial version of their software (its free for the first 30 days). I had her fill in all of the information needed and in a matter of two to three minutes she was in complete control of my desktop. The way it works is sheer beauty within itself it initiates an outgoing we traffic through my firewall on HTTP/TCP ports 80, 443 and /or 8200. Most firewalls have those ports already configured to allow outgoing web traffic, they taut that their connection is secured using the highest rated encryption available. However, a well-heeled hacker using their social engineering techniques now has a new tool at their disposal that is also very secure. If you visit their website they post a FAQ on how to stop your users from loading GOTOMYPC on their PC's at work. Simply block access to the host poll.gotomypc.com. This will prevent anyone from starting a connection to access any computer inside your firewall.

In the end I can only leave you with these few words. If your job is to protect your company's network, than keep on your toes, keep your users aware and well trained and keep track of all trends in the technology community.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

http://www.gocsi.com/soceng.htm - CSI Social Engineering: Examples and Countermeasures from the real world

http://packetstorm.widexs.nl/docs/social-engineering/aaatalk.html People Hacking

http://www.fcw.com/print.asp - Old-fashioned hacker deceit by Dan J. Ryan May 29, 2000

http://packetstorm.widexs.nl/docs/social-engineering/socialen.txt - The Complete Social Engineering FAQ

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci537875,00.html – Hackers tactics prey on gullible, curious by Kevin Komiega April 04, 2001

http://zdnet.com/filters/printerfriendly/0,6061,2604480-2,00.html – Mitnick teaches 'social engineering' by Robert Lemos July 17, 2000

http://www.senate.gov/~gov_affairs/032300_akaka.htm - Statement of Senator Daniel K. Akaka

http://nativeintelligence.com/awareness/pw-soci.asp - How "Social Engineering" is used to get people to divulge passwords

http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html - Methods of Hacking: Social Engineering by Rick Nelson

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html - Definition of Social Engineering.

www.gotomypc.com - Access top your PC from any Web Browser

http://www.defcon.org/html/defcon-3.html - Susan Thunder speaking at DEF CON III – Audio Real Audio Format

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced