Global Information Assurance Certification Paper

Kristopher Harms
GSEC ver 1.4b
Option 1

Internal Attack Countermeasures

Abstract

Among the most difficult attacks to protect a network against are those that originate from within the boundaries of the network. Careless, negligent and disgruntled employees are the main sources of these attacks and responsible for 70% of the damage done to networks. The implementation of a secure subnet, which will separate different administrators and production systems from the user population, and a strong employee termination policy, can successfully reduce the risk of these attacks.

Introduction

After the Exxon Valdez oil spill, a double-hull design became a requirement, which added a second layer of security to protect against a breach and ensure containment of the oil. Similar in concept is the implementation of a firewall by network administrators to protect the internal network from an outside attack. Taking this concept a step further, the hull of the modern warship is divided into multiple sections. This prevents the boat from sinking if a breach in the hull occurs and allows full functionality to the rest of the ship while repairs are made. Many network administrators have yet to take this step in the design of their networks and it has cost them dearly.

Eighty percent of the respondents from the 2002 Computer Security Institute survey acknowledged financial losses from computer breaches. Forty percent were willing to quantify their losses, which totaled roughly $455.8 million. [1] According to Gartner Inc. analyst John Pescatore, 70 % of (the attacks) come from outsiders, but the 70% that cause damage are the insiders. The majority of the damage caused by insider attacks is due to a lack of security, which could have reduced damage by containing the attack. Once inside the network, traffic was not restricted, and damage was easily done. Attacks from within can come from many different areas for various reasons. Disgruntled and improperly terminated employees or temporary contractors can be potential threats to a network. Even more dangerous than the angry employee is the vulnerable computer of a careless, or ignorant system administrator. Access through network and host based firewalls to production machines is available from this internal computer providing an easy path through security restrictions. Penetration of a system is done most easily through the path of least resistance though it may not be the most direct. Often it is easier to hack an administrator's computer that has access to the production machines, than to hack the production machine itself. Most critical machines are heavily guarded with firewalls, hardened configurations, and intrusion detection systems along with regular monitoring of logs. However, for a number of reasons, the security measures are not often used on the machines given access through the firewall for remote administration. In addition, activity in logs coming from an administrator's machine can easily be overlooked as legitimate traffic. Protection against these types of threats is critical and the risk can be reduced by the implementation of a secure subnet, which separates the administrators,

production systems, and general user populations. This will allow administrators to better secure all machines tied to production. Further steps are needed to secure remote access. These implementations coupled with security policy, such as a sound employment termination policy will allow administrators to better secure their environment.

The Secure Subnet

In a recent study of Information Security Administrators, 97% said their biggest worry is employee negligence and abuse. [2] The negligent employee can be as dangerous, if not more, than the disgruntled employee. Mitigating these risks can be an important step for a large network. It is even more important when it is not feasible to apply proper security measures to all machines present on the network. This is the case for many large corporations and universities across the country. The following is an outline of practices that can help protect the overall well being of a network by separating the critical systems and administrators from the normal network users.

Assessment

An assessment of the network design and a review of the related policy should be the first step. The network should contain a secure subnet. Within this secure subnet should be a properly configured and calibrated Intrusion Detection System (IDS), a means to regulate IP addresses, and a means to monitor network traffic between systems. A central logging server should be configured to log all necessary information. The machines within the subnet should be hardened and patched, require individual administrator usernames with strong password management, updated virus protection, and personal firewalls. These machines should be scanned on a regular basis. Fixing vulnerabilities identified through this process should be given the highest priority. A restricted programs list should be created and applied to all machines. Administrators of these machines should be required to subscribe to an internal security mailing list and go through security awareness training. With these recommendations, risk posed by disgruntled and negligent employees will be significantly reduced.

Intrusion Detection

Intrusion detection systems are a fundamental part of security, especially in large enterprise networks, for multiple reasons. One of the main deterrents to potential network attackers is the threat of being caught. “An IDS increases the perceived risk of discovery and punishment of attackers. This serves as a significant deterrent to those who would violate security policy”. [3, Rebecca Mace, Peter Mell] Some protection against negligent employees is provided as well. A properly configured IDS can detect a security breach in real-time and alert a security administrator so the problem can be addressed and fixed immediately, perhaps before significant damage can be done. In addition, the IDS has an

accurate log to locate the point of failure, whether it be the policy, the computer itself, or a negligent employee.

IP Address Management

IP address management is another key aspect in the creation of a secure subnet. Complete knowledge of all systems within the subnet is a priority. Any number of attacks can originate from a rogue computer inside the network. Whether it is a result of a failure in physical security measures, or a negligent employee puts a computer on the network that isn't secured properly, risk is greatly increased without this type of monitoring. Using a program such as NetARP, a network can be protected from the illegal use of IP-addresses. NetARP will respond to all Address Resolution Protocol Requests made to addresses not in its host list, thus causing a conflict if an unauthorized individual were to claim an IP. [8]

Network Monitoring

Along with management of IP addresses, monitoring of network also provides another layer of security. To an untrained eye, increased network traffic, or traffic between two machines that should not be communicating with each other is a difficult thing to spot. However if employees are properly trained to interpret anomalies, those logs could be the only notification of a security problem. For instance, perhaps a database server is communicating with more than one machine, when that database is only supporting one application on one additional server. Noticing this might trigger an investigation as to why that server is communicating with someone else. Network traffic monitoring can also show scanning activity originating with a machine infected with a virus, as well as compromised by an outside attacker or carrying out a denial of service (DOS) attack. Some of these actions may not be detected if an IDS is not present, or the proper signatures are not enabled.

Central Log Management

A server that collects logs from all the machines within the subnet is another level of defense that would protect against attacks originating from inside the subnet. Collecting and correlating logs as they are created and sending them over a virtual private network (VPN) to a logging server can provide similar results to an employee as an IDS. A centrally managed logging system could deter an employee from installing malicious programs on their machine for fear of someone seeing it in the logs. This also can prevent against a disgruntled employee who deletes the log files to cover his tracks. Prevention and protection against a hacker successfully deleting the log files on a machine they have compromised can provide an incident response team with valuable information.

Desktop Security

Hardening

The hardening of operating systems is one of the more difficult tasks, especially when the number one goal of most companies is functionality. Ideally, the system should be loaded with all services turned off, allowing the administrator to turn on only the services needed, but in a Windows world, usability is king. A balance between security and functionality has been an ongoing battle to achieve. Running services unknown to the user can be a major source of security incidents, so turning off all unnecessary services is a must. This can also provide a clue to a security administrator looking at scanning results. Seeing port 23 (telnet) open on a web server can be a dead giveaway that something is wrong. Perhaps it is an employee who has not been told that telnet is insecure, and usage of SSH recommended, or perhaps the machine has been compromised. Either way, hardening of the machine is absolutely necessary when it comes to preventing security incidents.

Anti-Virus

Anti-virus software is not only good for preventing viruses but for preventing headaches as well. Most security administrators consider viruses just another headache that could have been easily prevented. There are many software packages available on the market, but some are better than others. When choosing anti-virus software, features such as real-time protection, mail scanning and automatic updating of signatures should be included in the list of the requirements. [10] Some anti-virus software updates can be managed centrally, but if that server unknowingly goes down or is compromised, systems can be left vulnerable to viruses, worms, and trojans. Using anti-virus software on every computer in the secure subnet can prevent crippling scans from viruses such as CodeRed, and prevent any possibility of an infection spreading within the subnet itself.

Personal Firewalls

The use of personal firewalls on all machines is one of the most important security features that can be installed on a secure subnet to protect against disgruntled and negligent employees. This is truly what separates the bad from the good, and can mean a considerable security upgrade if instituted correctly. Personal firewalls can require a consuming installation, but its' advantages far outweigh the effort required. When deploying a personal firewall, the rule set should not only block all incoming traffic on unnecessary ports, but implement egress filtering as well. Screening all outgoing traffic can allow the administrator to inspect the logs for mysterious traffic. Examples of this occur when a custom trojan, not noticed by the anti-virus software, tries to connect to the client outside the network. Another example would be a dangerous keystroke logger trying to e-mail keystrokes to an attacker. Catching this type of connection can be

extremely critical. Not only has the attacker compromised a machine with access to critical information systems, but could also have recovered the username and password which would allow entry to any or all of the machines the administrator manages. This scenario can be detected and prevented with the use of egress filtering.

Username and Password Management

All administrators of machines should be given individualized usernames and passwords. Sharing of login credentials should be strictly prohibited in policy and in practice. This allows accountability and provides knowledge about who is doing what to which systems. This helps prevent the possibility of a sneaky employee changing system settings so the machine can be exploited with no one held accountable. Logging tells all. In addition to individual usernames, the strongest password requirements should be enforced on all machines with password expiration enabled. If finances are available, advanced authentication systems, such as the usage of a token, should be implemented. For a tighter budget, a strong password policy can be sufficient. This requirement forces the negligent employee to choose strong passwords. Just make sure there are no yellow sticky notes in the vicinity.

Vulnerability Scanning

Scanning using software such as Internet Security Systems' Internet Scanner or Nessus can provide checks to make sure that administrators are up-to-date with security updates, patches, and policy regarding personal firewall rule sets. Scanning can also provide insight to failures of other security measures such as personal firewalls, automatic updating of patches, IDS functionality, and rogue computers. Scanning can create awareness about a disgruntled employee who opened up a machine and created a vulnerability, a lazy employee who hasn't installed the latest patches, or perhaps installed them incorrectly. With the daily increasing number of vulnerabilities, auditing of the secure subnet is imperative and should be done everyday, ideally, or at least every week.

Restricted Programs List

With marketing and advertising companies becoming as stealthy as an elite hacker, spyware (see appendix A) is being installed on computers, opening up holes and creating vulnerabilities, putting the security of the machine at risk. Peer to Peer (P2P) applications are making the spread of trojans and viruses increasingly easy. Advertising companies install spyware on computers to log keystrokes and websites visited. All these programs can pose a threat to the secure subnet and programs that are not necessary for the functionality of the machine should not be installed. P2P programs such as Kazaa, and download agents such as WEB3000 or Downloadware, are good examples of programs containing hidden spyware that will automatically be installed with the main

program. [4] When dealing with computers that have remote administration privileges on other machines, a careful audit of running programs and services should be reviewed. There are two ways to restrict programs and services and depending on the nature of the organization, one may be more feasible than the other. Ideally, a list of programs allowed to be on the desktop should be distributed. This ensures that no random unsafe software makes it within the secure subnet. For a more open environment, and restriction list can be distributed.

Access Control

Many networks lack access control, giving all administrators access to all systems regardless of functionality. Access control should be limited to only the systems needed to perform their duties. This is also known as the principal of least privilege. Access controls can go as far as limiting the activities of users and administrators on certain systems. These controls successfully limit each user and administrator to only functions for which they are authorized. Using this type of restriction limits the type and extent of damage that can be done if a user's account information is compromised. [10]

Security Awareness

Security awareness training serves multiple purposes in protecting the internal network. First, awareness and training can increase understanding and reduce the user frustration of secure computing. Security administrators do not have a problem hardening machines and installing personal firewalls because that is what most are trained to do. Conversely, a system administrator may not be trained in security, therefore, trusting the system administrator to learn about security topics on their own time may not be a reasonable expectation. If training is a requirement, the system administrator will already know how to install and properly configure new machines and install desktop security measures. Secondly, it increases the chances of catching an attack initiated by a disgruntled employee. It sends the message, "we care about our network security." This can convey enough knowledge to prevent an incident from occurring. Thirdly, this reminds negligent employees that carelessness will not be tolerated. Disregard for security policy will not go unnoticed and appropriate sanctions will be enforced. [9]

Employment Termination

Another aspect in protecting production related systems is proper full-time, part-time, temporary employee and contractor termination. On February 20, 2003, a press release from the Department of Justice detailed an account of an ex-employee of the Airport Transportation Company who was arrested for allegedly hacking into computers and destroying data. [5] In another case released

September 9, 2002, a man plead guilty to illegally accessing his former employers computer and reading e-mail messages to acquire a commercial advantage at his new job. [6] The list of cases goes on, and more are released each day. Almost all security measures mentioned earlier are of no use if an ex-employee with valid physical access and account information can walk into the building, make a few network alterations, and destroy a corporate network. A few basic guidelines can be set to ensure that an ex-employee won't come back to haunt the company.

Policy

It is important to have a policy clearly outlining the steps that should occur when terminating employment of a full-time, part-time, or temporary employee. A detailed policy will help guide employees and managers, and layout all the tasks that need to take place, ensuring that one of these aspects isn't omitted.

Upper Level Management Guidelines

When the decision to terminate an employee occurs, upper level management must ensure that the information does not leak out and that proper execution of the process is upheld. Management needs to alert the employee's supervisor, if they were not part of the decision, and have the supervisor set the process in motion.

Guidelines

The first task is to request a police or security escort. This is necessary to mitigate the risk of a physical incident occurring with the employee and no other steps should be taken until the security guard arrives. The employee should then be isolated from the rest of the work environment. This removes the ability of the employee to do something drastic while sitting at his desk, such as destroying information, releasing a virus in the secured subnet, or encrypting data to hold hostage. After the employee is removed from the work environment, with the security guard present, the employee should be told of his termination and asked for all user account information. This information should be brought to a meeting of his co-workers that is being held simultaneously. This meeting can serve multiple purposes. The termination should be discussed to ensure the continuation of a good working environment, and the employee's account information should be given to one of the co-workers who can remove or change any necessary information. The supervisor should also audit this process. While in the meeting, the co-workers can also be questioned about any suspicious activity going on regarding the employee that is being fired. Sometimes, an employee that is going to be terminated is aware of the situation and has time to prepare an attack. In addition, all passwords must be changed on any machines to which the employee may have had access. This ensures that the employee has no knowledge of any current passwords.

In addition to changing passwords, all physical access should be restricted. Tokens should be collected, swipe card access should be disabled, any type of security badge collected, and any combinations to doors should be changed. Physical access to the building should be strictly prohibited unless constantly escorted by a security guard.

Regarding the employees personal computer, the physical connection to the employee's machine should be terminated and the IP address disabled, ensuring that when the employee returns to his desk, he does not have access to the network. In addition, a mirror image of the hard drive should be made. This provides protection against the employee encrypting data and holding it hostage after he finds out he has been terminated. After the image has been made, a security administrator, and a co-worker should go through and pull any pertinent information off the hard drive, and search for malicious software such as trojans, logic bombs, and any other aspects that could implicate possible harm to the company. Sometimes it is necessary to force the employee to leave at the moment of termination and return at a later date, so all the policy guidelines can be followed.

When the employee returns to collect his personal belongings, a security guard must always accompany him. When the employee returns to his computer to remove personal files if necessary, it is imperative that the supervisor escort him. The supervisor can watch for any type of technical action the employee might attempt, such as encryption, installation of a physical keystroke logger, camera, or anything out of the ordinary.

A timeline for this process is provided in appendix B

Temporary or Contractor Employment Termination

"Immediately after temporary or contract workers are done working for you, disable their user accounts on your computer systems." [7] How long the person has been working for the company will dictate the lengths taken by the company when the employment period has ended. If the employee is working for an outside contractor, any damage that occurs may cost the employee their job, leaving the other company liable for damages. This provides a safety net when an employee leaves. However, this does not allow a relaxed approach to remove all user accounts and all other applicable security procedures should be enforced.

Practice

Terminating an employee can be a very difficult. Many tasks need to be completed by fellow employees and if one mistake is made, a gaping security hole could put the entire network at risk. This is especially true when terminating an administrator who knows the intricacies of the network. That is why it is

important to practice and review such policies with current employees. All employees, in particular, the supervisor who oversees the entire process, need to be well trained in the policy guidelines when terminating an employee.

Conclusion

Complexity of our information systems is constantly growing. As networks become more complex, more vulnerabilities are discovered. Security is a constant battle and the minute a gap in security surfaces, the system can be compromised. Hundreds of millions of dollars are reported lost each year recovering from hacks, and even more are not reported. Security costs are extremely difficult to calculate, especially with regard to return on investment. Although only 30% or less are attacks originating from inside the network, these attacks cannot be ignored. Disgruntled and negligent employees are causing 70% of the damage, making companies squirm as insiders ravage their networks. [1] Full protection from those who administer it can never be guaranteed. The best anyone can do is to reduce the possibility of an incident occurring and lessen the damage when it does occur. Creating a secure subnet is part of the solution. Securing and separating the different groups of critical systems into secured subnets provides a damage control mechanism when an incident occurs. By properly terminating an employee, attempts and successes of attacks can both be reduced. The psychological aspect of showing employees that security is taken seriously, and offenders are taken even more seriously, may be enough to ward off a potential attack. These components when combined provide a powerful road map for maximum security from yourself.

Appendix A:

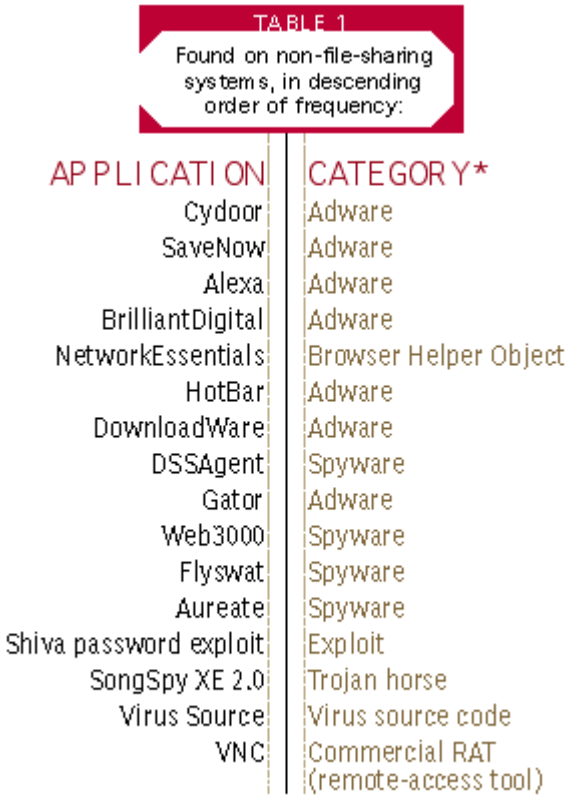

TABLE 1

Found on non-file-sharing systems, in descending order of frequency:

APPLICATION	CATEGORY*
Cydoor	Adware
SaveNow	Adware
Alexa	Adware
BrilliantDigital	Adware
NetworkEssentials	Browser Helper Object
HotBar	Adware
DownloadWare	Adware
DSSAgent	Spyware
Gator	Adware
Web3000	Spyware
Flyswat	Spyware
Aureate	Spyware
Shiva password exploit	Exploit
SongSpy XE 2.0	Trojan horse
Virus Source	Virus source code
VNC	Commercial RAT (remote-access tool)

* Categories derived from PestPatrol's Pest Encyclopedia.

TABLE 2

Found on file-sharing systems, in descending order of frequency:

APPLICATION	CATEGORY*
Cydoor	Adware
Gator	Adware
Grokster	Adware
Morpheus	Spyware/adware
BrilliantDigital	Adware
Kazaa	Adware
NCase	Spyware
SaveNow	Adware
WurldMedia	Adware
Hotbar	Adware
IMesh	Adware
BonziBuddy	Adware
Alexa	Adware
Fun Factory 1.0	Trojan horse
NetworkEssentials	Browser Helper Object
OnFlow	Adware
TwistedHumor	Adware
Virus Source	Virus source code
webHancer	Spyware
Aureate	Spyware
Web3000	Spyware
DownloadWare	Adware
DSSAgent	Spyware

* Categories derived from PestPatrol's Pest Encyclopedia.

Courtesy of PCMag.com
URL: http://www.pcmag.com/article2/0,4149,981708,00.asp

Appendix B:

Timeline for Employee Termination

	Management	Supervisor	Co-Workers	Employee	Security Guard
9:00 a.m.	Management makes decision to fire Employee	Supervisor is alerted of Management's decision to fire employee			
9:30		Supervisor breaks news to employee and asks for user account info		Employee called into a meeting with supervisor and awaiting security guard	Security Guard asked to appear in meeting with employee
9:45			Co-Workers called into a meeting directly after Employee		Physical access to building restricted, appropriate badges returned to Security
10:30			Co-workers change user account information		
11:00		Supervisor double checks the removal of employee user account information	Employee's personal computer removed from network, hard drive mirrored and searched with security administrator		
11:30				Employee Escorted out of building	
12:00 p.m. or Next Day					
12:30		Supervisor escorts employee back to desk		Employee returns to reclaim personal items	Security Escorts Employee back to desk
1:00				Employee escorted out of building	Security escorts Employee out of building
1:30					

Reference:

[1] Dignan, Larry. "Who Can You Trust" Baseline, Ziff Davis Media Inc. March 1, 2003. pg 23

[2] Ponemon, Larry. "What Keeps Security Professionals Up all Night?" April, 2003. URL: http://www.securitynewsportal.com/cgi-bin/news5.cgi?target=www.newsnow.co.uk/cgi/NGoto/27903170?-2622

[3] Bace, Rebecca, Peter Mell, "Intrusion Detection Systems", NIST Special Publication on Intrusion Detection. URL:http://www.snort.org/docs/nist-ids.pdf

[4] Metz, Cade,"Spyware" PC Magazine, April 22, 2003, pg 85.

[5] Department of Justice, Press Release "Ex-employee of Airport Transportation Company Arrested for Allegedly Hacking into Computer, Destroying Data". February 20, 2003
URL:http://www.cybercrime.gov/tranArrest.htm

[6] Department of Justice, Press Release "San Gabriel Valley Man Pleads Guilty to Illegally Accessing Former Employer's Computers". September 9, 2002.
URL:http://www.cybercrime.gov/doppsPlea.htm

[7] "Behind the Firewall – The Insider Threat" Symantec, April 15, 2003. URL:
http://enterprisesecurity.symantec.com/article.cfm?articleid=2122&EID=0#related

[8] NetARP Download site URL:
http://www.freedownloadscenter.com/Network_and_Internet/Misc__Networking_Tools/NetARP.html

[9] Pfleeger, Charles. Security in Computing Upper Saddle River: Prentice Hall, 1996

[10] Chirillo, John. Hack Attacks Denied New York: John Wiley and Sons. 2001