Global Information Assurance Certification Paper

Danger Within

Dennis Spalding
August 2001

GSEC Practical Assignment Version 1.2e

Dangers Within

"The attention given to hackers by the press is what gets the attention of upper management, and that's what they base their security purchases on. People need to be worried about the insiders because they know how to hurt the organization specifically, drastically and quickly [1]."

According to a recent survey conducted by NSC technology fewer than 10 percent of break-ins to IT systems come from external hackers[2]. This statistic though alarming mentions break-ins. The threats to a network come in many forms - from disgruntled employees, corporate espionage, lax system administrators, faulty products and poorly educated users. All of these fall into one of three categories: malicious attacks, misconfiguration (vendor or administrator), and user ignorance.

Malicious attacks

The malicious attacker is the individual or individuals that intentionally inflict damage to the network. This type of damage can consist of anything from releasing a virus, stealing information and poisoning data, to bypassing security controls to play games on the company's dime. According to the 2000 Computer Security Institute report a total of over $265 million dollars was lost due to security breaches. Almost 90% of the companies surveyed admitted to being hacked, yet only 25% of those reported that they had been hacked externally [3]. Nothing has brought this threat more to light than the recent incident involving 25-year veteran of the FBI Robert P. Hansen. Hansen is accused of using counterintelligence skills, computer programming knowledge and full access to government information over the last fifteen years to pass secrets to the now defunct Soviet Union. Hansen is every information security professional's worst nightmare. For a more detailed account of this incident go to [http://www.fbi.gov/majcases/hanssen/hanssenmaj.htm].

Misconfiguration

Another common threat to an organization's network from the inside is a simple misconfiguration of servers and firewalls - either from the manufacturer or the system administrators themselves. A system administrator's job is probably not envied by many. They have the responsibility to make sure patches are applied and systems are secure on a daily basis. Many times the system administrator does not find out about the possible hole in their system until after it is exploited, but sometimes that is not the case. This became evident in the recent Code Red worm I and II outbreak. The "Code Red" worm attempts to connect to TCP port 80 on randomly selected hosts trying to find a web server. If a successful connection to port 80 is made, the attacking host sends a HTTP GET request to the victim attempting a buffer overflow in the Indexing Service. Once this is done, it allows an attacker to run arbitrary code on infected machines giving them complete control over the server. According to the CERT advisory, in the first nine hours of the outbreak Code Red infected over 280,000 systems [4]. An article in

Network World magazine mentions how the Code Red II caused one major corporation to shut down their web services because the worm had infiltrated their Intranet [5].

Users

Users touch more systems on a company's network than any other entity in the organization. Users do the daily processing and perform functions that keep the organization running. Unfortunately they are not always aware of the risks involved with certain actions. For example, every time a user decides to insert a floppy to save or transfer data that they worked on while at home, they pose a risk of inadvertently infecting their system - and possibly the whole network - with a virus. Users are constantly downloading and running software from the Internet and unknowingly introducing viruses, trojans and other harmful code. A recent incident was the spread of the Melissa macro virus. The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment. When a user opened an infected .doc file in Microsoft Word97 or Word2000, the virus executed if macros were enabled. Upon execution, the virus first lowers the macro security settings to permit all macros to run when documents are opened in the future. Therefore, the user will not be notified when the virus is executed in the future. The macro then checks to see if the registry in HKEY_Current_User/Software/Microsoft/Office/Melissa has a value of "... by Kwyjibo". If that registry key does not exist or does not have a value of "... by Kwyjibo", the virus proceeds to propagate itself by sending an email message in the format described above to the first 50 entries in every Microsoft Outlook MAPI address book readable by the user executing the macro [6]. According to the MCERT analysis of this macro virus, human action (in the form of a user opening an infected Word document) is required for this virus to propagate. It is possible that under some mailer configurations, a user might automatically open an infected document received in the form of an email attachment. [6.1].

What to do?

Given all the issues that IT Security Professionals have to deal with from external attackers, they must also be ready for the internal issues. Though internal security issues may never be eliminated, there are some technologies and procedures that can minimize the potential damage they may cause.

Security Policy

Every organization should have a Computer Security Policy. Regardless of whether there are ten employees or ten-thousand, a well thought out security policy will help provide guidance in the protection of the network. The following is the SANS Institute definition of a Computer Security Policy: "*A security policy establishes what must be done to protect information stored on computers. A well-written policy contains sufficient definition of "what" to do so that the "how" can be identified and measured or evaluated".* [7]. According to the SANS Institute, A Security Policy should contain the following:

- Purpose
- Related documents
- Cancellation
- Background
- Scope
- Policy statement
- Responsibility
- Action
- Guide

Another good resource regarding Security Policies can be found at [http://www.sun.com/software/white-papers/wp-security-devsecpolicy/]

User Education

As with the Melissa virus much of the issues experienced by organizations could be prevented with simple user education. This doesn't mean talking down to users. Rather helping them understand that their actions really do effect the security and stability of the organization's network. Users need to understand that security is implemented for a valid reason. If users feel as if computer security is an unnecessary inconvenience, they WILL find ways to circumvent it. Educating users can also make them aware of non-technical attacks such as "social engineering." Social engineering can be regarded as "people hacking". Basically it's hacker speak for getting users to volunteer information unwittingly such as passwords and other security information. One of the most infamous cyber-criminals, Kevin Mitnick [8] was notorious for his social engineering skills.

Limit Authorization to Users and Groups

With the number of multiple users on computers and networks, it is a good rule of thumb to only give users access to what they need. This simple practice will save hours of troubleshooting and unnecessary incident response situations. Not only may this prevent "malicious" users from doing things outside of their scope of responsibilities, but may also prevent the "curious" users from unwittingly doing damage. One way to control this is Role Based Access Control (RBAC). Each user is assigned one or more roles and each role is assigned one or more privileges that are permitted to users in that role. Security administration with RBAC consists of determining the operations that must be executed by persons in particular jobs and assigning employees to the proper roles [9].

Authentication

Often times confused with authorization, *authentication* is the ability to verify that the person on the other end of the connection is who they say they are [10]. In a world of digital transactions, this process is becoming more and more important. Authentication can be broken into three factors:

1) Something a person has (smart card)
2) Something a person knows (password)
3) Something a person is (biometrics)

The more of these factors that can be used in conjunction with one another, the more trust can be placed in the authenticity of the individual on the other end of the login prompt.

Encryption

Encryption is used to ensure that only the intended recipients or owners of data are able to view that data. *Encryption* is the mathematical process of turning plain text (readable text) into cipher text (unreadable text) and visa versa. There are two main types of encryption, symmetric and asymmetric. Symmetric key or secret key encryption uses the same key to encrypt and decrypt data. This type of encryption, though very fast, has two main issues. As stated before, it uses the same key to encrypt and decrypt data. Foe example, if data encrypted in Dallas needs to be decrypted by someone in New York, the "key" or decoding secret needs to be shared between both places. The issue is how to transport that key securely. The other issue with symmetric key encryption is due to the algorithms used. These keys can be brute forced and used by an attacker to un-encrypt data. These two issues were solved in asymmetric encryption, also known as public key encryption. The term *public key encryption* is derived by the use of key pairs. One key is private (secret) and the other is public (known). In *public key encryption* data is encrypted with a "public" key and then decrypted with that public key's corresponding "private" key. The algorithms used generate the key pair such that the private key cannot be derived by attacking the public key thereby solving the brute force attack issue. In the example used above, the data in Dallas can be encrypted with the recipient's public key, sent to them in New York and decrypted with the recipient's private key. This allows secure transmission of the encrypted data without possible compromise of the decryption key.

Secure Socket Layer

Secure Socket Layer (SSL) is the secure communication between two devices. The SSL protocol uses a combination of public key and symmetric key to achieve the secure connection. The client sends information containing its SSL version, the ciphers it can use and some randomly generated data (a session key) to the server. The server then sends its information and its digital certificate back to the client. Using all the information exchanged, the client generates a symmetric key and encrypts that symmetric key and its digital certificate with the server's public key. This information is used by the server to generate an encrypted tunnel in which other TCP protocols can be passed, such as HTTP, LDAP and POP3 [11]. This technology allows for secure communication within an organization, by ensuring traffic can not be "sniffed' and that the server that is trying to be reached is indeed the intended server.

Public Key Infrastructure

Public Key Infrastructure (PKI) is defined as a system of Digital Certificates, Certificate Authorities and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction [12]. PKI has been touted by some security professionals as the "Holy Grail" of Information Security. PKI can combine all of the technologies above and incorporate them into a single infrastructure. PKI uses what is called "Digital Certificates" or "Digital IDs". Digital certificates are based on the concept of public key encryption. A digital certificate is made up of a public key signed by the root Certificate Authority (CA) or one of its Subordinate CAs. A Digital ID contains the owner's name, their public key, a serial number of the certificate, the certificate's expiration date and the root CA's expiration date. PKI uses a hierarchy to establish trust. This hierarchy consists of an implicitly trusted root Certificate Authority. This CA is at the top of the hierarchy and signs or verifies the validity of subordinate Cas, giving them Digital IDs. These subordinate CAs can be used for various types of functions. The function of subordinate CAs can consist of signing the following and making them Digital IDs:

- authentication Certificate Signing Requests (CSRs),
- SSL CSRs,
- Code Signing CSRs.

These Digital IDs can then be used to *authenticate* users proving they have the *authority* to execute certain tasks as well as providing them with the ability to encrypt and digitally sign data. As long as the root CA is still valid, anything under that hierarchy can be trusted. An excellent book on the subject is "Understanding PKI" by Carlisle Adams and Steve Lloyd (Macmillan Technical Publishing).

Conclusion

There will probably always be malicious attacks, viruses and worms, but there are definite ways to defend against them. Through the continued education of users viruses like Melissa and simple things like social engineering can be taken to a minimum. Though keeping up with patches and fixes can be a full time job in of its self it is critical to the safety of an organization's network. This holds true for the proper testing of system configurations as well. Nothing is worse than having to deal with a problem that could have been 100% prevented with just some simple configuration changes. Utilizing Role Based Access Control, encryption and strong authentication can help ensure that no one person holds the keys to the kingdom and only those with the proper "need-to-know" are accessing systems and data that they are authorized to see. With all the attention given to protecting the inside from the outside it's obvious that there needs to be the same intention given to protecting the inside from the inside. Anytime trust is given on the inside of the firewall there is always a danger to security. Not to say don't trust the users, they are what keep the company's running. Protect the users on the inside and in turn the organization is protected.

[1] O'Leary, John "The Enemy Within"5/08/2000
http://www.nwfusion.com/research/2000/0508feat.html;,

[2] "Survey: Hacking an Inside Job" August 6, 2001
http://www.zdnet.com/enterprise/stories/main/0,10228,2801830,00.html

[3]Tullet, John "Focus on Internal Security"
http://www.itp.net/features/99450469796016.htm

[4]CERT Advisory CA-2001-23 Continued Threat of the "Code Red" Worm July 26, 2001/August 23, 2001
http://www.cert.org/advisories/CA-2001-23.html

[5] NetworkWorld article august 13 2001

[6] CERT® Advisory CA-1999-04 Melissa Macro Virus March 27, 1999/March 31, 1999
http://www.cert.org/advisories/CA-1999-04.html

[6.1] CERT® Advisory CA-1999-04 Melissa Macro March 27, 1999 March 31, 1999
http://www.cert.org/advisories/CA-1999-04.html

[7] SANS GIAC Level One Security Essentials Study Guide

[8] Lemos, Robert Minick teaches "social engineering" Tuesday 18th July 2000
http://news.zdnet.co.uk/story/0,,s2080227,00.html

[9] NIST Role Based Access Control Last updated: 4/09/01
http://csrc.nist.gov/rbac/

[10] http://webopedia.internet.com/TERM/a/authentication.html

[11] Introduction to SSL
http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

[12] http://webopedia.internet.com/TERM/P/PKI.html