SECTION 9

Operating System Security Rules

This section addresses best practices for setting up security within operating systems. Authentication, file protection, virus checking, file sharing, network software, and security logging are discussed.

9.1 TRUSTED OPERATING SYSTEMS

Trusted operating systems have security features built into the operating system. The National Computer Security Center's Rainbow series Orange Book, *Trusted Computer Standards Evaluation Criteria* describes several levels of trust including C1, C2, B1, B2, and B3. Currently, there are no commercial operating systems that have been certified beyond B1. These B1 operating systems are used primarily by the government. To secure systems with any level of confidence, operating systems that are capable of C2 or B1 security should be used in your network environment.

9.1.1 B1 Trusted Operating Systems

B1 level trusted operating systems are considerably more expensive than C2 level operating systems because they are used in very selective markets. As the commercial segment begins to deploy these operating

systems in greater numbers, the price should come down. Currently, B1 operating systems should be used for government and military applications that need to transmit sensitive, but not secret, data and for commercial banking, financial services, and other commercial applications where security and confidentiality are very important.

9.2 AUTHENTICATION

✓ **INFOSEC Best Practice #68**

All server operating systems must have a minimum of a C2 level of trust.

C2 is a government designation for computer security that requires computers to have the ability to control access to the computer via usernames and passwords, and protect files by assigning ownership and access rights. Desktop operating systems are recommended to have at least C2 compliance to protect individual systems from unauthorized access. Without these features the data on a computer system is vulnerable to anyone having access to the physical system. Some versions of operating systems have most of the C2 features yet are not C2 compliant. This may be acceptable upon review of the missing features. Most systems such as UNIX and NT can be configured to meet C2 compliance. C2, however, is somewhat dated and has many limitations. Securing most server based operating systems will require going beyond C2 compliance with configuration and protection as specified in the Best Practices outlined in this manual. The government also has

more stringent security designations such as B1, B2, and B3. Mission-critical server operating systems may need to have B2 compliance. These security levels address the carrying of classification tags on all data. Data objects are tagged with a classification level such as secret, classified, confidential and unclassified. Access to these data objects is available only to other objects that carry the correct classification level. This type of classification scheme may also be applied to corporate data with differing levels of sensitivity.

✓ INFOSEC Best Practice #69

Username and password authentication must be used to access desktop computers.

Username and password authentication must be used to logon to server and desktop computer systems (Reference Green Book "Department of Defense Password Management Guideline" CSC-STD-002-85). Installing an operating system with this access control capability will allow the user to secure the computer when not in use and prevent illegal entry onto the system.

✓ INFOSEC Best Practice #70

Use one-time password generation hardware or software to authenticate users for access to systems with mission-critical data.

Systems that have sensitive corporate data must authenticate users with one-time passwords generated by handheld devices or software such as S/Key. S/Key requires that the remote host know a password that will not be transmitted over an insecure channel. When you connect to the host, you get a challenge response. The challenge information and password that you know plug into an algorithm that generates the appropriate response to the challenge from the remote host. The algorithm-generated response should match the challenge response if the password is the same on both sides. Thus, the password is never sent over the network, and the challenge is never used twice.

Hardware authenticators should be PIN/Synchronous and require keying in a PIN by the user to the authenticator device that then produces a password as a function of its internal clock. The user then enters the generated password into the computer system. This type of system authenticates the user in possession of the handheld authenticator and limits eavesdropping of passwords to non-network means. It increases security by requiring the user to know a password and additionally to carry an authenticator that usually has a limited distribution. Handheld authenticators should be kept in a secure area and issued to people only when they need to use the system and then returned after use. As an alternative to the handheld authenticator, a smart card can be used which requires entering a PIN into the smart card followed by generation of a one-time password. Interaction with the computer takes place via a smart card reader that doesn't require the user to enter the generated password. This may be done at initial login only, if multiple personnel use the machine.

✓ INFOSEC Best Practice #71

Use biometric authentication for systems that hold highly sensitive information.

Some systems with very sensitive or government classified data may require the use of a biometric device as the first step in a multilevel authentication process. A biometric device requires authentication of the user by scanning a physical attribute as proof of identity. Examples of biometric devices are fingerprint, retina scanners, handprint, and facial feature devices. These devices are all coming down in price, which make them more attractive for a variety of applications. This type of authentication requires the individual's presence and cannot be circumvented as easily as stolen smart cards or passwords.

As an example, a smart card can hold information about a person such as fingerprint, photo, and other identifying information. When a user desires access to a closed area or to a computer, a smart card is scanned, the fingerprint is scanned, and compared to what is on the card. If there is a match, then access is granted. Photos and other descriptive information are useful when there is a human guard that provides another level of check. This is useful for very secure environments such as airports.

✓ INFOSEC Best Practice #72

Expire passwords after a designated period of time.

Your corporate security policy should specify a schedule indicating how often each user's password must be changed. This schedule must be incorporated into the security policy for user accounts so that all user account passwords expire after a designated period. It is very important that user accounts *not* have a "never expire" flag set. Users do not want to change passwords often and system administrators do not want to be bothered about password expiration problems. Therefore, setting a sensible expiration password expiration policy increases the security of your system. Examples of periods often used for password expiration are 60 days and 90 days. The policy for expiration must be linked to the type of environment within an organization. For example, if there is a large turnover of personnel or temporary accounts that are granted on the system, then the expiration of passwords should be shorter as compared to systems with relatively few accounts and no organizational turnover.

✓ INFOSEC Best Practice #73

Use "pass phrases" or a mix of letters and numbers for passwords.

Passwords must NOT include the following:

a. a portion or variation of an account username,

b. a portion or variation of your real name, address or phone number,

c. words or variations of words in a dictionary,

d. words or variations of foreign words,

e. words spelled backward,

f. repeated character strings,

g. only numeric digits,

h. only alphabetic characters,

i. passwords less than six alphanumeric characters.

The weakest point in security is usually the password. People choose short, easy-to-remember passwords that they do not change often. Passwords must ideally consist of a mix of characters and numbers interspersed in a long cryptic sequence (i.e., k3k5k*&eklx!!!i0). This is too difficult to remember, therefore using a long phrase that is meaningful to you personally is a good alternative. This may be a code which has meaning for a user, such as "My real age is 43" or "I have 6 pointy-haired bosses."

✓ INFOSEC Best Practice #74

Check passwords against a password history file.

Sophisticated operating systems such as UNIX and Microsoft NT contain a user account option for maintaining a history of used passwords. The program will not let a user reuse an old password for a designated period of time. Therefore, the user must use new passwords that nobody else will know or remember.

✓ INFOSEC Best Practice #75

Enforce a minimum password length of at least six alphanumeric characters.

Most user account management programs allow the administrator to enforce a minimum length for a password. The longer the password, the less chance that a password cracking program will find your password. Most password cracking programs generate combinations of letters and numbers to create a password that is used to try to break into an account. The longer the password and the more characters that are used, the more difficult it is to crack it. A seven-letter word has 24^7 combinations, if letters are used, and 34^7 combinations if both letters and numbers are used. Each of those passwords has to be tried against an account on the system. However, it is possible that the password program will generate your password early in the password generation process. Using a phrase for your password makes it difficult to crack your password.

✓ INFOSEC Best Practice #76

Automatically disable the user account if there are more than six bad login attempts.

An attack on a user account will use a program that generates passwords one at a time against a user account until it successfully logs into the system. This usually requires many passwords to be tried, unless a common password is used. Most operating systems have an account

security feature that can be set by the system administrator to automatically disable an account after a designated number of login attempts. This flag is often set to disable the account after about six unsuccessful login attempts. It is highly unlikely that the user will enter their password incorrectly that many times. When the account is disabled only the administrator will be able to enable the account again. If an attack is actually occurring, the administrator must change the user name of the account and make sure the user selects a satisfactory password. A message must be sent to all users on the system warning users that attacks are occurring on the machine and that their passwords may have to be changed to comply with security guidelines.

✓ INFOSEC Best Practice #77

Use Kerberos authentication in highly vulnerable environments.

Kerberos is a network security protocol that uses strong encryption and a complex ticket-granting algorithm to authenticate users on a network and to allow encrypted data streams over an IP network. Some TCP/IP communication protocols such as FTP and TELNET transmit user IDs and passwords in clear text. Kerberos is a good solution in environments such as universities where other security mechanisms are difficult to implement and enforce and where the environment needs to be open. It is difficult to set up, but is becoming more ubiquitous and will be distributed in conventional operating systems.

9.3 ACCOUNT SECURITY

✓ INFOSEC Best Practice #78

Do not disclose a computer's identity until login is completed successfully.

Set up the operating system so that the system login screen does not identify the computer system by name or function until after login is complete. Unauthorized personnel do not need to know the identity of machines unless they need to use them. Hackers find this type of information valuable since it may identify valuable targets to break into.

✓ INFOSEC Best Practice #79

Use an automatic password generator to help the user with password creation.

The more constraints your security policy puts on creating an adequate password, the more trouble users will have in creating passwords. This may lead to frustration and complaints. To help the user in choosing a password, some account management programs have an automatic password generator that will produce a password according to your security policy criteria. The drawback to using a password generator is that it can create cryptic passwords that may be difficult to remember. Enabling this option, however, will at least provide some help to frustrated users. *Emphasis should be put on choosing your own creative passwords that you can more readily remember*.

✓ INFOSEC Best Practice #80

The password file must be encrypted by the operating system.

Passwords are encrypted by most operating systems. If you are using an old version of an operating system that does not encrypt passwords, upgrade to a newer version of the operating system or modify the login procedure to run your own program which reads a file encrypted by your own method. Storing passwords in a file on your system that is readable by everyone gives you no security and WILL lead to unauthorized access to your system(s). The password file should be modified only by the system administrator.

✓ INFOSEC Best Practice #81

Restrict access by time of day for high-risk users.

Some users such as part-time employees, temps and consultants may need to be given restricted access to a system only during business hours because they may be considered to be more risky employees. Most operating systems allow the system administrator to set time restrictions on an account based on time of day.

✓ INFOSEC Best Practice #82

Audit all login attempts and set alarms for repeated incorrect logins.

Keep security logging turned on and check the security log daily. The log will be able to tell the system administrator what is happening on the system and network. Suspicious activity may require more detailed monitoring with a sniffer, increased security protections, and notification of users. This may prevent or diminish the extent of damage if there is an attack on your system.

✓ INFOSEC Best Practice #83

Encrypt passwords that are transmitted over a network.

Authentication of users over a network typically involves sending a password to a file server in clear-text. Therefore, the password is detectable by any sniffer monitoring the network. When choosing an operating system be aware of this problem. Depending on your security policy, you may have to provide third-party mechanisms that encrypt passwords during authentication (e.g., Kerberos authentication, RSA MD4).

✓ INFOSEC Best Practice #84

Create an alternate administrator or system account; do not use the default.

The system account is one of the accounts that is typically attacked by a hacker. Disabling interactive access to it and using another account

as the administration account will force the hacker to find another legitimate username. Do not delete the system account since it may be needed by various system functions. Finding a legitimate username may not be difficult because most companies use very similar username naming conventions (e.g., gsmith – first letter of first name followed by last name, smithg – last name followed by first initial, etc.). Other accounts such as the guest account should be disabled and substituted with a less obvious account name. Other default accounts that should be disabled and substituted with new site specific accounts are field maintenance, testing, and database administration.

✓ INFOSEC Best Practice #85

Do not permit users to log on locally to a server.

If users other than an administrator have physical access to a server, then there are a number of things that they can do to try to break into the machine. Keep servers physically secure and do not permit local logon of users other than the system administrator. Some systems differentiate a local account database and network account database. Users should be authenticated onto the network using a network accounts database, not a local accounts database.

✓ INFOSEC Best Practice #86

Use a password to access BIOS setup.

To prevent users from getting around some of your security by booting an operating system from floppy disk, disable booting from floppy in BIOS and password protect your BIOS if your computer allows.

✓ INFOSEC Best Practice #87

Use a screen saver with a password.

When stepping away from your desk for a short period of time use a screen saver that kicks in after a few minutes of idle time and locks your computer with a password. This will prevent users from browsing your computer when it is unattended.

✓ INFOSEC Best Practice #88

Log off the computer when you are finished using it.

In order for your operating system security to have effect, log off your computer when you are done using it at the end of the day or if you will be away from your desk for a longer period of time.

✓ INFOSEC Best Practice #89

Do not keep copies of passwords for system access or decryption on the same machine that uses the password.

It is a good practice not to keep password lists on computers, but if it is necessary, then the password(s) must not be kept on the same machine that uses the password for access or decryption. Hackers look for files containing passwords that can gain them access to other machines, so don't make it easy for them.

9.4 FILE SYSTEM PROTECTION

File system protection is the next logical step in securing an operating system for use by multiple users. This is considered to be one of the key security requirements for C2 security. A poorly protected file system allows hackers or unscrupulous employees to gain access to files and data that may contain sensitive information.

✓ INFOSEC Best Practice #90

System administrators must have full access to all files.

Since system administrators are called upon to help users with a variety of problems, they must be able to get at user files. This makes it important that system administrators be chosen carefully for their trustworthiness. Often system administrators are chosen strictly for their academic and experience qualifications, but they should also be evaluated on their background in terms of trustworthiness. The system administrator can be the biggest security threat to the organization if not chosen wisely. Perform background checks on system administrators.

✓ INFOSEC Best Practice #91

Limit remote server administration to the system administrator.

Remote administration of servers is becoming a necessity in many organizations given the proliferation of servers and the reduction in information systems staff. Often, system administrators are required to administer more than one system for many departments within the organization. Remote administration allows the system manager to manage remote systems that are spread out throughout the organization without being physically present. Remote administration helps the system administrator be more efficient at the job and to solve problems quicker. Also, if there are local pseudo-system administrators that take care of the day-to-day tasks, then they may inadvertently have access to more machines within a domain than desirable. Often for convenience reasons, security is relaxed and the system administrator divulges the password for remote administration of some of the machines either by pressure from departments or just for convenience. Under this pressure the system administrator may divulge the password to solve a near-term problem, but in turn opens up a long-term security hole. To maintain security and not cave into the near-term pressures of any department, you must refer back to the official corporate security policy approved by the administration.

✓ INFOSEC Best Practice #92

Perform server administration at the console.

If system administration activities are taking place at the system administrator's office, then people can walk into the office and potentially see passwords, file protections, sensitive data, etc. Also, the system administrator may leave momentarily without securing the computer and thereby allow privileged access to the system. Therefore, system administration activities should preferably be done in a restricted area.

✓ INFOSEC Best Practice #93

Set file access rights for groups of users.

All files must be accessed using group access rights. Individual users must belong to groups. Groups can be organized in a hierarchical group structure. Files must not have rights associated for individual users since it is difficult to track, clean-up and change files distributed throughout the system. If a user should not access a file, then that user's account should be transferred to a more restrictive group. Cleaning up file protections becomes much easier.

✓ INFOSEC Best Practice #94

Restrict network file access by network share permissions that are granted on a need to use basis only.

Files accessed via a network connection on virtual drives must have network file access permissions. This is another layer of security on top of file protection. Network access of files on a virtual drive must be

group controlled. Both network share permissions and individual file permissions are used to restrict access to a file. This multi-level access control is very important because there are many users on an organization's entire network, including the internet, that may have access to virtual file services. Virtual file services on single user operating systems such as MS Windows 98 should be protected with passwords. An example of virtual file services are NFS (Network File System) a UNIX based system which has also been ported to Microsoft NT and 95, and Microsoft NT's network shares using SMB (System Message Block) communication.

✓ INFOSEC Best Practice #95

Set default file protection to be as restrictive as possible.

When installing a new operating system, the system administrator must first protect the entire file system for his own access only, and then incrementally open directories and files to those users with a need to access. Some operating systems have default protections open to everyone. The system administrator should not rely on defaults, but secure the system according to his or her own file protection best practices. Set file permissions for system administrators to full access (i.e., Read, Write, Execute, Delete, Change Ownership, etc.), but selectively restrict access for users based on their type of access needs. If a user only needs to execute a file, then give the group that the user belongs to "Execute" permission only. If a user should have the option of editing a file, provide "Write" access. Any combination of permissions may be given, but should be as restrictive as possible.

✓ INFOSEC Best Practice #96

Prevent users from viewing all directory names down a directory tree.

All directory names in a directory tree should not be seen by those users that do not have a need to access files at that directory level. The user should not have the option of exploring directories throughout the system in order to get clues to the type of information that is stored within those directories. Therefore, set permissions on directories so that users can have access down a directory tree without seeing the name of unauthorized directories. For instance, the higher up the directory hierarchy a user goes, the closer the user is to system related directories.

✓ INFOSEC Best Practice #97

Use access control lists to restrict access to files by individual users.

To further restrict access to files by a specific user, use access control lists to specify the type of access a user can have for a particular file. Even though a user may belong to a group that has full access to a file, an access control list can restrict a user specifically. When a user attempts to access a file, the operating system checks the user's access tokens to determine if any further restrictions found in the list should apply.

✓ INFOSEC Best Practice #98

Clean the swap or page file before releasing a computer to another party.

If a computer is reassigned to another user and it had originally stored sensitive data, then clean the swap or page file on the system. The swap or page file may still contain sensitive data that was paged out of physical memory to the pagefile on disk. There are software programs available that clean these swap or page files.

✓ INFOSEC Best Practice #99

Do not install more than one operating system on your computer.

If a less secure operating system is installed on your computer, then access can be granted by booting the less secure operating system. Also, do not have multiple versions of the same operating system for the same reason. Usually, the most current operating system is the most secure. This does not apply for developers working on projects requiring multiple operating systems.

9.5 VIRUS PROTECTION

✓ INFOSEC Best Practice #100

Use a virus scanner on every computer.

There are approximately 100 new viruses created every month. If you exchange files with other users or are connected to the internet, then you are susceptible to viruses. Even software officially distributed by vendors has been known to contain viruses. Since viruses can immobilize your computer and your productivity, destroy files on your system, and even damage the hardware on your system; it is imperative that virus protection be deployed on every computer. Viruses often create unusual, hard to duplicate symptoms that are different to diagnose. The user often does NOT guess that the cause may be a virus because the symptoms appear as if there may be a bug in the program or that the user is doing something wrong. Countless hours are lost trying to fix the problem or work around it. The best protection is to immunize the system with a virus scanner.

Each server must have virus-scanning software that scans any files from external sources. Anti-virus software must scan all incoming IP traffic from the internet, including incoming email and have support to scan some of the more common word processing files and macros. Also, if the server is used to backup any remote machines, the backup software should have a built in anti-virus scanner to scan files before being backed up. A backup report should note if viruses were found.

✓ **INFOSEC Best Practice #101**

Perform virus scanning of all IP packets at the bastion hosts and the gateway.

Scan all IP traffic coming into the site for viruses before it is sent to any machine on the internal network. Scanners should pick up most viruses if their databases are maintained on a monthly basis. Macro viruses embedded in word processing or spreadsheets must have virus scanners that can detect these types of viruses.

✓ INFOSEC Best Practice #102

Download the latest virus signatures for your virus scanner software every two weeks.

Since there are so many new viruses that are created each month, anti-virus software may become obsolete in a relatively short period of time. When you purchase anti-virus software you are usually entitled to download copies of the newest virus databases from the vendor's internet site. The vendors usually update their virus databases a couple of times per month. It is recommended that the user copy the software from the vendor's internet site to make the anti-virus software current and effective against the newest viruses. Most virus scanners have the capability of automatically downloading updates and virus signatures on a set schedule. System administrators and users often forget this task, therefore an automated download method should be used. Alternatively, it is recommended that the system administrator maintain the latest virus signatures on a server and that users have their PCs configured to directly access these files. The system administrator can also push these files down to user PCs. Do *not* get secondhand copies of the anti-virus databases; use the databases from the vendor directly.

✓ **INFOSEC Best Practice #103**

Perform virus scanning of each machine on a designated schedule.

Install the anti-virus software so that it starts when the system boots and is resident in memory when the system is running. This will provide continuous monitoring for viruses that may arrive at the computer either via floppy disks, mail, or the internet. A virus scanner will not guarantee a virus-free computer, but will significantly reduce the chance of a virus being present. Occasionally, some programs are incompatible with the anti-virus software. If this is the case, you must run your anti-virus software manually on a regular schedule once a week. Servers must be running anti-virus software continuously.

9.6 NETWORK FILE SHARING SECURITY

Most network file systems have some type of security weakness. The administrator must be aware of these problems and decide between the convenience of having network file services and the security holes that may be open when these services are used.

✓ **INFOSEC Best Practice #104**

Do not have virtual file services enabled for bastion host machines.

Virtual file services can be a method of accessing multiple machines once a single machine is compromised. Especially, do not have file services across your firewall. The firewall will need to have a port(s) open for that service and thereby provide a hole for entry into your internal network.

✓ INFOSEC Best Practice #105

Deploy NFS on an internal network, separated from a public network via a firewall.

If you need to use *NFS* (Network File System), then it must be deployed on an internal network because it uses simple clear-text authentication (e.g., host name user ID and group ID). This may be barely acceptable in secure networks where there is limited access to the network, but is not secure on public networks. UNIX systems will typically use this network file system to share files between users and to set up virtual drives for users. If NFS is to be used in an organization, then it should at a minimum be deployed behind a firewall separating the internal network from an external, public network. To increase security when using NFS, but with a performance decrease, use Secure NFS which uses Secure RPC and AUTH_DES encryption.

✓ INFOSEC Best Practice #106

Do not use X-Windows for mission-critical applications over a public network.

X-Windows cookies are transmitted over the network in clear text. Therefore, applications with sensitive data must not use X-Windows for network-based windowing on a public network.

9.7 NETWORK SOFTWARE

✓ INFOSEC Best Practice #107

Strictly control IP assignment.

One of the key pieces of information for a hacker is knowledge of the IP address ranges within an organization. Additionally, knowledge of the exact IP address of servers and other mission-critical machines can help a hacker focus an attack on these systems. IP addresses can be obtained by buying a block of addresses from Internic or from an organization's Internet Service Provider. Addresses can be bought as class C licenses (256 addresses) or class B licenses (32,000 addresses). Class B licenses are usually reserved for service providers and large companies. There are very few class B licenses around and they are very expensive. Almost all companies will purchase Class C licenses as blocks of 256. If there is no connection to a public network using IP and there are no plans to hook into such a public network in the future (highly unlikely), then the company can use their own IP addresses when setting up systems. Also, if firewalls and proxy servers are used to separate the internal network from the public network, then all the systems internal to the company do not need legal IP addresses since the proxy server will use its own address to communicate with the public network. Most companies buy blocks of legal licenses because they do not know how they might want to commu-

nicate in the future and therefore do not want to have to reconfigure their computers with new IP addresses. You must have legal IPs if you have any machine connected to a public network. Home PCs and small offices will get their IPs through their service provider.

✓ INFOSEC Best Practice #108

Use host to host authentication between two logical networks.

Operating systems currently do not use security protocols to establish host to host links to mail servers or file servers. By not having authentication software that can determine whether the host you are connecting to is really who it claims to be, the user is vulnerable to an attacker that is mimicking the destination host. Kerberos V5 should be used between two hosts that need to communicate for server based applications. Kerberos 5 is a server-based authentication mechanism that: 1) receives a message containing a user's username and current time encrypted with the user's password, 2) looks up the username to determine the password and, 3) tries to decrypt the encrypted time that was sent. If the Kerberos server can decrypt the current time, then it creates a ticket granting ticket containing a session key and ticket for the Kerberos Ticket Granting Service, encrypts it with your password and sends it to you. In this way the user's password is never transmitted across the network and public key cryptography is not used.

✓ INFOSEC Best Practice #109

Start up processes only for desired TCP applications.

Each process (daemon) that is running, but is not used is a potential vulnerability to the system. TCP/IP services such as FTP, Telnet, and others use TCP ports to communicate over the IP network. Potential hackers can try to access these ports and exploit the vulnerabilities of these TCP programs. Also, custom applications and database applications use specific TCP ports for client-server applications. These custom written programs may be more vulnerable than hardened TCP applications and provide a potential point for break-in to the machine. If these programs are running from an administrative account, then the hacker may have full access to the machine. To reduce the risk of potential break-ins through TCP ports, only run those TCP applications that you must use on the machine.

9.8 SECURITY LOGS

✓ INFOSEC Best Practice #110

Keep a security event log on your computer.

A security logger should be available as part of the operating system or as a third party product. All servers and workstations with restricted access must run a security logger. The security log must be turned on and record the following categories of events:

1. Logins and logoffs.
2. Object access (logging this data may lead to very large log files).
3. File permission changes.
4. File ownership changes.
5. Security policy changes.
6. Changes in user rights.
7. Group changes for an account.
8. System restarts and shutdowns.
9. Virus scans.

Security logs can grow to take up much disk space therefore the server must have a large enough disk. Periodic maintenance will need to be performed to archive or discard the logs.

✓ INFOSEC Best Practice #111

Review the security log on each server on a daily schedule.

Recording security events is a waste of resources if the system administrator does not review the logs on a daily basis. All it takes is five minutes each day to invoke the security log viewer and scan through the recorded events. Since most machines will have little hacker or mischievous activity, system administrators get complacent and stop reviewing the security log. If the machine is important enough for you to decide that security logging must be turned on in order to

comply with your established security policy, then the administrator must treat this task seriously. To ease the tedious nature of this task, there are security monitors available for some operating systems that review the security log automatically according to your designated criteria and issue an alarm about potential security breaches. There is a cost involved in purchasing such software, but it may help in enforcing the security policy at your organization.

✓ INFOSEC Best Practice #112

Archive all security logs.

Security logs should be archived on a periodic basis (i.e., yearly). Keeping archives will allow you to go back and check for suspicious activity (e.g., file and object accesses) that occurs on the system over time.

✓ INFOSEC Best Practice #113

Record security events on your firewall.

Your firewall computers must have security logging turned on. Firewall software has its own security and network event logging which must be turned on in addition to operating system security logging.