Global Information Assurance Certification Paper

System Administrator – Security Best Practices
Harish Setty

Introduction:

System Administrators are the people responsible for making computers work in the field. They are also responsible for the uninterrupted operation of the computers to take care of the business needs. System Administrator's knowledge on System security loopholes and their implications on business they are managing, is a good asset to any Enterprise/Company. By following simple practices during their administrative functions, they can build secure systems. These also help in reporting security incidents at an early stage and take corrective measures. Some of the best practices are discussed here, without getting into specifics of any particular operating system or version.

Knowledge update:

Know more about security of the systems you are administering. Read appropriate security bulletins available from the vendors, user groups and security institutes on a regular basis. Subscribe for security bulletins from vendors and security advisories. Generally at the vender site you can get the information on known security bugs of their systems and possible solutions. The solution may be a configuration change or applying a patch or some times a hardware issue like replacement/upgrade. It is also important to understand each security issue with relevance to your configuration and environment. Keep track of the changes on the systems, network and business needs, which may impact system security you are administering.

System and Console - Physical Security:

- The system console should be physically protected. Make sure to install systems in a secured location where only authorized personnel are allowed. If there is physical access to system console and the computer, it is easy for anyone to break-in or misuse. Most of the systems have back door entry or procedure to break into the system, using the console. In fact, this is an essential feature to break into the system when the superuser password is lost. Secure your console from some one keep guessing superuser password at the console.
- Machines need to be physically secured always. A person can simply turn off, if one has access to it. If one access to the console, he/she can interrupt the boot process and gain access. Some times it may be like booting from a floppy or CD etc. You should be cautious even if you are installing a system for temporary use or testing, before moving to the planned secured location. There is a chance that some one can misuse the system. If a hacker gains access to a system for a short period of time, he can misuse the opportunity to come back later, unless you detect and patch the hole he has made.
- Do not leave console logged in at any point of time, if you are away. Make a practice

to logout every time after completing your job.

- If your system supports timeout feature for system console, configure it. When you forget to logout, it will be timed out.
- System administrator's terminals or the terminals used by administrators are of high risk if they are not secured. If any intruder breaks into system administrator's terminal, there is a chance of getting access to multiple systems. System administrators generally have the habit of keeping multiple sessions/windows to different systems simultaneously to carry out administrative tasks. These terminals should be located in secured area. As an administrator, make sure to logout from your terminal or lock your screen when you are away from your terminal.

Keep your systems lean and mean:

Maintain your systems and servers with minimum services and packages possible. The more services and applications you are running, the greater risk of exposing the system for any exploitation of the system.

- During Operating System installation, try to minimize the components/packages. Install only essential components, which are required for running the services and applications, for which the system is intended. Always you can add additional components when they need for running additional services and applications. Similarly when ever you remove an application or a service on a system, remember to uninstall operating system components, if they are not used by other applications.
- Remove any extra service running on the system, which is not being used. Procedure for turning off a particular service varies depending upon the operating system and administrative tools you are using. Some times it may be turning off a particular switch in GUI or editing /etc/inetd.conf file, etc.
- Close unused TCP/UDP ports. Any open TCP/UDP service offers an attacker a possible entry into your system. Having any port open that is not absolutely necessary, then, should be avoided. Procedure to verify the open ports depends on the Operating System you are administering. Some of the procedures are checking the configuration files, using netstat utility, using port scanners, etc.

Superuser Password:

System Administrators should be very cautious about root password or Administrator password.

- Use lengthy password. More characters are better as long you can remember and the operating system supports.
- Make password easy for you to remember and hard to guess for others and use non-dictionary words.
- Never store password as plain text or write down on paper. Use encryption utilities if you have to store in a file for some reason.
- Use mixture of upper and lower characters.
- Insert punctuation marks or symbols like {, ^, #, @, $ etc.

- Configure password-aging feature, if available in the operating system. Minimum age and Maximum age has to be decided, depending on the environment.
- Use shadow password feature, if available on Unix systems. This will prevent some one who try to gain root access using a cracker, if encrypted passwords in /etc/passwd file is readable. Cracker is a program/utility, which could methodically test each encoded password in the file against their dictionary of commonly used passwords.

Delegating superuser tasks:

Some times you may need to give users the ability to use or access privileged commands. It is not a good idea to give complete privilege to the users. Instead you have to limit the permission to the tasks or commands they suppose to run. If the operating system you are supporting is trusted, you can take advantage of this feature. Assign appropriate privileges to the required users. HP, IBM, SCO offer trusted operating systems, developed by SecureWare in addition to their standard Unix variants. In some Operating Systems, you have to enable this mode, as default may be non-trusted mode.

If the operating system is not trusted, you may have to share the super user account or you have to give superuser password temporarily. Generally in Unix systems administration privileges are all or nothing. Here is a risk that someone will abuse his or her superuser status, the superuser account. When someone logs in as Superuser using the superuser password, it is impossible to trace an act of misconduct based on who logged into the computer. If the root account is a shared account, more number of people will have superuser privilege. In that situation, the more anonymity any one person has to abuse the system. In these situations, you may use sudo (Super User DO) utility. Sudo is a public domain program, which provides a flexible solution for delegating superuser privileges. You can give partial or complete root privileges to particular user. Also it logs every time these privileges are used.

User Passwords:

Good password scheme/policy is one of the basic security measures to prevent unauthorized access. However, setting up a policy on paper and encouraging your user to adhere to the policy will be difficult. Because most users want to have a password which is easy to remember and don't want to change. When you are managing user accounts, certain policies can be implemented so users have to follow them. The exact policy, which you can enforce, depends upon the operating system and version and business need.

- Password Aging: Setting password aging policy allows you to enforce the user to change his/her password periodically. You can define the minimum age, maximum age for user to change his password.
- Minimum Length: Enforce a minimum length of password to at least 6 characters.
- Non-dictionary words: If the operating system supports this feature, user is not allowed to select any password as a word from standard dictionary.
- Password Uniqueness: The Password uniqueness setting allows you to specify the

number of new passwords that user must select before they can reuse one that they have used previously.

- New Password: In some environments, you can set minimum number of characters should be different in new password from the previous password, when user tries to change password.

User Terminals:

- Unattended user terminals or when the user is away from his desk, there is possibility of misuse, by some one. If the terminals support timeout or screen lock out feature, implement it. It is basically locking the terminal if the terminal is idle (no keyboard activity) for certain period of time. When user comes back or wants to continue working, he/she has to unlock the screen or terminal with password.
- Set password lockout feature, if the operating system is capable, or use any utility. Here the user terminal or user account will be disabled after a set number of unsuccessful login attempts. This is a simple measure to protect against someone who keeps guessing password. You have to decide the parameters judiciously.

Restrict Users:

- If users of the system are not logging in from the console or terminals connected directly to the system, you have to be more cautious. You have to configure your systems to accept connections from only known I.P Addresses. In case you have to allow dial-in access to your users, you should have additional level of security like RADIUS or allowing only known telephone numbers etc. In some situations like web servers, this may not be practical. Then, you have to restrict by other means like passing user connections through firewall or VPN etc. If possible, it is good idea to restrict users by their source IP address or the time slot they are suppose to work on the system. This is an additional level of security for your system. Some of the operating systems have built-in features to enable this kind of restriction. If these features or not available, you may have to use additional tools and utilities like tcp wrappers, ssh etc.
- If the Operating System allow you to control user's environment, make use of it. For all common users, unless required, do not provide more access to the system resources than he/she suppose to do. To name a few, allowing application users only to log in through the application window (no shell or telnet access), configuring Restricted Shell for ordinary users etc.

User Education:

System administrator is the first level contact for users in the organization for system support. (Some times it is help-desk person). It is good idea for a System Administrator to educate users and help-desk personnel about basic security issues and practices to follow, either formally or informally. This will help in building secured systems. It is advantageous if the users are aware of the security issues and implications. Some of the best practices for users are, not to leave terminal logged in, not to share password with

some one, changing password periodically, not to write down password on paper, to use non-dictionary words for passwords etc. As a System Administrator, you will be aware of specific things in your environment, to educate users.

Keep your systems up to date:

Security patches from the system vendors can close most of the known security holes. Also called as Service Pack in some cases. After applying the latest security patches, you should stay update for new release of patches from the vendors of your systems. Whenever new security patch is available, you should carefully study the details of vulnerability and its impact on your systems and environment. Depending upon the risk you may decide how soon you have to install/apply those patches, because some times applying patches involves down time of the systems. Subscribing to vendor's patch release bulletins and having support contracts with vendors is one way to make sure to get latest information automatically.

You may adopt different strategies when applying security patches suitable to your system infrastructure. One method is to apply each and every security patch available to your operating system and applications you have. Other method is to verify the need of a particular patch to your system and install if required.

Vulnerability Testing:

Prevention is better than cure. As a System Administrator, if you are aware of the vulnerabilities, you can take corrective action, before some one exploiting them. There are many security vulnerabilities that are specific to the operating systems. There are tools available which scans the system and report security problems. Periodically scan your systems using appropriate tools like tiger (for Unix), WebTrends (for NT), etc. After getting the report, you have to analyze each vulnerability; about it's impact in your system environment. If it security risk is serious, take corrective action immediately. Otherwise you can plan for an earliest time slot, if the corrective action requires scheduled downtime of the system. And also scan the system after fixing the vulnerability to make sure. Many of the tools report each vulnerability with explanation and recommendations for corrective action.

Monitor your systems periodically:

Maintain system logs on your system, particularly if it is multi-user or networked. Configure for logging maximum information possible and also for a reasonable period of time. Depending upon the Operating System, the procedure may be as simple as touching (creating) a file or some times installing additional components of the Operating System. In some environments it may be installing and turning on audit subsystem, etc. Having huge amount of logs, can any we read these large files always? The remedy is to use Log Analyzers. Some Operating Systems have built-in Log Analyzers or audit tools. If not, use additional tools. Basically Log Analyzers are programs that read log files and reports

the summary or statistics either in graphic or tabular form. You can also use these tools for analyzing trends on your system, sending pre-defined Threshold Crossing Alarms, Login attempts and failures etc.

Monitor for any unauthorized modification of system files and configuration files. You may use scripts or tools to see any files being created/deleted or permissions and ACLs being modified. Here the primary idea is to build a database of, file size, file permissions, digital signature, number of files etc, on the file system. Keeping this as a reference, compare these attributes at a later date, for any change. If the change is genuine and authorized, it is fine. Other wise you have to investigate it further. Tripwire is one such tool, available on most of the Operating Systems today. Tripwire checks to see what has changed on your file system and give an extensive report. The program monitors key attributes of files that should not change, including binary signature, size, expected change of size, etc.

Configuration documentation:

It is a good practice to document any change in the system configuration either hardware or software. This is very helpful in situations like disaster recovery, detection for an intruder, trouble-shooting etc. If you have several System Administrators, it is more important to have every thing documented. It is recommended to maintain additional copy of the documentation on different machine or as a hard copy.

Backup and Disaster Recovery:

In spite of reliable hardware, software and administration, there are times when systems crash or fail. The failure may be due to hacking also. Always good system administration involves reliable backup and recovery procedure. Depending upon the business need, you have to plan backup procedures. You may use built-in backup and recovery tools in the Operating System or dedicated software from a different vender. Some times you may require, an additional hardware for backing up the data.
Some of the important facts to consider while planning backup are,

- How frequently you have to back up data and what is the best time to backup
- How much data to be backed up
- Off-site storage of the data in case of catastrophe
- How long the backup data to be stored
- Security of the backup data: Backup media should be stored in a secured place. If the data is stored on-line, securing the data from a hacker/intruder is equally important.
- Good documentation for backup and recovery procedure

Many of the considerations depends upon the business need and the corporate goal. Any backup and disaster recovery plan/procedure is not complete unless it is tested. Periodically you have to test if the data recovery is working. When you are planning for backup and disaster recovery, basic rules are, how fast you have to rebuild the system to the latest working state, if the entire system is destroyed and how much data you can

afford to lose.

Conclusion:

As information infrastructures and Internet became more complex and larger, it also became critical to maintain systems up and running all the time. Though the system administration tasks became easier in recent years, system administrators need to be more updated on the systems and networks they are managing. In recent years, as systems are exposed to Internet, there is increased challenge on the System Administrators to maintain these systems and protect from hackers. If the System Administrators are more security cautious and follow good practices during routine administrative tasks, we can have secured systems. This also helps any organization to be prepared in the event of any security violation or disaster.

References:

1. Seifried, Kurt. "Linux Administrator's Security Guide". URL: http://www.ibiblio.org/mdw/LDP/lasg/
2. Albano, Daniel. "The Challenge of Computer Security", September 1996. URL: http://www.magi.com/~mmelick/it96sept.htm
3. "Top Ten Best Practices for Unix System Administrators", March 11 1999. URL: http://www.more.net/security/unix10.html
4. Kessler, Gary. "Security Tools For Windows NT Networks", April 1999. URL: http://www.garykessler.net/library/nt_security_tools.html
5. Allen, Julia. "The CERT Guide to System and Network Security Practices" Addison Wesley. 2001.
6. Beale, Jay. "Tripwire – The Only Way to Really Know". URL: http://www.securityportal.com/topnews/tripwire20000711.html
7. "Managing Root Access with Sudo", November 25 2000. URL: http://unix.about.com/library/weekly/aa102500a.htm
8. "What are the major differences between trusted and non-trusted systems?" URL: http://www.faqs.org/faqs/hp/hpux-faq/section-66.html

Last Updated: July 22nd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor