System Administrator – Security Best Practices

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, Key without getting into specifies of any particular operating system or version.
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.

STEPS/PRECAUTIONS TAKEN TO PROTECT YOUR PC ARE AS FOLLOWS:-

1.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.

• 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

2. 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.

· 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.

· Insert punctuation marks or symbols like {, ^, #, @, $ etc.

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.

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 notallowed 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.

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.

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.

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.

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.

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.