International Journal of Computer and Communication Technology

Volume 1 | Issue 1 Article 9

January 2010

Hardening of UNIX Operating System

P.K . Patra Prof. (Dr.)
Dept of Computer Science and Engineering, College of Engineering & Technology, BPUT, Bhubaneswar-751003., pk.patra@gmail.com

P.L. Pradhan
Ph. D. Student, Dept. of Computer Science & Engineering, Sikha 'O' Anusandhan University. Bhubaneswar, Orissa, India, mail.pradhan@gmail.com

Recommended Citation
Patra, P.K . Prof. (Dr.) and Pradhan, P.L. (2010) "Hardening of UNIX Operating System," *International Journal of Computer and Communication Technology*: Vol. 1 : Iss. 1 , Article 9.
DOI: 10.47893/IJCCT.2010.1008
Available at: https://www.interscience.in/ijcct/vol1/iss1/9

Hardening of UNIX Operating System

Prof. (Dr.) P.K .Patra[1] & P.L. Pradhan[2]

[1]Dept of Computer Science and Engineering, College of Engineering & Technology, BPUT, Bhubaneswar-751003.
[2]Ph. D. Student, Dept. of Computer Science & Engineering, Sikha 'O' Anusandhan University. Bhubaneswar, Orissa, India

Abstract: Operating system hardening is the process to address security weaknesses in the operation systems by implementing the latest operating system patches, hot fixes and updates as well as follow up the specific procedures and policies to reduce attacks and system down time.

Hardening is a not a one time activity, it is a on going task to mitigate the risk to performing high quality of computing. We have to build-up the secure production server in such a way to remove the unwanted devices, fix up the miss configuration, not allow the default setting, enhancement the current configuration and develop the new system programming and applying new security patches before going to the production environment. Hardening of the operating system should be support to the high integrity, reliability, availability, privacy, scalability and confidentiality at the lowest level of risk to achieve the highest level of objective (benefits) from the critical IT infrastructure of the organization.

Safeguarding information and protecting the integrity of your network and systems are vital to our business. IT security professionals in many companies have established policies applicable to their entire organization, but it may be up to individual departments that manage the systems to implement security in accordance with these policies. Security professionals recognize the need for flexibility when it comes to implementation, due to the unique requirements of each department.

Hardening of an operating system involves the removal of all non essential tools, utilities and other systems administration options, any of which could be used to ease a hacker's path to your systems. Following this, the hardening process will ensure that all appropriate security features are activated and configured correctly. Again, 'out of the box' systems will likely be set up for ease of access with access to administrator account. Some vendors have now recognized that a market exists for the OS-hardened systems. This thesis especially focuses on the hardening of UNIX sun solaris operating system.

Keyword: (O.S) Operating System; (LK) Lock; (HTTP) Hypertext transfer protocol; CERT(Computer Emergency Response Team)

Reference to this paper should be as follows: Pradhan, P. "Hardening of UNIX Operating System", *Int. J.CCT,* Vol-1, No.1 , pp.71-84.

Biographical notes: Padma Lochan Pradhan, M.Sc (Physics with Electronics), DCA, PG DBA, UNIX SUN SOLARIS CERTIFIED. 22 Year in IT Field, Major strength in Unix System Programming (Sun, HP, IBM). My assignment was with Thomson Scientific, Philadelphia, USA, Sun Micro system Burlington MA, USA, Hardfort Insurance IBM USA. Raymod Ltd India, Indian Telephone Industries India, Kalyanpur cement India. Apart from 3 year teching experience in IT & System area. Now I am working in IS Security, Unix system programming, Security, Risk assessment, IS auditing & OS virtualization. Now, visiting professor of Sambalpur University in Computer Science Department.

1 Introduction

The idea of OS hardening is to minimize a computer's exposure to current and future threats by fully configuring the operating system and removing unnecessary applications as well as devices. Operating system hardening means installing a new server in a secure fashion and maintaining the security and integrity of the server and application software. The planning to own a Virtual Private Server (VPS) or planning to get a Dedicated Server, then we need to prepare server-hardening checklist before launching your web application on the server.

The running UNIX based server (almost 66% of INTERNET servers) first and mostly we must configure host and system file for (/etc/hostility & sysctl (etc/system) hardening. Making sure that our UNIX server is performing its best through configuration of the system control files is essential to optimized operation of our server. Apart from major optimizations, secure patch updates and hot fix up are the essential part to look into while hardening the server.

Every OS comes with some security vulnerabilities. We look at how Windows, UNIX and other operating systems can be hardened to reduce vulnerabilities. Unless we are specifically running a DNS server, in. named can return DNS information for intruders to make use in launching DNS-type attacks.

The IS manager looking after corporate servers, firewalls, VPNs and databases, it is critically important that he should know the fundamentals of OS hardening, especially in the light of recent exploits that turn even the smallest loopholes into open craters. OS hardening is the black art of ensuring that all known OS vulnerabilities are plugged, and that the OS is monitored continuously.

The OS and Network becomes very important for the secure computing. We must ensure network performance and security, prevent network problems, conduct effective troubleshooting and take actions quickly to solve possible problems. We need to know how our network bandwidth and other resources are used for accounting, auditing and for network planning purposes. We need to monitor network traffic and conduct forensic analysis to ensure that company policies are followed and violations are recorded and stopped timely. We may have problems in our newly deployed applications and must know what's wrong and fix the problems immediately. We need to develop a new application and need a handy tool to assist in debugging and testing by examining every packets and messages. The hardening of operating systems involves ensuring that the system to configured to limit the possibility of either internal or external attack. While the methods for hardening vary from one operating system to another the concepts involved are largely similar regardless of whether Windows, UNIX, Linux, Mac OS X or any other system is being base lined. Some basic hardening techniques are as follows:

- Non-essential services - It is important that an operating system only be configured to run the services required to perform the tasks for which it is assigned. For example, unless a host is functioning as a web or mail server there is no need to have HTTP or SMTP services running on the system.
- Patches and Fixes - As an ongoing task, it is essential that all operating systems be updated with the latest vendor supplied patches and bug fixes (usually collectively referred to as *security updates*).
- Password Management - Most operating systems today provide options for the enforcement of strong passwords. Utilization of these options will ensure that users are prevented from configuring weak, easily guessed passwords. As an additional levels of security include enforcing the regular changing of passwords and the disabling of user accounts after repeated failed login attempts.
- Unnecessary accounts - All guest, unused and unnecessary user accounts must be disabled or removed from operating systems. It is also vital to keep track of employee turnover so that accounts can be disabled when employees leave an organization.
- File and Directory Protection - Access to files and directories must be strictly controlled through the use of Access Control Lists (ACLs) and file permissions.

- File and File System Encryption - Some file systems provide support for encrypting files and folders. For additional protection of sensitive data it is important to ensure that all disk partitions are formatted with a file system type with encryption features (NTFS in the case of Windows).
- Enable Logging - It is important to ensure that the operating system is configured to log all activity, errors and warnings. (/var/adm/messages).
- File Sharing - Disable any unnecessary file sharing.

1.1 Service detail

Operating system threats are very real—and they're everywhere. In fact, our UNIX operating system can be susceptible to a number of internal and external attacks as a result of un patched vulnerabilities, disgruntled employees or even misconfigured server settings. The good news is that we can help in the following way.
We can Implementation Services for UNIX - OS hardening provides direct access to skilled UNIX and systems specialists who can help protect the organization against security breaches and malicious attacks. This service can improve the overall efficiency of the operating system environment by verifying user permissions, patching vulnerabilities, installing necessary software updates and deactivating unnecessary programs. We may also experience the following benefits:

- Improved security of critical, sensitive data on UNIX servers.
- Enhanced reliability and uptime of applications and server infrastructure.
- Increased employee productivity, trust and client confidence.

1.2 Services Identification

Identify the purpose of each Unix Server.
How the computer will be used.
What categories of information will be stored on the computer?
What kind of information will be processed on the computer?
What are the security requirements for that information?
What network service(s) will be provided by the computer?
What are the security requirements for those services?
Identify the network services that will be provided on the server. Servers as a general rule should be dedicated to a single service. This usually simplifies the configuration, which reduces the likelihood of configuration errors. In the case of the servers, the application server should be limited to www or https services. The db2 server should be ports 50000 (db2idb2inst1) and 50001 (db2idb2inst1). It also can eliminate unexpected and unsafe interactions among the services that present opportunities for intruders. In some cases, it may be appropriate to offer more than one service on a single host computer. For example, the server software from many vendors combines the file transfer protocol (FTP) and the hypertext transfer protocol (HTTP) services in a single package. It may be appropriate to provide access to public information via both protocols from the same server host but we do not recommend this, as it is a less secure configuration.

Determine how the servers will be connected to your network. There are concerns relating to network connections that can affect the configuration and use of any one computer. Many organizations use a broadcast technology such as Ethernet for their local area networks. In these cases, information traversing a network segment can be seen by any computer on that segment. This suggests that you should only place “trusted” computers on the same network segment, or else encrypts information before transmitting it. The servers should be in there own private subnet.

1.3 Environment Analysis

There are certain considerations that must be taken into account before any implementation can begin upon a UNIX server. What version of operating system exists on the system? Where will the server be located? What programs will be running on this server? These are but three of the many questions that need to be answered to direct the path of a security policy. Depending on the answer to many of these questions, the level of security can be determined. For instance, if a server is simply running audits for other hand, if it is running these audits, it is most likely to have the same subnet as the other servers. Because of the possibility of jumping from node to node, high security precautions must be implemented on this example system to ensure that the production servers are not exploited.

Here are a few sample questions that need to be answered prior to the start of building a security framework.

Discussion: Technical survey: Data collection.

If the answer yes, to more than half of these questions, the higher echelon of security features outlined should be implemented. If the unit does not seem to require high security, implement the standard features and review the enhanced security features and evaluate if they would be useful for certain clients.

The server in an open environment accessible by more than one system administrators? --The server may be physically vulnerable to Knoppix Live CD's or other threats.
There is proprietary information stored on the server dealing with a sensitive material? --Data needs to be secured and encrypted, as well as server security protecting these files from possible copying and removal. (File sharing & encryption Technology enforced)
The server on the same subnet as production servers? --One node can bring down an entire network.
In the production server, does the client want high security? --the client knows that the information on the server is sensitive to their business, they may request higher security. (Passwd policy)
In the Client interface with the server using their own system? --The client computers should not be trusted to remain secure and should be ready to be physically disconnected if there are signs of vulnerability. Work with the client to help them secure their own systems by advising them of security updates the exact patches.
The administrators are able to log into the server? --When more than one administrator is permitted to log in, a server may be vulnerable to employees with access. (ACL Policy)
There are people accessing the server that are not familiar with AIX/UNIX? --Untrained users may accidentally damage a system without knowledge of how to recover.

Planning

This is the part of the plan where you must define the overall security policies and goals. In many organizations, this initial step is performed at the corporate level, and is likely to have already been completed.

How much security is needed? (High, Medium &Low)

How much security can your business afford? (Cost & time)

What devices and components should be protecting?

Security Policy

A server has many types of security features implemented. There are two main approaches for stopping intruders and exploits: security policy to maintain the integrity and privacy of the system and server hardening features to avoid malicious penetrations and exploits. Both are equally important but separate fields. Security policies (like all features of security) must be universally applied to the entire subnet, if not the entire network. By ensuring that all possible nodes are secure, the likelihood of intrusion is substantially decreased.

The primary purpose of security policy is to inform those responsible for protecting assets such as hardware, software, and data of their obligations. Management establishes a security policy based on the risks it is willing to tolerate. The policy itself does not set goals, but serves as a bridge between management's goals and the technical implementation.

We must develop a server deployment plan that includes security issues. Most deployment plans address the cost of the computers, schedules to minimize work disruption, installation of applications software, and user training. In addition, you need to include a discussion of security issues. You can eliminate many networked systems vulnerabilities and prevent many security problems if you securely configure computers and networks before you deploy them. Vendors typically set computer defaults to maximize available functions, so you usually need to change defaults to meet your organization's security requirements. You are more likely to make decisions about configuring computers appropriately and consistently when you use a detailed, well-designed deployment plan. Developing such a plan will support you in making some of the hard trade-off decisions between functionality and security. Consistency is a key factor in security, because it fosters predictable behavior. This will make it easier for you to maintain secure configurations and help you to identify security problems (which often manifest themselves as deviations from common, expected behavior). Refer to the better practice that keeping the UNIX operating system and applications software up to date is an essential part of this strategy.

2 UNIX Server Hardening: Proposed work

There are number of hardening procedure are out line and reflected to minimize the risk. The hardening checklist is based on the comprehensive security policy & procedure develops by CIS (Information Security Officer) with a particular focus on configuration issue of the UNIX base files system. Mean while the current tools & technique are requiring for risk assessment after the hardening activities. (JASS, JAAS, BRAT, Solaris tool kits, Tripwire. ISS Real Secure). Installed the following tools as per policy and guide lines: mod_ventila for user security on the distributed systems, mod_perl for apache share share services, mod_ssl for HTTPS apache web server. SMART for hard drive. Disable unwanted devices & services UNIX OS & network services. Hardening the various components as per guide lines as per CERT (Computer Emergency Response Team).

2.1 Hardening Methods

There are number of hardening methods developed as per requirement of the secure computing to achieve the highest level of business objective.

Table [Ref S.N 30]

SN	Commands & Scripts	Description	Vulnerabilities	Action plan for hardening method.
1.	/etc/system	Server control files,kernel conf kernel harding.	High	To prevent buffer overflow attacks: set noexec_user_stack=1, set noexec_user_stack_log=1, chmod 000 /etc/system, kernel conf detail: kstat -a, uname -r
2	/etc/hosts	Host files	High	Update the scipts:allow/disallow as per policy, chmod 0= /etc/hosts.allow
3	etc/services	Third parties like ftp, telnet, tcp port no, printer	High	Disable the third parties services.
4.	#/etc/syslog.conf	Main files for system logs configuration. Risk can be reflected by these files.	High	System programming require for: in new server these files are not available: we have to construct these files. /var/log/syslog, /var/log/sulog, /var/adm/message Risk can be analysis by help of these files.
5.	/etc/rc.conf	Run Level scripts	High	Run level scripts have to update as per requirement. httpd_flags="NO"
6.	#lsof	lsof to list your system's open TCP and UDP ports	Medium	Make it restricted shell (bin/false)Run this as root since unprivileged users may not be allowed to view sockets, because they do not have own.
7.	/etc/xinetd.d/wu-ftpd	signal inetd to re-read its configuration	Medium	vi /etc/xinetd.d/wu-ftpd **(change** *disable = no* **to** *disable = yes***)** # pkill -HUP xinetd to update this scripts as per requirement
8.	etc/ssh/sshd_config	Secure shell configruation files	High	Cryptography enable through ssh implementation AES: 256 bits chiper chiper blowfish-cbc,aes256-cbc, aes256-ctr. ssh-keygen -b 1024 -f /etc/ssh_host_key -N " chmod /etc/ssh/sshd_config
9.	etc/security/audit_control etc/security/audit_user	Basic security module (bsm)	Medium	dir:/var/audit flags:lo,ad,pc,fc,fd,fm update the script as per policy
10	secure.bash_	Securing History	Medium	chattr +a .bash_history (append)

	history			chattr +i .bash_history
11	ENV=$HOME/.kshrc:set + 0 vi	Disable shell Environment	Medium	Disable vi editor, disable alias:/etc/unalias, #set + 0 vi, /etc/.profile file
12	#ifconfig,#route, #netstat -nr	IP Stacking	Medium	Add -set /dev/ip ip_forwarding 0 to /etc/init.d/inetint.
13	PROM, printenv	Disable flash PROM Update	High	/etc/rc2.d , mv S75flashprom s75flashprom
14	/use/bin/rsh, etc/pam.conf	Remote services	High	Disable all remote services: chmod 000 /usr/bin/rsh, rksh,rcp, ruser,rlogin, uptime
15	svcadm	Services mgmt facility (Sun Solaris 10)	Medium	Svcadm disable svc:/network/telnet, rpc/rstat, shell:default, pkgrm SUNWtnetr SUNWtnetd
20	#printenv	Open boot process	Medium	The following step is required: This prevents users from using the console to issue the break sequence to interrupt the Solaris OE and drop to the OpenBoot PROM level. Once at the PROM level, an attacker could render the system useless by modifying certain EEPROM settings. Once in suspend mode, integrity of the system data is at risk and can also core dump the kernel or other programs. echo "KEYBOARD_ABORT=disable" > /etc/default/kbd
21	#Ifconfig –a	By this scripts IP address can be identified	Medium	Disabled Auto Boot # eeprom auto-boot?=false When the server boots from a powered off state, it will stop at the OK prompt. Configured Unique MAC Addresses Solaris assigns the same MAC address to all NICs by default. This configuration has the potential to cause problems. (i.e. collisions and low performance). To avoid this risk, accomplish the following: # eeprom local-mac-address\?=true
22	/etc/system	Core Dump - enabled or disabled. (As per requirement as well as policy	High	Core Dump - enabled or disabled. (As per requirement as well as policy mgmt) This is an optional step however is recommended (skip this step only if coredumps are necessary on the server - not recommended).

		mgmt)		Core dumps often contain sensitive data (e.g. /etc/shadow information). This is a security concern. On the other hand, core dumps are often useful in order when debugging. The decision needs to be made ifcoredumps are required (preferably not). If not, then core dumps should be disabled. cat <> /etc/system * Prevent core dumps set sys:coredumpsize = 0
23	#login –p/l	Display user id	Medium	Assigned Disabled Accounts an Invalid Shell: as per policy. vi /sbin/noshell #!/bin/sh # chmod 000 /sbin/noshell, but depend on policy. # vi /etc/passwd daemon:x:1:1::/:/usr/sbin/noshell Assign the shell /sbin/noshell as the shell for accounts that should never be allowed to log in (i.e. daemon, bin, sys, adm, lp, smtp, uucp, nuucp, listen, nobody, and noaccess). As an alternative, the noshell binary can be used.
24	#login -l	Lock all Administrative Accounts	Medium	The easy way is to put "*LK*" in the password field of the */etc/shadow* file. ● Use the noshell program to log attempts to usesecured accounts.
25	Prevent TCP Services	Network issue High Risk	High	Prevent TCP Sequence Prediction (Helping IPS: Intrusion Prevention System) Attacks ● Modify the variable TCP_STRONG_ISS to be set to 2 in */etc/default/inetinit*
26	/etc/rc2.d	Run level 2	High	Disabled Auto Install # cd /etc/rc2.d # mv S72autoinstall s72autoinstall
27	#ps –ef\grep nfsd	Auto mounter high risk	Medium	Diasble the Automounter Depend on policy ● Automounter is controlled by the */etc/auto_** configuration files. ● Remove those files, and/or disable the / etc/rc2.d/S74autofs
28	/etx/default/login	Disable root login	High	Disable Network root logins, rlogin and rsh ● Enable the "CONSOLE" line in */etc/default/login*.

				● Remove */etc/hosts.equiv, /.rhosts /etc/hosts* ● Remove the "r" commands from */etc/inetd.conf* ● Refresh the inetd process with kill -HUP [inetd process id].
29	PCMCIA	Single user run level	High	Remove unneeded services The following services are generally not needed and should be disabled from sttartng on boot. /etc/rcS.d/S35cacheos.sh /etc/rcS.d/S41cachefs.root -- configures the devices when running cachefs) /etc/rcS.d/S10initpcmcia -- PCMCIA initialization /etc/rcS.d/S65pcmcia -- PCMCIA initialization chown -R root:sys /DISABLED chmod -R 000 /DISABLED
30	Driver hardening in Solaris 10	Solaris Security Toolkit	High	JASS_SCRIPTS parameter that should not be run. This approach is one of the most common ways to customize drivers. disable-autoinst.fin disable-automount.fin disable-keyboard-abort.fin disable-dtlogin.fin disable-lp.fin disable-nfs-client.fin disable-rpc.fin disable-vold.fin

3 SOLARIS-10.0 OS (Virtualization) DRIVER HARDENING

This paper provides reference information about using, adding, modifying, and removing drivers as per business requirement to minimize of technological risk. This chapter describes the drivers used by the Solaris Security Toolkit software to harden, minimize, and audit Solaris OS systems. A series of drivers and related files make up a security profile. The secure driver is the driver most commonly used as a starting point for developing a secured system configuration using the Solaris Security Toolkit software. The secure driver disables all services, including network services, not required for the OS to function, with the exception of the Solaris Secure Shell (SSH) software. This action might **not** be appropriate for your environment. Evaluate which security modifications are required for your system, and then make adjustments by using the information in this chapter.

3.1 Customizing Drivers

Modifying the Solaris Security Toolkit drivers is one of the tasks done most often because each organization's policies, standards, and application requirements differ, even if only slightly. For this

reason, the Solaris Security Toolkit software supports the ability to customize tasks undertaken by a driver.

The system and application requires some of the services and daemons that are disabled by the selected driver, or if we want to enable any of the inactive scripts by the Solaris Security Toolkit software.

Similarly, if there are services that must remain enabled, and the selected driver disables them, override the selected driver's configuration before executing the selected driver in the Solaris Security Toolkit software. Review the configuration of the software and make all necessary customization before changing the system's configuration. This approach is more effective than discovering that changes must be reversed and reapplied using a different configuration.

There are two primary ways in which services can be disabled using the Solaris Security Toolkit software. The first way involves modifying drivers to comment out or remove any finish scripts defined by the JASS_SCRIPTS parameter that should not be run. This approach is one of the most common ways to customize drivers.

For example, if your environment requires NFS-based services, you can leave them enabled. Comment out the disable-nfs-server.fin and disable-rpc.fin scripts by prepending a # sign before them in the local copy of the hardening driver. Alternatively, then remove them entirely from the file. As a general rule, it is recommended that any entries that are commented out or removed should be documented in the file header, including information such as:

- Name of the script that is disabled
- Name of the person who disabled the script
- Timestamp indicating when the change was made
- Brief description for why this change was necessary

Including this information can be very helpful in updating drivers over time, particularly when they must be updated for newer versions of the software and patches.

3.1 Hardening Driver

Most of the security-specific scripts included in the Solaris Security Toolkit software are listed in the hardening driver. This driver builds upon those changes by implementing additional security enhancements that are not included in the hardening driver. This driver, similar to the config.driver, defines scripts to be run by the driver run script.

The following scripts are listed in this driver:

- disable-keyboard-abort.fin
- disable-picld.fin
- print-rhosts.fin
- enable-bsm.fin
- install-strong-permissions.fin

This driver is provided as an example, based on the secure driver, to highlight what changes might be necessary to secure a system other than a Sun Fire high-end systems system controller. This script is a guide; therefore, you might need to customize it, depending on your environment. The differences between this and the secure driver are as follows:

- The following inetd services are *not* disabled: We have to take action as per policy.
- telnet (Telnet)
- ftp (File Transfer Protocol)
- dtspc (CDE subprocess control service)
- rstatd (kernel statistics server)
- rpc.smserverd (removable media device server)
- The following file templates are *not* used:
- /etc/dt/config/Xaccess
- /etc/syslog.conf
- The following finish scripts are commented out in the server-secure.driver:
- disable-autoinst.fin (Disable auto install)
- disable-automount.fin (Disable auto mount)
- disable-keyboard-abort.fin (Disable keyboard)
- disable-dtlogin.fin (Disable desktop login)
- disable-lp.fin (Disable line printer)
- disable-nfs-client.fin (Disable Network File system)
- disable-rpc.fin (Disable remote procedure call)
- disable-vold.fin (Disable CD drive)
- disable-xserver-listen.fin (Didable server connectivity)
- print-rhosts.fin (Disable remote host)

The Basic Auditing and Report Tool (BART) is a file-tracking tool that operates entirely at the file system level. Using BART allows you to quickly, easily, and reliably gathers information about the components of the software stack that is installed on deployed systems. Using BART can greatly reduce the costs of administering a network of systems by simplifying time-consuming administrative tasks.

BART enables you to determine what file-level changes have occurred on a system, relative to a known baseline. The bart create command creates a baseline or control manifest from a fully installed and configured system. The bart compare command compares this baseline with a snapshot of the system at a later time, generating a report that lists file-level changes that have occurred on the system since it was installed.

1.1 Risks – Results

There are three categories of results developed on the basis of hardening of Unix operation systems.
---> Monetary – Financial Loss relating to under performing and unsecured resources being used within the organization.
---> Productivity – Cost of fixing machines affected in terms of end-user and administrator lost productively due to a loss of functionality (server crash or compromise) and performance.

--->Trust – Loss of good faith of customer/users, it is impossible to regain in e-commerce environment.

1.2 Impact Analysis

There are some draw back scenario co-exist on the operating system hardening. Some time hardening cost may be more than the hardware cost. Exact skill manpower may not be available in due course of time to performing the activities. Management policy may be change due to business change. Technology may be change or obsolete. In around the IT infrastructure new application may not be fits to the existing tools due to customer requirement changing day by day. As per ITIL Principle, management have to follow up CMDB norms, mean while change mgmt & release mgmt may not be fix up as per ratio & proportion of the top management decision. Lot of documentation and follow up needed. In this scenario penetration testing as well as ethical hacking may be necessary to verification and validation process.

1.3 Benefits

Yet the cost for such solutions is high and the complexity of many such tools had stopped people from using them. Minimize the risk verses maximize the benefits. Mean while reduce the maintenance cost. The operating system hardening is short term as well as long term plan for any size of organization.
Establish the trust relationship and enhance the business with technology of other company and hence do more business as well as profit. We can have more confidence in the integrity of your data• Performance improvements can be experienced since unnecessary services are removed, and inefficiencies in system configuration are detected; The company's reputation is protected; Clients are happier as a result of fewer system failures or delays.

- Increased visibility throughput, accurate and continuous risk assessment process.
- Considerable time and labor reduction through automation of manual processes.
- Prioritized action plans for optimal remediation - focusing on the 1-2% exposures that really matter.
- Reduce resource dependency as well as ineffective patch or mitigation projects.
- Improve IT security by shrinking the window of exposure from weeks to hours.
- Compliance with risk management control objective and compensating controls documentation requirements. (Price water house, SOX, HIPAA, BS7799)
- Demonstrate effectiveness of compensating controls (such as, hardening OS, network, Database, Application, firewalls and intrusion prevention systems) for compliance reporting - can reduce workload by 95% or more.

4 Conclusion

- Risk can be mitigate by on going process of hardening of OS, Network, Database, Application and devices as well as relevant resources of the IT infrastructure.
- To minimize the risk, operating system hardening, preventive, detective and corrective action is the most well advanced action plan for the long-term business activities of the every organization. Therefore, contingency plan is the most effective & efficient plan for safe guard of the organizational assets. Therefore operating system hardening, anti-virus solution, periodically

security patches up dation is the most preventive, detective and corrective action plan of the any organization to survive. In summary, the risk assessment process is about making decisions to minimize the risk. The impact of a successful attack and the level of acceptable risk for any given situation is a fundamental policy decision. Likewise, vulnerabilities are design issues and must be addressed during the design, development & implementation of information resources.

- A fundamental problem of risk management then is to achieve a cost effective balance between design characteristics and the related counter measures to threats and impact. Today's computing environments are mostly distributed infrastructures. Any organization must develop intrusion detection strategies for the servers. I do not believe that there are any sensors on the internal network. Many of the common intrusion detection methods depend on the existence of various logs that OS can produce and on the availability of auditing tools that analyze those logs. This will help you with installing the appropriate software tools and configure these tools and the operating system to collect and manage the necessary information. Keep your computer deployment plan current. The Organization must update the computer deployment plan when relevant changes occur. Sources of change may include new technologies, new security threats, updates to your network architecture, the addition of new classes of users or new organizational units, etc. The environment will only work if the process is centralized. I also believe that there is not enough on-site experience and internal infrastructure to administer this project. The issues of 24/7 availability and the underlying issues of security in layers have to be addressed.
- It is important for financial institutions to develop and implement appropriate information security programs. Whether systems are maintained in-house or by third-party vendors, appropriate security controls and risk management techniques must be employed. A security program includes effective security policies and system architecture, which may be supported by the risk assessment tools and practices discussed in this guidance paper and appendix. Information security threats and vulnerabilities, as well as their countermeasures, will continue to evolve. As such, institutions should have a proactive risk assessment process that identifies emerging threats and vulnerabilities to information systems.
- A sound information security policy identifies prevention, detection, and response measures. The appendix provides more details on risk assessment tools and practices that may be used to improve information security programs. Preventive measures may include regularly using vulnerability assessment tools and conducting periodic penetration analyses. Intrusion detection tools can be effective in detecting potential intrusions or system misuse. Institutions should also develop a response.
- By reading through this paper and utilizing the checklist that accompanies it, an OS and Security administrator now has a base knowledge of security, server hardening, intrusion detection, auditing, and security tools. This knowledge can be directly applied to their servers and many vulnerable holes will now be filled. Bear in mind that many holes that exist have yet to be discovered. Therefore, it is critical that every UNIX security-minded administrator maintains their knowledge of security by researching and referring to the Internet resources that have been attached. If there is ever a question about implementation of any of the suggested features, refer to the Unix Security manuals that were designated with the specified feature (all features have been documented).
- Help other administrators by documenting all changes and vulnerabilities found. Many times administrator will find a hole and fix it, while many other servers that may be on the same network are left vulnerable. Communication and documentation is essential to keep UNIX servers secure. By utilizing this paper and the checklist, the overall security of all UNIX systems will be dramatically improved.

References

[1] Ron Weber, Information System audit & control PHI 2002(Chap 7 P- 243-285)
[2] Shon Harrish, CISSP Exam study guide, Dreamtech year 2002 DRP/BCP (Chap 9 P 591-603)
[3] Shon Harrish, Security Mgmt Practices, Wiley, Dreamtech CISSP Exam Year 2002 study guide 2003 (Chap 4 P 57-92)
[4] Mcl.ean, Kevin & Lenwatts (1996) Risk Analysis Methodology " IS audit & Control Journal III 32-36
[5] O' Reilly, Essentail of System Administration (Chap 10, P467- 485) & Chap 6(p201-243), Chap11
[6] Coriolis , CISSP Exam cram, dreamtech year 2002 (Chap 4 p 61-77)
[7] Pressman, Software Engg 5th Edn, year 2001 MGH,Chap 6 (P 145- 162)
[8] ISACA Monthly Journal Vol 2,Vol5 2003
[9] William Stalling, Cryptography and Network Security Chap 19.2 pp-609-614
[10] Bruce Schneier, Applied Cryptography, Wiley 2nd Edition 1996 Chap7.1 pp-155
[11] O' Reilly & Associates, Internet 1996
[12] The Unix Auditor Practical Handbook. Chap: 2,3, 5,7
[13] CISA Review Mannual 2003, Chap 4, pp226-230
[14] Bagchi, K. and G. Udo (2003) "An Analysis of the Growth of Computer and Internet Security Breaches," *Communications of the Association for Information, Systems* (12), pp. 684-700.
[15] Pichnarczyk, Karen, Weeber, Steve & Feingold, Richard. "*Unix Incident Guide: How to Detect an Intrusion CIAC-2305 R.1*". C I A C Department of Energy. December, 1994.
[16] Bento, A. (2003) "Soho Security: A Technical Briefing," *Proceedings of the Americas Conference on Information Systems.* Tampa, Florida.
[17] Bookholdt, J. L. (1989) "Implementing Security and Integrity in Micro-Mainframe Networks," *MIS Quarterly* (13) 2, pp. 135-144.
[18] CERT/CC (2004) "CERT/CC Statistics 1988-2004" http://www.cert.org/stats/cert_stats.html (current September 29, 2004)
[19] CERT/CC(2002)."Overview of Attack Trends" http://www.cert.org/archive/pdf/attack_trends.pdf (September 29, 2004)
[20] Federal Communications Commission (2004) "Local Telephone Competition and Broadband Deployment" http://www.fcc.gov/wcb/iatd/comp.html (current September 29, 2004).
[21] Federal Computer Incident Response Center (2004) "U.S. CERT Federal Incident Statistics" http://www.us-cert.gov/federal/statistics/ (current September 29, 2004)
[21] Bagchi, K. and G. Udo (2003) "An Analysis of the Growth of Computer and Internet Security Breaches," *Communications of the Association for Information, Systems* (12), pp. 684-700.
[22] Sumitabh Dash, Unix Concept & Application, Year 2006.