GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

UNIX System Management and Security: Differences between Linux, Solaris, AIX and HP-UX

© SANS Institute 2007, Author retains full rights.

Haral Tsitsivas,
Edits by Jim O'Gorman, Michael Cope, Daniel Givens, Jim Alcorn
GSEC Practical Assignment, version 1.4b, Option 1
February 18, 2003
Updates: 7-13-07, 7-26-07, 8-24-07

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Abstract

Understanding the capabilities and limitations of an operating system, its software installation and management procedures and how to configure and manage other system software is a key ingredient of keeping systems secure. This paper discusses the differences in system configuration, management and security between some of the most common versions of UNIX (Red Hat Linux, Solaris, HP-UX and AIX), including management and security tools available on these systems. The “man” pages should be consulted on each platform for details on additional options for the commands and/or system calls discussed here. All of the discussed systems conform to the System V standard with Berkeley extensions, although each system provides its own software installation and system management utilities and kernel configuration methods. Vendor-provided and open source software are discussed and compared where applicable.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Introduction

Good system and network security starts with a good understanding of the operating environment. Organizations that keep things simple (e.g. use only one system type) can have a good understanding of their operating environment and its limitations and vulnerabilities and should be able to secure their system relatively easily. Not many companies however have the luxury of operating in a single vendor / single operating system environment because PC desktops exist in the most entrenched UNIX shops and UNIX computers also exist in a lot of PC shops. The relative easy of porting applications between UNIX versions also contributes to a proliferation of different Operating System types and versions, making the job of securing such organizations harder, because even though there are many similarities between the different OS types there also many differences. While a system administrator may have a lot of experience with one version of UNIX, administering another version of UNIX may require some additional information in order to maintain the same quality of service and security stance.

This paper discusses the differences in system configuration, management and security between some of the most common versions of UNIX (Red Hat Linux, Solaris, HP-UX and AIX), including management and security tools available on these systems. The "man" pages should be consulted on each platform for details on additional options for the commands and/or system calls discussed here. All of the discussed systems conform to the System V standard with Berkeley extensions, although each system provides its own software installation and system management utilities and kernel configuration methods. Vendor-provided and open source software are discussed and compared where applicable. Although this subject matter was covered in part by the GSEC study material, the discussion in the study material was mostly limited to Linux and to Solaris, so this paper attempts to expand on issues that were not discussed in the study material and to address two more UNIX systems common to corporate and government data centers. As such, details covered in the study guide will not be further elaborated on unless it is required for comparison purposes to the newly discussed operating systems, although access to the GSEC study guide is not required when reading this comparison.

Finally, this paper is intended for system administrators and other IT personnel whose organizations are running or are thinking of running a multi-OS environment, although IT personnel may also use this paper to better understand how some of these differences may affect the security configuration of their organization.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Software Installation and Patch Management

	RH Linux	Solaris	HP-UX	AIX
Install	rpm –i *file*	pkgadd –d *pkgfile*	swinstall –s *depot software*	installp –a [-c] *FileSet*
Update	rpm –U/F *file*	pkgadd –d *pkgfile*	swinstall –s *depot software*	installp –a *FileSet*
List	rpm –q	pkginfo	swlist –l product	lslpp –L all
Remove	rpm -e	pkgrm *package*	swremove *software*	installp –u *FileSet*
Patches	rpm -u	patchadd	swinstall	installp
List Patches	rpm –q -a	showrev –p	swlist –l product	lslpp –L all
Patch Check	up2date/yum	patchdiag($) PatchPro	security_patch_check	compare_report

As evidenced by the rash of last year's security exploits (Code Red, Nimda, SQL Slammer Worm, RPC buffer overflows, SSH vulnerabilities and others…) a good patch security policy is imperative to maintaining secure systems and networks. Organizations with a good patch security policy, that had applied all known patches to the target systems were not affected or were only minimally affected, while some organizations with lax patch security policies experienced severe problems, downtime of several days and even loss of work (data and code).

All of the examined systems have their own methods for applying patches. Furthermore, Solaris, HP-UX and AIX program and patch installation methods allow the removal of an application or a patch by restoring any overwritten files when the "save" option is used (which is the default). The ability to remove a (recalled) patch simplifies patch management on these systems freeing the administrator from devising custom methods for patch management and allowing the administrator to concentrate on enhancing system security.

Sun, HP and IBM provide standard patch bundles for download (free of charge for security and recommended patches) a few times per year, as well as individual patch downloads and patch notification services by email (with free registration). Individual patch downloads are available from the vendor's web sites as well as a few mirrors for Red Hat Linux. The availability of both options is important, because standard patch bundles simplify the regular application of patches and eliminate the need for multiple reboots and/or system configuration changes, while individual patch downloads allow the application of a security patch as soon as it is available.

All of the examined vendors provide free security patch check tools, which compare installed system patches with available patches, although a free

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

registration may be needed to use these tools. Generally all of these tools can be used as part of a nightly/weekly batch/cron script to automatically report the patch status of the monitored system.

Security_patch_check for HP-UX is available from HP's Software Depot [1], and it can download a patchlist to compare with the installed patches and generate lists in verbose or machine readable formats for download from HP's patch download site [2]. The patches still have to be downloaded manually from HP's ITRC site but can be packaged into a single depot before applying them. A premium service is also available, the Custom Patch Manager, which allows the upload of the system configuration for comparison and the generation of a custom patch bundle.

Compare_report for AIX is available on a default system installation (part of the bos.rte.install fileset), and can compare installed filesets with filesets available from IBM's Fix Delivery Center [3]. The generated report file can then be uploaded to the Fix Delivery Center in order to generate a set of patches to be downloaded to bring the system to the latest maintenance level.

Sun's *patchdiag* is only available to SunSpectrum service contract customers. Non-contract customers can only download individual patches and the maintenance updates (patch clusters) from Sun's Patch Support Portal [4], however administrators can sign up for the free patch notification service (also available from HP and IBM) in order to stay informed of any new patches affecting their installed systems. Sun's Support Portal now has a new tool available, PatchPro, which requires a SunSolve account. PatchPro is capable of generating lists of (signed) patches needed to update the system, downloading the required patches and installing them. The download process includes checking the digital signatures of the patches for validation. PatchPro can also be run from automation scripts (e.g. from cron) further simplifying patch management on Solaris systems.

Individual patches can be downloaded for free for one of the Community supported editions (e.g. Fedora Core) which official Redhat distributions usually track. For official Red Hat releases, the Red Hat Network [5] allows the registration of a System Profile for each Red Hat Linux machine that needs to be updated and eases the determination of which patches need to be applied. Each system must have its own subscription license. In Red Hat Enterprise Linux 5, up2date has been replaced by the yum program, which is based on the Yum project (http://linux.duke.edu/projects/yum/). Yum establishes repositories and is an automatic updater and package installer/remover for rpm systems, making it easier to maintain groups of systems.

These various options of staying informed and dealing with patches allow administrators to remain proactive in their system maintenance duties and ensure that all security problems are promptly addressed.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Services Startup

	Linux	Solaris	HP-UX	AIX
Init default	3 or 5	3	3 or 4	2
Startup File	/etc/inittab	/etc/inittab	/etc/inittab	/etc/inittab
Startup scripts	/etc/rc.d/rcX.d [/init.d]	/etc/rcX.d	/sbin/rcX.d	/etc/rc.d/rcX.d /etc/rc.*
Other	chkconfig			SRC (System Resource Controller) srcmstr, startsrc, stopsrc, lssrc
inetd	xinetd	inetd (/etc/inet/ inetd.conf)	inetd	inetd

The multi-user init level determines which programs and services are started when the system boots. When maintaining a multi-OS environment it is important to keep track of the programs and services that are started at the proper level for each OS in order to maintain a secure environment. It is strongly suggested that inittab and the associated "rc" files are regularly audited for unauthorized changes that may breach system security. Because of the possibility that an intruder with physical access to the system can reboot the system in single user mode and add services, add accounts or modify passwords to gain root access, it is also suggested that the machines are physically secure in a restricted area and additional passwords are used. These additional passwords can be set at these levels: a BIOS or power-on password to prevent the rebooting of a machine from bootable media (such as a CD) in order to bypass the system's security configuration; a maintenance mode password to prevent the machine from booting into single user or system maintenance mode either from the hard drive or other bootable media to gain access to restricted access or directories and/or modify the standard system security mode; having a security procedure in place for when the root password should be used during system maintenance or when responding to emergencies by other IT personnel.

The multi-user init level differs somewhat between the examined systems although the end-result is usually the same. The default init level noted in the table above is the multi-user state where all services are enabled and the graphical login interface is enabled. Accidentally using state 5 on a Solaris system though will cause a shutdown and power off, although state 5 is not used on AIX and HP-UX. Generally, state 0 means shut the system down; state S is the single-use state using for system administration tasks, and should be entered only when the system first boots since entering this state from another level does not terminate other system activity; state 1 runs a subset of essential system

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

services and puts the system in maintenance mode without any logged-in users; state 2 is the multi-user state in most systems and starts all network services on AIX; state 3 starts network services on Linux, Solaris and HP-UX; state 5 starts X11 on Linux while it signals a shutdown and power-off on Solaris; state 6 reboots the system on Linux and Solaris; state q forces init to re-examine the inittab file; and states a, b and c start additional processes without changing the current state or affecting currently running processes. States not already mentioned are reserved for local use.

Linux provides the newer xinetd service startup method, while the other systems provide the traditional inetd method. While inetd provides a method to start systems services listed in /etc/services on an as needed basis, xinetd provides additional features such as the number of instances the service can run, access control and logging. In order to achieve access control and logging with inetd, TCP wrappers (also discussed in the System and Network Security section) must be used. There is however no easy way to achieve the other features provided by xinetd (limits on the number of concurrently running processes and servers, and periodic consistency checks).

A non-standard service startup method exists on AIX, where basic system services and the System Resource Controller (SRC) are started from inittab, while additional services are started using SRC. SRC provides service manipulation commands such as “srcmstr” which can be used from the “rc” scripts to start other services/subsystems. Most of the stand-alone network daemons are started from the /etc/rc.tcpip script (which is started from inittab). The NIS/YP and NFS services are started from the /etc/rc.nfs script, although it should be noted that NIS is disabled by default. There are also other rc.* scripts (rc.C2, rc.bsdnet, rc.dacnet, rc.dt, rc.ike, rc.net, rc.pkcs11, rc.powerfail, rc.qos), also started from inittab.

On AIX, the rc.d/rcX.d directories are empty by default, however they provide a compatibility mode for administrators wishing to startup additional services and used to the System V standard used by the other UNIX systems. If these process/service startup methods are not used locally, AIX administrators can disable their use from inittab in order to enhance security, since they are not used by the OS in the default configuration and could be “accidentally” used by users with administrative access.

An important part of hardening a system includes a thorough review of the services started at each run level (this is also discussed in the OS hardening section later in this paper) and the removal of any services not required by the organization, and/or the replacement of inherently insecure services (such as rsh, rcp, and telnet) with more secure services (such as ssh). Failure to disable unnecessary services exposes a site to buffer overflow attacks, denial of service attacks and even script vulnerability attacks [12 (pg. 40)].

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

As of Solaris 10, Sun has moved to a new start up system called Service Management Facility (SMF). This retains the "rc" style start up for compatibility purposes, but prefers that items are added to the new framework. Be sure to check /var/svc/log and /etc/svc/volatile for log files relating to start up. SMF can be found documented at http://www.sun.com/bigadmin/content/selfheal/smf-quickstart.html.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

	Linux	Solaris	HP-UX	AIX
Default Syslog Output	/var/log (messages, secure, boot.log)	/var/adm/ messages, /var/log/syslog	/var/adm/syslog/ (mail.log, syslog.log)	/tmp or none!
System Accounting (login & process)	/var/run/utmp /var/log/wtmp /var/account/ pacct	/var/adm/utmpx /var/adm/wtmpx /var/adm/pacct	/var/adm/utmp /var/adm/wtmp /var/adm/pacct	/etc/utmp /var/adm/wtmp /var/adm/pacct
Login Errors	/var/log/btmp, /var/log/ messages	/var/adm/ loginlog sulog	/var/admlastb /var/adm/sulog	/etc/security failedlogin, /var/adm/ sulog

All systems can log the same type of information, although sometimes the filenames and directory locations differ. There are several facilities that could generate messages of eight levels from *debug* to *emerg* ("man syslogd" for more information on the facilities and levels). The information collected by syslog is a valuable resource in determining the health of the system, and when reviewed regularly can provide an advance warning for some types of attacks.

AIX is the only system that does not log any syslog information by default, so the configuration file (/etc/syslog.conf) should be modified to start logging interesting events immediately after system installation. It should be noted that syslogd will not write to a file that does not exist, so the log files should be touch'ed to start logging after any syslog.conf configuration changes. The minimum syslog.conf changes to log debug mail messages to mail_log, error messages (and higher) to errorlog, informational messages (and higher) to syslog and broadcasting critical messages to all logged in users, would consist of something like this:

```
mail.debug    /var/log/mail_log
*.crit        *
*.err         /var/log/errorlog
*.info        /var/log/syslog
```

Additional syslog.conf configuration suggestions for AIX are made in the IBM online tutorial Securing AIX Network Services [21].

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

To improve security on all of the discussed systems, the syslog UDP port (514) should be blocked at the firewall in order to reduce the likelihood of a buffer overflow attack or other vulnerability, and remote logging should be disabled unless the host acts as a central log server.

The standard system accounting files can provide a wealth of system usage information if analyzed on a regular basis and additionally can be used for both chargeback and capacity planning purposes. "Wtmp" or "wtmpx" and "pacct" are the standard UNIX system accounting files, containing login information and resource usage information by processes respectively. The "last" and "acctcom" can be used to view detailed usage data while the "acctcon" and "acctprc" / "acctcms" can be used to view summarized data.

Commercial products (such as UNISOL JobAcct [7] from UniSolutions Associates) can simplify the presentation of system usage data for chargeback. UNISOL JobAcct can generate system usage reports by user, group, project or cost-center, for one or several machines on the network. Analysis of system usage data can be very useful in improving system performance or in the detection of intrusions since anomalies in chargeback data can sometimes reveal inefficient applications and/or misuse of computer resources.

A few scripts and tools also exist that can be used by system administrators to summarize and monitor the syslog and login accounting files. A syslog summary tool is *newlogcheck* [8], which enhances security by reducing the amount of log entries administrators have to examine, and categorizing the log entries. *Sentryd* [9] is a Perl script that monitors the syslog and *wtmp* files for unusual events and bad login attempts, and notifies users (by broadcast) of selected events.

There are several tools available for more specialized syslog analysis (e.g. analyzing firewall data in syslog files). A good resource pointing to these tools can be found on Counterpane's web site (http://www.counterpane.com/log-analysis.html#gen-parcing). Counterpane is one of the companies that provide remote log analysis services as part of their managed security services (http://www.counterpane.com/services-msm.html).

Managed security services also include firewall log analysis, intrusion detection, virus protection, gateway services, and vulnerability assessment and policy compliance services. Other companies providing managed security services include Guardent (http://www.guardent.com/mss_overview.html), Symantec (http://enterprisesecurity.symantec.com/SecurityServices/content.cfm?ArticleID=682&EID=0), TruSecure (http://www.trusecure.com/solutions/managed/), VeriSign (http://www.verisign.com/consulting/managed/), and also system vendors like IBM(http://www.ibm.com/services/continuity/recover1.nsf/mss/mss+home).

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Organizations considering outsourcing certain security services should consult the paper *Outsourcing Managed Security Services* [18] from CERT in order to better understand the benefits [18a] and risks [18b] involved with hiring a Managed Security Service Provider (MSSP) and get maximum value for their security budget without compromising system security and giving up too much control.

Finally, checking for login errors should also be performed regularly, perhaps by incorporating the process together with an automated syslog analysis procedure. The file location of the logged login errors differs from machine to machine but all of the examined systems log the same type of login errors. Pulling together all of the logs and analyzing them regularly (preferably in an automated process) is the first step in establishing an incident response policy. An automated log analysis process that notifies administrative personnel promptly can be an invaluable tool to providing a quick response to system attacks or other significant security events, that can stop a security breach early enough before irreparable damage can take place.

© SANS Institute 2007, Author retains full rights

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Login Access Control

	Linux	Solaris	HP-UX	AIX
Mgmt App	User Manager Nautilus	SMC, admintool	SAM SCM	SMIT WebSM
Shadow	/etc/shadow	/etc/shadow	/tcb/files/auth/*	/etc/security/ passwd
PAM?	/etc/pam.d/ system-auth	/etc/pam.conf	/etc/pam.conf SAM gui	/etc/pam.conf (add-on), /etc/security/ user (LDAP)
TCB	-	-	yes	yes
Admin Roles	yes (selinux)	yes (SMC)	yes (SCM)	yes

Login access control has traditionally been the first line of defense against unauthorized system access. The value of login access controls and a good password policy cannot be overestimated in providing the first line of defense toward guarding a system from intruders. All of the examined systems provide the standard password management controls (account locking, minimum password lengths, and password expiration and aging) while some (HP-UX and AIX) also provide features such as password generation, password restrictions, and login controls.

By default, the /etc/passwd file does not contain the encrypted passwords on most current UNIX systems, however, the /etc/passwd file on HP-UX contains the plain-text encrypted passwords unless TCB (Trusted Computing Base) is enabled. If TCB is enabled however, the shadow file does not exist as a single file but is distributed over several directories and files in a directory structure that is similar to other Unix systems with C2 security enhancements. The C2 security level conforms to the Trusted Computer System Evaluation Criteria (TCSEC), which has already been superseded by the Common Criteria security requirements.

Since password cracking programs such as "crack" and "John the Ripper" can quickly crack weak passwords, it is important to not only employ shadow files, but also to make them inaccessible to normal users. Leakage of the encrypted passwords would eventually lead to system compromise since even hard to guess passwords can be eventually guessed given the encrypted password text and enough computing time. Some level of additional security can be achieved by employing passwords encrypted with *MD5* or *Blowfish*, John the Ripper can also crack these type of passwords, as well as TCB type passwords. Finally, sites can enhance login security by employing one-time passwords, aided either by hardware (smart cards, challenge/response) or software (SKEY).

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

SMC (Solaris Management Console), WebSM (Web-based System Manager) and SMIT (System Management Interface Tool) are full-featured system management tools capable of adding users to configuring devices, while providing administrative role management. SAM (System Administration Manager) for HP-UX is also a full-featured system management tool but not provide role management. HP though provides an additional system management tool for download from its Software Depot site, Service Control Manager (SCM) 3.0 which supports role-based management. SCM provides a web-based user interface and is capable of managing up to 1024 nodes.

Roles define user capabilities to perform certain tasks. The supported roles range from user management to log and network security management, allowing for a secure distribution of tasks among support staff. SMC and WebSM provide a java-based user interface while SAM and SMIT provide Motif style interfaces, thus SAM and SMIT provide a faster user interface than SMC and WebSM. On Solaris, the old admintool program is still available, although it gives a warning about being obsolete on Solaris 9 before starting up! Admintool is not capable of role management, but may still be used by the root user when a quick user interface is needed.

The User Manager (*redhat-config-users*) under Red Hat Linux is loosely integrated with a collection of other system management tools under the *Nautilus* graphical shell for GNOME. Although usually Nautilus is integrated with the GNOME desktop, it can also be started with any window manager with the command "*nautilus start-here: --no-desktop*". This startup method also allows for the use of the standard system management graphical user interface commands from a remote administrative workstation. The various system management tools of course could still be individually used, without the aid of Nautilus.

NSA Security-Enhanced Linux (SELinux) is an implementation of a flexible mandatory access control architecture in the Linux operating system. The SELinux architecture provides general support for the enforcement of many kinds of mandatory access control policies, including those based on the concepts of Type Enforcement®, Role-Based Access Control, and Multi-Level Security. Background information and technical documentation about SELinux can be found at http://www.nsa.gov/selinux.
Webmin [19] is a web-based interface for system administration and is available for all of the examined systems, although support is best currently for Solaris and Linux (Red Hat in Particular) and is available for distribution under the BSD license. Webmin is a simple web server with a number of CGI programs (modules) that makes it extensible by anyone willing to contribute to the development effort. Only Webmin and SAM (from the examined system management software) provide support for PAM configuration.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

	Linux	Solaris	HP-UX	AIX
Mount Table	/etc/fstab	/etc/vfstab	/etc/fstab	/etc/ filesystems
OS Apps	/usr & /opt	/usr & /opt	/usr & /opt	/usr /usr/lpp
Vendor Apps	/usr or /opt	/opt	/opt	/opt
Kernel config	/etc/sysctl.conf	/etc/system	SAM, /usr/conf/ master.d/*	SMIT, lsattr / chdev / vmtune / no (rc.net)
Filesystems	ext2, ext3, reiserfs, xfs	ufs,zfs	hfs, vxfs, jfs	jfs, jfs2
LVM	LVM cmds	DiskSuite SMC	SAM, lvm/vg commands	SMIT, Mklv/crfs
Auto mount	automount	Automount + vold	automount	automount

In this section there are many differences between each system since each vendor was free to differentiate their OS software offerings and these areas are only loosely covered (or not covered at all) by POSIX standards. Since correct configuration of the kernel and the subsystems and applications is important to system security differences between the examined systems will be discussed.

The filesystem mount table (that defines which filesystems are mounted and with what options) is similar on Linux, Solaris and HP-UX (although the file location is different on Solaris) while AIX uses an entirely different format. The mount options can also vary from system to system, so consult the local man page for the available mount options on each system. The standard options for all systems are rw (read-write), ro (read-only) and suid/nosuid (set-user-ID allowed / denied). Additional options varying by filesystem type are available on each system (e.g. for quota, special device handling, handling of case in filenames, etc…).

On the systems examined, operating system files are usually installed in the /usr directory, with some optional features on Solaris and HPUX systems installed in /opt and on AIX in /usr/lpp. Sites are also free to establish their own standards / conventions. The most common conventions for local software installations are to install local or externally supplied software in /usr/local or /opt.

Kernel configuration differs greatly between the examined systems, however, where available, the vendor provided system management tools simplify

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

configuration for the average administrator. SMIT allows the configurations of some kernel options (mainly buffer cache and I/O settings). "Sysctlconfig" on Linux allows settings for a large number of resources (from buffer cache settings to TCP timeout settings) as does SAM's kernel configuration capabilities for HP-UX, allowing even the most novice system administrator to easily modify kernel configuration parameters. Kernel configuration on Solaris requires manual configuration of the /etc/system file although Solaris does allow the configuration of network driver parameters through the command-line "ndd" program. Ndd [11] can be used to examine and/or set kernel module parameters for the network drivers (arp, icmp, ip, tcp, udp, ip6, icmp6, tcp6, udp6, ipsecesp and ipsecah). A reference manual on the Solaris tunable parameters (in the /etc/system file) can be found on Sun's documentation web site [24].

Filesystem types also differ with each OS. All of the filesystems in the table above except ufs and hfs are capable of journaling, with the exception of Solaris's ufs implementation. Journaling improves filesystem stability by recording pending file system updates in an intent log, allowing fsck to run an intent log replay for quick recovery.

Logical Volume Management allows the allocation of hard drives into one or more physical volumes which are then combined into logical volume groups, capable of spanning many hard drives. Logical volume groups are divided into logical volumes which can be later resized and are assigned mount points / filesystems. Logical Volume Management can be an important component of disaster recovery, especially when combining RAID technology such as disk mirroring for quick recovery from hardware failures or with 3-way mirrors or occasional mirroring for use in upgrades and/or quick recovery from damage caused by a security breach. As of Red Hat Linux 8.0, LVM is available at system installation time [22]. Some limitations with the existing LVM implementations are HP-UX requires the logical volume to be unmounted while changes are made. The LVM implementations on RH Linux 8.0, AIX and HP-UX divide the disk into logical and physical extends (e.g. 4 MB chunks) which are then allocated into logical volumes. AIX has the only LVM implementation that allows the addition (extension) of disk space to a logical volume on the fly, while the volume is still in use.

With the addition of Solaris 10, sun has introduced zfs. zfs is both a file system and a LVM, allowing the creation of mirrors, raidz (like raid5), snapshots, and replication. ZFS is documented at http://docs.sun.com/app/docs/doc/819-5461.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Backup / Restore

	Linux	Solaris	HP-UX	AIX
Backup	dump	ufsdump	dump / vxdump / fbackup	backup
Restore	restore	ufsrestore	restore / vxrestore / frecover	restore
Other	Anaconda	Live-upgrade	Ignite-ux	mksysb / mkcd

All of the examined systems provide versions of the same basic backup and restore programs (dump/restore). Additionally, some systems provide tools that simplify cloning or disaster recovery procedures.

Solaris Live-Upgrade allows the creation of a cloned system disk for the purpose of upgrading and modifying the OS while the current OS is up and running. A reboot from the upgraded cloned disk would make the upgraded OS available. HP-UX's Ignite-UX, RedHat's Anaconda and AIX's mksysb and mkcd allow the creation of a bootable tape (or CD) that can restore the OS portion of the system (and any other selected filesystems) in its current state after a disaster. Mksysb can also clone the system disk to an alternate disk and apply filesets or fix bundles to the alternate disk after cloning. This feature is also useful when applying a set of patches that would typically have to be applied in single user mode (or a quiet system) by reducing system downtime to the time of a reboot. Procedures for cloning disks are also useful when recovering from a damaged system to security breach by helping preserve the state of the compromised system for further analysis or as evidence of the compromise. When cloning procedures are used together with LVM technology, recovery time from a security breach can be minimal, resulting in minimal downtime and quick resumption of business services, often critical to continued customer good-will or just staying in business.

Finally, there exist many commercial backup products that can simplify the backup and restore of user files both locally and over the network. A network backup product that allows users to query online file catalogs and request or initiate (with administrator approval) restoration of their files is UNISOL BART [10]. A widely used freeware backup product is Amanda [20], although Amanda doesn't currently support the spanning of large filesystems across multiple tapes.

It should be noted that regardless of the backup/restore product/procedure used, physical security of backup tapes is very important to a secure datacenter, just as physical security of the computer system itself is important.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

File Security

	Linux	Solaris	HP-UX	AIX
ACL	yes	yes	yes (HFS only)	yes
-- commands	getfacl/setfacl	getfacl/setfacl	lsacl/chacl getaccess chmod	aclget/aclput
--syscalls		acl/facl aclcheck/aclsort	[f]getaclentry [f]setaclentry [f]cpacl chownacl	[f]chacl/[f]statacl acl_[f]put acl_[f]get acl_[f]set acl_[f]chg

Access Control Lists (ACL) for files extend the standard UNIX file/directory permission model (read/write/execute for user, group and other) and allow a more granular approach to file/directory security.

The ACL interfaces provided by the examined Unix systems consist of a set of system calls to get and set the access control information of a file, as well as a set of user level commands that perform these functions. The function names though as well as the commands differ in each operating system since each vendor implemented their own ACL's. ACL's consist of sets of (user.group, mode) entries associated with a file and specify permissions. There are both restrictive (deny access that would otherwise be granted by less-specific entries) and permissive (grant access that would otherwise be denied by less specific entries) entries.

ACL entries may be lost if a backup/restore program is used that does not preserve ACL's (e.g. cpio). Therefore an alternate method of preserving and restoring ACL's must be devised if such a backup/restore program is used for disaster recovery purposes.

The unavailability of ACL's on HP-UX on the vxfs or jfs filesystems also makes these types of filesystems unsuitable for use on mount points where ACL's are strongly desired/required.

ACL's are available in beta mode for Linux systems and are not suggested for production use yet. Red Hat has removed ACL's from its latest production version (8.0) after including them in a couple of beta releases, but they are likely to re-appear in a later version.

HP-UX 11.11 now comes with ACL support for jfs filesystem by default and patches are available to enable ACLs for jfs filesystems on HP 11.00.

RHEL 3 and newer have come with ACL support by default.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

System Auditing

	Linux	Solaris	HP-UX	AIX
System Calls	yes	yes	yes	yes
Events	yes	yes	yes	yes
Users	yes	yes	yes	yes

Auditing is the ability of an operating system to log system activity at a granular level. The logs are intended for later review (manual or automatic) to gauge conformance of system and user activity to the organization's security policy and to detect suspicious activity. Auditing should be fine-tuned to the organization's security policy and determined risk in order to avoid auditing a too-wide range of events and risk overwhelming the administrator who must review the audit logs and not adversely affect system performance.

Although the examined audit subsystems provide the same general functionality, their configuration methods differ on each system (due to the different implementations).

HP-UX audit configuration can be performed from SAM, from the command line or programmatically, although the easiest way is through SAM. Audit logs (which usually reside in /.secure/etc) can be viewed from SAM or from the command line. From the command line, *audsys* is used to start, halt, set and display audit file information, *audomon* is the audit overflow monitor daemon, *audevent* is used to change or display event or system call status, and *audisp* displays audit information. Programmatically, *audctl* can be used to start, halt, set and get audit files, audswitch can suspend or resume auditing on the current process, audwrite writes audit records, getaudid/setaudid gets/sets the audit id (for the current process), getaudproc/setaudproc get/set the audit process flag, and getevent/audevent get/set events and syscalls audited.

AIX audit configuration can be performed from the command line or programmatically. AIX audit configuration files are stored in the directory /etc/security/audit. *Events* to audit are configured in the *events* file and can be grouped into classes in the *classes* stanza of the *config* file. Audit classes can be assigned to users (also) in the *config* file. Audit events can be assigned to an object (file) by modifying the *objects* file. The *audit* command is used to start and stop the audit subsystem and to query the subsystem for which events and objects are audited. The *auditselect*, *auditpr* and *auditstream* commands are used to select and display audit records, and *lsaudrec* and *rmaudrec* can display and even remove records from the audit log. Programmatically, *auditbin* defines files to contain audit records, *auditread*/*auditwrite*/*auditproc* read/write/set audit records/state, and auditevents gets/sets status of system event auditing.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Solaris audit configuration can be performed through the command line (commands *auditconfig***,** *auditon***,** and *audit*), while audit reporting is performed with the *praudit* command. A programmatic interface can also be used to construct and write audit records (*au_open*, *au_write*, *au_close*, *audit*, and *au_to_*)* and to get and manipulate audit file information (*getacinfo*) and audit class entries and events (*getauclassent*, *getauevent*). Auditing is enabled in run level 1 with the bsmconv command. More information on setting up auditing on Solaris systems is available from Sun's BluePrints site [23].

Redhat auditing can be enabled by doing a chkconfig of the auditd daemon. The /etc/audit.conf file controls the configuration for the audit daemon and the /etc/audit.rules daemon controls the audit rules to be loaded at startup. Linux now has an audit daemon available (auditd). RHEL5 ships with it, but it is disabled by default.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

	Linux	Solaris	HP-UX	AIX
At/cron.allow	yes	yes	yes	yes
Sendmail	8.11.6	8.11.6 / 8.12.2	8.9.3 / 8.11.0	8.11.0
TCP Wrappers	yes	yes	yes	yes
SSH	OpenSSH	OpenSSH	Secure Shell	OpenSSH
IPsec	FreeS/WAN	IPsec	IPsec	IPsec
Firewall	Iptables GNOME_Lokkit	SunScreen Lite/ipfilter or SunScreen ($)	IPFilter AAA/RADIUS	ipfilter/ iptables
IDS	snort	snort	snort IDS 9000	snort
OS hardening	Titan Bastille	Titan JASS "configurator" YASSP	Bastille	-

While some of these subjects have already been discussed in previous sections (e.g. services), the table above lists the methods and/or tools providing the first line of defense from external sources for the examined systems. While most systems in an organization will be behind a firewall, there will be some systems and/or services that will be exposed to the internet. Good security practices however must be followed for all systems within an organization since only one weak system is needed for a worm or other exploit to gain a beachhead inside a network from where other systems can be infected.

All of the examined systems support the use of the at/cron.allow/deny files to restrict access to scheduled jobs by users. These should be used to allow batch access only for legitimate/approved uses since they can be used to implement a future programmed attack (time-bomb).

HP-UX provides a range of free network security tools for download at the HP Software Depot (www.software.hp.com/ISS_products_list.html). These tools provide their own user interface application and are not integrated with SAM.

With versions of sendmail (the standard UNIX Mail Transfer Agent) being released at a fast pace, none of the vendors ship the most recent version of sendmail, although vendors try though to ship a version that is relatively secure, with no known vulnerabilities. No version however proved secure from the recent remote buffer overflow in header parsing reported by Mark Dowd of ISS X-Force. Since advance notice was given to all vendors, most vendors had patches available for download from their web sites within the next few days (HP had a patch available the next day, while Sun had a patch available within 3 days).

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Sites can always download and install the latest version available from sendmail.org (currently version 8.12.8).

It should be noted that sendmail is being used less and less and postfix seems to be the new MTA of choice for most linux distros. Many distros (e.g. Debian) go with Exim by default for a "normal"install, but postfix is usually used in its place for a mail server.

TCP wrappers can be installed and used on any of the examined systems. Both inetd and xinetd allow the configuration changes required for the implementation of TCP wrappers.

OpenSSH versions are also available for download and installation for the examined systems. Secure Shell on HP-UX is an HP implementation of OpenSSH. IBM makes available for download OpenSSH 3.4p1 in installp format for AIX 5.1 and 5.2L at the IBM developerWorks web site which is a good starting point for optional software downloads for AIX (www.ibm.com/developerworks).

IPsec is provided by default on AIX 5L and Solaris 9 with DES and 3DES encryption, and is available for download for HP-UX from HP's Software Depot. An encryption supplement kit for Solaris also adds AES and Blowfish encryption algorithms for IPsec, while HP's IPsec implementation supports DES, 3DES and AES. The open source FreeS/WAN software is an implementation of IPsec and IKE for Linux, and is available from www.freeswan.org. FreeS/WAN currently uses tripleDES and Blowfish encryption, with AES support in Beta mode.

Further, OpenVPN (http://openvpn.net/) has made inroads in cross platform VPNs. It allows SSL based VPNs between supported systems in point to point and remote access deployments. It does not run in kernel space, and makes use of system-provided tun drivers as its interface.

While in today's corporate environments Linux machines are more likely to be configured as a firewall than most Solaris, HP-UX or AIX systems, both Sun and HP provide software for free download that provide firewall functionality. AIX also provides by default Iptables and IPsec functionality, integrated into the OS and managed from SMIT. Lokkit is a simple firewall setup tool for Linux that configures a simple firewall (mainly for home based users) based on responses to some setup questions, while more complex configurations can be performed using the *firewall-config* program which generates the /etc/sysconfig/ipchains file.

The SunScreen Lite software allows a Solaris machine prior to version 10 to act as a firewall in a small environment (less than 10 machines) by providing such functions as basic packet filtering and VPN support, including IKE support. The full functioning Suncreen software (provided for a fee) provides access control, authentication, network data encryption, NAT support, Proxies and RADIUS and SecureID support.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

With the move to Solaris 10, Sun has provided IPFilter as a system default installation. Other changes in Solaris 10 includes Sun's "secure by default" effort, mimicking OpenBSD's effort to have as minimal a system footprint as possible on initial system installation. However, "secure by default" is not the default, and must be enabled with the command "svccfg apply /var/svc/profile/generic_limited_net.xml". This will disable all network services except for ssh.

In addition to the free IPFilter and IPsec software, HP also makes available for free download the AAA Server software which provides authentication, authorization and accounting of user network access by using the RADIUS protocol. Furthermore, the availability of the IDS 9000 software (an intrusion detection product with a Java-based administration GUI) makes a properly configured HP-UX machine a welcome addition to a secure network environment.

The open-source snort software, a network intrusion detection system, can be used on any of the examined systems. Snort is capable of performing real-time traffic analysis, packet logging and protocol analysis, and, can detect a variety of attacks. It has been ported to all of the examined systems and is available from www.snort.org.

It is suggested that if organizations are exposed to the internet and do not have on-site security expertise, they consider contracting with a Managed Security Service Provider (MSSP). MSSP's (discussed in the System Logging section of this paper) can provide a range of security services and can help an organization set security policies and maintain a secure environment.

Finally, before any one of the examined OS's can be exposed to the internet without the benefit of complete firewall protection, some level of OS hardening must be performed since there is a multitude of vulnerabilities that exist on a just installed OS for any of these platforms. One step of OS hardening consists of disabling unnecessary services, exposing system services to the network. To list the network ports open by system services the "netstat –af" command ("netstat –a –inet" on Linux) can be used, followed by cross-referencing non-named ports with the /etc/services file, and, reviewing the inetd configuration file.

Two noteworthy papers that discuss OS hardening procedures are *Solaris Operating Environment Security* [11] and *The Official Red Hat Linux Security Guide* [12]. The paper *Strengthening AIX Security: A System Hardening approach* [6] from IBM can be helpful for AIX systems, with a description of system services and recommendations for services to disable on pages 29-43. IBM's web site also contains links to additional papers and tutorials on tightening AIX security. While internet facing systems would generally be protected by a

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

firewall and would not expose usually internal services to possible outside attacks, unnecessary services can be exploited by intruders that have gained a foothold in the local network and should thus be disabled to eliminate any possible exploits. Services that can be disabled on back room servers or on internet facing servers are: bootp, chargen, comsat, time, daytime, discard, dtspc, echo, exec, finger, rlogin, pcnfsd, rexd, quotad, rstatd, rusersd, rwalld, rwhod, rsh, sprayd, talkd, telnet, ftp, tftp, ttdbserver, uucp, automountd, ttdbserver, X11/CDE, dchpd, rpc.yppasswd, ypupdated, and sendmail (except on mail server). A more aggressive approach would also disable NFS type services unless the system is actually an NFS file server (nfs, biod, keyserv, rpc.lockd, rpc.mountd, rpc.statd), lpd, documentation (web) servers, and automountd. The papers sited above provide more detail about each service that may be disabled and the situations on which each service may be required.

Some tools also exist that aid in OS hardenings: *JASS* (from Sun [13]), "*configurator*" (from Hal Pomeranz [14]), *Titan* [16], and *Bastille* [17].

JASS [13], also known as the Solaris Security Toolkit is comprised of a set of scripts implementing the recommendations of the Solaris Security papers in BluePrints. To tighten network security, JASS performs its work largely by invoking the *ndd* command, which gets and sets driver configuration parameters for the ARP, ICMP, IP, TCP and UDP protocols.

Configurator [14] is a tool created by Hal Pomeranz that implements the procedures discussed in his book *Solaris Security: Step-by-Step [15]*.

Titan [16] is a collection of programs that either fix or tighten potential security problems, and runs on Solaris and (somewhat minimally) on Linux and Free BSD.

The *Bastille* [17] Hardening System supports Linux (Red Hat, Mandrake, Debian) and HP-UX (HP offers for download an HP-UX version at its Software Depot). Bastille draws from several sources including SANS' Securing Linux Step-by-Step and Kurt Seifried's Linux Administrator's Security Guide.

The Center for Internet Security has worked to develop security benchmarks and scoring tools for Operating Systems. It has benchmarks for Solaris 2.5 – 9, Solaris 10, AIX, HP-UX and Redhat. The Center provides Internet security benchmarks based on recognized best practices for deployment, configuration, and operation of networked systems. The Center's security-enhancing benchmarks encompass all three factors in Internet-based attacks and disruptions: technology (software and hardware), process (system and network administration) and human (end user and management behavior). The benchmarks are open, that is, publicly available to everyone

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Since it seems that there is a definite wealth of reference material and tools to aid IT organizations in securing their systems. The best approach to system hardening would be to categorize each machine by function (e.g. development workstation, development server, backroom server, internet facing server), develop a set of hardening procedures for each category and perform the hardening of each system as a matter of routine.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Conclusion

Maintaining secure systems and networks is an ongoing process fraught with difficulties, which are further exacerbated in heterogeneous, multi-Operating System environments by the multitude of differences between the various operating systems and the procedures that must be followed in order to maintain a high level of system and network security. A good understanding of the configuration differences and the tools available on each operating system is key to maintaining a secure environment and in helping IT personnel select the best operating system for the intended IT function, when a choice is possible.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

References

[1] HP Software Depot , <http://www.software.hp.com/>. Security_patch_check is available from: <http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA>.

[2] HP IT Resource Center, <http://support.itrc.hp.com>, requires (free) login.

[3] IBM Fix Delivery Center for AIX Version 5, <https://techsupport.services.ibm.com/server/aix.fdc>.

[4] SunSolve Patch Support Portal, <http://sunsolve.sun.com/patches>.

[5] Red Hat Network <https://rhn.redhat.com>.

[6] "Strengthening AIX Security: A System Hardening Approach – white paper" <http://www.ibm.com/servers/aix/whitepapers/aix_security.pdf>. Additional papers are available from <http://www.ibm.com/servers/esdd/articles/unixsecurity.html>. Online tutorials can be found at <http://www.ibm.com/servers/esdd/tutorials.html>.

[7] UNISOL JobAcct is resource accounting and chargeback software for UNIX and Windows systems from UniSolutions Associates <http://www.unisol.com/jobacct.html>.

[8] newlogcheck.sh, <http://www.campin.net/newlogcheck.html>.

[9] sentryd, <http://www.cpan.org/scripts/admin/sentryd>

[10] UNISOL BART is a network backup, archive, restore and tape management product from UniSolutions Associates <http://www.unisol.com/bart.html>.

[11] pages 5, 9-25, "Solaris Operating Environment Security <Updated for Solaris 8 Operating Environment)" by Alex Noordergraaf and Keith Watson, Sun BluePrints Online – April 2001, available from <http://www.sun.com/solutions/blueprints/1200/network-updt1.pdf>

[12] "The Official Red Hat Linux Security Guide for Red Hat Linux 8.0", <http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/pdf/rhl-sg-en-80.pdf>.

[13] JASS, the "Solaris Security Toolkit", available from <http://www.sun.com/solutions/blueprints/tools> (free license required).

[14] Configurator, is a set of scripts and configuration files available from <http://www.deer-run.com/~hal/jumpstart/configurator/config.tar.Z>.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

[15] “Solaris Security: Step-by-Step”, by Hal Pomeranz, available from <http://store.sans.org/store_item.php?item=21>.

[16] Titan: <http://www.fish.com/titan>.

[17] Bastille is available from <http://www.bastille-linux.org/> and from the HP Software Depot <http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6849AA>

[18] “Outsourcing Managed Security Services” from CERT, discusses the [18a] benefits and [18b] risks of retaining MSSP’s, and can be found at <http://www.cert.org/security-improvement/modules/omss/index.html>.

[19] Webmin is a web-based interface for system administration for UNIX: <http://www.webmin.com/>.

[20] Amanda is the “Advanced Maryland Automatic Network Disk Archiver”: <http://www.amanda.org/>.

[21] syslog.conf configuration, section 4, page 3 of “*Securing AIX Network Services”*: <http://www-1.ibm.com/servers/esdd/tutorials/aix/4_3.html>.

[22] “Chapter 10, LVM Configuration” of the “*Red Hat Linux 8.0: The Official Red Hat Linux Customization Guide”* <http://www.redhat.com/docs/manuals/linux/RHL-8.0-Manual/custom-guide/ch-lvm.html>.

[23] Pages 5-21, “Auditing in the Solaris 8 Operating Environment “(February 2001) *by William Osser and Alex Noordergraaf* <*http://www.sun.com/blueprints/0201/audit_config.pdf>.*

[24] The “*Solaris Tunable Parameters Reference Manual”*, can be downloaded from: <ftp://docs-pdf.sun.com/806-7009/806-7009.pdf>.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.