Computing Resources
The Lister Hill National Center for Biomedical Communications

LHC Unix System Hardening Guidelines

A Companion Document to the CIS Solaris and Linux Guidelines

Sarah Ward
June 22, 2005

Document Log

Date	Description	Author
4/7/05	Created document	Sarah Ward
4/8/05	Revision to Section 1.3	Sarah Ward
4/15/05	Revision to Section 1.3 and Section 2.5	Sarah Ward
5/11/05	Add Section 1.49	Quang Le
6/22/05	Add Section 3 and re-format the document	Kevin Sung

Table of Contents

1 LHC Production Systems Hardening Guidelines for Unix

The CIS Solaris and Linux guidelines are to be followed when hardening Unix systems along with the LHC recommendations to follow. Please make special note of the exceptions to the CIS guidelines highlighted in Section 2 of this document.

Below is a list of hardening guidelines for use with Production Unix servers. Production servers are particularly in need of hardening due to the fact that they are running public facing services. The underlying principal to the hardening is least privileges: services only run if they are absolutely required to support the business critical mission of the server. Production systems are not, as a rule, allowed to communicate with private, desktop, development or internal use systems. Any communications that must be allowed to support the system is performed through a secure channel that is tightly controlled by an administrator that has been strictly authenticated.

The guidelines below are principally to set forth policy, not necessarily to provide a cookbook of how to carry out the policy.

1.1 Disable all services that are not absolutely necessary.

Disable all services that are not absolutely necessary to directly support the business critical function of the public server.
- REQUIRED

1.2 Create non-root users to perform non-root tasks.

- REQUIRED

1.3 Create separate user accounts for each person required to access the machine.

- REQUIRED

- The system administrator of each machine will have a local account that follows the LHC account naming convention.

- The system administrator of each machine will have a local administrator account. The naming convention will be the first initial of the first name plus the first initial of the last name plus ‘root’. If the name collides with an existing name, use the initial of either the middle name or the second letter of the last name until a unique name is found.

- Each system is required to have the LHC system administrator(s) local account and local administrator account added. Initially the following accounts will need to be

added manually or automatically using the jumpstart server:

User name: qle
Description: Quang Le

User name: qlroot
Description: Quang's root account

- Internal Unix machines will be allowed to use centralized user account such as NIS or LDAP in the future.

- For public-facing servers, NIS must not be used. Make sure /etc/nsswitch.conf entries do not use "nis", "nisplus", or "compat". For Linux systems, do "/sbin/chkconfig ypbind off". For Solaris, remove the file /etc/defaultdomain, if present.

1.4 Do not allow "root" to login remotely.

Root is gained only through a user that is logged on and has permissions to "su". Root is allowed to login only at the physical console
- REQUIRED (except at console)

1.5 Do not allow service accounts to log in.

Only individual users may log in, providing an audit trail.
- REQUIRED

1.6 Use a non-existent directory where possible.

If a service account requires a /home directory, use a non-existent directory where possible. In the production environment the /home directory must not store personal information. Directories specific to each project will be created.
- REQUIRED

1.7 Service Account users should not have a valid login shell in /etc/passwd.

Use something such as /bin/false. There are cases where there has to be a shell for the program to work
- STRONGLY RECOMMENDED, but do this where possible

1.8 Set the sticky bit on a directory.

So that a user can remove only files within it that are owned by that user. This should be used in /tmp. And /var/tmp
- REQUIRED

1.9 Carefully examine the need for suid and sgid bit

whenever it is found in conjunction with programs that are not required to support the business function of the public server. Avoid using suid and sgid where possible.
- REQUIRED

1.10 Scan (using chron) for changes to suid and sgid

Report the output of the scan to show all suid and all sgid bit application
The number of apps using these should be very small
Look at all auto homes
- STRONGLY RECOMMENDED

1.11 Separate the roles of public and back-end servers.

Do not allow a single server to perform multiple critical functions or provide both public services and support services. (Do not allow a single server to be syslog, mail, web, etc.)
- REQUIRED

1.12 Remote log to a tightly controlled box;

a purpose-built syslog server. Use Swatch.
- REQUIRED

1.13 Consider using the chattr command.

When syslogging files, consider using the chattr command. The +a option in chattr puts the messages in append-only mode. The syslog process can continue to send logs and makes it very difficult to tamper with old logs. (This will help foil script kiddies that don't know to chattr -a) [Especially on syslog server]
- RECOMMENDED

1.14 Maintain and store off machine checksums for directories

such as bin, sbin, lib, and etc.

1.15 Run Tripwire or AIDE.

Run the baseline on the freshly completed build to create the baseline and store the baseline off server. Baseline to read-only media.
- REQUIRED

1.16 Run tripwire or an MD5 hash scan to look for unauthorized changes.

Run the scan weekly for Production systems.
- STRONGLY RECOMMENDED

1.17 Remove version banners from sendmail, apache, etc

- STRONGLY RECOMMENDED

1.18 Check for RPC services using Nmap.

Any services that must run should use ipchains/iptables rules to allow access only by appropriate hosts. Use /etc/hosts.allow to restrict which machines can access the portmapper.
- REQUIRED

1.19 Do not use NFS on production systems

- VERY STRONGLY RECOMMENDED

1.20 If NFS must be used, it must not be auto-mounted

- REQUIRED

1.21 Use read only when using NFS.

If you must use NFS, use read only. Restrict NFS to specific addresses with ipchains or similar.
- REQUIRED

1.22 Wrap and/or firewall RPC.

With NFS it is possible to determine what other hosts are on the network by seeing where filesystems are exported to. Wrap and/or firewall RPC.
- REQUIRED

1.23 Don’t allow hosts to mount NFS volumes as “root” and do not allow “suid”.

If you must use NFS, don't allow hosts to mount NFS volumes as “root” and do not allow “suid”.
- REQUIRED

As with everything else that is blocked by the firewalls, make sure not to allow port 2049 so that you do not expose “showmount”.

1.24 Examine /etc/exports.

If you must use exports, examine /etc/exports to make sure nothing is being exported read/write to the world. /etc/exports should be as limited as possible. Nothing should ever be exported to the world. Export to specific host/user only.
- REQUIRED

1.25 XDM – Remove X windows services on production systems.

If you absolutely require X on a production system (and I don't know why this would be the case) configure Xdm to be local only. Tell Xdm not to accept remote Xdm requests, edit /etc/X11/xdm/xdm-config and add the line DisplayManager.requestPort:0, then comment out all lines in the /xdm/Xaccess, specifically the one with the * at the beginning of the line: * # allow any host to conect. If you require X add network filters that allow only specific clients to connect. Use ipchains/iptables rules to allow only specific and deny all others. Do not allow X to listen. Add-nolisten tcp options to all entries in the /etc/X11/xdm/Xservers file. SSH has X11 forwarding built in (placing forwardx11 yes in /etc/ssh/ssh_config and ~/.ssh/config, but disable X11 forwarding if not needed). Consider using xauth and the -auth argument. Check permissions on .Xauthority.
I.E. DISABLE XDM on any production system where possible.
- STRONGLY RECOMMENDED

1.26 Do not allow XDM to accept remote requests.

- REQUIRED

1.27 Disable ssh-agent forwarding.

- REQUIRED

1.28 Do not allow SSH auth keys in /home directories.

Use SSH only after it has been compiled so it will not allow users to create their own individual auth keys. If SSH auth keys are required, it is only via an exemption, which requires Security Administrator written approval on a per application basis. If using SSH auth keys, logging into other systems must require a pass-phrase. Auto-authentication is not allowed.
- REQUIRED

1.29 Turn off all “r” commands, such as rlogin.

- REQUIRED

1.30 Do not use multiple-use passwords on any production systems.

Instead, use SecurID single use passwords on all production systems. Each user will require an RSA token for system access.
- REQUIRED

1.31 Move DNS to its own host, keep services separated.

- REQUIRED

1.32 Turn off source routing in the Linux kernel;

"routed" should not be running. Additionally use a host firewall, such as ipchains/iptables.
- REQUIRED

1.33 Prevent new route additions.

Kill "routed" and "gated", disable them in /etc/rcX.d. Point to a purpose-built router exclusively. There is no need for routing protocols on a production server.
- REQUIRED

1.34 Deny ICMP redirects, change the /proc entry.

- RECOMMENDED

1.35 Use on-board SSL certificates to validate communication is only occurring from trusted hosts.

- RECOMMENDED, as supported by services.

1.36 Disallow anonymous LDAP access on production servers.

- REQUIRED

1.37 Make sure history files are readable only by the owner.

If you do not wan to log history commands, unset the HISTFILE environment variable and turn off history logging.

- Use BASTILLE
- Enforce limit to size of history file
- Store in shell only
- Delete history files on log out

1.38 Do not store authentication information in .netrc for FTP.

If they are running FTP and not using SCP, but otherwise, wherever possible use SFTP in place of FTP.
- REQUIRED

1.39 Enforce separation of services.

Production servers should not be running print servers.
- REQUIRED

1.40 Eliminate the use of "." in paths.

Do not include "." in the user PATH variable.
- REQUIRED

1.41 Mount /home (and possibly /tmp /var/tmp) with the noexec flag,

wherever possible. No suid.
- REQUIRED

1.42 Create separate partitions for each of the following directories:

- /home (best practice)
- /var (best practice)
- /tmp (best practice on Linux, already done on Solaris)
  - BEST PRACTICE, outside the scope of security

1.43 Validate, security test applications prior to going live.

Inspect and validate all CGI programs. Validate user input. Sanitize input. Check fields. Use MD5 digests to validate the integrity of hidden fields. Check length. Etc. Use automated tools to test validation of script input. This must be done as part of a validation process prior to the server being allowed to go live.
- REQUIRED

1.44 Remove anything in cgi-bin or bin that shouldn't absolutely be there.

- STRONGLY RECOMMENDED

1.45 Turn off PHP register-globals in httpd.conf wherever possible.

- REQUIRED

1.46 Implement host access controls using inetd and TCP Wrappers.

Check TCP wrappwr rule validity with tools like tcpdchk and tcpdmatch.
- REQUIRED

1.47 Chroot applications into a jail, application by application.

Use jails with service applications. Not root to run service applications. Required wherever possible.
- REQUIRED

1.48 No compilers are allowed on production servers

- REQUIRED

1.49 RSA SecureID has been activated for remote logins

- REQUIRED

2 Exceptions to CIS Guidelines

2.1 Skip 8.1 – Block System Accounts

2.2 Skip 2.8 – Only enable CDE-related daemons if absolutely necessary

2.3 Skip 3.17 - Only enable GUI login if absolutely necessary

2.4 Edit /etc/init.d/syslog

Edit /etc/init.d/syslog so that syslog starts with the "-t" option. This tells syslogd not to listen to JDP port 514 for messages from other systems. Obviously, this should not be done on the loghost.

2.5 Skip 7.13 – Set EEPROM security-mode and log failed access

3 Additional exceptions for internal machines to CIS Guidelines

3.1 For Solaris 9 machine

3.1.1 Run – 3.7 “enable Windows-compatibility servers”

3.1.2 Run – 3.8 “enable NFS server processes”

3.1.3 Run – 3.9 “enable NFS client processes”

3.1.4 Run – 3.10 “enable automount daemon”

3.1.5 Run – 3.11 “enable other RPC-based services”

3.1.6 Run – 3.17 “enable GUI login”

3.2 For Solaris 10 machine

3.2.1 Run – 2.2 “enable RPC-based services”

3.2.2 Run – 2.3 “enable secure RPCs”

3.2.3 Run – 2.5 “enable NIS client daemons”

3.2.4 Run – 2.11 “enable GUI”

3.2.5 Run – 2.14 “enable Windows-compatibility servers”

3.2.6 Run – 2.15 “enable NFS server processes”

3.2.7 Run – 2.17 “enable NFS client processes”

3.2.8 Run – 2.18 “enable automount daemon”

3.3 For LINUX machine

3.3.1 Skip – 3.4 “Disable GUI login”

3.3.2 Skip – 3.5 “Disable X font server”

3.3.3 Run – 3.7 “enable SMB (Windows filesharing) processes”

3.3.4 Run – 3.8 “enable NFS server processes”

3.3.5 Run – 3.9 “enable NFS client processes”

3.3.6 Run – 3.11 “enable NIS client processes”

3.3.7 Run – 3.12 “enable RPC portmap process”