Global Information Assurance Certification Paper

Installing and Securing an SSH Server with HP Secure OS Software for Linux and Cryptography

SANS GIAC GCUX Practical Assignment v1.7

Kenneth Gallo
October 2001

Section 1 - Overview

1.1 - Executive Summary

HP Secure OS Software for Linux (HP-LX) is Hewlett-Packard's new high security version of Linux. Designed for running applications and services in high-risk environments, HP-LX v1.0 is a hardened Red Hat 7.1 base integrated with innovative security technologies like strong compartments and kernel-level auditing.

HP-LX combined with a cryptographic filesystem further enhances security by introducing another layer to the multiple layers of defense already present. Those defenses protect the system and reduce the risks to data.

This paper will detail, step-by-step, how to create a secure SSH server running with a cryptographic filesystem on HP-LX v1.0.

1.2 - What is HP Secure OS Software for Linux?

HP Secure OS Software for Linux (HP-LX) is a high security version of Red Hat 7.1 Linux that implements a defense-in-depth model: multiple independent layers of security. If an attack bypasses one layer, the next layer will stop it. HP-LX uses these layers to prevent and contain attacks, protecting the system and its services.

Several innovative layers of security are introduced by HP-LX:

System Hardening – Most Linux systems install with weak file permissions and service configurations, making them easy targets for attackers. HP-LX files and services are tightened from the start, and are further tightened by a hardening script after installation.

Security Compartments – Linux depends on discretionary access controls to protect files, processes, and users. Users control their own protection, and may unintentionally open security holes. HP-LX adds mandatory access controls, configured by administrators and enforced by the kernel. The additional controls create distinct security compartments, or virtual rooms, for each critical service or device. No communication of any kind is allowed in or out of a compartment unless an administrator has specifically authorized it.

Enhanced Auditing – Linux comes with a limited auditing system (syslog). In addition to using syslog, HP-LX adds a flexible new auditing system at the kernel level. Being located on the kernel interface allows the system to monitor more activity, and makes it very hard for an attacker to bypass.

Following the defense-in-depth model, additional layers can bring additional security. HP-LX already has several very strong layers; on top of those this paper will add a cryptographic filesystem layer. It will detail, step-by-step, how to create a secure SSH server running on HP-LX v1.0 with a cryptographic filesystem.

Section 2 – System Installation

2.1 - System Requirements

HP-LX 1.0 is based on Red Hat 7.1, and works on any x86 hardware supported by Red Hat. For a list, see http://www.redhat.com/support/hardware/.

This paper assumes readers will implement the checklist on an x86 computer. The following hardware was used to test the checklist, and should be considered as a reasonable minimum:

- Pentium III 500mhz
- 2GB hard disk
- 128mb RAM
- CD-ROM drive
- Floppy diskette drive
- 2 Network Interface cards

Note: any remote computer that will be used to administer or access the HP-LX system must have an SSH v2 compatible client.

Print out Appendix A and use it as a checklist to record progress.

2.2 - Installation

A) **Network Status**
Make sure the system is disconnected from network. A new system runs a higher risk of being compromised if it is connected before it is secured.

Note: Because of this, a separate computer with Internet access and a CD burner will be needed to transfer certain files in **Section 3: Cryptographic Filesystem**.

B) **Boot from HP-LX Disc 1**
Enter the text installer mode when prompted:

```
boot: text
```

If the system cannot boot from a CD, make a boot diskette with the utilities on HP-LX disc 1 under /images.

Note: a boot diskette made with standard Red Hat 7.1 will not work.

C) **Installation Language & Keyboard Selection**
The HP-LX installer menus operate very similarly to the Red Hat 7.1 installer. Choose the most appropriate installer language & keyboard settings.

D) **Install Type**
Unlike Red Hat 7.1, there are no options for Workstation, Laptop, or Custom installations. Select the only available option: Server installation.

E) **Hard Disk Partitioning**
Choose to 'Initialize' the hard disk, then select 'Disk Druid' as the partitioning tool. Use the following table as minimum guidelines:

Mount Point:	Minimum Size:
/	256mb
/boot	31mb
/usr	512mb
/var	256mb
/home	32mb
<swap>	256mb *
/data	640mb

Be sure to save the changes to the partition table, and format each partition.

Note: HP-LX documentation instructs the creation of a /compt partition. Do not do this yet, it will be added later as a mount point for the cryptographic filesystem.

* - Swap partition size is largely dictated by the amount of physical RAM installed. As a general rule, make the partition twice the size of installed RAM.

F) **File Integrity Checking**
Select 'Enable Tripwire', then enter site and local Tripwire passwords. In the e-mail field be sure to enter an address that is not on the local box.

It is critical that Tripwire has strong passwords: 10 or more characters; non-dictionary word; includes numbers, symbols, upper & lower case [1]. Enter different passwords for the site and local password fields.

HP-LX uses the open-source free version of Tripwire v2.3.1.2 to maintain watch on the system. Tripwire makes scheduled fingerprints of key files on the system, comparing them to older fingerprints to detect changes. Unexpected file changes may indicate an intruder and Tripwire emails reports of those changes to email address supplied above.

G) **Network Configuration**
Enter the correct settings for the network the system will be attached to. Static I.P. addresses are required for each interface because DHCP is disabled by default for security reasons.

As part of the HP-LX mandatory access control model, no network traffic is allowed unless it is specifically authorized. Therefore, DHCP will not work because there are no rules authorizing such traffic.

Note: DNS access, which also requires network traffic, will partially work. This is because the system automatically creates rules specifically authorizing that communication for certain applications.

Enter the hostname for the new system when prompted.

H) **Mouse Selection**
Choose the most appropriate mouse setting.

[1] HP-LX Install Guide, p.1-5.

I) **Language & Time Zone Selection**
Select the most appropriate language and time zone settings according to system location or company policy.

Optionally, set the system clock to UTC (Universal Time Coordinated) instead of the local time zone. This will allow easier management and security event correlation if managing systems in different parts of the world.

J) **Account Creation**
This step sets the root password and creates a non-privileged user on the system; be sure to make at least one such user.

It is critical that the root account has a strong password: 10 or more characters; non-dictionary word; includes numbers, symbols, upper & lower case [1].

When connecting over the network, HP-LX enforces a good security practice by requiring the root user to first login as a non-privileged user, then '`su`' to root when required for specific actions. Additionally, the system will later be configured to allow only the root user the ability to login at the console (the keyboard attached to the system).

All other accounts can only be accessed over the network, and only via SSH public-key authentication. However, non-privileged user accounts should also have strong passwords, even though those passwords will probably never be used. This is part of the defense-in-depth strategy: adding another layer of security in case the first one is compromised.

Note: HP-LX automatically creates a user called "tlinuxadm" to function as an administrator for special security functionality. The "tlinuxadm" user is a non-privileged user under the conventional Linux discretionary access controls, but is all-powerful under the HP-LX mandatory access controls. By default, not even the root user has the same access to the special utilities allowed to "tlinuxadm".

K) **Package selection**
HP-LX makes package selection easy; there are only four optional package categories available: X Windows, KDE, Development, and Utilities.

Do not select any package categories. HP-LX includes an SSH server by default, all other applications will be added later as needed.

Note: This is an example of another good security practice: only install what is absolutely needed for the system to perform its duties. Any additional applications merely function as more opportunities for an attacker to compromise the system.

L) **Bootdisk Creation**
It is recommended that this opportunity be taken to create a boot diskette. A boot diskette is required in the event the primary boot image becomes corrupted. After creation, remove the diskette and store it in a safe place away from the system.

[1] HP-LX Install Guide, p.1-5.

M) **SSH Key Uploading**

Only SSH v2 is permitted for remote shell access to an HP-LX system. Therefore any systems that will be used for remote administration or access must have an SSH v2 client. As added security protection, all SSH connections must be authenticated with public keys rather than simple passwords.

On the remote system, generate an SSH public key of at least 1024 bits. Syntax will vary depending on the choice of SSH client; consult the relevant client's documentation. Save the SSH public key to a floppy diskette.

When prompted by the HP-LX installation program, insert that floppy diskette into the new system. The SSH key will be the only valid key for remote access to the "tlinuxadm" user.

N) **Reboot**

Remove the SSH key diskette and HP-LX disc, then reboot.

O) **Set the Hostname**

The hostname must be re-entered. Replace the "`name`" string below with the hostname defined in step G:

```
[root@localhost /]# hostname name
```

Edit the '/etc/sysconfig/network' file, and modify the "HOSTNAME" variable to equal "`name`".

Note: The hostname of the system described in this paper is "HP-LX".

Section 3 – Cryptographic Filesystem

3.1 - Cryptographic Filesystem Background

By default HP-LX uses the ext2 filesystem, the same found in most standard Linux systems. The ext2 filesystem, a stable and mature solution, typically relies on discretionary access controls for security. As will be described in a later section, HP-LX further protects the filesystem via mandatory access controls managed by the kernel.

However, even with the combination of discretionary and mandatory access controls, there are still risks to the filesystem:

Kernel-Bypassing
A very sophisticated attacker might exploit a weakness in the system to bypass part or all of the kernel, allowing access to particular sectors or inodes on the disk.

Physical Access
A more likely risk: an attacker has physical access to the system. The attacker steals the disk, mounts it in a separate system she already controls, then can easily read any file on that disk. The same result is reached if the attacker can circumvent the BIOS password protection and boot the system from a compromised floppy diskette.

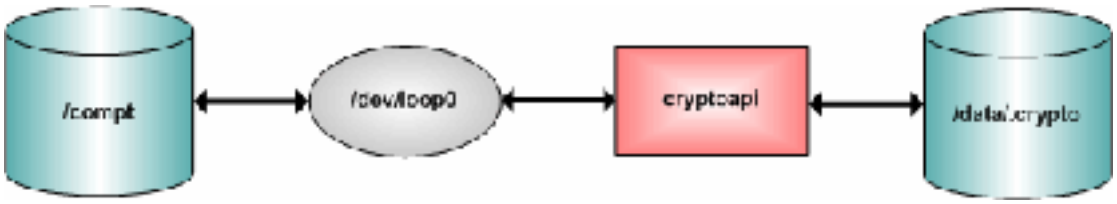
One of the design assumptions of any commercial OS, including HP-LX, is that physical access to the machine is secure. Adding a cryptographic filesystem below the ext2 filesystem can help relax that assumption and significantly reduce the above risks. Even if the kernel is bypassed, the disk is stolen, or the system is booted off a floppy diskette, an attacker only gets encrypted bits. This solution allows all the benefits of cryptography, while retaining all the strengths of ext2.

This cryptographic filesystem is not only useful for SSH servers. A web, database, or file server would also gain the same benefits described above.

There are several encrypted filesystem solutions available for Linux. The Cryptoapi v2.4.7.0 solution was chosen because it:

- requires very little modification of the underlying OS.
- is mature and stable
- is the official result of the 'International Linux Kernel' project: (http://www.kerneli.org)

Here is a representation of how the cryptographic filesystem will be implemented:



Visual Metaphor of Cryptographic Filesystem

The directory '/compt' is actually a mountpoint attached to '/dev/loop0'. '/dev/loop0' is, in turn, attached to the file '/data/.crypto'. The '/data/.crypto' file is a single large file with all of the encrypted data. Inside that encrypted data is an ext2 filesystem.

All of this functionality is transparent to users and applications. Write and read requests for files in '/compt' get sent to '/dev/loop0'. '/dev/loop0' calls the cryptoapi to encrypt or decrypt the stream of bits going to or from '/data/.crypto'. [2]

3.2 – Installing Cryptography

A) Certain files must be downloaded from Internet, however it is not yet safe to plug the system into a network. As a workaround, download the following files to a separate computer, then copy them to a CD-R:
ftp://ftp.kernel.org/pub/linux/utils/util-linux/util-linux-2.11k.tar.gz
http://prdownloads.sourceforge.net/cryptoapi/cryptoapi-2.4.7.0.tar.gz

Installing the cryptographic functionality will require a valid kernel include tree to be present. There are also certain minor issues with the kernel module path in the kernel that ships with HP-LX v1.0. To correct these issues, a new HP-LX kernel will need to be compiled and loaded. The fixed kernel is available at:
ftp://ftp.hp.com/pub/security/hplx_source/v1.0/kernel_patches.tar
ftp://ftp.hp.com/pub/security/hplx_source/v1.0/kernel_extensions.tar

Note: All of the above files were current as of publication. Download newer versions if they are available and adjust the version numbers below accordingly.

B) If the current user is not already root, run the following command:
```
[user@hp-lx /]# su
```

Then insert and mount that CD-R in the HP-LX system and copy all the new files to '/tmp'. Eject the disc.

C) Because no optional application packages were selected during installation, the system does not yet have the ability to compile the kernel and other programs.

Insert and mount HP-LX Disc 1 in the HP-LX system. Run the following commands in the order below:
```
[root@hp-lx /]# cd /mnt/<cdrom device>/RedHat/RPMS/
[root@hp-lx RPMS]# rpm -ivh kernel-headers-2.4.2-2.i386.rpm
[root@hp-lx RPMS]# rpm -ivh glibc-devel-2.2.2-10.i386.rpm
[root@hp-lx RPMS]# rpm -ivh binutils-2.10.91.0.2-3.i386.rpm
[root@hp-lx RPMS]# rpm -ivh cpp-2.96-85.i386.rpm
[root@hp-lx RPMS]# rpm -ivh gcc-2.96-85.i386.rpm
[root@hp-lx RPMS]# rpm -ivh libstdc++-devel-2.96-85.i386.rpm
[root@hp-lx RPMS]# rpm -ivh gcc-c++-2.96-85.i386.rpm
[root@hp-lx RPMS]# rpm -ivh make-3.79.1-5.i386.rpm
[root@hp-lx RPMS]# rpm -ivh patch-2.5.4-9.i386.rpm
```

[2] Mutz, URL.

```
[root@hp-lx RPMS]# rpm –ivh perl-5.6.0-12.i386.rpm
[root@hp-lx RPMS]# rpm –ivh ncurses-devel-5.2-8.i386.rpm
```

All of these packages will at the end of this section. Eject HP-LX Disc 1.

D) The kernel must be extracted and patched.
First, extract the 'kernel_patches' file:
```
[root@hp-lx /tmp]# tar –xzvf kernel_patches.tar.gz
```

Inside the above file is a copy of the standard Linux kernel. Extract that into to the '/usr/src' directory:
```
[root@hp-lx /tmp]# cd /usr/src/
[root@hp-lx src]# tar –xzvf /tmp/kernel_patches/linux-2.4.5.tar.gz
```

There are only a few lines difference between the standard Linux kernel and the HP-LX kernel. The following makes that change:
```
[root@hp-lx src]# cd linux/
[root@hp-lx linux]# patch -p1 < /tmp/kernel_patches/patch-2.4.5
```

The following are additional patches to fix unrelated issues in the kernel:
```
[root@hp-lx linux]# patch -p1 < /tmp/kernel_patches/linux-2.4.5-
aacraid-030101.patch
[root@hp-lx linux]# patch -p1 < /tmp/kernel_patches/linux-2.4.5-
axboe-scsi-max-sec.patch
[root@hp-lx linux]# patch -p1 < /tmp/kernel_patches/linux-2.4.5-
initrd-swapper-oops.patch
```

In order for the cryptographic filesystem to perform reliably, the following patch is needed to address a bug in Linux kernel versions < 2.4.6:
```
[root@hp-lx linux]# cd /tmp
[root@hp-lx /tmp]# tar –xzvf cryptoapi-2.4.7.0.tar.gz
[root@hp-lx /tmp]# cd /usr/src/linux/
[root@hp-lx linux]# patch –p1 < /tmp/cryptoapi-2.4.7.0/doc/loop-iv-
2.4.6.patch
```

Finally, the HP-LX kernel configuration file must be copied into '/usr/src/linux'. First, look at the last seven characters returned by the following command:
```
[root@hp-lx linux]# ls /lib/modules/2.4.5*
```

Then take those characters, and append them to the "/tmp/kernel_patches/kcfg/" string in the following command:
```
[root@hp-lx linux]# cp /tmp/kernel_patches/kcfg/
/usr/src/linux/.config
```

E) Now the new kernel must be compiled and installed, allow some time for these operations:
```
[root@hp-lx linux]# make menuconfig
```

Do not make any changes. Exit and, when prompted, save the kernel configuration. Then run the following commands:
```
[root@hp-lx linux]# make dep
[root@hp-lx linux]# make bzImage
```

```
[root@hp-lx linux]# make modules
[root@hp-lx linux]# cp arch/i386/boot/bzImage /boot/tlinux-2.4.5-
hplx
[root@hp-lx linux]# chmod 755 /boot/tlinux-2.4.5-hplx
[root@hp-lx linux]# ln -sf /boot/System.map-2.4.5-hplx
/boot/System.map
[root@hp-lx linux]# make modules_install
```

F) The bootloader must be updated to load the new kernel. In the '/etc/lilo.conf' file change the line that begins with "image=/boot/tlinux-2.4.5…" to "image=/boot/tlinux-2.4.5-hplx". Save the changes to the '/etc/lilo.conf' file, then run:

```
[root@hp-lx /etc]# lilo -v
```

Note: If any issues are encountered, consult the "Linux Kernel How-to" at http://www.linuxdocs.org/HOWTOs/Kernel-HOWTO.html.

G) A special kernel module powers most of the added security functionality in HP-LX. Compile and install that module with the following commands:

```
[root@hp-lx /etc]# cd /tmp
[root@hp-lx /tmp]# tar -xzvf kernel_extensions.tar.gz
[root@hp-lx /tmp# cd kernel_extensions/
[root@hp-lx kernel_extensions]# make
[root@hp-lx kernel_extensions]# mkdir /lib/modules/2.4.5-hplx/misc
[root@hp-lx kernel_extensions]# cp lns.o /lib/modules/2.4.5-
hplx/misc/
```

H) Now the system must be rebooted. Make sure the floppy diskette and CD-ROM drives in the system are empty, then run the following command:

```
[root@hp-lx /kernel_extensions]# shutdown -ry 0
```

I) Log back in as root when the system finishes rebooting. Now the cryptoapi kernel module must be compiled and installed:

```
[root@hp-lx /]# cd /tmp/cryptoapi-2.4.7.0
[root@hp-lx cryptoapi-2.4.7.0]# ./configure
```

Ignore the warning about "iv-mode-sector", this was fixed in step D.

```
[root@hp-lx cryptoapi-2.4.7.0]# make
[root@hp-lx cryptoapi-2.4.7.0]# make install
```

For security purposes, HP-LX prevents kernel modules from being loaded and unloaded during runtime. Disable the protection, load the cryptoloop module, then re-enable the protection:

```
[root@hp-lx cryptoapi-2.4.7.0]# /sbin/tlmodctrl -disable_modperms
[root@hp-lx cryptoapi-2.4.7.0]# depmod
[root@hp-lx cryptoapi-2.4.7.0]# modprobe cryptoloop
[root@hp-lx cryptoapi-2.4.7.0]# /sbin/tlmodctrl -enable_modperms
```

J) Certain system utilities have to be updated to handle an encrypted filesystem:

```
[root@hp-lx cryptoapi-2.4.7.0]# cd /tmp
[root@hp-lx /tmp]# tar -xzvf util-linux-2.11k.tar.gz
[root@hp-lx cryptoapi-2.4.7.0]# cd /tmp/util-linux-2.11k
[root@hp-lx util-linux-2.11k]# patch -p1 < /tmp/cryptoapi-
2.4.7.0/doc/util-linux-2.11b.patch
[root@hp-lx util-linux-2.11k]# ./configure
```

```
[root@hp-lx util-linux-2.11k]# make
```

Do not run '`make install`'. Instead, backup the files below and copy the new versions over the old ones:

```
[root@hp-lx util-linux-2.11k]# cp /bin/mount /bin/mount.old
[root@hp-lx util-linux-2.11k]# cp /bin/umount /bin/umount.old
[root@hp-lx util-linux-2.11k]# cp /sbin/losetup /sbin/losetup.old
[root@hp-lx util-linux-2.11k]# cp mount/mount /bin/mount
[root@hp-lx util-linux-2.11k]# cp mount/umount /bin/umount
[root@hp-lx util-linux-2.11k]# cp mount/losetup /sbin/losetup
```

K) Finally, all the extra files and application packages introduced in this section must be removed:

```
[root@hp-lx util-linux-2.11k]# rm -r /tmp/*
[root@hp-lx util-linux-2.11k]# rpm -e ncurses-devel-5.2-8
[root@hp-lx util-linux-2.11k]# rpm -e perl-5.6.0-12
[root@hp-lx util-linux-2.11k]# rpm -e patch-2.5.4-9
[root@hp-lx util-linux-2.11k]# rpm -e make-3.79.1-5
[root@hp-lx util-linux-2.11k]# rpm -e gcc-c++-2.96-85
[root@hp-lx util-linux-2.11k]# rpm -e libstdc++-devel-2.96-85
[root@hp-lx util-linux-2.11k]# rpm -e gcc-2.96-85
[root@hp-lx util-linux-2.11k]# rpm -e cpp-2.96-85
[root@hp-lx util-linux-2.11k]# rpm -e binutils-2.10.91.0.2-3
[root@hp-lx util-linux-2.11k]# rpm -e glibc-devel-2.2.2-10
[root@hp-lx util-linux-2.11k]# rpm -e kernel-headers-2.4.2-2
```

3.3 – Creating Encrypted Filesystems

This section is based on Mutz, Marc. "Linux Encryption HOWTO." v02.2. 04 October 2000. URL: http://encryptionhowto.sourceforge.net/previous/Encryption-HOWTO-0.2.2.html (01 October 2001).

A) Create a large file of pseudo-random bits in the '/data' directory called '.crypto'. Size according to how much space all the protected users will need. The following example creates a 100mb file (10240k * 10):

```
[root@hp-lx /]# dd if=/dev/urandom of=/data/.crypto bs=10240k
count=10
```

B) Now a cipher must be setup on a kernel loop device, and that device tied to the file '/data/.crypto':

```
[root@hp-lx /]# losetup -e aes /dev/loop0 /data/.crypto
```

The system will ask what key size the cipher should use, choose 256 bits. Next the system will ask for a password, enter a strong password of at least 10 characters. Type carefully, as the system will not give a second password prompt.

Note: the cipher chosen above is "AES" (a.k.a Rijndael). Other available choices are: Blowfish, DES, Idea, Mars, RC5, RC6, Serpent, and TwoFish.

C) The ext2 filesystem must be placed in the '/data/.crypto' file, which is now represented by '/dev/loop0'. The loop device acts just like any other block device (like, for example, a hard disk partition: /dev/hda3). Run the following command:

```
[root@hp-lx /]# mke2fs /dev/loop0
```

D) The next step is to create a mount point. The mount point will be '/compt' because that is where HP-LX expects to store its security compartments:

```
[root@hp-lx /]# mkdir /compt
```

The final step is to mount the loop device to the new mount point:

```
[root@hp-lx /]# mount -t ext2 /dev/loop0 /compt
```

Now any files created in '/compt' are actually translated through '/dev/loop0' and created inside the encrypted file '/data/.crypto'.

3.4 – Remounting Encrypted Filesystems

For security purposes, the system will not remember the cipher or password if '/compt' is unmounted. This will happen most often after a system reboot. To remount the encrypted file system:

A) First, the cryptoapi kernel module must be loaded. HP-LX prevents kernel modules from being loaded and unloaded during runtime. Disable the protection, load the cryptoloop module, then re-enable the protection:

```
[root@hp-lx /]# /sbin/tlmodctrl -disable_modperms
[root@hp-lx /]# depmod
[root@hp-lx /]# modprobe cryptoloop
[root@hp-lx /]# /sbin/tlmodctrl -enable_modperms
```

B) Now the cipher must be setup on a kernel loop device, and that device tied to the file '/data/.crypto':

```
[root@hp-lx /]# losetup -e aes /dev/loop0 /data/.crypto

Note: Enter the same cipher key size and password used last time, or
else the data will not be decrypted.
```

C) Mount the kernel loop device to '/compt':

```
[root@hp-lx /]# mount -t ext2 /dev/loop0 /compt
```

Section 4 – System Hardening

4.1 – Tllockdown Script

HP-LX installs with many files and services already configured in a secure manner. It also ships with a comprehensive hardening script called '`tllockdown`'. The script, very similar to the better-known Bastille script, implements many safeguards including:

- **Restricts console access** – An attacker has many more options if they have console (physical) access to the system. The script reduces the valid number of console logins to one: root.
- **Limits Resources** – A denial-of-service will occur if an attacker can cause the system to use up too many resources. The script limits the filesizes, core files, and number of processes that users can create.
- **Improves logging** – A key to detecting an attack is good logs. The script configures syslog to capture additional error messages to log files. The syslog service will be used in addition to HP-LX enhanced auditing.
- **Password Expiration** – The longer a password stays the same, the more likely that password will be cracked. The script configures the system to expire passwords after 90 days.
- **Removes SUID and SGID** – Certain utilities (`mount, passwd, crontab, …`) have SUID (setuserid) and SGID (setgroupid) properties to allow non-privileged user access. This may allow users to inappropriately escalate their privileges. The script removes SUID and SGID properties from several key files.
- **Reduces Permissions** – Some utilities (`ifconfig, insmod, su, …`) are dangerous in non-privileged hands. The script tightens permissions on several dozen key utilities to allow only root execution.

Due to copyright limitations, the entire list of '`tllockdown`' actions cannot be reproduced here. To see the list, run:

```
[root@hp-lx /sbin]# tllockdown -vn
```

Note: HP-LX v1.0 is supposed to run the '`tllockdown`' script automatically during installation. It does not[3], and therefore the script should be run manually now:

```
[root@hp-lx /sbin]# tllockdown -v
```

The '`tllockdown`' script will probably be replaced by Bastille in future versions of HP-LX. [4]

4.2 – Other Measures

A) **Bios Configuration**
An x86 system can be configured to boot off a floppy diskette or CD-ROM, bypassing most security controls on the hard drive(s). Configure the system BIOS to only allow booting from the hard drive(s). Further protect the system by assigning

[3] HP-LX Release Notes, p.1-6.
[4] Edwards, et al., p.5.

password protection to the BIOS. Different systems use different syntax; consult the relevant system documentation for these operations.

B) **Protect lilo**
Prevent an attacker from entering command-line options during system boot. Edit the '/etc/lilo.conf' file to include the following two lines before the first "image=" line: [5]

```
password = strong_password
restricted
```

Replace the string "strong_password" with a new password. Be careful, however, because it is stored in plain text. Do not enter a password used anywhere else.

Reduce the permissions on '/etc/lilo.conf' to prevent non-privileged users from reading or modifying it: [6]

```
[root@hp-lx /]# chmod 600 /etc/lilo.conf
```

Next, the configuration file should be made immutable, to prevent attackers from changing it: [7]

```
[root@hp-lx /]# chattr +i /etc/lilo.conf
```

Load the new configuration by entering:

```
[root@hp-lx /]# lilo -v
```

C) **Limit # of Logins**
A denial-of-service will occur if an attacker can cause the system to use up too many resources. Limit the number of simultaneous logins per user to 2 by editing the '/etc/security/limits.conf' file to include the following line:

```
*  hard  maxlogins   2
```

D) **Single User Mode Password**
An attacker will sometimes try to boot the system into single user mode to bypass some security controls. Prevent this by assigning a password to single user mode. Edit the '/etc/inittab' file to include [8]: "`~~:S:wait:/sbin/login`" after "`si::sysinit:/etc/rc.d/rc.sysinit`"

E) **Protect inittab**
The /etc/inittab file controls the start and shutdown of several key Linux, and in particular, HP-LX processes. Protect the file from changes by running [8]:

```
[root@hp-lx /etc]# chattr +i /etc/inittab
```

F) **Warning Banners**
In many cases, especially in the United States, an attacker can declare innocence by claiming ignorance of the fact they were unwelcome. Close this loophole by making a warning statement appear at login time. Consult company policy for the proper wording, and place the warning in the '/etc/motd', '/etc/issue' and '/etc/issue.net files'.

[5] Hatch, et al., p.171.
[6] Hatch, et al., p.172.
[7] Hatch, et al., p.173.
[8] Pryor, p.34.

Be sure to uncomment the "`Banner /etc/issue.net`" line in the '/etc/ssh/sshd.conf' file so the warning will appear to SSH users.

Good examples of warning banners can be found at:
http://www.ciac.org/ciac/bulletins/j-043.shtml

G) **Physical Locks**
If they have physical access, only encryption will stop an attacker from stealing data. Slow them down anyway, make sure system cases have locks. If the system is in a rack, make sure the rack has a locking door. Put all of this in a locked room.

H) **Check Red Hat and HP for Security Updates**
A good security practice for any system is to regularly (at least once a week) check the OS and application vendors for any security updates. The most common cause of system compromises is unpatched software.

Check Red Hat at: http://www.redhat.com/support/errata/rh71-errata-security.html
Check Hewlett-Packard at: http://www.hp.com/security/products/linux/

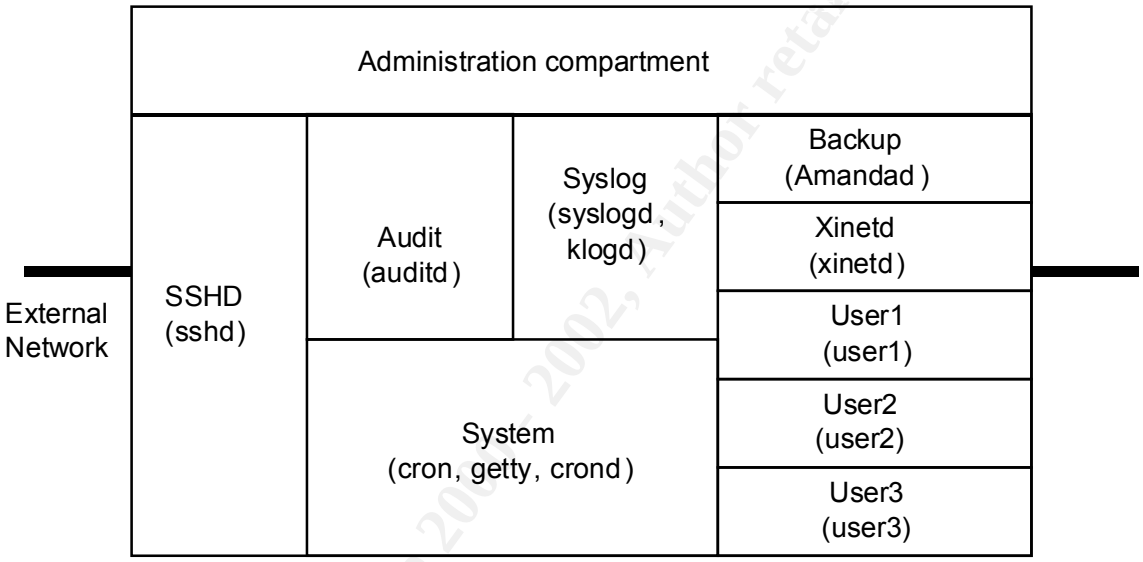
Note: As of publication, HP-LX is current with patches through the end of August 2001.

Section 5 – Security Compartments

5.1 – Security Compartments Background

This background section is based on the HP Secure OS Software for Linux: Administration Guide, v1.0 2001, pages 3-1 through 3-6, unless otherwise noted.

The key HP-LX innovation is security compartment technology. A security compartment is essentially a virtual room. Inside that room applications, users, processes and files operate and live. Each application (examples: SSH, Apache, syslog) has its own room. Some devices, like network interfaces, also have their own rooms. Nothing is allowed in our out of any room unless specifically authorized.



Visual Metaphor of Compartments
Based on Edwards, et al. A Secure Linux Platform.[9]

This functionality prevents system or application compromises because attackers have less to work with. Buffer overflows in an application will often fail because processes in that compartment were never authorized access to the system compartment. Web server cgi exploits are much more difficult to run because Apache compartments have very limited authorization into the cgi compartments.

In the event that an application is compromised, the compartment acts to contain the attacker. An attacker can do nothing outside the compartment that has not been previously authorized by an administrator. The situation is like breaking into a locked room, there is simply nowhere to go.

All file, network, and inter-process communication between compartments is controlled via mandatory access controls enforced by the kernel. Compartments can be created and destroyed, or their configurations altered, on the fly. The number of compartments is limited only by the memory and disk space on the system.

[9] Edwards, et al., p.8.

5.2 – Security Compartments Configuration

HP-LX uses mandatory access controls only when policing communication between compartments. Therefore, in order to protect users with HP-LX security, each user must have its own compartment.

A) **Compartment Creation**
Create a compartment named 'user1' with a chroot environment:
```
[root@hp-lx /]# tlcompadd -r -i user1
```

B) **User Creation**
Create a user called 'user1' with a home directory in '/compt/user1/home':
```
[root@hp-lx /]# useradd user1 -d /compt/user1/home -p password
```

Replace the string "password" above with a strong password.

C) **SSH Key Installation**
Place the authorized SSH key for this user on a floppy diskette. Mount that floppy and install the key:
```
[root@hp-lx /]# mount /dev/fd0 /mnt/floppy
[root@hp-lx /]# mkdir /compt/user1/home/.ssh
[root@hp-lx /]# cp /mnt/floppy/authorized_keys2
/compt/user1/home/.ssh/
[root@hp-lx /]# umount /dev/fd0
[root@hp-lx /]# chown user1 /compt/user1/home/.ssh/authorized_keys2
[root@hp-lx /]# chgrp user1 /compt/user1/home/.ssh/authorized_keys2
```

D) **Default Compartment**
When the user logs in, she should be placed into her own compartment. Edit the '/etc/tlinux/user/access' file and add the following line:
user1:user1: :

The first field is the username. The second field is the compartment name. The third field is for detailing HP-LX administration rights. Because this user should not be an administrator, the third field is left blank.

Note: The third field is blank, but not null. If it is left null, HP-LX will put the user into the 'system' compartment. Be sure to put a space or other character in the field to correct this.

E) **File Access Rule Configuration**
Create a file called '/etc/tlinux/fs/user1' and add the following lines:
```
user1    /compt/user1            read,write,append active
user1    /compt                  none              active
user1    /bin                    read              active
user1    /boot                   none              active
user1    /home                   none              active
user1    /lib                    read              active
user1    /mnt                    none              active
user1    /sbin                   read              active
user1    /usr                    read              active
user1    /etc                    read              active
user1    /etc/tlinux             none              active
user1    /opt                    none              active
user1    /proc                   read              active
user1    /root                   none              active
```

```
user1    /tmp                    none              active
user1    /var                    none              active
```

These lines define: compartment name, directory or file, authorized access, and whether or not the rule should be enforced (active).

To load the rules, the compartment must be stop and restarted:

```
[root@hp-lx /]# tlcompstop user1
[root@hp-lx /]# tlcompstart user1
```

F) **Network and Process Rule Configuration**

User access to this compartment should be limited to only one network interface from one trusted host, minimizing the compartments exposure. Create a file called '/etc/tlinux/rules/user1' and add the following line:

```
HOST <Trusted Address> -> COMPARTMENT user1 PORT 22 METHOD tcp
NETDEV eth1
```

The line says: allow only the <Trusted Address> to connect to compartment 'user1' via port 22 and tcp and only on network interface eth1.

HP-LX configures SSH to always perform reverse DNS lookups on connections. This verifies the originating system's address and provides an extra layer of assurance that the user is valid. However, the SSH compartment has not been authorized to initiate outbound communication to a DNS server. Make this authorization now by adding the following lines to the '/etc/tlinux/rules/ssh' file:

```
COMPARTMENT ssh -> HOST <DNS Address> PORT 53 METHOD udp NETDEV any
HOST <DNS Address> PORT 53 -> COMPARTMENT ssh METHOD udp NETDEV any
```

The first line says: allow compartment 'ssh' to connect to <DNS Address> via port 53 and udp on any network interface. The second line says: allow from <DNS Address> from port 53 connection to compartment 'ssh' with udp on any network interface.

Note: Rules for all communication except TCP are uni-directional. HP-LX automatically writes rules allowing return traffic for TCP network communications on the fly.

Run the following command to delete any old rules and load the new rule files:

```
[root@hp-lx /]# tlrules -d /etc/tlinux/rules/ssh
[root@hp-lx /]# tlrules -a /etc/tlinux/rules/user1
[root@hp-lx /]# tlrules -a /etc/tlinux/rules/ssh
```

No rules for inter-process communication need to be made because there is no need for such communication in or out of the "user1" compartment.

G) **Next User**

Repeat steps A through F for each additional user, replacing the string "user1" with "user2" (or whatever the company's account name policy is) and so on.

Note: HP-LX will not be able to start the user compartments at boot time. This is because the encrypted /compt partition cannot be mounted until after boot time (see **Section 3.4: Remount Encrypted Filesystems**). Be sure to start the compartments as follows:

```
[root@hp-lx /]# tlcompstart user1
```

Section 6 – Enhanced Auditing & Tripwire

6.1 – Enhanced Auditing Background

This background section is based on the HP Secure OS Software for Linux: Administration Guide, v1.0 2001, pages 5-1 and 5-5.

A key to system security is auditing. Auditing is the writing and reviewing of events related to security on the system. HP-LX greatly enhances Linux auditing abilities by adding kernel-level auditing functionality.

Kernel-level auditing is important because all processes on the system depend on the kernel for some basic services. By placing the auditing device on the system call interface of the kernel, HP-LX captures detailed evidence of most significant actions as they occur. As an added benefit, the location thwarts attackers from bypassing or tampering with the auditing.

HP-LX also includes an API that allows applications to write to the audit subsystem. Certain applications, for example '`login`', are already configured to utilize the API.

HP-LX runs both the base Linux auditing system (syslog) and the enhanced auditing system separately. Additionally, HP-LX protects each auditing system by running it in its own security compartment.

6.2 – Enhanced Auditing Configuration

A) **Configure Audit Daemon**
The operation of the enhanced auditing daemon is controlled by the '/etc/tlinux/audit/auditd.conf' file. Edit the file as follows:

Change "`<audit FailureAction="Drop"/>`" to "`<audit FailureAction="Panic"/>`"
This setting controls how the system responds to audit system failure. Default action is to drop any records in queue, stop recording records, and hope the audit system recovers. This is dangerous because, if the auditing outage was caused by an attack, there will be no records of the attackers actions.
A safer solution is to have the system shutdown (Panic) until the problem with auditing can be diagnosed.

Change "`<audit Autostart="No"/>`" to "`<audit Autostart="Yes"/>`"
This setting configures the audit system to start at boot time.

B) **Select Events to Audit**
HP-LX can audit 221 different kernel-level system calls, but the 81 most security-relevant are already configured in the '/etc/tlinux/audit/filter.conf'.

The default filter configuration is already well-suited for an SSH server. If company policy requires extra kernel or application-level items to be recorded, change the

'/etc/tlinux/audit/filter.conf' file accordingly. See chapter 5 of "HP Secure OS Software for Linux: Administration Guide" for more information.

C) **Enable Auditing**
First check that the configuration file is correct by running:

```
[root@hp-lx /sbin]# auditd -v
```

Then turn enhanced auditing on by running:

```
[root@hp-lx /sbin]# auditd -e
```

6.3 – Reviewing Audit Records

The best records in the world are useless if nobody reads them. HP-LX is able to output its audit records into human or machine-readable formats via customizable templates. Sample text and xml format templates are included with HP-LX.

While it is important to read the records, the volume of audit records that systems generate will overwhelm any human. Use a host intrusion detection tool to actively monitor and react to the audit logs. An example of a good freeware tool is:

Swatch: The Simple WATCHer (requires Perl)
http://www.oit.ucsb.edu/~eta/swatch/

Host intrusion detection tools provide the additional benefit of moving key parts of the audit records off the system, onto the monitoring system. This functions as a sort of a filtering remote shadow log. If an attacker gains control of the system, they often try to edit the local audit records. At that point, local records cannot be trusted, and it is important to have copies of those records stored outside the system.

More information on HP-LX auditing can be found in chapter 5 of "HP Secure OS Software for Linux: Administration Guide".

6.4 - Tripwire

HP-LX uses the open-source free version of Tripwire v2.3.1.2 to maintain watch on the system. Tripwire makes scheduled fingerprints of key files on the system, comparing them to older fingerprints to detect changes. Unexpected file changes may indicate an intruder and Tripwire automatically emails reports of those changes to a security administrator.

Because Tripwire was selected during installation, HP-LX has automatically configured Tripwire to monitor key Linux and HP-LX files and generate daily reports [10].

The actions in this paper caused several monitored files to change, and the Tripwire reports will reflect those changes. To update the Tripwire database, and accept the current state of the system as a trusted baseline, perform the following:

[10] HP-LX Administration Guide, p.6-2.

A) Find the latest report file under the '/var/lib/tripwire/report/' directory.

B) Run the following, replace the "reportname" string with the filename from step A:
```
[root@hp-lx sbin]# tripwire --update --twrfile
/var/lib/tripwire/report/reportname
```

C) The report will be displayed in *vi*. Exit and save the file by hitting the <ESC> key then typing '`:wq`' (without the quotes).

D) When prompted, enter the Tripwire local password. The local password was defined in Section 2.2 F.

More information on Tripwire can be found in chapter 6 of "HP Secure OS Software for Linux: Administration Guide" or at http://www.tripwire.org/.

Conclusion

This paper detailed the creation of a relatively secure SSH system running on HP-LX. Now the system is ready to be connected to the network and put into production. The server installation, cryptographic filesystem, system hardening, security compartments, and enhanced auditing techniques have been brought together to make a bastion Linux host that can be trusted with the most sensitive data.

Security is a journey, not a destination. Continue security education and also be sure to check with HP and Red Hat regularly for security updates.

Special Thanks to:
Scott Ruff
Joubert Berger
Warren Timmer

References

1) Hewlett-Packard. HP Secure OS Software for Linux v1.0: Installation Guide. Hewlett-Packard, 2001: Page 1-5.

2) Mutz, Marc. "Linux Encryption HOWTO." v02.2. 04 October 2000. URL: http://encryptionhowto.sourceforge.net/previous/Encryption-HOWTO-0.2.2.html (01 October 2001).

3) Hewlett-Packard. HP Secure OS Software for Linux v1.0: Release Notes. Hewlett-Packard, 2001: Page 1-5.

4, 9) Edwards, et al. A Secure Linux Platform. 5th Annual Linux Showcase & Conference, 2001: Pages 5 and 8.

5-7) Hatch, et al. Hacking Linux Exposed. Berkeley: McGraw Hill, 2001: Pages 171-173.

8) Pryor, Janice D. "Installing and Securing a DNS/Mail Server Using Red Hat 7.1 Linux." 12 August 2001. URL: http://www.sans.org/y2k/practical/Janice_Pryor_GCUX.zip (01 October 2001).

10) Hewlett-Packard. HP Secure OS Software for Linux v1.0: Administration Guide. Hewlett-Packard, 2001: Pages 3-1 through 3-6, 5-1, 5-5, 6-2.

Appendix A – Checklist

The following is an alternative presentation of the instructions presented in the main body of the paper. Almost all of the explanative text has been removed to make it easier to follow the instructions as a checklist. To find more information about a particular checklist item, cross-reference it with the section number in the main body.

____ 2 – System Installation
____ 2.1 – System Requirements

Does the system at least meet the following specifications?:

- Pentium III 500mhz
- 2GB hard disk
- 128mb RAM
- CD-ROM drive
- Floppy diskette drive
- 2 Network Interface cards

____ 2.2 – Installation
____ A) Unplug system from network.
____ B) Boot the system from CD-ROM HP-LX Disc 1

```
boot: text
```

____ C) Choose Installation Language & Keyboard.
____ D) Choose "Server Installation".
____ E) Initialize, partition and format the hard disk to at least meet the following guidelines:

/	256mb
/boot	31mb
/usr	512mb
/var	256mb
/home	32mb
<swap>	256mb
/data	640mb

____ F) Enable Tripwire. Enter passwords and email address.
____ G) Configure network interfaces, use static IP addresses. Set hostname.
____ H) Choose the most appropriate mouse setting.
____ I) Choose system language and time zone.

____ J) Set root password and create at least one non-privileged user.
____ K) Do not install any package categories.
____ L) Create a bootdisk.
____ M) Upload SSH key for "tlinuxadm" user.
____ N) Remove floppy and CD-ROM discs, then reboot.
____ O) Login as root. Set the hostname again:

```
[root@localhost /]# hostname name
```

Also edit the '/etc/sysconfig/network/' file to reflect the hostname.

____ 3 – Cryptographic Filesystem
____ 3.2 – Installing Cryptography
____ A) Copy the following files into /tmp:

ftp://ftp.kernel.org/pub/linux/utils/util-linux/util-linux-2.11k.tar.gz
http://prdownloads.sourceforge.net/cryptoapi/cryptoapi-2.4.7.0.tar.gz
ftp://ftp.hp.com/pub/security/hplx_source/v1.0/kernel_patches.tar
ftp://ftp.hp.com/pub/security/hplx_source/v1.0/kernel_extensions.tar

____ B) If not already root, 'su' to root.
____ C) Temporarily install some applications. Mount HP-LX Disc 1, run the following commands:

```
[root@hp-lx /]# cd /mnt/<cdrom device>/RedHat/RPMS/
[root@hp-lx RPMS]# rpm -ivh kernel-headers-2.4.2-2.i386.rpm
[root@hp-lx RPMS]# rpm -ivh glibc-devel-2.2.2-10.i386.rpm
[root@hp-lx RPMS]# rpm -ivh binutils-2.10.91.0.2-3.i386.rpm
[root@hp-lx RPMS]# rpm -ivh cpp-2.96-85.i386.rpm
[root@hp-lx RPMS]# rpm -ivh gcc-2.96-85.i386.rpm
[root@hp-lx RPMS]# rpm -ivh libstdc++-devel-2.96-85.i386.rpm
[root@hp-lx RPMS]# rpm -ivh gcc-c++-2.96-85.i386.rpm
[root@hp-lx RPMS]# rpm -ivh make-3.79.1-5.i386.rpm
[root@hp-lx RPMS]# rpm -ivh patch-2.5.4-9.i386.rpm
[root@hp-lx RPMS]# rpm -ivh perl-5.6.0-12.i386.rpm
[root@hp-lx RPMS]# rpm -ivh ncurses-devel-5.2-8.i386.rpm
```

____ D) Extract and patch the new kernel:

```
[root@hp-lx /tmp]# tar -xzvf kernel_patches.tar.gz
[root@hp-lx /tmp]# cd /usr/src/
[root@hp-lx src]# tar -xzvf /tmp/kernel_patches/linux-2.4.5.tar.gz
[root@hp-lx src]# cd linux/
[root@hp-lx linux]# patch -p1 < /tmp/kernel_patches/patch-2.4.5
[root@hp-lx linux]# patch -p1 < /tmp/kernel_patches/linux-2.4.5-aacraid-030101.patch
[root@hp-lx linux]# patch -p1 < /tmp/kernel_patches/linux-2.4.5-axboe-scsi-max-sec.patch
```

```
[root@hp-lx linux]# patch -p1 < /tmp/kernel_patches/linux-2.4.5-initrd-swapper-oops.patch
[root@hp-lx linux]# cd /tmp
[root@hp-lx /tmp]# tar –xzvf cryptoapi-2.4.7.0.tar.gz
[root@hp-lx /tmp]# cd /usr/src/linux/
[root@hp-lx linux]# patch -p1 < /tmp/cryptoapi-2.4.7.0/doc/loop-iv-2.4.6.patch
```

First, look at the last seven characters returned by the following command:

```
[root@hp-lx linux]# ls /lib/modules/2.4.5*
```

Then take those characters, and append them to the "/tmp/kernel_patches/kcfg/" string in the following command:

```
[root@hp-lx linux]# cp /tmp/kernel_patches/kcfg/ /usr/src/linux/.config
```

____ E) Now compile and install the new kernel:

```
[root@hp-lx linux]# make menuconfig
```

Do not make any changes. Exit and, when prompted, save the kernel configuration. Then run the following commands:

```
[root@hp-lx linux]# make dep
[root@hp-lx linux]# make bzImage
[root@hp-lx linux]# make modules
[root@hp-lx linux]# cp arch/i386/boot/bzImage /boot/tlinux-2.4.5-hplx
[root@hp-lx linux]# chmod 755 /boot/tlinux-2.4.5-hplx
[root@hp-lx linux]# ln –sf /boot/System.map-2.4.5-hplx /boot/System.map
[root@hp-lx linux]# make modules_install
```

____ F) In the '/etc/lilo.conf' file change the line that begins with "image=/boot/tlinux-2.4.5…" to "image=/boot/tlinux-2.4.5-hplx". Save the changes to the '/etc/lilo.conf' file, then run:

```
[root@hp-lx /etc]# lilo –v
```

____ G) Compile and install the HP-LX kernel module with the following commands:

```
[root@hp-lx /etc]# cd /tmp
[root@hp-lx /tmp]# tar –xzvf kernel_extensions.tar.gz
[root@hp-lx /tmp# cd kernel_extensions/
[root@hp-lx kernel_extensions]# make
[root@hp-lx kernel_extensions]# mkdir /lib/modules/2.4.5-hplx/misc
[root@hp-lx kernel_extensions]# cp lns.o /lib/modules/2.4.5-hplx/misc/
```

____ H) Remove any floppy and CD-ROM discs, then reboot:

```
[root@hp-lx /kernel_extensions]# shutdown –ry 0
```

____ I) Log back in as root. Compile and install the cryptoapi kernel:

```
[root@hp-lx /]# cd /tmp/cryptoapi-2.4.7.0
[root@hp-lx cryptoapi-2.4.7.0]# ./configure
[root@hp-lx cryptoapi-2.4.7.0]# make
[root@hp-lx cryptoapi-2.4.7.0]# make install
[root@hp-lx cryptoapi-2.4.7.0]# /sbin/tlmodctrl -disable_modperms
[root@hp-lx cryptoapi-2.4.7.0]# depmod
[root@hp-lx cryptoapi-2.4.7.0]# modprobe cryptoloop
[root@hp-lx cryptoapi-2.4.7.0]# /sbin/tlmodctrl -enable_modperms
```

____ J) Update certain system utilities for encryption:

```
[root@hp-lx cryptoapi-2.4.7.0]# cd /tmp
[root@hp-lx /tmp]# tar -xzvf util-linux-2.11k.tar.gz
[root@hp-lx cryptoapi-2.4.7.0]# cd /tmp/util-linux-2.11k
[root@hp-lx util-linux-2.11k]# patch -p1 < /tmp/cryptoapi-2.4.7.0/doc/util-linux-2.11b.patch
[root@hp-lx util-linux-2.11k]# ./configure
[root@hp-lx util-linux-2.11k]# make
[root@hp-lx util-linux-2.11k]# cp /bin/mount /bin/mount.old
[root@hp-lx util-linux-2.11k]# cp /bin/umount /bin/umount.old
[root@hp-lx util-linux-2.11k]# cp /sbin/losetup /sbin/losetup.old
[root@hp-lx util-linux-2.11k]# cp mount/mount /bin/mount
[root@hp-lx util-linux-2.11k]# cp mount/umount /bin/umount
[root@hp-lx util-linux-2.11k]# cp mount/losetup /sbin/losetup
```

____ K) Finally, all the extra files and application packages introduced in this section must be removed:

```
[root@hp-lx util-linux-2.11k]# rm -r /tmp/*
[root@hp-lx util-linux-2.11k]# rpm -e ncurses-devel-5.2-8
[root@hp-lx util-linux-2.11k]# rpm -e perl-5.6.0-12
[root@hp-lx util-linux-2.11k]# rpm -e patch-2.5.4-9
[root@hp-lx util-linux-2.11k]# rpm -e make-3.79.1-5
[root@hp-lx util-linux-2.11k]# rpm -e gcc-c++-2.96-85
[root@hp-lx util-linux-2.11k]# rpm -e libstdc++-devel-2.96-85
[root@hp-lx util-linux-2.11k]# rpm -e gcc-2.96-85
[root@hp-lx util-linux-2.11k]# rpm -e cpp-2.96-85
[root@hp-lx util-linux-2.11k]# rpm -e binutils-2.10.91.0.2-3
[root@hp-lx util-linux-2.11k]# rpm -e glibc-devel-2.2.2-10
[root@hp-lx util-linux-2.11k]# rpm -e kernel-headers-2.4.2-2
```

____ 3.3 – Creating Encrypted Filesystems

____ A) Create an encrypted file, change ‘bs’ variable to required size divided by 10:

```
[root@hp-lx /]# dd if=/dev/urandom of=/data/.crypto bs=10240k count=10
```

____ B) Set up the kernel loop device. Enter a cipher key size and password when prompted:

```
[root@hp-lx /]# losetup -e aes /dev/loop0 /data/.crypto
```

____ C) Install a filesystem on the loop device:

```
[root@hp-lx /]# mke2fs /dev/loop0
```

____ D) Create a mountpoint and mount the new partition:

```
[root@hp-lx /]# mkdir /compt
[root@hp-lx /]# mount -t ext2 /dev/loop0 /compt
```

____ 4 – System Hardening

____ 4.1 – Tllockdown

Run the 'tllockdown' script:

```
[root@hp-lx /sbin]# tllockdown -v
```

____ 4.2 – Other Measures

____ A) Assign a password to the BIOS, and configure it to only allow the system booting from the hard drive(s).

____ B) Protect lilo:

Edit the '/etc/lilo.conf' file to include the following two lines before the first "image=" line:

```
password = strong_password
restricted
[root@hp-lx /]# chmod 600 /etc/lilo.conf
[root@hp-lx /]# chattr +i /etc/lilo.conf
[root@hp-lx /]# lilo -v
```

____ C) Limit the number of simultaneous logins per user to 2 by editing the '/etc/security/limits.conf' file to include the following line:

```
*     hard  maxlogins   2
```

____ D) Single user mode password

Edit the '/etc/inittab' file to include: "`~~:S:wait:/sbin/login`" after "`si::sysinit:/etc/rc.d/rc.sysinit`"

____ E) Protect inittab from changes by running:

```
[root@hp-lx /etc]# chattr +i /etc/inittab
```

____ F) Warning banners:

Consult company policy for the proper wording, and place the warning in the '/etc/motd', '/etc/issue' and '/etc/issue.net files'. Be sure to uncomment the "`Banner /etc/issue.net`" line in the '/etc/ssh/sshd.conf' file so the warning will appear to SSH users.

____ G) Make sure the system case is locked. If the system is in a rack, lock the rack door. Place all of this in a locked room.

____ H) Check Red Hat and HP for security updates now and on a regular basis.

____ 5 – Security Compartments

____ 5.2 – Security Compartments Configuration

____ A) Create a compartment named ‘user1’ with a chroot environment:

```
[root@hp-lx /]# tlcompadd -r -i user1
```

____ B) Create a user:

```
[root@hp-lx /]# useradd user1 -d /compt/user1/home -p password
```

____ C) Place the authorized SSH key for this user on a floppy diskette. Mount that floppy and install the key:

```
[root@hp-lx /]# mount /dev/fd0 /mnt/floppy
[root@hp-lx /]# mkdir /compt/user1/home/.ssh
[root@hp-lx /]# cp /mnt/floppy/authorized_keys2 /compt/user1/home/.ssh/
[root@hp-lx /]# umount /dev/fd0
[root@hp-lx /]# chown user1 /compt/user1/home/.ssh/authorized_keys2
[root@hp-lx /]# chgrp user1 /compt/user1/home/.ssh/authorized_keys2
```

____ D) Set default compartment for user, edit the ‘/etc/tlinux/user/access’ file and add the following line:

```
user1:user1: :
```

Note: The third field is blank, but not null. If it is left null, HP-LX will put the user into the ‘`system`’ compartment. Be sure to put a space or other character in the field to correct this.

____ E) Configure file access rules, create a file called ‘`/etc/tlinux/fs/user1`’ and add the following lines:

```
user1 /compt/user1          read,write,append active
user1 /compt                none              active
user1 /bin                  read              active
user1 /boot                 none              active
user1 /home                 none              active
user1 /lib                  read              active
user1 /mnt                  none              active
user1 /sbin                 read              active
user1 /usr                  read              active
user1 /etc                  read              active
user1 /etc/tlinux           none              active
user1 /opt                  none              active
user1 /proc                 read              active
user1 /root                 none              active
user1 /tmp                  none              active
user1 /var                  none              active
```

To load the rules, the compartment must be stop and restarted:

```
[root@hp-lx /]# tlcompstop user1
[root@hp-lx /]# tlcompstart user1
```

____ F) Configure network access rules, create a file called '`/etc/tlinux/rules/user1`' and add the following line:

```
HOST <Trusted Address> -> COMPARTMENT user1 PORT 22 METHOD tcp NETDEV eth1
```

Add the following lines to the '/etc/tlinux/rules/ssh' file:

```
COMPARTMENT ssh -> HOST <DNS Address> PORT 53 METHOD udp NETDEV any
HOST <DNS Address> PORT 53 -> COMPARTMENT ssh METHOD udp NETDEV any
```

Run the following command to delete any old rules and load the new rule files:

```
[root@hp-lx /]# tlrules -d /etc/tlinux/rules/ssh
[root@hp-lx /]# tlrules -a /etc/tlinux/rules/user1
[root@hp-lx /]# tlrules -a /etc/tlinux/rules/ssh
```

____ G) Repeat steps A through F for each additional user, replacing the string "user1" with "user2" (or whatever the company's account name policy is) and so on.

____ 6 – Enhanced Auditing & Tripwire

____ 6.2 – Enhanced Auditing Configuration

____ A) Edit the '/etc/tlinux/audit/auditd.conf' file as follows:

Change "`<audit FailureAction="Drop"/>`" to "`<audit FailureAction="Panic"/>`"

Change "`<audit Autostart="No"/>`" to "`<audit Autostart="Yes"/>`"

____ B) If company policy requires extra kernel or application-level items to be recorded, change the '/etc/tlinux/audit/filter.conf' file accordingly.

____ C) Enable auditing:

```
[root@hp-lx /sbin]# auditd -v
[root@hp-lx /sbin]# auditd -e
```

____ 6.4 – Tripwire

____ A) Find the latest report file under the '/var/lib/tripwire/report/' directory.

____ B) Run the following, replace the "reportname" string with the filename from step A:

```
[root@hp-lx sbin]# tripwire --update --twrfile /var/lib/tripwire/report/reportname
```

____ C) The report will be displayed in *vi*. Exit and save the file by hitting the <ESC> key then typing '`:wq`' (without the quotes).

____ D) When prompted, enter the Tripwire local password. The local password was defined in Section 2.2 F.

Last Updated: June 23rd, 2017

Upcoming Training

SANS London July 2017	**London, United Kingdom**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**