Nortel Networks

HP-UX 11 Operating System Hardening Guideline Document

Issue 1.0

Issue Date	November, 2003
Author	Nortel Networks

Summary

This document provides background information and detailed steps that should be taken in order to harden the HP-UX 11 operating system against common network security attacks. Please note however that operating system hardening procedures cannot be followed blindly. Operating system hardening involves, among other things, turning off all services that are not required for particular application. For this reason, each operating system hardening instance must be customized and this document should only be considered as a general guideline to follow during this customization.

Please Note

THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY AND DOES NOT CONSTITUTE ADVICE. ANY RELIANCE UPON THIS DOCUMENT SHALL BE AT YOUR OWN RISK. THE INFORMATION CONTAINED HEREIN IS PROVIDED "AS IS" WITHOUT ANY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) FROM USE OF OR RELIANCE UPON THE INFORMATION CONTAINED HEREIN, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Table of Contents

About this document

This document provides background information and detailed steps that should be taken in order to harden the HP-UX 11 operating system against common network security attacks. Please note however that operating system hardening procedures cannot be followed blindly. Operating system hardening involves, among other things, turning off all services that are not required for particular application. For this reason, each operating system hardening instance must be customized and this document should only be considered as a general guideline to follow during this customization.

This guide assumes that the OS has been installed from a known source and that the system has been patched with the necessary patches (see Appendix F for information on how to patch HP-UX 11). It further assumes that the network security personnel have working knowledge of HP-UX 11 system administration.

Introduction

Computers and network elements connected to networks are vulnerable to any number of attacks, including:

1. Backdoor programs
2. Sniffing programs
3. Password grabber and cracking tools
4. Exploitation of defects in operating system services
5. Denial of service (DoS)

Some of these attacks are based on well-publicized techniques, with scripts and other tools available to make it possible for less knowledgeable crackers to apply exploits against systems. Once a system has been compromised, an intruder can do a number of things, among which are:

1. Modify or destroy information
2. Disclose sensitive information
3. Install malicious code to gather information
4. Use the compromised server to attack other systems

Our goal is to provide an easy to follow guide that the Packet Core Network of GPRS/UMTS network security personnel can use to improve the resistance of their HP-UX 11-based systems to attacks. We present what we believe to be sound practices you can follow during the installation and configuration of the operating system.

While no system is absolutely secure, we are confident that following these guidelines will result in systems that are harder for crackers to compromise. Continued vigilance is required to keep systems secure.

HP-UX 11 Hardening Procedures

Step 0: Installing minimum system and applying patches

It is assumed that the server has had the smallest possible OS image installed and the latest patches applied. Reduced size implies less services and greater security. But it may also cause a loss of convenience. Choose security over convenience – if in doubt about the necessity of a service, turn it off and see what breaks.

Refer to Managing Systems and Workstations: A Guide for HP-UX System Administrators available at http://docs.hp.com/ for procedures on how to install a minimum system and on how to apply patches. Version specific documentations can also be found at the following URLs:

http://docs.hp.com/hpux/os/10.x/index.html
http://docs.hp.com/hpux/os/11.x/index.html

It is recommended that the basic configuration look something like the following:

```
   Primary Swap Size              [ 256Mb  ->]
   Secondary Swap Size            [ None   ->]
   Software Selection             [ Minimal system, networking (Eng.)   ->]
   Software Language              [ English        ->]
   Locale Setting                 [ default (C)                        ->]
   File System file name length   [ Long   ->]
   /home Configuration            [ None           ->]
   How many disks in root group   [ One         ->]
   Make volatile dirs separate    [ True   ->]
   Create /export volume          [ False  ->]
```

It is recommended that the following additional packages be loaded:

```
   Accounting      ->        Accounting
   InternetSrvcs   ->        General network applications and daemons
   MailUtilities   ->        User mail agents and related tools
   Networking      ->        HP-UX_11.x_LanLink_Product
   NonHP-Terminfo  ->        Non HP terminfo files
   OS-Core         ->        Core Operating System
   SecurityMon     ->        SecurityMon
   SystemAdmin     ->        HP-UX System Administration Tools
   TextEditors     ->        TextEditors
   TextFormatters  ->        TextFormatters
```

You must register yourself at http://us-support.external.hp.com/ to get a copy of the patch matrix. You can download the required patches from ftp://us-support.external.com/ using your registered ID and password.

Step 1: Removing unnecessary services

Many unnecessary services are installed by default when setting up an HP-UX 11 server. If the box comes with HP-UX 11 pre-installed, then the first step to harden the operating system is to strip it down.

The command to list installed services is:

```
	swlist –l product
```

Compare your output with the following list from a basic system and consider removing unnecessary services:

```
	Accounting
	DCE-Core
	InternetSrvcs
	LVM
	MailUtilities
	Networking
	NonHP-Terminfo
	OS-Core
	ProgSupport
	SW-DIST
	SecurityMon
	Streams
	Streams-TIO
	SystemAdmin
	TextEditors
	TextFormatters
```

Use swremove command to remove unnecessary products. You may need to use –x autoreboot=true option if the product requires rebooting the machine upon removal.

Processes are started at boot time by adding files in /sbin/rc[2-4].d directories. Many of these startup scripts run processes that you absolutely do not want running on your secure server. NFS is a prime example.

Rename all the auto-configuration links so that the unnecessary services associated with them will not be automatically brought up for run level 2 upon system reboot. A more radical approach would be to delete them completely. It is recommended that the files be renamed first and be removed after thorough tests have been done to make sure the system works as expected.

Change directory to /sbin/rc2.d and do a file listing:

```
	cd /sbin/rc2.d
	ls
```

Compare your output with the following list from a barebone system:

```
	S008net.sd
	S120swconfig
	S200clean_ex
	S204clean_tmps
	S206clean_adm
```

```
S220syslogd
S230ptydaemon
S300nettl
S320hpether
S340net
S500inetd
S700acct
S730cron
S760auditing
S800spa
```

Consider disabling unnecessary services so that they don't get started upon system reboot. The following is a sample list for your reference; you may find some missing or you may find some extra startup files depending on your specific configuration.

```
S345cue_nettune
S565SnmpHpunix
S370named
S565SnmpMib2
S742diagnostic
K900nfs.server
S400nfs.core
S565SnmpTrpDst
S410nis.server
S570dce
S660xntpd
S770audio
S100swagentd
S420nis.client
S580dfs
S780hub
S430nfs.client
S590ncs
S780slsd
S490mrouted
S600iforls
S202clean_uucp
S604ovlmd
S827aiclient
S510gated
S610rbootd
S880swcluster
S520rdpd
S620xfs
S898snmpd
S525autopatch
S630vt
S899dmond
S525rarpd
S899slap
S528autoapps
S990ai
S530rwhod
S710hparray
S999WPMS
S323hpbase100
```

```
S550ddfa
S720lp
S999y2koscheck
S560SnmpMaster
S722pd
S540sendmail
```

You can use a simple script to facilitate renaming those files. Break the above list into manageable chunks and cut and paste them to the script. Here is an example:

```
cd /sbin/rc2.d
for file in S540sendmail S722pd S560SnmpMaster S999y2koscheck
do
 mv $file .NO$file
done
```

Then do the same for the next run level:

```
cd /etc/rc3.d

for file in S100nfs.server S940ov500 S990dtlogin.rc\
 S981OptAp S983OptSA
do
mv $file .NO$file
done
```

Next do the same for run level 4. Since the server is headless, there should not be any services running for that run level.:

```
cd /etc/rc4.d

for file in *
do
mv $file .NO$file
done
```

In order to ensure that all of the startup scripts run with the proper umask, create and execute the following script:

```
umask 022 # make sure umask.sh gets created with the proper mode
echo 'umask 022' >/sbin/init.d/umask.sh
for d in /sbin/rc?.d
do
      ln /sbin/init.d/umask.sh $d/S000umask.sh
done
```

Remove crontab files. You should remove all files from /var/spool/cron/crontabs except the root file. Open the root crontab file and comment out the jobs that you should not be running. Examine the contents of the root crontab file by executing the following command as root:

```
crontab -l
```

Commenting out the jobs that you think you need not be running by executing the following command:

```
crontab -e
```

In order to log as much information about your system, make sure your /etc/syslog.conf has the following entries:

```
mail.debug              /var/adm/syslog/mail.log
*.info;mail.none        /var/adm/syslog/syslog.log
*.alert                       root
*.emerg                 *
```

Note: Tabs must be used to separate the fields.

This will log mail entries to /var/adm/syslog/mail.log and everything else to /var/adm/syslog/syslog.log.

Set the permissions on the log files as follows:

```
chmod 600 /var/adm/syslog/*.log
```

Disable IP forwarding and turn on random TCP packet sequence numbering by adding the following two lines to /sbin/init.d/net between "start)" and ";; # faill through":

```
/usr/contrib/bin/nettune –s ip_forwarding 0
/usr/contrib/bin/nettune –s tcp_random_seq 2
```

The operating system has been stripped down with all unnecessary services being disabled or removed. Reboot.

Step 2: Setting up time synchronization using NTP

System timekeeping can be done via both xntpd (daemon) and ntpdate (client). While the daemon may provide more network functionalities, it also presents volunerabilities, one of which is xntpd buffer-overflow. Unlike xntpd which listens on port 123 constantly for connections, ntpdate is a client to be executed only when needed to get the time of day from a pre-defined NTP server.

It is recommended that ntpdate be used to set system clock according to the NTP server on the Packet Core Network. For precise timekeeping run this command from a cron job every hour on the hour:

```
        0 * * * * /usr/sbin/ntpdate –s NTP_server_addr >> /var/log/ntpdate.log
```

The –s switch will log ntpdate actions via the syslog facility rather than sending it to the standard output.

Step 3: Configuring additional logging

Syslogd provides both local and remote logging. It is able to send messages to a remote host running syslogd. To forward messages to another host, prepend the hostname with the at sign (``@'').

For maximum security of the logging information, it is recommended that logs be sent to both the local files and dedicated logging host. Make sure that the logging server is located within the same protected management network because syslogd does not have access control and would be subject to denial of service attacks if the server is exposed to the public network such as the Internet.

Do the following to expand on the default system logging function and make sure all authentication errors are logged:

Add the following to /etc/syslog.conf to log the authentication errors to the local log file and everything including the authentication erros to the remote log server:

```
auth.info    /var/adm/authlog
*.*               @remote_logging_host
```

Create /var/adm/authlog.

```
touch /var/adm/authlog
chown root /var/adm/authlog
chmod 600 /var/adm/authlog
```

Inetd logs can be enabled by launching inetd with the –l option. If inetd logs are enabled, a log entry is created every time an inetd service is requested

Create a log rotation script to rotate these logs. A sample can be found in Appendix A of this document. Modify the root crontab file to run this every day.

Step 4: Disabling sendmail service

Sendmail has been disabled as a service. But it should be started periodically from crontab to process queued mail from programs and processes that use mail to send out messages.

Replace the installed sendmail.cf file with the minimal sendmail.cf in Appendix B.

Add the following entry to root's contab to flush the mail queue once per hour:

```
        0 * * * * /usr/lib/sendmail -q
```

Step 5: Enforcing access controls

First set up network access controls. Disable network root logins with the following command:

```
      echo "console" > /etc/securetty
```

Except from the console, a user has to login as herself and then uses the command su to become root.

Then either remove all "pseudo" account entries in the /etc/passwd file or set them up with locked password fileds to prevent their being used for interative logins.

Disable use of FTP by root and other system accounts via the following commands:

```
      touch /etc/ftpusers

      for user in root daemon bin sys nobody\
         noaccess nobody4 uucp nuucp adm lp \
         smtp listen
      do
         echo $user >> /etc/ftpusers
      done

      chown root /etc/ftpusers
      chgrp root /etc/ftpusers
      chmod 600 /etc/ftpusers
```

Remove .rhosts support from /etc/pam.conf.

```
      grep -v rhosts_auth /etc/pam.conf > \
         /etc/pam.new

      mv /etc/pam.new /etc/pam.conf
      chown root /etc/pam.conf
      chgrp sys /etc/pam.conf
      chmod 644 /etc/pam.conf
```

Install TCP Wrapper binary tcpd in /usr/sbin from ftp://ftp.cert.org/pub/tools/tcp_wrappers. If you must leave telnet and FTP on the system, put them behind the TCP Wrapper. Replace the /etc/inetd.conf file with the sample file in Appendix C.

Make sure /etc/hosts.deny file contains the following uncommented entry only:

```
      ALL:ALL
```

Make sure /etc/hosts.allow file contains uncommented entries only for the hosts you want to grant remote login access to. Example:

```
      ALL: trusted_host1, trusted_ip1
```

It is recommended that SSH be used instead of telnet and FTP. For more information on purchasing a commercially available and supported SSH solution, visit http://www.ssh.com.

Create the files /etc/motd and /etc/issue. A sample message is in Appendix D.

Next is to set up filesystem access controls. Remove write group permissions for /etc directory via the chmod –R g-w /etc command. Set up permissions on /etc/utmp via the chmod 644 /etc/utmp command.

Use the following commands to find all setuid and setgid programs in the system:

```
      find / -perm –4000 -print
      find / -perm –2000 -print
```

Many of the setuid and setgid programs on HP-UX 11 are used only by root, or by the user or group-id to which they are set. Evaluate the files with the setuid and setgid bit set to determine if this is required for the SIG and other users that must use the permissions to get work done.

It is recommended that setuid bit be removed from the following files:

```
   /usr/bin/ppl
   /usr/sbin/swacl
   /usr/sbin/swlist
   /usr/sbin/swreg
   /usr/sbin/lvcreate
   /usr/sbin/lvdisplay
   /usr/sbin/lvreduce
   /usr/sbin/pvchange
   /usr/sbin/pvmove
   /usr/sbin/landiag
   /usr/sbin/swinstall
   /usr/sbin/swconfig
   /usr/sbin/swremove
   /usr/sbin/swmodify
   /usr/sbin/lvdisplay
   /usr/sbin/lvextend
   /usr/sbin/lvremove
   /usr/sbin/pvcreate
   /usr/sbin/acct/accton
   /usr/lbin/expreserve
   /usr/sbin/swinstall
   /usr/sbin/swcopy
   /usr/sbin/swverify
   /usr/sbin/lvchange
   /usr/sbin/lvextend
   /usr/sbin/lvlnboot
   /usr/sbin/lvrmboot
   /usr/sbin/pvdisplay
   /usr/sbin/lanadmin
   /usr/lbin/exrecover
```

The command is chmod u-s filename.

It is recommended that setgid bit be removed from the following files:

```
   /usr/bin/netstat           /usr/sbin/wall
```

The command is chmod g-s filename.

Then create a master list of remaining setuid and setgid programs on the HP-UX 11 system and check that the list remains static over time.

Step 6: File system lockdown

The next step is to lock down the filesystem so that OS binaries can not be modified. At this point, it is assumed that all required software is already installed on the sytem.

In addition to prevent unauthorized modification of binaries, we would also like to stop rogue setuid programs from showing up. In order to do that, we will modify the /etc/fstab file and set the appropriate flags. The “ro” option is a software switch to prevent filtsystem modifications. The “nosuid” option causes the suid bit on all programs on that partition to be ignored. This option should never be applied to anonymous FTP areas or to the filtsystem where /tmp resides. Since root is mounted before /etc/fstab is available, the root partition can not be mounted with the nosuid option set.

Edit the /etc/fstab file

```
      vi /etc/fstab
```

The final vfstab file should look like the example below. The last column is the area of interest.

Example /etc/fstab

```
   /dev/vg00/lvol3 /            hfs defaults 0 1
   /dev/vg00/lvol1 /stand       hfs nosuid   0 1
   /dev/vg00/lvol4 /local_admin hfs nosuid   0 2
   /dev/vg00/lvol5 /tmp         hfs defaults 0 2
   /dev/vg00/lvol6 /usr         hfs ro       0 2
   /dev/vg00/lvol7 /var         hfs nosuid   0 2
```

Make sure you have double checked everything at this point. Once you finish here, you will reboot to verify everything. If you have not added all your components properly, you will not easily be able to make changes due to all the non root file systems being read-only.

Step 7: Converting to “trusted” system

Unlike the Trusted Solaris system which is a special operating environment to purchase from Sun Microsystems, the “trusted system” for HP-UX is just another mode of operation and needs no installation of extra packages. The system can be easily converted to the “trusted” mode via SAM – the system administration manager.

The following steps are performed by SAM during the conversion process:

- /etc/passwd file is copied to /etc/passwd.old.save backup file
- passwords are copied from /etc/passwd to /.secure/etc/passwd without world read access – similar to the shadow password for Solaris.
- encrypted passwords in the original file are replaced with “*”.
- Audit ID is created for each user.
- the audit flag is set on for all users
- at, batch and crontab files are converted to use Audit ID.

Execute /usr/sbin/sam
Select "Auditing and Security"
Select "Audited Events"
Select "YES" from the following panel:

> You need to convert to a Trusted System before proceeding. The conversion process does the following things:
>
> 1. Creates a protected database on the system for storing security information.
> 2. Moves user passwords in "/etc/passwd" to this database.
> 3. Replaces all password fields in "/etc/passwd" with "*".
>
> For more details, refer to the "System Security" chapter of the "System Administration Tasks" manual.
>
> Do you want to convert to a Trusted System now?

After the system has been converted, select "Turn Auditing ON" from the *Actions* pull-down menu.

Remove, lock, or comment out unnecessary accounts, including "sys", "uucp", " nuucp", and "listen". The cleanest way to shut them down is to disable them using **sam**.

Disable rlogin/rsh access by removing /etc/hosts.equiv, /.rhosts, and all of the "r" commands in /etc/inetd.conf.

Appendix A: Sample newsyslog script

```
#! /bin/sh
#
# Copyright(c) 1997, by Sun Microsystems, Inc.
# All rights reserved.
#
#ident @Z%newsyslog     1.3     97/03/31 SMI
#
LOG=messages
cd /var/adm
test -f $LOG.2 && mv $LOG.2 $LOG.3
test -f $LOG.1 && mv $LOG.1 $LOG.2
test -f $LOG.0 && mv $LOG.0 $LOG.1
mv $LOG   $LOG.0
cp /dev/null $LOG
chmod 644    $LOG
#
LOGDIR=/var/adm
LOG=syslog
if test -d $LOGDIR
then
        cd $LOGDIR
        if test -s $LOG
        then
                test -f $LOG.6 && mv $LOG.6  $LOG.7
                test -f $LOG.5 && mv $LOG.5  $LOG.6
                test -f $LOG.4 && mv $LOG.4  $LOG.5
                test -f $LOG.3 && mv $LOG.3  $LOG.4
                test -f $LOG.2 && mv $LOG.2  $LOG.3
                test -f $LOG.1 && mv $LOG.1  $LOG.2
                test -f $LOG.0 && mv $LOG.0  $LOG.1
                mv $LOG    $LOG.0
                cp /dev/null $LOG
                chmod 644    $LOG
                sleep 40
        fi
fi
#
kill -HUP `cat /etc/syslog.pid`
```

Appendix B: Minimal sendmail configuration file

```
# Minimal client sendmail.cf

### Defined macros
# The name of the mail hub - PUT APPROPRIATE HOSTNAME FOR YOUR SITE
HERE!!!
DRmailhost

# Define version
V8

# Whom errors should appear to be from
DnMailer-Daemon

# Formatting of the UNIX from line
DlFrom $g $d

# Separators
Do.:%@!^=/[]

# From of the sender’s address
Dq<$g>

# Spool directory
OQ/usr/spool/mqueue

### Mailer Delivery Agents
# Mailer to forward mail to the hub machine
Mhub,   P=[IPC],     F=mDFMuCX,    S=0, R=0, A=IPC $h
# Sendmail requires these, but are not used
Mlocal, P=/dev/null, F=rlsDFMmnuP, S=0, R=0, A=/dev/null
Mprog,  P=/dev/null, F=lsDFMeuP,   S=0, R=0, A=/dev/null

### Rule sets -- WHITESPACE BETWEEN COLUMNS MUST BE TABS!!!

S0
R@$+  $#error $: Missing user name
R$+   $#hub $@$R $:$1         forward to hub
S3
R$*<>$*     $n                handle <> error address
R$*<$*>$*   $2                basic RFC822 parsing
```

Appendix C: Sample /etc/inetd.conf file

```
# /etc/inetd.conf customized sample file for Packet core network
# @(#)inetd.conf $ Revision: 1.22.212.9 $ $Date: 1996/11/14 17:10:13 $
# @(#) $Id: inetd.conf,v 1.8 1996/11/14 17:10:13 cuebase Exp $
#
# Inetd  reads its configuration information from this file upon execution
# and at some later time if it is reconfigured.
#
# A line in the configuration file has the following fields separated by
# tabs and/or spaces:
#
#       service name            as in /etc/services
#       socket type             either "stream" or "dgram"
#       protocol                as in /etc/protocols
#       wait/nowait             only applies to datagram sockets, stream
#                               sockets should specify nowait
#       user                    name of user as whom the server should run
#       server program          absolute pathname for the server inetd
will
#                               execute
#       server program args.    arguments server program uses as they
normally
#                               are starting with argv[0] which is the
name of
#                               the server.
#
# See the inetd.conf(4) manual page for more information.
##
# $Log: inetd.conf,v $
# Revision 1.8  1996/11/14 17:10:13  cuebase
# Replaced with 10.120 Vanilla and recustomized. MJE
#
# Revision 1.7  1996/10/16 14:20:30  cuebase
# Added entries that CDE adds aas configure steps. I was blowing them away
on
# a clone install. Fixes proact 97013885 and 97015593.  MJE
#
# Revision 1.6  1996/05/29  21:18:39  cuebase
# Made changes to HP-UX 10.10 Vanilla for CUE Base. MJE
#
#
#
#       ARPA/Berkeley services
#
##
ftp          stream tcp nowait root /usr/local/bin/tcpd      ftpd -l
telnet       stream tcp nowait root /usr/local//bin/tcpd  telnetd
#
```

Appendix D: Sample /etc/issue and /etc/motd file

```
This system is for the use of authorized users only. Individuals using this
computer system without authority, or in excess of their authority, are subject to
having all of their activities on this system monitored and recorded by system
personnel.

In the course of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users may also be
monitored.

Anyone using this system expressly consents to such monitoring and is advised that
if such monitoring reveals possible evidence of criminal activity, system personnel
may provide the evidence of such monitoring to law enforcement officials.
```

Appendix E: TCP Wrapper generic configuration file

```
vi /etc/hosts.allow
#
# Only allow access from the management network. Explicit
# deny policy in /etc/hosts.deny
#

# The IP addresses allocated from the management network
/usr/local/bin/sshd: 172.16.1.0/255.255.255.0

vi /etc/hosts.deny
#
# Explicitly deny access from all stations except those
# that match the allow rule in /etc/hosts.allow
#

ALL : ALL
```