

Contents

hp-ux 11.0 Security Checklist	1
Contents	2
1.0 Initial Installation.....	3
1.1 Install the Latest Patches.....	3
1.2 File Systems	3
1.3 Time Settings	3
1.4 Software Selection	4
1.5 Minimize boot services or daemons	4
1.6 Message Text for users attempting to log on.....	4
1.7 Privileged Account Login Source	4
1.8 Network driver configuration.....	5
2.0 System Network Services	6
2.1 Network Services Summary	6
2.4 File Transfer.....	7
2.5 Electronic Mail.....	7
2.8 Domain Name Service	7
2.9 X11.....	7
2.12 Remote shell / copy services	7
2.13 File Share Facilities.....	8
2.14 Firewall Selection	9
3.0 System Accounts and User Rights	10
3.1 Account Characteristics	10
3.2 Standard Accounts	10
3.3 Unauthenticated Access	10
3.4 Appropriate Administrative Authentication	10
3.5 Authentication Configuration	10
4.0 File and Object Access.....	12
4.2 Umask settings	12
4.4 Permissions tightening	12
4.5 SUID or SGID files.....	12
4.6 System access configuration files locked	13
5.0 System Auditing.....	14
5.1 Auditing Overview.....	14
5.2 Initial Installation.....	14
5.3 Protecting the audit configuration files	14
5.5 Monitoring User access.....	14
6.0 Application security	15
6.1 Patches	15
6.2 Minimize services offered.....	15
6.3 Configure users and authentication.....	15
6.4 Auditing	15
6.5 Object access, permissions	15

The following is a recommended security checklist for hp-ux 11.0 servers. This document should be used as a guide to the installation and configuration of hp-ux 11.0 servers in conjunction with an agreed security plan for the identified systems. The document is designed for use by experienced system administrators.

Some of the settings may be dependant on the patch levels of the components in use, and therefore differences may exist between this document and the actual file paths and access control settings on your machine.

1.0 Initial Installation

1.1 Install the Latest Patches

In most cases distribution vendors will provide an update facility for the distribution of patches. The latest system patches should be installed prior to operational deployment if compatible with the applications and middleware used. Particular attention should be paid to those network services that the operating system makes available to remote clients (e.g.: Web (Apache), Mail (sendmail/postfix/imapd), and so on.

Before installing patches always make sure, additional software products like databases or applications support them.

It is recommended that the system be updated with newly released patches as soon as operational circumstances allow. However this does apply to individual patches only if they solve a known problem or security issue. Otherwise wait for tested software release bundles (can be ordered through the itrc web page) to come out.

Patches also should be tested on a test server that preferably runs the same software as the productive node. A procedure should be in place for propagating these patches after a given time, allow 3 months for this at least.

Bypassing the vendor, and installing patches directly from the application provider (eg: from apache.org) may also be appropriate in some circumstances, where the problem in question is significant, or the distribution vendor response to security issues is poor.

Latest Patches can be found at <http://itrc.hp.com/>

In order to stay updated with latest vulnerabilities on hp-ux systems and patches required for it register to the hp patch mailing list and/or the IT newsletter at <http://hp.m0.net/m/p/hpi/hpr/newsletter.asp>

1.2 File Systems

Per default hp-ux mounts remote or local file systems with read-write privileges and suid or sgid enabled. Turn these off in /etc/fstab if not needed.

1.3 Time Settings

All the servers should have the same time settings in order to be able to evaluate logs properly.

1. There should be a time-zone entry in /etc/TIMEZONE containing $tz=MET$.
2. There should be a NTP system installed with timeservers configured for synchronisation (fx. /etc/ntp.conf should contain server a.b.c.d prefer)

Timeservers in Oss/Bss are 10.130.200.70 or 10.130.200.80

In Management network 10.10.8.70 or 10.10.8.80

1.4 Software Selection

If a system is freshly installed, do a core installation and install only packages that are required for operation of the system.

All the external packages that can't be patched should be kept updated to the latest operational version if there are known security issues with older versions or bugs that affect operation (fx. SSH package should be version 3.4.1 or higher).

All unnecessary modules should be also removed.

1.5 Minimize boot services or daemons

All unnecessary daemons or services starting during boot time (/sbin/rc.d) should be disabled.

1.6 Message Text for users attempting to log on

/etc/motd

Place the following message (or a similar one) into this file. It contains a message that will be printed after a successful login.

This is a private computer facility. The owner must specifically authorize access for any reason. Unless you are so authorized, your continued access and any other use may expose you to criminal and/or civil proceedings. Usage may be monitored.

/etc/issue (may also be hardlinked to /etc/motd)

Place the following message (or a similar one) into this file. It contains a message that will be printed during the login process.

This is a private computer facility. The owner must specifically authorize access for any reason. Unless you are so authorized, your continued access and any other use may expose you to criminal and/or civil proceedings. Usage may be monitored.

NOTE: The users may see both the /etc/motd and the /etc/issue messages when they login.

The ssh daemon should be configured to display the message by putting this line into sshd_config: *Printmotd yes*

1.7 Privileged Account Login Source

In order to ensure security of the root account there should be limitations placed on the source of login.

Root should be able to log into the system only locally (via console or with su command).

This can be ensured by :

1. In /etc/securetty only enable /dev/console
2. In sshd_conf put line *PermitRootLogin no*

1.8 Network driver configuration

Make the following adjustments to the **end** of */etc/rc.config.d/nddconf* to protect the machine from SYN floods, ARP spoofs, smurf attacks and from being unwitting allies to DDoS attackers.

```
TRANSPORT_NAME[0]=ip
NDD_NAME[0]=ip_forward_src_routed
NDD_VALUE[0]=0
TRANSPORT_NAME[1]=ip
NDD_NAME[1]=ip_forward_directed_broadcasts
NDD_VALUE[1]=0
TRANSPORT_NAME[2]=tcp
NDD_NAME[2]=tcp_conn_request_max
NDD_VALUE[2]=4096
TRANSPORT_NAME[3]=tcp
NDD_NAME[3]=tcp_syn_rcvd_max
NDD_VALUE[3]=4096
TRANSPORT_NAME[4]=tcp
NDD_NAME[4]=tcp_ip_abort_cinterval
NDD_VALUE[4]=60000
TRANSPORT_NAME[5]=ip
NDD_NAME[5]=ip_send_redirects
NDD_VALUE[5]=0
TRANSPORT_NAME[6]=arp
NDD_NAME[6]=arp_cleanup_interval
NDD_VALUE[6]=60000
TRANSPORT_NAME[8]=ip
NDD_NAME[8]=ip_forwarding
NDD_VALUE[8]=0
```

Make the system stack non-executable:

```
/usr/sbin/kmtune -s executable_stack=0 &&
mk_kernel &&
kmupdate
```

Use better TCP sequence numbers (for HP-UX 10.x only)

```
echo "/usr/contrib/bin/nettune -s tcp_random_seq 2" >> \
/sbin/rc2.d/S339nettune
```

2.0 System Network Services

2.1 Network Services Summary

All the unnecessary network services should be switched off.

1. /etc/inetd.conf should not contain any entries unless specifically required by applications.

Here is a quick rundown of the risks associated with services started in /etc/inetd.conf:

ftp: enables an FTP server that introduces a variety of insecurities and is the cause of many intrusions. Disable this and use [sftp](#) instead to transfer files between systems.

telnet, shell, login, exec: allows users from other systems to log into and run commands on your machine. This is useful, but the more useful something is, the more likely it is that someone will find a way to exploit it. Disable these services and, if you do need to allow remote logins, use [ssh](#) instead.

talk: allows users to communicate by typing at each others' terminals. If you need to use this feature, restrict access to the service using TCPwrappers and [IPFilter/IPChains](#).

uucp: Nobody uses uucp anymore - disable this. While you are at it, you may as well turn off execute permission on the uucp-related shell commands.

tftp: FTP without any security. This should be needed only if your system will be used for booting workstations. If this is the case, you must invoke the daemon with the -s flag, as in:

```
tftp dgram udp wait root in.tftpd -s /tftpboot
```

If you don't, tftp can be used to retrieve any file from your system, anonymously. Also make all the files in the bootfile directory read-only.

Finally, restrict access to the service using TCPwrappers and

This is often enabled by ignite but can safely be disabled again, if you do not need to use this machine as an ignite server (golden image).

[IPFilter/IPChains](#).

finger: this gives out information on who is logged in, or people's phone numbers and offices. Unfortunately this information can be used to find accounts to attack by a potential intruder. You may wish to disable this, run a custom finger daemon, or restrict access to it using TCPwrappers and [IPFilter/IPChains](#).

systat, netstat: these services give out information about your system. The comments for finger apply to these.

time: Gives out the system time to any remote host that asks for it. Probably safe but can be disabled without impacting the system.

echo, discard, daytime, chargen: these are used for testing, and are generally safe, though there have been reports of TCP packets with forged IP source addresses being used to trick a system into sending echo packets to itself, causing a packet storm on the local ethernet segment. Disable them and only turn them on while testing.

rexid - this is the Remote Procedure Call mechanism. It has minimal authentication, so disable it and use [ssh](#) instead.

walld: allows people to send messages to all logged in users. Useful, but easily abused. Disable this service or restrict access to it using TCPwrappers and [IPFilter/IPChains](#).

tttserverd (tooltalk): used by some convenient desktop elements but not important from a system operation standpoint. Some versions of this service contain serious remote exploits and should be disabled (disabling this service causes virtually no operational degradation).

rpc.cmsd (calendar manager): used to share calendar information over the network but not important from a system operation standpoint. Some versions of this service contain serious remote exploits and should be disabled.

others: Other services such as sadmind (once found to be vulnerable to remote root exploit) and kerberos can be disabled without impacting the system.

2. There should not be any services listening on the network unless required by applications.

2.4 File Transfer

Ftp service should be disabled and secure ftp or secure copy should be used.

/etc/ftpusers should contain all the account names except those that should be allowed to access the system via FTP. ftp access should be restricted through TCPwrappers and [IPFilter/IPChains](#).

2.5 Electronic Mail

There should be no email service running on the system for local use (email servers have email agents installed as application and should follow the application security part of this document). Disable the start of sendmaild during bootup.

2.8 Domain Name Service

There should be no DNS servers running on the system (DNS servers should be treated as an application and should follow application security part of this document).

2.9 X11

X servers should be run in nolisten mode if possible. X connections still can be tunneled through ssh in most cases. Some applications like OmniBack require the X11UseLocalhost set to no in sshd_config for this to work.

2.12 Remote shell / copy services

All the systems should have the latest [ssh](#) installed in order to allow remote administration of the server with encrypted interconnection.

sshd_config should contain also these features:

```
Protocol 2
UsePrivilegeSeparation yes
ServerKeyBits 768
SyslogFacility AUTH
LogLevel INFO
LoginGraceTime 600
```

PermitRootLogin no
StrictModes yes
RSAAuthentication yes
PubkeyAuthentication yes
RhostsAuthentication no
IgnoreRhosts yes
RhostsRSAAuthentication no
HostbasedAuthentication no
PermitEmptyPasswords no
PasswordAuthentication yes
PrintMotd yes
PrintLastLog no
MaxStartups 10:30:60
ReverseMappingCheck yes

2.13 File Share Facilities

There should be no file sharing facilities, unless there is a application using it.

NFS service can be disabled with this script:

```
if [ ! -f /sbin/rc2.d/S430nfs.client ]
then mv /sbin/rc2.d/S400nfs.core \
/sbin/rc2.d/.NOS400nfs.core
fi
mv /sbin/rc3.d/S100nfs.server \
/sbin/rc3.d/.NOS100nfs.server
cat << EOF >> /etc/rc.config.d/nfsconf
NFS_SERVER=0
PCNFS_SERVER=0
NUM_NFSD=0
NUM_NFSIOD=0
START_MOUNTD=0
EOF
```

If there is no need for NFS client it can be disabled also:

```
cd /sbin/rc2.d
mv S430nfs.client .NOS430nfs.client
if [ ! -f /sbin/rc3.d/S100nfs.server ]
then mv S400nfs.core .NOS400nfs.core
fi
cat << EOF >> /etc/rc.config.d/nfsconf
NFS_CLIENT=0
AUTOFS=0
AUTOMOUNT=0
EOF
```

2.14 Firewall Selection

Every system should have a filtering capability at disposal for later use. Filtering capabilities should enable limitation of certain IP addresses to certain services. This is not a standard part of the hp-ux distribution. Only to be installed if needed.

3.0 System Accounts and User Rights

3.1 Account Characteristics

By default, hp-ux operates on the assumption that all users are local users. Explicit package installation needs to be undertaken on most hp-ux distributions in order to facilitate a distributed authentication framework such as LDAP.

Other features:

1. User home directories should be mode 755 or more restrictive
2. No user dot-files should be group/world writable
3. Standard Password policy should be checked

3.2 Standard Accounts

Several of the accounts in */etc/passwd* are unnecessary. In order to secure them you should:

1. effectively disable them.
2. ensure these accounts cannot use **ftp**, **cron** or **at**.
3. remove valid shells from daemon accounts.

3.3 Unauthenticated Access

There should be no possible unauthenticated access enabled on the system.

1. */etc/hosts.equiv*, */.rhosts*, */.netrc* should be empty or non existent
2. No empty password fields in password files

3.4 Appropriate Administrative Authentication

Access to root account via *su* should be only possible from wheel group. All users that are system administrators should be in wheel group.

3.5 Authentication Configuration

In order to enforce system authentication to use standard unix authentication facility */etc/pam.conf* should contain these entries:

```
# PAM configuration
# Authentication management
login auth required /usr/lib/security/pam_unix.so.1
su auth required /usr/lib/security/pam_unix.so.1
dtlogin auth required /usr/lib/security/pam_unix.so.1
other auth required /usr/lib/security/pam_unix.so.1
#
# Account management
login account required /usr/lib/security/pam_unix.so.1
su account required /usr/lib/security/pam_unix.so.1
dtlogin account required /usr/lib/security/pam_unix.so.1
other account required /usr/lib/security/pam_unix.so.1
#
# Session management
su session required /usr/lib/security/pam_unix.so.1
```

```
other session required /usr/lib/security/pam_unix.so.1  
#  
# Password management  
other password required /usr/lib/security/pam_unix.so.1
```

If http authentication is supposed to be used then there should be extra entries specifying http authentication facility.

4.0 File and Object Access

4.2 Umask settings

Set user file creation mask

In each of the files `/etc/.login`, `/etc/cshrc` and `/etc/profile`, there should be an invocation of the `umask` command. This invocation should be positioned immediately after the initial comments. The value passed to `umask` is an octal mask of the mode bits that are *not* set when a file is created. Acceptable values are 022, 026 (suggested) and 027. Each of these has advantages and disadvantages. Please read the `umask` manual page prior to selecting the value to be set.

Set FTP file creation mask

Add the following to the `ftpd` call in `/etc/inetd.conf`: `-u 026`. The value shown here is for demonstration purposes only. The `umask` value chosen for the user file creation mask (above) should be used.

4.4 Permissions tightening

Minimize file or object access to only groups or users that will access them (fx.

Oracle daemon should be executable by user oracle only)

Crontab access restrictions should be put into `/var/adm/cron/cron.allow` (permissions set to read).

At access restrictions should be put into `/var/adm/cron/at.allow` (permissions set to read).

4.5 SUID or SGID files.

Check for `setuid` files, and modify them, as appropriate. Administrators who wish to obtain a list of the `set-UID` and `set-GID` programs currently installed on the system may run the following commands:

```
for part in \  
`awk '($3 ~ /^(hfs|vxfs)$/) { print $2 }' /etc/fstab`  
do  
find "$part" \( -perm -04000 -o -perm -02000 \) \  
-type f -xdev -print  
done
```

NOTE: A server should be checked for `setuid` files after patches are updated, and after third-party packages (source or binary) are installed.

Fx the following programs ship with some versions of HP-UX as `set-UID`, have a history of significant security risk as a result of shipping `set-UID`, are not required to be `set-UID` in most circumstances, and therefore are recommended to be set not to be `set-UID`:

```
/opt/audio/bin/Aserver  
/opt/sharedprint/bin/pcltotiff  
/sbin/shutdown  
/usr/bin/bdf  
/usr/bin/df  
/usr/bin/elm
```

```
/usr/bin/kermit
/usr/sbin/expreserve
/usr/sbin/exrecover
/usr/sbin/wall
/usr/contrib/bin/X11/xconsole
```

4.6 System access configuration files locked

In every user's directory there should be configuration files created (.rhosts or .ssh) with root as the owner and writable only by root.

Note: This requires the home directory to be owned by root as well. .profile should cd to a user owned directory and source a user owned .profile.

5.0 System Auditing

5.1 Auditing Overview

All the messages and log information should be centrally processed on a remote log server.

In OSSBSS there is a syslog server at disposal. Syslog.conf entry should look like this:

```
*.* @10.130.200.40
```

or

```
*.* @10.10.8.40
```

5.2 Initial Installation

Syslog messages sent to a centralized log server

1. /etc/syslog.conf should contain this entry **.* @logserver*
2. Put logserver into your local /etc/hosts file once it has been defined.
3. Turn on `crond` logging

5.3 Protecting the audit configuration files

Integrity verification service should be done to a remote host.

Logs should be stored safely on a read only media or on a secured media not accessible by all the system users.

5.5 Monitoring User access.

Create a log for authentication information. These logs go to /var/adm/syslog/syslog.log at the moment. It makes sense to reroute authentication information to another log file, preferably on a remote host.

6.0 Application security

6.1 Patches

Install all the latest patches and fixes for the application. If possible upgrade application to the latest version.

6.2 Minimize services offered

Switch off or remove services that are not required to perform application's function in the system.

Fx. Apache web server with basic HTML functionality required doesn't need CGI, imap module or Java servlets configured.

6.3 Configure users and authentication

Every user should have his/her own login with proper authentication method used. Their permissions should not include more than necessary (read only user should have only read only access) and if necessary for every role a user has there should be an account with proper permissions for that role.

Fx. User XY ; role: application tester (read only access to data)

 User XY ; role application developer (read write to development environment)

 User XY ; role application administrator (full access to application configuration)

6.4 Auditing

If possible application should produce a log documenting its tasks that are performed as well as requests, queries or user input.

1. major or critical application errors
2. users login/logout
3. modification of application settings (security settings, logging settings, operational settings)
4. (optional) business data modifications

6.5 Object access, permissions

If possible application should have restrictions on objects (files, items or tables) so that only authorized sources can read, modify or delete them.

Fx. Access to SNMP system IDs in NetCool database should be limited to NetCool administrator only.

Oracle progressor database access granted only to progressor application.