the CENTER for INTERNET SECURITY

HP-UX Benchmark v1.4.2

June 2008

Edited by Chris Calabrese and Robert Fritz

http://www.CISecurity.org/

TERMS OF USE AGREEMENT

Background.

The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No Representations, Warranties, or Covenants.

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties, or covenants of any kind.

User Agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**We**") agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;

2. We are using the Products and the Recommendations solely at our own risk;

3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and

6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without

limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of Intellectual Property Rights; Limitations on Distribution.
The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled “Grant of limited rights.”

Subject to the paragraph entitled “Special Rules” (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special Rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

Terms of Use Agreement Version 2.1 - 02/20/04

CIS HP-UX Benchmark

Dedication

This HP-UX Benchmark is dedicated to the memory of Chris Calabrese, whose dedication and skill over the years made it possible.

A Word about Shaded Items

Desktop systems typically have different security expectations than server-class systems. In an effort to facilitate use of this benchmark on these different classes of machines, shaded text has been used to indicate questions and/or actions that are typically not applicable to desktop systems in a large enterprise environment. These shaded items may be skipped on these desktop platforms.

Root Shell Environment Assumed

The actions listed in this document are written with the assumption that they will be executed by the `root` user running the `/sbin/sh` shell, using a `umask` of `077` (‘`umask 077`’), and without `noclobber` set (‘`set +o noclobber`’).

Executing Actions

The actions listed in this document are written with the assumption that they will be executed in the order presented here. Some actions may need to be modified if the order is changed, or if earlier actions are omitted. Actions are written so that they may be copied directly from this document into a `root` shell window with a "cut-and-paste" operation. In addition, while each action has likely been tested at some point, on the various authors’ systems, versions of HP-UX differ in their configuration. Where known, such differences are noted, but in all cases, it is the responsibility of the user of this document to ensure the provided scripts work in the user’s environment.

Reboot Required

Rebooting the system is required after completing all of the actions below in order to complete the re-configuration of the system. In many cases, the changes made in the steps below will not take effect until this reboot is performed.

Backup Key Files

Before performing the steps of this benchmark, it is **strongly recommended** that administrators make backup copies of critical configuration files that may get modified by various benchmark items. The script provided in Appendix A of this document will automatically back up all files that may be modified by the actions below. If this step is not performed, then the site may have no reasonable back-out strategy for reversing system modifications made as a result of this document.

Note that an executable copy of this script is also provided in the archive containing the PDF version of this document and the CIS scoring tool. This archive creates a "cis" subdirectory when unpacked, so assuming the administrator is in the directory where the archive has been unpacked, the command to execute the backup script would be:

```
cis/do-backup.sh
```

To roll back the changes performed by this benchmark, first run 'bastille -r' followed by restoring any benchmark-changed filesdo-restore.sh, and all changes will be backed up by do-backup.sh aboveout.

IMPORTANT: Note that these backup and restore scripts have not been tested with this version of the benchmark, so are intended for reference.

Notes About Bastille

Bastille is an open source application that hardens a number of operating systems, including Linux, HP-UX and OSX. Using it will simplify hardening.

It is available as part of the default install for 11.23, and 11.31, and available for 11.00 and 11.11 at http://hp.com/go/bastille.

For ease of reference, a "Bastille" icon is beside each question that is addressed at least partially by Bastille.

1 Patches and Additional Software

1.1 Apply latest OS patches

Action *(HP-UX 11i)*:

1. Download and install HP-UX Software Assistant from https://www.hp.com/go/swa if not already installed on the system. Follow the installation instructions available the above page.

2. Run Software Assistant (SWA) as

```
swa report
```

   Note that the above command assumes direct network connectivity from the system you are running SWA on to HP's servers. See the swa(1M) *man* page for dealing with issues such as specifying proxy servers, etc.

3. Perform the actions specified by Software Assistant. This may involve:

   a. Manual actions such as removing files or changing file permissions. This is typically done by reading the HP Security Bulletin specified by the SWA tool and implementing the recommended actions if they apply to this system's configuration. If they do not apply, update the `$HOME/.swa/ignore` file to suppress this issue in future reports as directed in the swa(1M) *man* page.

   b. Installing updated versions of software applications such as the Apache HTTP server, SAMBA software, etc. This is done by downloading the software updates from locations specified in the HP Security Bulletin, such as: http://software.hp.com, http://support.openview.hp.com, or http://www.hp.com/go/java and then installing with `swinstall`.

   `c.` Installing patches: This is typically done by downloading the specified patches, plus any patches those patches depend upon. The easiest way to do this is to create a depot and then install its contents:

```
swa get -t <directory to make depots>
```

   after un-`shar`ing the patches:

```
swinstall -s <depot location> \*
```

   Alternatively, you may consider `swcopy`ing the depots together and installing once.

   d. Removing obsolete software: In some cases, an HP security bullet may recommend replacing vulnerable software with an updated version or an equivalent but different product, such as replacing Netscape with Mozilla. This is typically done using the `swremove` command.

Action *(older HP-UX releases)*:

Strongly consider upgrading to HP-UX 11i.

Discussion:

Installing up-to-date vendor patches and developing a procedure for keeping up with vendor patches is critical for the security and reliability of the system. Vendors will issue operating system updates when they become aware of security vulnerabilities and other serious functionality issues, but it is up to their customers to actually download and install these patches.

During the patch installation process, some patches may not be installed. Administrators may ignore individual patch installations that fail because they patch a software sub-system that is not installed on the system. If a patch installation fails for any other reason, the administrator should consult the patch installation log in `/var/adm/sw/swagentd.log`.

Additionally, consider installing HP's quarterly patch updates available from HP's IT Resource Center (http://itrc.hp.com/service/patch/releaseIndexPage.do), and/or using the "swa get" command. Similarly, HP-UX administrators should run SWA daily and/or subscribe to HP's Security Bulletins Digest, which directs you to install specific security patches and other updates as they come out. Using SWA to analyze relevance of security bulletins and partially automate their application is much easier and more reliable than performing that analysis manually, so SWA is by far the easier option in most cases.

Information on how to subscribe to the Security Bulletins Digest is available from the HP IT Resource Center (http://itrc.hp.com).

Note that much of this benchmark assumes the system is current with respect to security-bulletin-announced patches, and that the applicable Quality Packs are installed.

Finally, security patches are no longer available for HP-UX 11.00 and earlier releases, HP-UX 11.00 having reached its official End of Life on December 31st 2006. Sites running HP-UX 11.00 and earlier releases should strongly consider upgrading to HP-UX 11i.

1.2 *Install and configure SSH*

Action *(HP-UX 11i)*:

1. Download and install the pre-compiled OpenSSH software from `http://software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=T1471AA` if not already installed on the system. Installation instructions can be found at http://h20293.www2.hp.com/portal/swdepot/displayInstallInfo.do?productNumber=T1471AA. Note that the OpenSSH is installed by default on HP-UX 11iv2 and later.

2. Perform the following post-installation action:

```
cd /opt/ssh/etc
cp -p sshd_config sshd_config.tmp
awk '
  /^Protocol/                 { $2 = "2" };
  /^X11Forwarding/            { $2 = "yes" };
  /^IgnoreRhosts/             { $2 = "yes" };
  /^RhostsAuthentication/     { $2 = "no" };
  /^RhostsRSAAuthentication/ { $2 = "no" };
  /(^#|^)PermitRootLogin/     {
        $1 = "PermitRootLogin";
        $2 = "no" };
  /^PermitEmptyPasswords/     { $2 = "no" };
  /^#Banner/                  {
        $1 = "Banner";
        $2 = "/etc/issue" }
  { print }' sshd_config.tmp > sshd_config
rm -f sshd_config.tmp
chown root:sys ssh_config sshd_config
chmod go-w ssh_config sshd_config
```

Action *(older HP-UX releases)*:

Consider upgrading to HP-UX 11i, or see http://www.openssh.org/ for information on building OpenSSH from source.

Discussion:

OpenSSH is a popular free distribution of the standards-track SSH protocols, which allows secure encrypted network logins and file transfers. However, compilation of OpenSSH is complicated by the fact that it is dependent upon several other freely-available software libraries that also need to be built before OpenSSH itself can be compiled. In order to simplify the installation process, we make use of a pre-compiled version of OpenSSH, available from Hewlett-Packard. Note, however, this pre-compiled version is only available for HP-UX 11.x releases. Sites running HP-UX 10.20 or earlier must build OpenSSH from source.

For more information on building OpenSSH from source, see http://www.openssh.org/.

1.3 Install and Run Bastille

Action (*HP-UX 11.x*):

Download and install Bastille HP-UX from https:// www.hp.com/go/bastille

After Bastille is installed, copy the `bastille_hpux.CIS.conf` file provided in the archive containing the PDF version of this document (and in Appendix C) to `/etc/Bastille/config`. Run Bastille in batch mode as shown:

```
   cp /path/to/bastille.CIS.conf config
   /opt/sec_mgmt/bastille/bin/bastille -b
```

At this point, Bastille commits the changes.

Action (*HP-UX 10.20*):

Strongly consider upgrading to HP-UX 11i.

Discussion:

Bastille is a series of Perl scripts that ask you questions and hardens your machine based on the answers. The Benchmark will then walk you through opening up your system for the services that have a legitimate Business need.

2 Minimize `inetd` network services

2.1 Disable Standard Services

Action:

```
cd /etc
touch /var/adm/inetd.sec

for svc in echo discard daytime chargen dtspc \
     exec ntalk finger uucp ident auth \
     instl_boots registrar recserv; do
  awk "(\$1 == \"$svc\") { \$1 = \"#\" \$1 }; {print}" \
    inetd.conf > inetd.conf.new
  cp inetd.conf.new inetd.conf
  grep -E -q "^$svc[ ]+deny[ ]*$" /var/adm/inetd.sec \
  || echo "$svc deny" >> /var/adm/inetd.sec
done
for svc in rpc.rstatd rpc.rusersd rpc.rwalld \
     rpc.sprayd rpc.cmsd kcms_server; do
  awk "/\\/$svc/ { \$1 = \"#\" \$1 }; { print }" \
    inetd.conf > inetd.conf.new
  cp inetd.conf.new inetd.conf
done

for svc in printer shell login telnet ftp tftp \
     bootps kshell klogin; do
  awk "(\$1 == \"$svc\") { \$1 = \"#\" \$1 }; {print}" \
    inetd.conf > inetd.conf.new
  cp inetd.conf.new inetd.conf
  grep -E -q "^$svc[ ]+deny[ ]*$" /var/adm/inetd.sec \
  || echo "$svc deny" >> /var/adm/inetd.sec
done
for svc in rpc.rquotad rpc.ttdbserver; do
  awk "/^$svc\\// { \$1 = \"#\" \$1 }; { print }" \
    /etc/inetd.conf > /etc/inetd.conf.new
  cp inetd.conf.new inetd.conf
done


chown root:sys inetd.conf
chmod go-w,a-xs inetd.conf
rm -f /etc/inetd.conf.new
```

Discussion:

The stock /etc/inetd.conf file shipped with HP-UX contains many services which are rarely used, or which have more secure alternatives. Indeed, after enabling SSH (see item *1.2*) it may be possible to completely do away with all inetd-based services, since SSH provides both a secure login mechanism and a means of transferring files to and from the system. In fact, the actions above will disable all services normally enabled in the HP-UX inetd.conf file.

The rest of the actions in this section give the administrator the option of re-enabling certain services—in particular, the services that are disabled in the last two loops in the **Action** section above.

Bastille Notes:

Rather than disabling and then re-enabling these services, Bastille operates by disabling only those services that are unnecessary for the systems.

Also note that Bastille only disables those *inetd* services that are enabled by default, so it is possible that a service that has been turned on manually will not be turned off when using Bastille.

2.2 Only enable `telnet` if absolutely necessary

Question:

Is there a mission-critical reason that requires users to access this system via telnet*, rather than the more secure SSH protocol?*

If the answer to this question is yes, perform the actions below.

Action:

```
awk '/^#telnet/ {
  $1 = "telnet"
  print $0 " -b /etc/issue"; next}
  { print }
' inetd.conf > /etc/inetd.conf.new
cp inetd.conf.new inetd.conf
grep -Ev '^telnet[ ]+deny[ ]*$' \
  /var/adm/inetd.sec > /var/adm/inetd.sec.new
cp /var/adm/inetd.sec.new /var/adm/inetd.sec
rm -f /etc/inetd.conf.new /etc/inetd.sec.new
```

Discussion:

telnet uses an unencrypted network protocol, which means data from the login session (such as passwords and all other data transmitted during the session) can be stolen by eavesdroppers on the network, and also that the session can be hijacked by outsiders to gain access to the remote system. The freely-available SSH utilities (see item1.2– *Install SSH*) provides an encrypted alternative to telnet (and other utilities) and should be used instead.

2.3 Only enable FTP if absolutely necessary

Question:

Is this machine an (anonymous) FTP server, or is there a mission-critical reason why data must be transferred to and from this system via ftp, rather than scp?

If the answer to this question is yes, perform the actions below.

Action:

```
awk '
  /^#ftp/ { $1 = "ftp"; print $0 "-l" ; next}
  { print }
' inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
grep -Ev '^ftp[ ]+deny[ ]*$' \
  /var/adm/inetd.sec > /var/adm/inetd.sec.new
cp /var/adm/inetd.sec.new /var/adm/inetd.sec
rm -f /etc/inetd.conf.new /etc/inetd.sec.new
```

Discussion:

Like telnet, the FTP protocol is unencrypted, which means passwords and other data transmitted during the session can captured by sniffing the network, and that the FTP session itself can be hijacked by an external attacker. SSH provides two different encrypted file transfer mechanisms—scp and sftp—and should be used instead. Even if FTP is required because the local system is an anonymous FTP server, consider requiring non-anonymous users on the system to transfer files via SSH-based protocols. For further information on restricting FTP access to the system, see Item 6.2 below.

Sites may also consider augmenting the "ftpd -l" above with '-v' (10.x and 11.x) or '-L' (11.x only) for additional logging of FTP transactions, or with '-a' (11.x only) for fine grain FTP access control through the use of a configuration file – see the ftpd(1M) man page on your systems for details.

2.4 Only enable rlogin/remsh/rcp if absolutely necessary

Question:

Is there a mission-critical reason why rlogin/remsh/rcp must be used instead of the more secure ssh/scp?

If the answer to this question is yes, perform the actions below.

Action:

```
sed 's/^#shell/shell/; s/^#login/login/' \
  inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
grep -Ev '^(shell|login)[ ]+deny[ ]*$' \
  /var/adm/inetd.sec > /var/adm/inetd.sec.new
cp /var/adm/inetd.sec.new /var/adm/inetd.sec
rm -f /etc/inetd.conf.new /etc/inetd.sec.new
```

Discussion:

SSH was designed to be a drop-in replacement for these protocols. Given the wide availability of free SSH implementations, there are few cases where these tools cannot be replaced with SSH (again, see item 1.2 – *Install SSH*).

2.5 Only enable TFTP if absolutely necessary

Question:

Is this system a boot server or is there some other mission-critical reason why data must be transferred to and from this system via TFTP?

If the answer to this question is yes, perform the actions below.

Action:

```
sed 's/^#tftp/tftp/' inetd.conf >inetd.conf.new
cp inetd.conf.new inetd.conf
grep -Ev '^tftp[ ]+deny[ ]*$' \
  /var/adm/inetd.sec > /var/adm/inetd.sec.new
cp /var/adm/inetd.sec.new /var/adm/inetd.sec
rm -f /etc/inetd.conf.new /etc/inetd.sec.new
mkdir -p /var/opt/ignite
```

Discussion:

TFTP is typically used for network booting of diskless workstations, X-terminals, and other similar devices. TFTP is also used during network installs of systems via the HP-UX Ignite facility. Routers and other network devices may copy configuration data to remote systems via TFTP for backup. However, unless this system is needed in one of these roles, it is best to leave the TFTP service disabled.

2.6 Only enable printer service if absolutely necessary

Question:

Is this machine a print server for your network?

If the answer to this question is yes, perform the actions below.

Action:

```
sed 's/^#printer/printer/' inetd.conf >inetd.conf.new
cp inetd.conf.new inetd.conf
grep -Ev '^printer[ ]+deny[ ]*$' \
  /var/adm/inetd.sec > /var/adm/inetd.sec.new
cp /var/adm/inetd.sec.new /var/adm/inetd.sec
rm -f /etc/inetd.conf.new /etc/inetd.sec.new
```

Discussion:

`rlpdaemon` provides a BSD-compatible print server interface. Even machines that are print servers may wish to leave this service disabled if they do not need to support BSD-style printing.

2.7 *Only enable `rquotad` if absolutely necessary*

Question:

Is this system an NFS file server that requires the use of disk quotas?

If the answer to this question is yes, perform the actions below.

Action:

```
awk '
    $6 ~ /\/rpc.rquotad$/ { sub(/^#/, "") }
  { print }
' inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
rm -f /etc/inetd.conf.new
```

Discussion:

`rquotad` allows NFS clients to enforce disk quotas on file systems that are mounted from the local system. If your site does not use disk quotas, then you may leave the `rquotad` service disabled.

2.8 *Only enable CDE-related daemons if absolutely necessary*

Question:

Is there a mission-critical reason to run a CDE GUI on this system?

If the answer to this question is yes, perform the actions below.

Action:

```
awk '
  $6 ~ /\/rpc.ttdbserver$/ { sub(/^#/, "") }
  { print }
' inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
rm -f /etc/inetd.conf.new
```

Discussion:

The `rpc.ttdbserver` service supports HP's CDE windowing environment. This service has a history of security problems. Not only is it vital to keep up to date on vendor patches, but also *never* enable this service on any system which is not well protected by a complete network security infrastructure (including network and host-based firewalls, packet filters, and intrusion detection infrastructure).

Note that since this service uses ONC RPC mechanisms, it is important that the system's RPC portmapper (`rpcbind`) also be enabled when this service is turned on. For more information see Item 3.12 below.

2.9 Only enable Kerberos-related daemons if absolutely necessary

Question:

Is the Kerberos security system in use at this site and is there a mission-critical reason that requires users to access this system via Kerberized `rlogin/remsh`, rather than the more secure SSH protocol?

If the answer to this question is yes, perform the actions below.

Action:

```
sed 's/^#kshell/kshell/; s/^#klogin/klogin/' \
  inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
grep -Ev '^(kshell|klogin)[ ]+deny[ ]*$' \
  /var/adm/inetd.sec > /var/adm/inetd.sec.new
cp /var/adm/inetd.sec.new /var/adm/inetd.sec
rm -f /etc/inetd.conf.new /etc/inetd.sec.new
```

Discussion:

Kerberized `rlogin/remsh` offers a higher degree of security than traditional `rlogin`, `remsh`, or `telnet` by eliminating many clear-text password exchanges from the network. However it is still not as secure as SSH, which encrypts all traffic. Given the wide availability of free SSH implementations, there are few cases where these tools cannot be replaced with SSH (again, see item 1.2– *Install SSH*). For more information on Kerberos see `http://web.mit.edu/kerberos/www/`.

2.10 Only enable BOOTP/DHCP daemon if absolutely necessary

Question:

Is this server a BOOTP/DHCP server for the network?

If the answer to this question is yes, perform the actions below.

Action:

```
sed 's/^#bootps/bootps/' \
  inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
grep -Ev '^bootps[ ]+deny[ ]*$' \
  /var/adm/inetd.sec > /var/adm/inetd.sec.new
cp /var/adm/inetd.sec.new /var/adm/inetd.sec
rm -f /etc/inetd.conf.new /etc/inetd.sec.new
```

Discussion:

BOOTP/DHCP is a popular protocol for dynamically assigning IP addresses and other network information to systems on the network (rather than having administrators manually manage this information on each host). However, if this system is not a BOOTP/DHCP server for the network, there is no need to be running this service.

3 Minimize boot services

Minimizing the number of running services also minimizes potential vulnerabilities, especially with respect to network services. For network services that cannot be eliminated, the local administrator should consider minimizing access to them with external firewalls or host-based firewalls such as HP's IPFilter/9000.

3.1 Disable `login:` prompts on serial ports

Question:

Is there a mission-critical need to provide login capability from any serial ports (such as for a modem)?

If the answer to this question is yes, then ***do not*** perform the actions below.

Action:

```
cp -p /etc/inittab /etc/inittab.tmp
sed 's/^[^#].*getty.*tty.*$/#&/' \
  /etc/inittab.tmp  > /etc/inittab
rm -f /etc/inittab.tmp
chown root:sys /etc/inittab
chmod go-w,ug-s /etc/inittab
```

Discussion:

By disabling the `login:` prompt on the system serial devices, we make it more difficult for unauthorized users to attach modems, terminals, and other remote access devices to these ports. Note that this action may safely be performed even if console access to the system is provided via the serial ports, as the line in the `/etc/inittab` file that corresponds to the console does not match the supplied pattern (i.e., it doesn't contain the string '`tty`').

Note that when serial port connectivity is needed, `/etc/dialups` and `/etc/d_passwd` can be set to require an extra password for serial port access. See the `dialups(4)` manual page for more information.

Note: By default, in HP-UX 11i, only the console has a getty instance running on it.

3.2 Disable NIS/NIS+ related processes, if possible

Question:

Does this machine need NIS/NIS+ facilities (as a client or server)?

If the answer is yes, then ***do not*** perform the actions below..

Action:

```
ch_rc -a -p NIS_MASTER_SERVER=0 -p NIS_SLAVE_SERVER=0 \
  -p NIS_CLIENT=0 -p NISPLUS_SERVER=0 \
  -p NISPLUS_CLIENT=0 /etc/rc.config.d/namesvrs
```

Discussion:

Clearly there is no need to run the NIS/NIS+ related daemons on hosts that are not NIS/NIS+ servers or clients.

Bastille Note:

Bastille disables NIS processes, but not NIS+.

3.3 Disable printer daemons, if possible

Question:

Is this system a print server, or is there a mission-critical reason why users must submit print jobs from this system?

If the answer to this question is yes, then ***do not*** perform the actions below.

Action:

```
ch_rc -a -p XPRINTSERVERS="''" /etc/rc.config.d/tps
ch_rc -a -p LP=0 /etc/rc.config.d/lp
ch_rc -a -p PD_CLIENT=0 /etc/rc.config.d/pd
```

Discussion:

If users will never print files from this machine and the system will never be used as a print server by other hosts on the network, then it is safe to disable these services and remove this software. The Unix print service has generally had a poor security record—be sure to keep up-to-date on vendor patches. The administrator may wish to consider converting to the LPRng print system (see http://www.lprng.org/) which was designed with security in mind and is widely portable across many different Unix platforms. Note, however, that LPRng is not supported by Hewlett-Packard.

Bastille Notes:

Bastille disables only *lp*. *Xprintservers* and *pd_client* are not shipped with all versions of HP-UX.

3.4 Disable GUI login, if possible

Question:

Is there a mission-critical reason to run a GUI on this system?

If the answer to this question is yes, then ***do not*** perform the actions below.

Action:

```
ch_rc -a -p DESKTOP="" /etc/rc.config.d/desktop
chmod go-w,ug-s /usr/dt/bin/dtaction \
  /usr/dt/bin/dtappgather /usr/dt/bin/dtprintinfo \
  /usr/dt/bin/dtsession
```

Discussion:

The X Windows-based CDE GUI on HP-UX systems has had a history of security issues. Never run any GUI-oriented service or application on a system unless that machine is protected by a strong network security infrastructure.

3.5 Disable email server, if possible

Question:

Is this system a mail server—that is, does this machine receive and process email from other hosts?

If the answer to this question is yes, then ***do not*** perform the actions below.

Action:

```
ch_rc -a -p SENDMAIL_SERVER=0 /etc/rc.config.d/mailservs
cd /var/spool/cron/crontabs
crontab -l >root.tmp
echo '0 * * * * /usr/lib/sendmail -q' >>root.tmp
crontab root.tmp
rm -f root.tmp
```

Discussion:

It is possible to run a Unix system with the Sendmail daemon disabled and still allow users on that system to send email out from that machine. Running Sendmail in *"daemon mode"* (with the `-bd` command-line option) is only required on machines that act as *mail servers*, receiving and processing email from other hosts on the network. The actions above will result in a machine that can send email but not receive it.

Note that after disabling the `-bd` option on the local mail server on systems running Sendmail v8.12 or later (8.13 is currently shipped as part of HP-UX 11iv3), it is also necessary to modify the `/etc/mail/submit.cf` file. Find the line that reads "`D{MTAHost}localhost`" and change `localhost` to the name of some other local mail server for the organization. This will cause email generated on the local system to be relayed to that mail server for further processing and delivery.

Note that if the system is an email server, the administrator is encouraged to search the Web for additional documentation on Sendmail security issues. Some information is available at http://www.deer-run.com/~hal/dns-sendmail/DNSandSendmail.pdf and at http://www.sendmail.org/.

3.6 Disable SNMP and OpenView Agents
(If remote management or monitoring is not needed)

Question:

Are hosts at this site remotely monitored by Openview or another tool that relies on SNMP such as MRTG or Cricket?

If the answer to this question is yes, then ***do not*** perform the actions below.

Action:

1.
```
cd /sbin/rc2.d
for file in S565OspfMib S941opcagt S570SnmpFddi
do  mv -f $file .NO$file
done

ch_rc -a -p SNMP_HPUNIX_START=0 \
  /etc/rc.config.d/SnmpHpunix
ch_rc -a -p SNMP_MASTER_START=0 \
  /etc/rc.config.d/SnmpMaster
ch_rc -a -p SNMP_MIB2_START=0 \
  /etc/rc.config.d/SnmpMib2
ch_rc -a -p SNMP_TRAPDEST_START=0 \
  /etc/rc.config.d/SnmpTrpDst
```

2. Remove any software packages related to HP OpenView NNM using `swremove.  These are designated as packages that begin with OVOPC.`

Discussion:

If you are using SNMP to monitor the hosts on your network, experts recommend changing the default community string used to access data via SNMP. On HP-UX systems, this parameter can be changed by modifying the `get-community` and `set-community` parameters in `/etc/SnmpAgent.d/snmpd.conf`

Bastille Notes:

Bastille does not disable the OV agents

3.7 Disable other standard boot services

Action:

```
ch_rc -a -p START_SNAPLUS=0 -p START_SNANODE=0 \
  -p START_SNAINETD=0 /etc/rc.config.d/snaplus2
ch_rc -a -p MROUTED=0 -p RWHOD=0 \-p DDFA=0 \
  -p START_RBOOTD=0 /etc/rc.config.d/netdaemons
ch_rc -a -p DCE_KRPC=0 -p DFS_CORE=0 -p DFS_CLIENT=0 \
  -p DFS_SERVER=0 -p DFS_EPISODE=0 -p EPIINIT=0 \
  -p DFSEXPORT=0 -p BOSSERVER=0 -p DFSBIND=0 \
  -p FXD=0 -p MEMCACHE=0 -p DFSGWD=0 \
  -p DISKCACHEFORDFS=0 /etc/rc.config.d/dfs
ch_rc -a -p RARPD=0 -p RDPD=0 /etc/rc.config.d/netconf
ch_rc -a -p PTYDAEMON_START=0 /etc/rc.config.d/ptydaemon
ch_rc -a -p VTDAEMON_START=0 /etc/rc.config.d/vt
ch_rc -a -p NAMED=0 /etc/rc.config.d/namesvrs
ch_rc -a -p PEER_SNMPD_START=0 \
  /etc/rc.config.d/peer.snmpd
ch_rc -a -p START_I4LMD=0 /etc/rc.config.d/i4lmd
ch_rc -a -p RUN_X_FONT_SERVER=0 /etc/rc.config.d/xfs
ch_rc -a -p AUDIO_SERVER=0 /etc/rc.config.d/audio
ch_rc -a -p SLSD_DAEMON=0 /etc/rc.config.d/slsd


ch_rc -a -p RUN_SAMBA=0 /etc/rc.config.d/samba
ch_rc -a -p RUN_CIFSCLIENT=0 \
  /etc/rc.config.d/cifsclient
ch_rc -a -p NFS_SERVER=0 \
  -p NFS_CLIENT=0 /etc/rc.config.d/nfsconf
ch_rc -a -p NS_FTRACK=0 /etc/rc.config.d/ns-ftrack
ch_rc -a -p APACHE_START=0 /etc/rc.config.d/apacheconf
mv -f /sbin/rc2.d/S400nfs.core \
  /sbin/rc2.d/.NOS400nfs.core
```

Discussion:

Setting these variables in the `/etc/rc.config.d` configuration files will effectively disable a wide variety of infrequently used subsystems. Variables are merely set (rather than renaming or removing startup scripts) so that the local administrator can easily "restore" any of these services if they discover a mission-critical need to have it. Additionally, HP-UX patches tend to supply fresh copies of the startup scripts, so they may get inadvertently re-enabled, whereas setting configuration variables usually survives patch installs. Finally, setting configuration variables is the method recommended and supported by HP. Note that not all of the configuration files listed above will exist on all systems (some are only valid for certain releases, others only exist if certain OEM vendor software is installed).

The rest of the actions in this section give the administrator the option of re-enabling certain services – in particular, the services that are disabled in the second block of the **Action** section above. Rather than disabling and then re-enabling these services, experienced administrators may wish to simply disable only those services that they know are unnecessary for their systems.

Bastille Notes:

Bastille only disables those services listed above that are enabled by default, so it is possible that a service that has been turned on manually will not be turned off when using Bastille.

3.8 Only enable Windows-compatibility server processes if absolutely necessary

OS Revisions:

This item only applies to HP-UX 11i servers.

Question:

Does this machine provide authentication, file sharing, or printer sharing services to systems running Microsoft Windows operating systems?

If the answer to this question is yes, then perform the actions below.

Action:

```
ch_rc -a -p RUN_SAMBA=1 /etc/rc.config.d/samba
```

Discussion:

HP-UX 11i now includes the popular Open Source Samba server for providing file and print services to Windows-based systems. This allows an HP-UX system to act as a file or print server on a Windows network, and even act as a Domain Controller (authentication server) to older Windows operating systems. However, if this functionality is not required by the site, this service should be disabled.

3.9 Only enable Windows-compatibility client processes if absolutely necessary

OS Revisions:

This item only applies to HP-UX 11i servers.

Question:

Is there a mission-critical reason why this system must access file systems from remote servers via SMB?

If the answer to this question is yes, then perform the actions below.

Action:

```
ch_rc -a -p RUN_CIFSCLIENT=1 /etc/rc.config.d/cifsclient
```

Discussion:

In addition to the Samba server, HP-UX 11i now includes the popular Open Source Samba client for receiving file and print services from Windows-based systems. However, if this functionality is not required by the site, this service should be disabled.

3.10 Only enable NFS server processes, if absolutely necessary

Question:

Is this machine an NFS file server?

If the answer to this question is yes, then perform the action below.

Action:

```
ch_rc -a -p NFS_SERVER=1 /etc/rc.config.d/nfsconf
```

Discussion:

NFS is frequently exploited to gain unauthorized access to files and systems. Clearly there is no need to run the NFS server-related daemons on hosts that are not NFS servers. If the system is an NFS server, the admin should take reasonable precautions when exporting file systems, including restricting NFS access to a specific range of local IP addresses and exporting file systems "read-only" and "`nosuid`" where appropriate. For more information consult the `exportfs`(1M) manual page. Much higher levels of security can be achieved by combining NFS with secure RPC or Kerberos, although there is significant administrative overhead involved in this transition.

Note that since this service uses ONC RPC mechanisms, it is important that the system's RPC portmapper (`rpcbind`) also be enabled when this service is turned on. For more information see Item 3.12 below.

Also note that some releases of Oracle software for HP-UX require NFS services in order to install properly. Therefore, the NFS server process may need to be started by hand on systems on which Oracle software is to be installed/updated. This can be accomplished by temporarily setting `NFS_SERVER=1`, `NUM_NFSD=1`, and `NUM_NFSIOD=1` in `/etc/rc.config.d/nfsconf` and then executing

```
   /sbin/init.d/nfs.core start
   /sbin/init.d/nfs.server start
```

NFS services can be turned back off by executing

```
   /sbin/init.d/nfs.core stop
   /sbin/init.d/nfs.server stop
```

and then resetting `NFS_SERVER=0`, `NUM_NFSD=0`, and `NUM_NFSIOD=0` in `/etc/rc.config.d/nfsconf`.

3.11 Only enable NFS client processes, if absolutely necessary

Question:

Is there a mission-critical reason why this system must access file systems from remote servers via NFS?

If the answer to this question is yes, then perform the action below.

Action:

```
ch_rc -a -p NFS_CLIENT=1 /etc/rc.config.d/nfsconf
```

Discussion:

Again, unless there is a significant need for this system to acquire data via NFS, administrators should disable NFS-related services. Note that other file transfer schemes (such as rdist via SSH) can often be more secure than NFS for certain applications, although again the use of secure RPC or Kerberos can significantly improve NFS security. Also note that if the machine will be an NFS client, then the rpcbind process must be running (see Item 3.12 below).

Note that since this service uses ONC RPC mechanisms, it is important that the system's RPC portmapper (`rpcbind`) also be enabled when this service is turned on. For more information see Item 3.12 below.

3.12 Only enable RPC-based services, if absolutely necessary

Question:

Are any of the following statements true?

- *This machine is an NFS client or server*
- *This machine is an NIS (YP) or NIS+ client or server*
- *This machine runs a GUI or GUI-based administration tool*
- *The machine runs a third-party software application which is dependent on RPC support (example: FlexLM License managers)*

If the answer to this question is yes, then perform the action below.

Action:

```
mv -f /sbin/rc2.d/.NOS400nfs.core \
  /sbin/rc2.d/400nfs.core
```

Discussion:

RPC-based services typically use very weak or non-existent authentication and yet may share very sensitive information. Unless one of the services listed above is required on this machine, it is best to disable RPC-based tools completely. If you are unsure whether or not a particular third-party application requires RPC services, consult with the application vendor. Note that disabling this service by renaming the startup file may not survive the install of RPC-related patches.

3.13 Only enable Web server suite, if absolutely necessary

Question:

Is there a mission-critical reason why this system must run a Web server?

If the answer to this question is yes, then perform the actions below.

Action:

```
ch_rc -a -p NS_FTRACK=1 /etc/rc.config.d/ns-ftrack
ch_rc -a -p APACHE_START=1 /etc/rc.config.d/apacheconf

ch_rc -a -p HPWS_APACHE32_START=1
/etc/rc.config.d/hpws_apache32conf

ch_rc -a -p HPWS_TOMCAT_START=1
/etc/rc.config.d/hpws_tomcatconf

ch_rc -a -p NS_FTRACK=1 /etc/rc.config.d/ns-ftrack

ch_rc -a -p HPWS_WEBMIN_START=1
/etc/rc.config.d/hpws_webminconf
```

Discussion:

Even if this machine is a Web server, the local site may choose not to use the Web server provided with HP-UX in favor of a locally developed and supported Web environment. If the machine is a Web server, the administrator is encouraged to search the Web for additional documentation on Web server security. A good starting point is http://httpd.apache.org/docs-2.0/misc/security_tips.html.

Note that this action only disables the default web server shipped with the system. Other webservers instances may still be running..

3.14 Only enable BIND DNS server, if absolutely necessary

Disabled by default in HP-UX 11i

Question:

Is there a mission-critical reason why this system must run a DNS server?

If the answer to this question is yes, then perform the actions below.

Action:

```
ch_rc -a -p NAMED=1 /etc/rc.config.d/namesvrs
```

Discussion:

The BIND DNS server, or `named`, maps IP addresses to hostnames across the Internet and supplies these services to other hosts on the local local network. Though it has been widely implemented, BIND has a long history of security flaws, especially in the BIND 8.x release tree generally shipped with HP-UX 11.x systems. Therefore, if you are going to run BIND, you should strongly consider moving to the BIND 9.x release-tree. HP has supported BIND 9 packages available from http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=BIND9.2. Or it is available directly from the Internet Software Consortium (the developers of BIND), whose website is at http://www.isc.org.

4 Kernel Tuning

4.1 Enable stack protection

Action *(HP-UX 11iv2 and later)*:

```
kctune -K executable_stack=0
```

Action *(older HP-UX 11i releases)*:

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

Action *(older HP-UX releases)*:

Strongly consider upgrading to HP-UX 11i.

Discussion:

Buffer overflow exploits have been the basis for many of the recent highly publicized compromises and defacements of large numbers of Internet connected systems. Many of the automated tools in use by system crackers exploit well-known buffer overflow problems in vendor-supplied and third-party software. Enabling stack protection prevents certain classes of buffer overflow attacks and is a significant security enhancement. Note that HP-UX 11i is much more capable in this and other security areas than older releases; therefore, administrators should strongly consider upgrading from older releases.

Note that this action requires a subsequent reboot to take effect in some versions of HP-UX.

4.2 Network parameter modifications

Action (for HP-UX 11.x systems):

```
cd /etc/rc.config.d
cat <<EOF > nddconf
# Increase size of half-open connection queue
TRANSPORT_NAME[0]=tcp
NDD_NAME[0]=tcp_syn_rcvd_max
NDD_VALUE[0]=4096
# Reduce timeouts on ARP cache
TRANSPORT_NAME[1]=arp
NDD_NAME[1]=arp_cleanup_interval
NDD_VALUE[1]=60000
# Drop source-routed packets
TRANSPORT_NAME[2]=ip
NDD_NAME[2]=ip_forward_src_routed
NDD_VALUE[2]=0
# Don't forward directed broadcasts
TRANSPORT_NAME[3]=ip
NDD_NAME[3]=ip_forward_directed_broadcasts
NDD_VALUE[3]=0
# Don't respond to unicast ICMP timestamp requests
TRANSPORT_NAME[4]=ip
NDD_NAME[4]=ip_respond_to_timestamp
NDD_VALUE[4]=0
# Don't respond to broadcast ICMP tstamp reqs
TRANSPORT_NAME[5]=ip
NDD_NAME[5]=ip_respond_to_timestamp_broadcast
NDD_VALUE[5]=0
# Don't respond to ICMP address mask requests
TRANSPORT_NAME[6]=ip
NDD_NAME[6]=ip_respond_to_address_mask_broadcast
NDD_VALUE[6]=0
# Don’t respond to broadcast echo requests
TRANSPORT_NAME[7]=ip
NDD_NAME[7]=ip_respond_to_echo_broadcast
NDD_VALUE[7]=0
EOF
chown root:sys nddconf
chmod go-w,ug-s nddconf
```

Action *(for older HP-UX releases)*:

Strongly consider upgrading to HP-UX 11i.

Discussion:

In HP-UX 11.x, we are modifying the configuration file that sets network parameters at boot time. This is not supported in HP-UX 10.20, and administrators should strongly consider upgrading to HP-UX 11i to take advantage of this and other security features.

Note that HP-UX 11.11 systems require patch PHNE_25644 for `ndd` to set `arp_cleanup_interval` from `/etc/rc.config.d/nddconf`, as required in the above **Action**.

Bastille Notes:

Bastille performs a similar action but does not support the particular changes in the above **Action**.

4.3 Use better TCP sequence numbers

OS Revisions:

This item applies to HP-UX 10.20 systems only. HP-UX 11.x releases use high quality TCP sequence numbers by default and require no action.

Action *(HP-UX 10.x only)*:

```
echo "/usr/contrib/bin/nettune -s tcp_random_seq 2" >> \
  /sbin/rc2.d/S339nettune
chown root:sys /sbin/rc2.d/S339nettune
chmod 555 /sbin/rc2.d/S339nettune
```

Discussion:

Setting this parameter causes the system to use a better randomization algorithm for generating initial TCP sequence numbers. This makes remote session hijacking attacks more difficult, as well as any other network-based attack that relies on predicting TCP sequence number information. Note that HP-UX 11i is much more capable in this and other security areas than older releases; therefore, administrators should strongly consider upgrading from older releases.

4.4 Additional network parameter modifications

Question:

Is this system going to be used as a firewall or gateway to pass network traffic between different networks?

If the answer to this question is yes, then ***do not*** perform the actions below.

Action (for HP-UX 11.x systems):

```
cat <<EOF >> /etc/rc.config.d/nddconf
# Don’t act as a router
TRANSPORT_NAME[8]=ip
NDD_NAME[8]=ip_forwarding
NDD_VALUE[8]=0
TRANSPORT_NAME[9]=ip
NDD_NAME[9]=ip_send_redirects
NDD_VALUE[9]=0
EOF
```

Action *(for older HP-UX releases)*:

```
cat << EOF > /sbin/rc2.d/S339nettune
#!/sbin/sh -
/usr/contrib/bin/nettune -s ip_forwarding 0
EOF
```

Discussion:

The actions above will result in a machine that cannot forward TCP/IP packets between multiple networks, even if the machine has multiple network adapters connected to multiple networks.

5 Logging

The items in this section cover enabling various different forms of system logging in order to keep track of activity on the system. Tools such as Swatch (http://www.oit.ucsb.edu/~eta/swatch), Logcheck (http://sourceforge.net/projects/sentrytools), and HP's IDS/9000 for HP-UX 11 (http://www.software.hp.com/ISS_products_list.html) can be used to automatically monitor logs for intrusion attempts and other suspicious system behavior. Note that Swatch and Logcheck are not officially supported by HP.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s).

Log centralization is typically done in HP-UX environments using the standard Unix Syslog capability, though HP also supports the more secure and robust Systlog-NG as part of the HP Distributed Systems Administration Utilities (DSAU), shipped with later updates of HP-UX 11i v2.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) experts recommend establishing some form of time synchronization among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. More information on NTP can be found at http://www.ntp.org.

5.1 *Enable system accounting*

Action:

```
cat <<END_SCRIPT >/sbin/init.d/newperf
#!/sbin/sh
PATH=/usr/sbin:/usr/bin:/sbin
case "$1" in
    'start_msg')
        echo "Starting System Accounting""
        ;;
    'start')
        /usr/bin/su sys -c \
          "/usr/lbin/sa/sadc /var/adm/sa/sa\`date +%d\`"
        ;;
    *)
```

```
        echo "usage: $0 {start|start_msg}"
        exit 1
        ;;
esac
exit 0
END_SCRIPT
chown root:sys /sbin/init.d/newperf
chmod 744 /sbin/init.d/newperf
rm -f /sbin/rc2.d/S21perf
ln -s /sbin/init.d/newperf /sbin/rc2.d/S21perf
mkdir –p /var/adm/sa
chown sys:sys /var/adm/sa
chmod 700 /var/adm/sa
/usr/bin/su sys -c crontab <<END_ENTRIES
0,20,40 * * * * /usr/lbin/sa/sa1
45 23 * * * /usr/lbin/sa/sa2 -s 0:00 -e 23:59 -i 1200 -A
END_ENTRIES
```

Discussion:

System accounting gathers baseline system data (CPU utilization, disk I/O, etc.) every 20 minutes and archives this data for one week (administrators may wish to archive the `/var/adm/sa` directory on a regular basis to preserve this data for longer periods). The data may be accessed with the `sar` command.

5.2 Enable kernel-level auditing

Question:

Is this system running in HP-UX Trusted Mode (see item 7.1), or does it have Standard-Mode security extensions enabled?

If yes, then perform the actions below.

Action (*HP-UX 10.20*):

Use SAM to turn on kernel level auditing (`Auditing And Security … Audited Events … Actions … Turn Auditing On`).

Action (*HP-UX 11.x*):

Use Bastille to turn on kernel level auditing

Discussion:

Kernel-level auditing provides information on commands and system calls that are executed on the local system. The audit trail may be reviewed with the `audisp` command.

Kernel-level auditing can consume large amounts of disk space and even cause a system performance impact, particularly on heavily used machines. Sites may wish to consider logging less information to help reduce the amount of disk space and other system resources consumed by the auditing process. See the `audevent`(1M) manual page for more information.

5.3 Enable logging from `inetd`

Action:

```
ch_rc -a -p INETD_ARGS=-l /etc/rc.config.d/netdaemons
```

Discussion:

If `inetd` is running, it is a good idea to make use of the "logging" (`-l`) feature of the HP-UX `inetd` that logs information about the source of any network connections seen by the daemon, allowing the administrator (or software) to scan the logs for unusual activity. This is especially powerful when combined with the access control capabilities accessible through `inetd`'s `/var/adm/inetd.sec` configuration file.

This information is logged via Syslog and by default HP-UX systems deposit this logging information in `var/adm/syslog/syslog.log` with other system log messages. Should the administrator wish to capture this information in a separate file, simply modify `/etc/syslog.conf` to log `daemon.notice` to some other log file destination.

IPFilter, which comes with HP-UX, can log inetd and other connections or attempted connections with its “ipmon” daemon as either a compliment or alternative to inetd logging.

5.4 Turn on additional logging for FTP daemon

Action *(HP-UX 11.x)*:

```
cd /etc
awk '/^ftpd/ && !/-L/ { $NF = $NF " -L" }
  /^ftpd/ && !/-l/ { $NF = $NF " -l" }
  { print }' inetd.conf > inetd.conf.tmp
cp inetd.conf.tmp inetd.conf
rm –f inetd.conf.tmp
```

Action *(HP-UX 10.x)*:

```
cd /etc
awk '/^ftpd/ && !/-l/ { $NF = $NF " -l" }
  { print }' inetd.conf > inetd.conf.tmp
```

```
cp inetd.conf.tmp inetd.conf
rm -f inetd.conf.tmp
```

Discussion:

If the FTP daemon is left on, it is recommended that the command logging (`-L`) and connection logging (`-l`) flags also be enabled to track FTP activity on the system, allowing the administrator (or software) to scan the logs for unusual activity. This is especially powerful when combined with the access control capabilities accessible through `inetd`'s `/var/adm/inetd.sec` configuration file.

Note that this setting has no effect if the FTP daemon remains de-activated from item 2.1.

Also note that enabling command logging on the FTP daemon (HP-UX 11.x only) can cause user passwords to appear in clear-text form in the system logs, if the user accidentally types their password at the username prompt.

Information about FTP sessions will be logged to Syslog and by default HP-UX systems deposit this logging information in `/var/adm/syslog/syslog.log` with other system log messages. Should the administrator wish to capture this information in a separate file, simply modify `/etc/syslog.conf` to log `daemon.notice` to some other log file destination.

5.5 Confirm permissions on system log files

Action:

```
awk < /etc/syslog.conf '
    $0 !~ /^#/ && $2 ~ "^/" {
        print $2
    }
' | sort -u | while read file
do  if [ -d "$file" -o -c "$file" -o \
         -b "$file" -o -p "$file" ]
    then    :
    elif [ ! -f "$file" ]
    then    mkdir -p "$(dirname "$file")"
            touch "$file"
            chmod 640 "$file"
    else    chmod o-w "$file"
    fi
done
hostname=`uname -n`
chmod o-w \
    /tmp/snmpd.log \
    /var/X11/Xserver/logs/X0.log \
    /var/X11/Xserver/logs/X1.log \
    /var/X11/Xserver/logs/X2.log \
    /var/adm/automount.log \
    /var/adm/snmpd.log \
    /var/opt/dce/svc/error.log \
    /var/opt/dce/svc/fatal.log \
    /var/opt/dce/svc/warning.log \
    /var/opt/dde/dde_error_log \
    /var/opt/hppak/hppak_error_log \
    /var/opt/ignite/logs/makrec.log1 \
    /var/opt/ignite/recovery/fstab \
    /var/opt/ignite/recovery/group.makrec \
    /var/opt/ignite/recovery/passwd.makrec \
    /var/opt/resmon/log \
    /var/opt/scr/log/scrlog.log \
    /var/opt/scr/log/scrlog.old \
    /var/sam/hpbottom.dion \
    /var/sam/hpbottom.iout \
    /var/sam/hpbottom.iout.old \
    "/var/sam/$hostname.dion" \
    "/var/sam/$hostname.iout" \
    "/var/sam/$hostname.iout.old" \
    /var/sam/lock \
    /var/sam/log/samlog \
    /var/sam/log/sam_tm_work \
    /var/adm/sw \
    /var/adm/sw/save \
    /var/adm/sw/patch
```

Discussion:

It is critical to protect system log files from being modified by unauthorized individuals. Also, certain logs contain sensitive data that should only be available to the system administrator.

The first half of the **Action** above ensures that files created by the HP-UX `syslog` system are so protected by reading `/etc/syslog.conf` to determine what files `syslog` will log to, making sure those files exist, and making sure they have proper permissions. The second half (starting with "`hostname=`") applies to other system log files. The files referenced above are known to be created as world-writable under some circumstances in HP-UX.

6 File/Directory Permissions/Access

6.1 Set Sticky Bit on World Writable Directories

Action:

Administrators who wish to obtain a list of world writable directories that do not have the sticky bit set may execute the following commands

```
find / \( -fstype nfs -o -fstype cifs -o \

-fstype cachefs \) -prune -o -type d -a \( -perm -0002 \

-a ! -perm -1000 \) -print
```

Notes:

When the so-called "sticky bit" is set on a directory, then only the owner of a file may remove that file from the directory (as opposed to the usual behavior where anybody with write access to that directory may remove the file). Setting the sticky bit prevents users from overwriting each other's files, whether accidentally or maliciously, and is generally appropriate for most world-writable directories. However, consult appropriate vendor documentation before blindly applying the sticky bit to any world writable directories found in order to avoid breaking any application dependencies on a given directory.

6.2 Find world-writable files and unauthorized SUID/SGID executables

Action:

The automated testing tool supplied with this benchmark will flag unexpected world-writable files and SUID/SGID files on the system.

Administrators who wish to obtain a list of the world-writable files currently on the system may run the following command, delivered with the benchmark. Note that this script uses the Installed-Product Database, which is not protected against a malicious root user. Any operating system that has been compromised can be manipulated to mask changes from the local user.:

```
checkperms
```

Discussion:

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity. Generally removing write access for the "other" category (`chmod o-w` <*filename*>) is advisable, but always consult relevant vendor documentation in order to avoid breaking any application dependencies on a given file.

6.3 Find "unowned" files and directories

Action:

The automated testing tool supplied with this benchmark will flag files and directories where the user or group owner of the file is not listed in the system password or group databases such as `/etc/passwd` and `/etc/group`.

Administrators who wish to locate these files on their may run the following command:

```
find / \( -nouser -o -nogroup \) -print
```

Discussion:

Sometimes when administrators delete users from the system they neglect to remove all files owned by those users from the system. A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended. It is a good idea to locate files that are owned by users or groups not listed in the system configuration files, and make sure to reset the ownership of these files to some active user on the system as appropriate.

6.4 Ensure patch backup directories are not accessible

Action:

```
chmod go-rwx /var/adm/sw/save
```

Discussion:

HP-UX systems save backup copies of system files into `/var/adm/sw/save` when patches are installed. It is important that these old versions of the system files not be accessible as they may have been replaced due to security bugs.

7 System Access, Authentication, and Authorization

7.1 Enable Password Hiding

Question:

Does this system run applications that read the encrypted password entries in /etc/passwd directly?

If the answer to this question is yes, then ***do not*** perform the actions below.

Action:

Use Bastille to convert to Shadowed Mode or Trusted Mode as appropriate, by selecting the "password hiding" option in Bastille, or via SAM/SMH.

Discussion:

Without hidden passwords, an intruder could use any user's account to obtain hashed passwords and use `crack` or similar utilities to find easily guessed passwords. Password aging (covered in item 8.3) ensures that users change their passwords on a regular basis and helps stop the use of stolen passwords.

Note that Trusted-Mode conversion on HP-UX 11iv1requires the HP-UX Shadow Password package available from http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=ShadowPassword.

7.2 Create `/etc[/ftpd]/ftpusers`

Action:

```
if [[ "$(uname -r)" = B.10* ]]; then
   ftpusers=/etc/ftpusers
else
   ftpusers=/etc/ftpd/ftpusers
fi
for name in root daemon bin sys adm lp \
   uucp nuucp nobody hpdb useradm
do
   echo $name
done >> $ftpusers
sort –u $ftpusers > $ftpusers.tmp
cp $ftpusers.tmp $ftpusers
rm –f $ftpusers.tmp
chown bin:bin $ftpusers
chmod 600 $ftpusers
```

Discussion:

`ftpusers` contains a list of users who *are not* allowed to access the system via FTP. Generally, only normal users should ever access the system via FTP—there should be no reason for "system" type accounts to be transferring information via this mechanism. Certainly, the `root` account should *never* be allowed to transfer files directly via FTP.

Also note that more fine-grained FTP access controls can be placed in `/etc/ftpd/ftpaccess` under HP-UX 11.x.

7.3 *Prevent Syslog from accepting messages from the network*

OS Revisions:

This item only applies to HP-UX 11i servers.

Question:

Is this machine a log server, or does it need to receive Syslog messages via the network from other systems?

If the answer to this question is yes, then ***do not*** perform the actions below.

Action *(HP-UX 11.x)*:

```
SYSLOGD_OPTS="`sh -c '. /etc/rc.config.d/syslogd ;
  echo "$SYSLOGD_OPTS"'`"
if [[ "$SYSLOGD_OPTS" = *-N* ]]; then
  ch_rc -a -p SYSLOGD_OPTS="-N $SYSLOGD_OPTS" \
    /etc/rc.config.d/syslogd
fi
```

Action *(older HP-UX releases)*:

Strongly consider upgrading to HP-UX 11i.

Discussion:

By default the system logging daemon, `syslogd`, listens for log messages from other systems on network port 514/udp. Unfortunately, the protocol used to transfer these messages does not include any form of authentication, so a malicious outsider could simply barrage the local system's Syslog port with spurious traffic—either as a denial-of-service attack on the system, or to fill up the local system's logging file systems so that subsequent attacks will not be logged.

Note that it is considered good practice to setup one or more machines as central “log servers” to aggregate log traffic from all machines at a site. However, unless a system is set up to be one of these “log server” systems, it should not be listening on 514/udp for incoming log messages.

7.4 *Disable XDMCP port*

Action:

```
if [ ! -f /etc/dt/config/Xconfig ]; then
    mkdir -p /etc/dt/config
    cp -p /usr/dt/config/Xconfig /etc/dt/config
fi
cd /etc/dt/config
awk '/Dtlogin.requestPort:/ \
    { print "Dtlogin.requestPort: 0"; next }
    { print }' Xconfig > Xconfig.new
cp Xconfig.new Xconfig
rm -f Xconfig.new
```

Discussion:

The standard GUI login provided on most Unix systems can act as a remote login server to other devices (including X terminals and other workstations). Access control is handled via the `Xaccess` file—by default under HP-UX, this file allows any system on the network to get a remote login screen from the local system. We can override this behavior in the `/etc/dt/config/Xaccess` file.

7.5 Set default locking screensaver timeout

Action:

```
for file in /usr/dt/config/*/sys.resources; do
 dir="$(dirname "$file" | sed 's|^/usr/|/etc/|')"
 mkdir -p "$dir"
 echo 'dtsession*saverTimeout: 10' >>"$dir/sys.resources"
 echo 'dtsession*lockTimeout: 10' >>"$dir/sys.resources"
done
```

Discussion:

The default timeout is between 10 and 30 minutes of keyboard/mouse inactivity before a password-protected screen saver is invoked by the CDE session manager depending on the OS release and the locale. The above **Action** uniformly reduces this default timeout value to 10 minutes, though this setting can still be overridden by individual users in their own environment.

7.6 Configure `inetd` security

Action:

```
netblocks='<system-or-network> <system-or-network> ...'
awk  < /etc/inetd.conf '
  /^[    ]*(#|$)/ { next }
  /^     / { next }
  /^rpc[  ]/ { services[$9]=1; next }
  { services[$1]=1; next }
  END {
    for(service in services) {
      print service " allow '"$netblocks"'"
      print service " deny"
    }
  }
  '>> /var/adm/inetd.sec
```

Where where each *<system-or-network>* represents one discrete system or network block in use by your organization that requires access to this system. For example, you might use '`192.168.1.* 10.3.8.* myserver.mycompany.com`'. See the `inetd.sec`(4) manual page for details.

Discussion:

The HP-UX `inetd` security mechanism (`inetd.sec`) allows the administrator to control who has access to various network services based on the IP address or system name of the remote end of the connection.

Note: This is unnecessary if adequate IP-range limitations are created in IPFilter, if inetd is disabled, or if all the services in inetd.conf are disabled

Also note that the above actions will only provide filtering on services spawned by inetd. To protect other system services, or to limit what outbound network connections that the system can make, consider implementing IPFilter as described in SN.9.

7.7 Restrict `at/cron` to authorized users

Action:

```
cd /var/adm/cron
rm -f cron.deny at.deny
echo root >cron.allow
echo root >at.allow
chown root:sys cron.allow at.allow
chmod 400 cron.allow at.allow
```

Discussion:

The `cron.allow` and `at.allow` files are a list of users who are allowed to run the `crontab` and `at` commands to submit jobs to be run at scheduled intervals. On many systems, only the system administrator needs the ability to schedule jobs.

Note that even though a given user is not listed in `cron.allow`, `cron` jobs can still be run as that user. `cron.allow` only controls administrative access to the `crontab` command for scheduling and modifying `cron` jobs.

7.8 Restrict crontab file permissions

Action:

```
cd /var/spool/cron/crontabs
```

```
chown root:sys *
chmod 400 *
```

Discussion:

The system crontab files are accessed only by the cron daemon (which runs with superuser privileges) and the crontab command (which is set-UID to root). Allowing unprivileged users to read or (even worse) modify system crontab files can create the potential for a local user on the system to gain elevated privileges.

7.9 Restrict root logins to system console

Action:

```
echo console > /etc/securetty
chown root:sys /etc/securetty
chmod 600 /etc/securetty
```

Discussion:

Anonymous root logins should never be allowed, except on the system console in emergency situations. At all other times, the administrator should access the system via an unprivileged account and use some authorized mechanism to gain additional privilege , such as the su command, the freely-available sudo package discussed in item SN.6, or the HP Role Based Authorization system also discussed in item SN.6. These mechanisms provide at least some limited audit trail in event of problems

7.10 Set retry limit for account lockout

Action:

```
logins -ox \
| awk -F: '($8 != "LK" && $1 != "root") { print $1 }' \
| while read logname; do
  /usr/lbin/modprpw -m umaxlntr=10 "$logname"
done
modprdef -m umaxlntr=10
echo AUTH_MAXTRIES=10 >> /etc/default/security
```

Discussion:

The commands above set the number of failed login attempts a user is allowed before their account is disabled. Setting this number to a reasonably low value helps discourage brute force password guessing attacks. Note that use of this setting may lead to a “Denial of Service” situation in the event of a widespread password guessing attack, possibly caused by a network security audit. However, choosing not to implement this setting raises the risk of such an attack being successful unless passwords are made harder to guess such as by increasing the minimum password length or diversity requirements on the system as indicated in item 8.4. Note that some other standards suggest fewer retries, in the range from three to five. You may choose to weigh the helpdesk load versus brute-force-attack defense in your own environment, favoring smaller values when password complexity requirements are not implemented, and there are a large number of user accounts on the server, in an LDAP/NIS-enabled environment, for example. In all cases, CIS recommends no greater than 10 attempts for the Level 1 benchmark.

Note that the above /etc/default/security setting is only valid for certain patch-levels. Also, use of modprpw assumes the use of "trusted mode." If trusted mode is not used, use of userdbset is recommended… see userdbset man page for more detail.

Bastille Notes:

Bastille sets the retry limit to ten (10) only when converting a system to trusted mode.

7.11 Disable "nobody" access for secure RPC

Action:

```
KEYSERV_OPTIONS="`sh -c '. /etc/rc.config.d/namesvrs ;
  echo "$KEYSERV_OPTIONS"'`"
ch_rc -a -p KEYSERV_OPTIONS="-d $KEYSERV_OPTIONS " \
  /etc/rc.config.d/namesvrs
```

Discussion:

The `keyserv` process stores user keys that are utilized with the ONC secure RPC mechanism. The above action prevents `keyserv` from using default keys for the "nobody" user, effectively stopping this user from accessing information via secure RPC.

8 User Accounts and Environment

Note that the items in this section are tasks that the local administrator should undertake on a regular, ongoing basis. The administrator can automate the auditing these items by running the host-based scanning tools provided from the Center for Internet Security on a regular basis—perhaps in an automated fashion via `cron`. These scanning tools are available for free download from http://www.CISecurity.org/.

Also, note that the use of modprpw below is only for use with trusted system mode, userdbset and the equivalent parameters should be used on systems where trusted mode is not used. This command is only available if Standard Mode Security Extensions are installed or the HP-UX version is 11iv3 or greater.

8.1 Block system accounts

Action:

```
for user in www sys smbnull iwww owww sshd \
hpsmh named uucp nuucp adm daemon bin lp \
nobody noaccess hpdb useradm; do
    passwd -l "$user"
    /usr/sbin/usermod -s /bin/false "$user"
    if [[ "$(uname -r)" = B.10* ]]; then
        /usr/lbin/modprpw -w "*" "$user"
    else
        /usr/lbin/modprpw -w "$user"
    fi
done
```

Discussion:

Accounts that are not being used by regular users should be locked. Not only should the password field for the account be set to an invalid string, but the shell field in the password file should contain an invalid shell.

Access to the `uucp` and `nuucp` accounts is only needed when the deprecated Unix to Unix Copy (UUCP) service is in use. The other listed accounts should never require direct access. The above Action locks the passwords to these accounts (on systems converted to Trusted Mode only) and sets the login shell to `/bin/false`.

Note that the above is not an exhaustive list of possible system/application accounts that could be installed on the system. An audit of all users on the system is the only way to be sure that only authorized accounts are in place.

8.2 Verify that there are no accounts with empty password fields

Action:

The command

```
logins -p
```

should return no lines of output.

Discussion:

An account with an empty password field means that anybody may log in as that user without providing a password at all. All accounts should have strong passwords or should be locked by using a password string like "`*`", "`NP`", or "`*LOCKED*`", such as supplied by the following for HP-UX 10.x:

passwd –l *<logname>*
`/usr/lbin/modprpw -w "*"` *<logname>*

Or the following for HP-UX 11.x:

passwd –l *<logname>*
`/usr/lbin/modprpw -w` *<logname>*

8.3 Set account expiration parameters on active accounts

Action:

```
logins -ox \
| awk -F: '($8 != "LK" && $1 != "root") { print $1 }' \
| while read logname; do
  passwd -x 91 -n 7 -w 28 "$logname"
  /usr/lbin/modprpw -m exptm=90,mintm=7,expwarn=30 \
   "$logname"
done
echo PASSWORD_MAXDAYS=91 >> /etc/default/security
echo PASSWORD_MINDAYS=7 >> /etc/default/security
echo PASSWORD_WARNDAYS=28 >> /etc/default/security
/usr/lbin/modprdef -m exptm=90,mintm=7,expwarn=30
```

Discussion:

It is a good idea to force users to change passwords on a regular basis. The commands above will set all active accounts (except the `root` account) to force password changes every 90 days (91 days when not running in HP-UX Trusted Mode) and then prevent password changes for seven days (one week) thereafter. Users will begin receiving warnings 30 days (28 days when not running in HP-UX Trusted Mode) before their password expires. Sites also have the option of expiring idle accounts after a certain number of days (see the on-line manual page for the `usermod` command, particularly the `-f` option).

These are recommended starting values, but sites may choose to make them more restrictive depending on local policies.

8.4 Set strong password enforcement policies

Action:

```
ch_rc -a -p MIN_PASSWORD_LENGTH=7 /etc/default/security
ch_rc -a -p PASSWORD_HISTORY_DEPTH=10 \
  /etc/default/security

ch_rc -a -p PASSWORD_MIN_UPPER_CASE_CHARS=1 \

  /etc/default/security

ch_rc -a -p PASSWORD_MIN_DIGIT_CHARS=1 \

  /etc/default/security

ch_rc -a -p PASSWORD_MIN_SPECIAL_CHARS=1 \

  /etc/default/security

ch_rc -a -p PASSWORD_MIN_LOWER_CASE_CHARS=1 \

  /etc/default/security


modprdef -m nullpw=NO
modprdef -m rstrpw=YES
```

Discussion:

The policies set here are designed to force users to make better password choices when changing their passwords.

Sites often have differing opinions on the optimal value of the MIN_PASSWORD_LENGTH and PASSWORD_HISTORY_DEPTH parameters. A minimum password length of seven is in line with industry standards, especially the Payment Card Industry (PCI) Security Standard; however, a longer value may be warranted if account locks are not enabled (item 7.10). A password history depth of ten combined with passwords that expire four times per year (item 8.3) means users will typically not re-use the same password in any given year.

Requiring an upper/lowercase and special character password will dramatically increase the password search space and lower the chances for brute-force attack significantly. These settings are known to exist for HP-UX 11iv2, 0512 and later. The man page for security(5) will indicate if these exist on your particular system.

Be sure to consult your local security standards before adopting the values given above.

8.5 Verify no legacy '+' entries exist in `passwd` and `group` files

Action:

The command

```
   grep '^+:' /etc/passwd /etc/group
```

should return no lines of output.

Discussion:

'+' entries in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on HP-UX systems, but may exist in files that have been imported from other platforms. These entries may provide an avenue for attackers to gain privileged access on the system. They should be deleted if they exist.

8.6 No '`.`' or group/world-writable directory in `root` `$PATH`

Action:

The automated testing tool supplied with this benchmark will alert the administrator if action is required.

Discussion:

Including the current working directory ('`.`') or other writable directory in `root`'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program. To execute a file in the current directory when '`.`' is not in the `$PATH`, use the format "`./filename`".

8.7 User home directories should be mode 750 or more restrictive

Action:

```
logins -ox \
| awk -F: '($8 == "PS" && $1 != "root") { print $6 }' \
| grep /home/ \
| while read dir
do  chmod g-w,o-rwx "$dir"
done
```

Discussion:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges. While the above modifications are relatively benign, making global modifications to user home directories without alerting your user community can result in unexpected outages and unhappy users.

8.8 No user dot-files should be group/world writable

Action:

```
logins -ox \
| awk -F: '($8 == "PS") { print $6 }' \
| while read dir
do  ls -d "$dir/".[!.]* |
    while read file
    do  if [ ! -h "$file" -a -f "$file" ]
        then    chmod go-w "$file"
        fi
    done
done
```

Discussion:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges. While the above modifications are relatively benign, making global modifications to user home directories without alerting your user community can result in unexpected outages and unhappy users.

8.9 Remove user `.netrc`, `.rhosts` and `.shosts` files

Action:

```
logins -ox | cut -f6 -d: | while read h
do for file in "$h/.netrc" "$h/.rhosts" "$h/.shosts"
   do  if [ -f "$file" ]
       then  echo "removing $file"
             rm -f "$file"
       fi
   done
done
```

Discussion:

`.netrc` files may contain unencrypted passwords that may be used to attack other systems, while `.rhosts` files used in conjunction with the BSD-style "r-commands" (`rlogin`, `remsh`, `rcp`) implement a weak form of authentication based on the network address or host name of the remote computer (which can be spoofed by a potential attacker to exploit the local system). While the above modifications are relatively benign, making global modifications to user home directories without alerting your user community can result in unexpected outages and unhappy users.

8.10 Set default `umask` for users

Action:

```
cd /etc
for file in profile csh.login d.profile d.login
do  echo umask 077 >> "$file"
done
ch_rc –a -p UMASK=077 /etc/default/security
```

Discussion:

With a default `umask` setting of `077`, files and directories created by users will not be readable by any other user on the system. The user creating the file has the discretion of making their files and directories readable by others via the `chmod` command. Users who wish to allow their files and directories to be readable by others by default may choose a different default `umask` by inserting the `umask` command into the standard shell configuration files (`.profile`, `.cshrc`, etc.) in their home directories. A `umask` of `027` would make files and directories readable by users in the same Unix group, while a `umask` of `022` would make files readable by every user on the system.

Bastille Notes:

Bastille also sets the default `umask`, but uses a `umask` of 027 rather than the 077 in the **Action** above.

8.11 Set "`mesg n`" as default for all users

Action:

```
cd /etc
for file in profile csh.login d.profile d.login
do  echo mesg n >> "$file"
done
```

Discussion:

"`mesg n`" blocks attempts to use the `write` or `talk` commands to contact the user at their terminal, but has the side effect of slightly strengthening permissions on the user's `tty` device. Since `write` and `talk` are no longer widely used at most sites, the incremental security increase is worth the loss of functionality. Note that this setting is the default on HP-UX 11i.

9 Warning Banners

Presenting some sort of statutory warning message prior to the normal user logon may assist the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific attacks at a system. Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. Clearly, the organization's local legal counsel and/or site security administrator should review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. A more complete discussion of the topic can be found at http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm.

Note that if TCP Wrappers are being used to display warning banners for various `inetd`-based services, it is important that the banner messages be formatted properly so as not to interfere with the application protocol. The `Banners.Makefile` file provided with the TCP Wrappers source distribution (available from `ftp.porcupine.org`) contains shell commands to help produce properly formatted banner messages.

9.1 Create warning banners for terminal-session logins

Action:

```
banner="Authorized users only. All activity may \
be monitored and reported."
echo "$banner" >> /etc/motd
echo "$banner" > /etc/issue
chown root:sys /etc/motd
chown root:root /etc/issue
chmod 644 /etc/motd /etc/issue
```

Discussion:

The contents of the `/etc/issue` file are displayed prior to the login prompt on the system's console and serial devices, as well as for remote terminal-session logins such as through SSH or Telnet.

`/etc/motd` is generally displayed after all successful logins, no matter where the user is logging in from, but is thought to be less useful because it only provides notification to the user after the machine has been accessed.

9.2 Create warning banners for GUI logins

Action:

```
banner="Authorized users only. All activity may \
be monitored and reported."
for file in /usr/dt/config/*/Xresources; do
  dir="$(dirname "$file" | sed 's|^/usr/|/etc/|')"
  mkdir -p "$dir"
  if [ ! -f "$dir/Xresources" ]; then
       cp –p "$file" "$dir/Xresources"
  fi
  echo "Dtlogin*greeting.labelString: $banner" \
   >> "$dir/Xresources"
  echo "Dtlogin*greeting.persLabelString: $banner" \
   >> "$dir/Xresources"
done
chown root:sys /etc/dt/config/*/Xresources
chmod 644 /etc/dt/config/*/Xresources
```

Discussion:

The standard graphical login program for HP-UX requires the user to enter their username in one dialog box and their password in a second separate dialog. The commands above set the warning message on both to be the same message, but the site has the option of using different messages on each screen. The `Dtlogin*greeting.labelString` is the message for the first dialog where the user is prompted for their username, and `.perslabelString` is the message on the second dialog box. Note that system administrators may wish to consult with their site's legal counsel about the specifics of any warning banners.

9.3 Create warning banners for FTP daemon

Action:

```
banner="Authorized users only. All activity may \
be monitored and reported."
if [ -d /etc/ftpd ]; then
  echo "banner /etc/issue" >>/etc/ftpd/ftpaccess
  chmod 600 /etc/ftpd/ftpaccess
  chown root:sys /etc/ftpd /etc/ftpd/ftpaccess
fi
```

Discussion:

The FTP daemon in HP-UX 11 is based on the popular Washington University FTP daemon (WU-FTPD), which is an Open Source program widely distributed on the

Internet. Note that this setting has no effect if the FTP daemon remains de-activated from item 2.1.

Appendix A: File Backup Script

```
#!/bin/sh

# Provided for reference as a starting place for your own
script.

ext=`date '+%Y%m%d-%H:%M:%S'`

cp -rp /etc/rc.config.d /etc/rc.config.d-preCIS.$ext
cp –rp /var/spool/cron/crontabs /var/spool/cron/crontabs-preCIS.$ext

for file in     /.rhosts                /.shosts                \
                /etc/fstab              /etc/ftpd/ftpusers      \
                /etc/ftpusers           /etc/ftpd/ftpaccess     \
                /etc/hosts.equiv        /etc/inet/ntp.conf      \
                /etc/inetd.conf         /etc/inittab            \
                /etc/issue              /etc/motd               \
                /etc/securetty          /etc/ssh/ssh_config     \
                /etc/ssh/sshd_config                            \
                /opt/ssh/etc/ssh_config                         \
                /opt/ssh/etc/sshd_config                        \
                /var/adm/cron/at.allow                          \
                /var/adm/cron/cron.allow                        \
                /etc/dt/config/*/Xresources
do  [ -f $file ] && cp –p $file $file-preCIS.$ext
done
```

Appendix B: Log Rotation Script

```
#!/bin/ksh
# Provided for reference as a starting place for your own
script.



# rotate -- A script to roll over log files
# Usage: rotate /path/to/log/file [mode [#revs] ]

FILE="$1"
MODE="${2:-644}"
typeset –i DEPTH="${3:-4}"

DIR="$(dirname "$FILE")"
LOG="$(basename "$FILE")"
DEPTH=$(($DEPTH - 1))

if [ ! -d "$DIR" ]; then
        echo "$DIR: Path does not exist"
        exit 255
fi
cd "$DIR"

while [ $DEPTH -gt 0 ]
do
        OLD=$(($DEPTH - 1))
        if [ -f "$LOG.$OLD" ]; then
                mv "$LOG.$OLD" "$LOG.$DEPTH"
        fi
        DEPTH=$OLD
done

if [ $DEPTH -eq 0 -a -f "$LOG" ]; then
        mv "$LOG" $LOG.0
fi

cp /dev/null "$LOG"
chmod "$MODE" "$LOG"

/sbin/init.d/syslog stop
/sbin/init.d/syslog start
```

Appendix C: Additional Security Notes

The items in this section are security configuration settings that have been suggested by several other resources and system hardening tools. However, given the other settings in the benchmark document, the settings presented here provide relatively little incremental security benefit. Nevertheless, none of these settings should have a significant impact on the functionality of the system, and some sites may feel that the slight security enhancement of these settings outweighs the (sometimes minimal) administrative cost of performing them.

None of these settings will be checked by the automated scoring tool provided with the benchmark document. They are purely optional and may be applied or not at the discretion of local site administrators.

SN.1 Enable process accounting on bootup

Action:

```
ch_rc -a -p START_ACCT=1 /etc/rc.config.d/acct
```

Discussion:

Process accounting logs information about every process that runs to completion on the system, including the amount of CPU time, memory, etc. consumed by each process.

While this would seem like useful information in the wake of a potential security incident on the system, kernel-level auditing (as enabled in Item 7.2) provides more information about each process execution in general (although kernel-level auditing does not capture system resource usage information).

Both process accounting and kernel-level auditing can be a significant performance drain on the system, so enabling both seems excessive given the large amount of overlap in the information each provides.

SN.2 Create symlinks for dangerous files

Action:

```
for file in /.rhosts /.shosts /etc/hosts.equiv /.netrc
do
    rm -f $file
    ln -s /dev/null $file
done
```

Discussion:

The `/.rhosts`, `/.shosts`, and `/etc/hosts.equiv` files enable a weak form of access control (see the discussion of `.rhosts` files in item 8.9). Similarly

/.netrc files may contain the root password to other systems. Attackers will often target these files as part of their exploit scripts. By linking these files to /dev/null, any data that an attacker writes to these files is simply discarded (though an astute attacker can still remove the link prior to writing their malicious data).

SN.3 File systems are mounted either 'ro' or 'nosuid'

Action:

```
cp -p /etc/fstab /etc/fstab.tmp
awk '
$0 ~ /^[\t ]*#/ \
|| $3 ~ /^(swap|ignore)$/ \
|| $2 ~ "^(swap$|/$|/usr($|/))" { print; next }
{
    if($2 ~ "^/opt($|/)") {
        if($4 !~ /(^|,)ro($|,)/) {
            $4 = $4 ",ro"
        }
        sub(/(^|,)(rw|delaylog),/, ",", $4)
    } else if ($4 !~ /(^|,)nosuid($|,)/) {
        $4 = $4 ",nosuid"
        sub(/(^|,)suid,/, ",", $4)
    }
    sub(/^(defaults,|,)/, "", $4)
    print
}
' /etc/fstab.tmp >/etc/fstab
rm -f /etc/fstab.tmp
chmod a-wx,ug-s /etc/fstab
```

Discussion:

It is important to protect the system from the introduction of unauthorized software, particularly set-UID programs. Since most of the standard set-UID utilities are provided under the /usr and /opt file systems, we mount /opt read-only to help prevent tampering (HP-UX systems cannot start if /usr is mounted read-only on boot-up). Note that administrators may make /opt read-write with the mount -o remount,rw /opt command, but must reboot the system to return the file system to read-only mode.

Other file systems should be mounted "nosuid" where possible in order to prevent the introduction of rogue set-UID programs. If a file system is mounted "nosuid" then the set-UID bit on executables in that file system is ignored—these programs will execute with the privileges of the user running the program, rather than the privileges of the owner of the binary.

The action above operates by first making a backup copy of the /etc/fstab file and then walks through the file line by line applying the following logic:

1. If the entry refers to a non-filesystem partition (i.e., swap or ignore), to the '/' filesystem, or to the /usr filesystem (or any filesystem mounted below /usr), then leave this entry alone.
2. Otherwise if the entry refers to the /opt filesystem, or any filesystem mounted below /opt, then modify the entry to mount the filesystem read-only (ro).
3. Otherwise modify the entry to mount the filesystem nosuid.

Beyond simple file system level protections, experts recommend using a file system integrity checking tool such as Tripwire™, which is available in both free and commercial versions (see http://www.tripwire.com/products/tripwire_asr/ and http://www.tripwire.org/ for information on obtaining free versions of this software).

SN.4 Disable inetd, if possible

Action:

```
if grep -Evq '^[  ]*(#|$)' /etc/inetd.conf
then    :
else    mv -f /sbin/rc2.d/S500inetd \
         /sbin/rc2.d/.NOS500inetd
fi
```

Discussion:

If the actions in Section 2 of this benchmark resulted in no services being enabled in /etc/inetd.conf, then the revised boot script created here will prevent the inetd daemon from even being started. For further information on logging inetd connections if inetd is running, see Item 7.3 below.

SN.5 Change default greeting string for Sendmail

Action:

```
cd /etc/mail
awk '/O SmtpGreetingMessage=/ \
  { print "O SmtpGreetingMessage=mailer ready"; next}
  { print }' sendmail.cf >sendmail.cf.new
mv sendmail.cf.new sendmail.cf
```

Discussion:

The default SMTP greeting string displays the version of the Sendmail software running on the remote system. Hiding this information is generally considered to be good practice, since it can help attackers target attacks at machines running a vulnerable version of Sendmail. However, the actions in the benchmark document prevent Sendmail from responding on port 25/tcp in most cases, so changing this default greeting string is something of a moot point unless the machine happens to be an email server.

SN.6 Install and configure `sudo`

Action:

Download and install `sudo` as part of the HP-UX Internet Express package at:

- (11.23) `http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXIEXP1123`, or
- `(11.11)http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXIEXP1111`
- Older systems can obtain a HP-UX-packaged depot from the HP-UX porting and archive center at `http://hpux.cs.utah.edu/`.

Discussion:

`sudo` is a package that allows the System Administrator to delegate activities to groups of users. These activities may be beyond the administrative capability of that user – restarting the web server, for example. If frequent web server configuration changes are taking place (or you have a bug and the web server keeps crashing), it becomes very cumbersome to continually engage the system administrator just to restart the web server. `sudo` allows the administrator to delegate just that one task using `root` authority without allowing that group of users any other `root` capability.

Once `sudo` is installed, configure it using `visudo` – do not `vi` the config file. `visudo` has error checking built in. Experience has shown that if `/etc/sudoers` gets botched (from using `vi` without `visudo`'s error checking feature), recovery may become very difficult.

System administators may also wish to explore the HP-UX Role Based Authorization system and the "*privrun*" command that is part of it.

SN.7 Remove Compilers

Question:

Is there a mission-critical reason to have a compiler or assembler on this machine?

If the answer is no, perform the action below.

Action:

```
swremove aCC gcc
```

Discussion:

Compilers pose a potential threat to production systems and should not be installed. Compilers should be installed on select development systems – those systems that have a Business need for a compiler – and the resulting output binaries deployed onto other development and production systems using the existing Enterprise change processes.

SN.8 Verify that no UID 0 accounts exist other than `root`

Action:

The command

```
   logins -d | grep ' 0 '
```

should return no output.

Discussion:

Any account with UID 0 has superuser privileges on the system. The only superuser account on the machine should be the `root` account, and it should normally be accessed by logging in as an unprivileged user and using the `su` command to gain additional privilege. In fact, UID's should not be shared in general. This assertion can be tested with:

```
   logins -d
```

There is the recognized occasional need for direct administrative console access. For these situations, having multiple uid 0 accounts may be used by experienced administrators to provide individually assigned superuser passwords to eliminate or reduce usage of a shared root password, and to increase accountability. However some tools and situations do not always handle multiple uid 0 accounts as expected or desired, therefore testing is required. Specifically most of the GUI X-windows administration tools, if run by a non-privileged user, will prompt for the "`root`" password. There may be other applications or tools that behave unexpectedly, so testing is required.

Finer granularity access control for administrative access can also be obtained by using the freely-available `sudo` program as described in SN.6 or the HP Role Based Authorization system also described in SN.6.

SN.9 Install and configure IPFilter

Action (HP-UX 11i)

1. Download and install IPFilter from `http://hp.com/go/ipfilter`. Installation instructions are available from that site as well.

2. Edit the Bastille configuration files to allow the desired traffic.

   - If more inbound protocols are needed than SSH, edit the IPFilter questions in the `CIS.config` file that CIS bundles with this Benchmark to change the appropriate answers from "*yes*" to "*no*."
   - You may also need to edit `/etc/opt/sec_mgmt/bastille/ipf.customrules` to include other custom rules for your environment.

3. Run Bastille as indicated in item 1.4

Discussion

HP-UX IPFilter (B9901AA) is a stateful system firewall that controls IP packet flow in or out of a machine.

Appendix D: References

The Center for Internet Security

Free benchmark documents and security tools for various OS platforms and applications:
http://www.cisecurity.org/

Pre-compiled software packages for various OS platforms:
ftp://ftp.cisecurity.org/

Hewlett-Packard

IT Resource Center:
http://www.itrc.hp.com

HP-UX Software Assistant:
http://www.hp.com:/go/swa

HP-UX Bastille:
http://www.hp.com/go/bastille

Other HP-UX Security Software (HP-UX Secure Shell, IDS/9000, HP-UX IPFilter, etc.):
http://h20293.www2.hp.com/portal/swdepot/displayProductsList.do?category=ISS

Other Misc. Documentation

Information on NTP – http://www.ntp.org/

Information on MIT Kerberos – http://web.mit.edu/kerberos/www/

Apache "Security Tips" document:
http://httpd.apache.org/docs-2.0/misc/security_tips.html

Information on Sendmail and DNS:
http://www.sendmail.org/
http://www.deer-run.com/~hal/dns-sendmail/DNSandSendmail.pdf

Software

Pre-compiled software packages for HP-UX:
http://www.software.hp.com/
http://hpux.cs.utah.edu/

OpenSSH (secure encrypted network logins):

www.openssh.org

TCP Wrappers source distribution:
ftp.porcupine.org

PortSentry (monitors unused network ports for unauthorized access):
http://sourceforge.net/projects/sentrytools/

Open Source Sendmail (email server) distributions:
ftp://ftp.sendmail.org/

LPRng (Open Source replacement printing system for Unix):
http://www.lprng.org/

`sudo` (provides fine-grained access controls for superuser activity):
http://www.courtesan.com/sudo/

Appendix E: Change History

Version	Date	Changes
1.4.2	6/2008	- Added Change History
1.4.1	11/2007	- Reorganized document (Logging)
1.4.0	9/2007	- Removed 'Install TCP Wrappers' from Section 'Patches and Additional Software' - Added 'Install and Run Bastille' to Section 'Patches and Additional Software' - Removed 'Disable inetd, if possible' from Section 'Minimize boot services' - Removed 'Verify passwd and group file permissions' from Section 'File/Directory Permissions/Access' - Removed 'Run hp_checkperms' from Section 'File/Directory Permissions/Access' - Removed 'Strip dangerous/unneeded SUID from system executables' from Section 'File/Directory Permissions/Access' - Combined recommendations for finding world-writable and SUID/SGID files/directories in Section 'File/Directory Permissions/Access' - Added 'Restrict crontab file permissions' to Section 'File/Directory Permissions/Access' - Added 'Disable inetd, if possible' to Section 'Additional Security Notes' - Added 'Change default greeting string for Sendmail' to Section 'Additional Security Notes' - Added 'Install and configure sudo' to Section

		'Additional Security Notes' - Added 'Remove Compilers' to Section 'Additional Security Notes' - Added 'Verify that no UID 0 accounts exist other than root' to Section 'Additional Security Notes' - Added 'Install and configure IPFilter' to Section 'Additional Security Notes'
1.3.1	10/2005	- Typo corrections - Section 1.2: Added step 2
1.3.0	--	- Globally changed version from 1.1.0 to 1.3.0 to match Solaris draft - Globally changed "Proceed with" to "Perform" to match language in current Solaris draft - Globally changed 'Consider upgrading to HP-UX 11i' to 'Strongly consider...' - Backup Key Files section changed to refer to do-backup.sh as per current Solaris draft - Section 1.1: Specified patch distros to be loaded into /var/adm - Section 1.1: Removed instructions for (no longer support-by HP) HP-UX 10.20 in favor of language recommending upgrade to 11i - Section 1.1: Removed forward references to (deleted) item for read-only file systems - Updated to refer to new version of HP Security Patch Check tool (language QA'd by Keith Buck of HP) - Section 1.2: Changed action to match current Solaris draft - Added Section 1.15 ‘Only enable BIND DNS Server if absolutely necessary. This is in response to feedback that we were turning off named but had no item to turn it back on if necessary. It also matches the tack taken in the FreeBSD benchmark draft. - Section 2.8: Added note about need for RPC to support CDE - Section 3.1: Added 'chown root:sys /etc/inittab' to match current Solaris draft - Section 3.3: Remove action to disable 'pwgr' as this apparently is used beyond NIS - Section 3.4: Added note that LPRng is not supported by HP to match language in current Solaris draft - Section 3.6: Put Question in gray to match current Solaris draft - Section 3.9: Removed incorrect negation in question (i.e., proceed vs do not proceed) - Section 3.10: Removed incorrect negation in question

		similar to 3.9 - Section 3.10: Removed incorrect shading - Section 3.11: Added notes on Secure RPC, Kerberos, rpcbind, and security vs SSH to match language in current Solaris draft - Section 3.12: Added notes on Secure RPC, Kerberos, rpcbind, and security vs SSH to match language in current Solaris draft. - Section 3.14: Removed incorrect negation in question (i.e., proceed vs do not proceed) - Section 4.2: Deleted tcp_ip_abort_rinterval and ip_send_redirects, added ip_responde_to_echo_broadcast, and added 'chmod root:sys nddconf' to match current Solaris draft. - Section 4.4: Added ip_send_redirects to match current Solaris draft. - Removed Section 5.1 on mounting filesystems reaadonly or nosuid – becomes SN.3 - Added Section 5.6 – "Find 'unowned' files and directories" - Section 5.8: Changed 'chmod 700' to 'chmod go-rwx' - Section 6.1: Added note that Trusted Mode does not work when nsswitch.conf points to LDAP. - Section 6.1: Addedreference to HP's Shadow password package as an option for systems that can't run Trusted Mode - Moved Section 6.1 'Symlinks and Dangerous files' to SN.2 to match Solaris draft. - Section 6.2: Added sort/unique logic to action from Solaris draft - Section 6.2: Slight changes to Discussion to clean up the language - Added Section 6.3 'Prevent syslog from accepting messages from the network' - Removed Section 6.4 (/etc/shells) - Section 6.4 (xdmcp): Modified Action to modify Xconfig vice Xaccess - Moved item on Warning Banners to own section (now section 9) as in Solaris draft. - Section 6.8 (root logins): Added 'chwon root:sys /etc/securetty' to match Solaris benchmark - Added section 6.9 'Limit number of failed login attempts' to match Solaris draft - Added 6.10 'Disable "nobody" access for secure RPC to match Solaris draft. - Changed introduction to Section 7 to match Solaris

		draft. - Section 7.1: Changed Action to actually start system accounting – old action enabled process accounting - Section 7.3: Changed discussion to match Solaris draft. - Added Section 7.4 'Turn on additional loggin for FTP daemon to match Solaris draft. - Section 7.5: Added verbiage to Description to match Solaris draft. - Section 8.1: modified actions to they work with both HPUX Trusted Mode and the new Shadow Password package - Section 8.2: modified actions to they work with both HPUX Trusted Mode and the new Shadow Password package - Section 8.3: modified actions to they work with both HPUX Trusted Mode and the new Shadow Password package - Section 8.10: Added chaning UMASK in /etc/default/security for HPUX 11i - Added Section 9 on Warning Banners to match Solaris draft. Moved items here from other section where they dealt entirely with warning banners. - Added Appendix A 'File Backup Script' - Added Appendix B: 'Log Rotation Script' - Added Appendix C: 'Additional Security Notes to match Solaris draft; - References Section: Deleted references to Tripwire and updated URLs
1.1.0	--	--