the CENTER for
INTERNET SECURITY

Security Configuration Benchmark For

HP-UX 11i

Version 1.5.0
September 17, 2009

http://cisecurity.org
feedback@cisecurity.org

Terms of Use Agreement

Background.

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 and 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 any Product or Recommendation. 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:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

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;

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;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

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:

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;

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.

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. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for HP-UX 11i*, provides prescriptive guidance for establishing a secure configuration posture for *HP-UX 11i* v2 and v3 through Update 4. When appropriate, additional notes are provided for *HP-UX 11i* v1, however this document does not directly address that version. This guide was tested against *HP-UX 11i v2 and v3* as installed with the Data Center Operating Environment (OE). To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

This guide was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal. If you'd like to join the consensus process, please email feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that are based on a HP-UX 11i platform.

Acknowledgements

The Center for Internet Security would recognize the individuals that significantly contributed to creation of this guide.

Authors
Robert Fritz
Michael Louie
Chris Calabrese (v1.4.2)

Contributors and Reviews
Alex Noordergraaf
Anders Thulin
Andre Carrington
Andrew Gilmore
Aurobindo Sundaram
Bill Barto
Blake Frantz
Buck Keith
Calabrese Christopher
Carlisle Childress
James A. Finegan
James B Horwath
James Finegan
James G. McIntyre
James Philput
Jay Beale
Jeff Pike
Jennifer Friend
Jim Becher
Jim Finegan
Randy Bowie
Randy Marchany
Randy Young
Ratan Nalumasu
Richard Bejtlich
Rich Murphey
Robert W. Maloy
Rodney McKee
Ronald Luman
Ron Colvin

Carole Fennelly
Chad Thunberg
Chris Calabrese
Chris Coffin
Crist J. Clark
Dan Casey
Dan Goodman
Darryl Rathbun
Dave Shackleford
Dave Waltermire
David A. Kennel
David Bailey
David Bell
David Waltermire
David Whitcliff
Ed Skoudis
Edward Clay
Gary Gapinski
Gary Geisbert
George M. Jones
George Toft
Giacomo G. Brussino
Glenn Brunette
Hal Pomeranz
Huba Leidenfrost
Ivan Ristic
Jack Simons
Jimmy G. Devenport
Jim Smith
Joel Kirch
Joe Wulf
Johannes Ullrich
John Banghart
John Pyle
John Traenkenschuh
Joseph Wulf
King Brian
Laurie Zirkle
Leslie Geyer
Mario Fullum
Mark Phillips
Matt Fearnow
Michael A. Davis
Michael Cope
Michael F. Angelo
Michael Gough
Michael Katz
Michael Rash
Michael Starks
Mike Cash
Nancy Whitney
Nguyen Thi Xuan Thu
Nithya Raman
Ralph Durkee
Ryan Barnett
Sidney Faber
Stephen John Smoogen
Steve Grubb
Susan Diller
Terry Cutler
Terry Sherald
Tim Maletic
Tom Maloy
Tom Rhodes
Trevor Vaughan
Valdis Kletnieks
William Stearns
Wong Onn Chee
Wood Timothy
Zack Yang

Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

- be practical and prudent;
- provide a clear security benefit; and
- not negatively inhibit the utility of the technology beyond acceptable means

Level-II Benchmark settings/actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:

- may negatively inhibit the utility or performance of the technology
- acts as defense in depth measure

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

1. Recommendations

1.1 Install patches and supplementary software

1.1.1 Apply the latest OS patches (Level 1, Scorable)

Description:
Install the most current HP-UX patches and establish procedures for keeping up with future patches using HP-UX Software Assistant and HP Security Bulletin service.

HP's quarterly patch updates are 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 HP-UX Quality Packs are installed. Note: 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 v3.

Rationale:
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 install. 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.

Remediation:
Perform the following:

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.

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.

Bastille Note: Bastille can set up the checking of the system as a one-time action or as part of a `cron` job. For "safety" reasons, the administrator controls and initiates the update.

Audit:
See step 2, above. If there are no needed updates, the system is at the appropriate patch/update level**.**

References:

1. HP-UX Software Assistant: https://www.hp.com/go/swa
2. HP Security Bulletin subscription information: http://itrc.hp.com
3. Quarterly patch updates from HP ITRC: http://itrc.hp.com/service/patch/releaseIndexPage.do

1.1.2 Install and configure HP-UX Secure Shell (Level 1, Scorable)

Description:
OpenSSH is a popular free distribution of the standards-track SSH protocols which allows secure encrypted network logins and file transfers. HP-UX Secure Shell is HP's pre-compiled and supported version of OpenSSH.

Rationale:
Common login and file transfer services such as telnet, FTP, rsh, rlogin, and rcp use insecure, clear-text protocols that are vulnerable to attack. OpenSSH provides a secure, encrypted replacement for these services. Security is improved by further constraining services in the default configuration.

Remediation:
Perform the following to install and securely configure Secure Shell (SSH)

1. Download and install HP-UX Secure Shell if not already installed on the system.
2. Perform the following post-installation actions to secure the SSH service:

   a. Change to the `/opt/ssh/etc` directory
   b. Open `sshd_config`
   c. Set the `Protocol` token to `2`. If it is absent, add and set it.
   d. Set the `X11Forwarding` token to `yes`. If it is absent, add and set it.
   e. Set the `IgnoreRhosts` token to `yes`. If it is absent, add and set it.
   f. Set the `RhostsAuthentication` token to `no`. If it is absent, add and set it.
   g. Set the `RhostsRSAAuthentication` token to `no`. If it is absent, add and set it.
   h. Set the `PermitRootLogin` token to `no`. If it is absent, add and set it.
   i. Set the `PermitEmptyPasswords` token to `no`. If it is absent, add and set it.
   j. Set the `Banner` token to `/etc/issue`. If it is absent, add and set it.
   k. Set `root` as the owner of `sshd_config` and `ssh_config`.
   l. Set `sys` as the group owner of `sshd_config` and `ssh_config`.
   m. Restrict write access to `sshd_config` and `ssh_config` to the file owner.

The following script will perform the above procedure:

```
cd /opt/ssh/etc
cp -p sshd_config sshd_config.tmp
awk '
  /^Protocol/                { $2 = "2" };
  /^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
```

Audit:

1. Confirm Secure Shell is installed by executing the following:

```
swlist –l bundle SecureShell
```

2. Review the `sshd_config` file to verify that the post-installation defaults are as defined in step two above:

```
more /opt/ssh/etc/sshd_config
```

References:

1. www.openssh.org
2. HP-UX Secure Shell download from: http://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA
3. Secure Shell installation instructions at http://h20293.www2.hp.com/portal/swdepot/displayInstallInfo.do?productNumber=T1471AA

1.1.3 Use Bastille to report security configuration state

Description:
Bastille is a security hardening, lockdown tool supplied with HP-UX to assist administrators in securing their systems. Included is an assessment function that covers a wide range of lockdown items including most all items in this Benchmark. Bastille can serve as a reporting and audit tool. Appendix D provides a mapping of Benchmark items to related Bastille configuration items.

Rationale:
An automated, tested, and vendor supported reporting tool such as Bastille is more efficient and less error-prone than most manual or custom scripted methods.

Remediation:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

Audit:
See the Remediation section above.

References:

1. https://www.hp.com/go/bastille

1.2 Minimize inetd network services

1.2.1 Disable Standard Services (Level 1, Scorable)

Description:
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 1.1.2) 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. The steps articulated in the Remediation section 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 below.

Rationale:
The stock `/etc/inetd.conf` file shipped with HP-UX contains services that are rarely used or have more secure alternatives. Removing these from `inetd` will avoid exposure to possible security vulnerability in those services.

Remediation:
Perform the following to disable standard `inetd`-based services:

1. Change to the `/etc` directory
2. Open `inetd.conf`
3. Disable the following services by adding a comment character (`#`) to the beginning of its definition:

```
a. echo
b. discard
c. daytime
d. chargen
e. dtspc
f. exec
g. ntalk
q. rpc.rwalld
r. rpc.sprayd
s. rpc.cmsd
t. kcms_server
u. printer
v. shell
w. login
```

h. finger
i. uucp
j. ident
k. auth
l. instl_boots
m. registrar
n. recserv
o. rpc.rstatd
p. rpc.rusersd
x. telnet
y. ftp
z. tftp
aa. bootps
bb. kshell
cc. klogin
dd. rpc.rquotad
ee. rpc.ttdbserver

4. Save `inetd.conf`.
5. Set `root` as the owner of `inetd.conf`.
6. Set `sys` as the group owner of `inetd.conf`.
7. Restrict write access to `inetd.conf` to the file owner.
8. Remove the executable and sticky bit from `inetd.conf`.
9. Invoke inetd to reread it's config file: `inetd -c`

The following script will perform the above procedure:

```
cd /etc

for svc in echo discard daytime chargen dtspc \
     exec ntalk finger uucp ident auth \
     instl_boots registrar recserv; do
  awk "(\$1 == \"$svc\") { \$1 = \"#\" \$1 }; {print}" \
    inetd.conf > inetd.conf.new
  cp inetd.conf.new inetd.conf
  done
for svc in rpc.rstatd rpc.rusersd rpc.rwalld \
     rpc.sprayd rpc.cmsd kcms_server; do
  awk "/\\/$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 == \"$svc\") { \$1 = \"#\" \$1 }; {print}" \
    inetd.conf > inetd.conf.new
  cp inetd.conf.new inetd.conf
  done
for svc in rpc.rquotad rpc.ttdbserver; do
  awk "/^$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
inetd -c
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

References:

1. http://docs.hp.com/en/B2355-60130/inetd.conf.4.html

1.2.2 Only enable telnet if absolutely necessary (Not scorable)

Description:
Re-enable telnet.

`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. HP-UX Secure Shell (OpenSSH) provides an encrypted alternative to `telnet` (and other utilities) and should be used instead.

Rationale:
There is a mission-critical reason that requires users to access the system via `telnet` instead of the more secure SSH protocol.

Remediation:
Perform the following to re-enable telnet:

1. Open `/etc/inetd.conf`.
2. Delete the comment character (#) from the `telnet` service definition.
3. Add `-b /etc/issue` to the end of the telnet service definition. This will cause telnet to display the contents of `/etc/issue` to users attempting to access the system via telnet.
4. Save `/etc/inetd.conf`.

The following script will perform the above procedure:

```
awk '/^#telnet/ {
  $1 = "telnet"
  print $0 " -b /etc/issue"; next}
  { print }
' inetd.conf > /etc/inetd.conf.new
cp inetd.conf.new inetd.conf
rm -f /etc/inetd.conf.new
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.2.3 Only enable FTP if absolutely necessary (Not scorable)

Description:
Re-enable ftp.

Like `telnet`, the FTP protocol is unencrypted, which means passwords and other data transmitted during the session can be captured by sniffing the network, and that the FTP session itself can be hijacked by an external attacker.

SSH provides two alternative, encrypted file transfer mechanisms, `scp` and `sftp`, which should be used instead of FTP. Even if FTP is required because the local system is an anonymous FTP server, consider requiring authenticated users on the system to transfer files via SSH-based protocols. For further information on restricting FTP access to the system, see item 1.6.2 below.

Sites may also consider augmenting the “`ftpd -l`” below 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.

Rationale:
This machine serves as an (anonymous) FTP server or other mission-critical role where data must be transferred via FTP instead of the more secure alternatives.

Remediation
Perform the following to re-enable FTP:

1. Open `/etc/inetd.conf`.
2. Delete the comment character (#) from the `ftp` service definition.
3. Save `/etc/inetd.conf`.

The following script will perform the above procedure:

```
awk '
  /^#ftp/ { $1 = "ftp"; print $0; next}
  { print }
' inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
rm -f /etc/inetd.conf.new
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.2.4 Only enable rlogin/remsh/rcp if absolutely necessary (Not scorable)

Description:
Re-enable `rlogin/remsh/rcp`.

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 1.2.1 – Install SSH).

Rationale:
There is a mission-critical reason to use `rlogin/remsh/rcp` instead of the more secure `ssh/scp`.

Remediation:
Perform the following to re-enable rlogin/remsh/rcp:

1. Open `/etc/inetd.conf`.
2. Delete the comment character (#) from the `shell` and `login` service definitions.
3. Save `/etc/inetd.conf`.

The following script will perform the above procedure:

```
sed 's/^#shell/shell/; s/^#login/login/' \
  inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
rm -f /etc/inetd.conf.new
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.2.5 Only enable TFTP if absolutely necessary (Not scorable)

Description:
Re-enable TFTP.

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

Rationale:
This system serves as a boot server or has other mission-critical roles where data must be transferred to and from this system via TFTP.

Remediation:
Perform the following to re-enable TFTP:

1. Open `/etc/inetd.conf`.
2. Delete the comment character (#) from the `tftp` service definition.
3. Save `/etc/inetd.conf`.

The following script will perform the above procedure:

```
sed 's/^#tftp/tftp/' inetd.conf >inetd.conf.new
cp inetd.conf.new inetd.conf
rm -f /etc/inetd.conf.new
mkdir -p /var/opt/ignite
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.2.6 Only enable printer service if absolutely necessary (Not scorable)

Description:
Re-enable rlpdaemon based printer service.

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.

Rationale:
This machine a print server for your network.

Remediation:
Perform the following to re-enable the rlpdaemon based printer service:

1. Open `/etc/inetd.conf`.
2. Delete the comment character (#) from the `printer` definition.
3. Save `/etc/inetd.conf`.

The following script will perform the above procedure:

```
sed 's/^#printer/printer/' inetd.conf >inetd.conf.new
cp inetd.conf.new inetd.conf
rm -f /etc/inetd.conf.new
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.2.7 Only enable rquotad if absolutely necessary (Not scorable)

Description:
Re-enable rquotad.

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.

Rationale:
This system an NFS file server that requires the use of disk quotas

Remediation:
Perform the following to re-enable rquotad:

1. Open `/etc/inetd.conf`.
2. Delete the comment character (#) from the `rquotad` definition.
3. Save `/etc/inetd.conf`.

The following script will perform the above procedure:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.2.8 Only enable CDE-related daemons if absolutely necessary (Not scorable)

Description:
Re-enable CDE-related daemons.

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.

Rationale:
There a mission-critical reason to run a CDE GUI on this system.

Remediation:
Perform the following to re-enable CDE-related daemons:

1. Open `/etc/inetd.conf`.
2. Delete the comment character (#) from the `rpc.ttdbserver` definition.
3. Save `/etc/inetd.conf`.

The following script will perform the above procedure:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.2.9 Only enable Kerberos-related daemons if absolutely necessary (Not scorable)

Description:
Re-enable Kerberos-related daemons.

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.

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

Remediation:
Perform the following to re-enable Kerberos-related daemons:

1. Open `/etc/inetd.conf`.
2. Delete the comment character (#) from the `klogin` definition.
3. Save `/etc/inetd.conf`.

The following script will perform the above procedure:

```
sed 's/^#kshell/kshell/; s/^#klogin/klogin/' \
  inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
rm -f /etc/inetd.conf.new
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.2.10 Only enable BOOTP/DHCP daemon if absolutely necessary (Not scorable)

Description:
Re-enable BOOTP/DHCP services.

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

Rationale:
This server a BOOTP/DHCP server for the network

Remediation:
Perform the following to re-enable BOOTP/DHCP services:

1. Open `/etc/inetd.conf`.
2. Delete the comment character (#) from the `bootps` definition.
3. Save `/etc/inetd.conf`.

The following script will perform the above procedure:

```
sed 's/^#bootps/bootps/' \
  inetd.conf > inetd.conf.new
cp inetd.conf.new inetd.conf
rm -f /etc/inetd.conf.
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3 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.

1.3.1 Disable login: prompts on serial ports (Level 1, Scorable)

Description:
Disable the `login:` prompt on the system serial devices to make it more difficult for unauthorized users to attach modems, terminals, and other remote access devices to these ports.

Rationale:
If there is not a mission-critical need to provide login capability from any serial ports (such as for a modem) then disabling the `login:` prompt on the system serial devices reduces the risk of unauthorized access via these ports.

Remediation:
Perform the following to disable the `login:` prompt on the system serial devices:

1. Open `/etc/inittab`.
2. Disable each `getty` instance associated with a `tty` device by adding a comment character (`#`) to the beginning of the line.
3. Save `/etc/inittab`.*

The following script will perform the above procedure:

```
cp -p /etc/inittab /etc/inittab.tmp
sed 's/^[^#].*getty.*tty.*$/#&/' \
  /etc/inittab.tmp  > /etc/inittab
rm -f /etc/inittab.tmp
```

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 that by default in HP-UX 11i, only the console has a `getty` instance running on it.

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.2 Disable NIS/NIS+ related processes, if possible (Level 1, Scorable)

Description:
Disable NIS/NIS+ related processes.

Network Information Service (NIS) is a distributed database providing centralized control of names, addresses, services, and key configuration files throughout a network of servers and clients. NIS was formerly known as Yellow Pages (YP).

NIS+ is a replacement for NIS services, and is more scalable, flexible, and secure. It adds a security system with authentication and authorization services to validate users on the network and to determine if they allowed to access or modify the information requested.

However, both systems have known security vulnerabilities, and have been an entry point for security attacks.

Rationale:
Eliminate exposure to NIS/NIS+ vulnerabilities by not running related daemons on hosts that are not NIS/NIS+ servers or clients.

Remediation:
Perform the following to disable the startup of NIS/NIS+ related processes:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.3 Disable printer daemons, if possible (Level 1, Scorable)

Description:
Disable printer daemons.

The Technical Print Service (TPS) is a printer service used in the X-Windows and/or CDE environment. It is recommended that this service be disabled if the hosting system does not participate in print services

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.

Rationale:
Disabling unused services, such as TPS, will reduce the remote and local attack surfaces of the hosting system.

Remediation:
Perform the following to disable printer daemons:

1. Set the `LP` parameter to zero in the `lp` system configuration file `/etc/rc.config.d/lp`
2. Set the `XPRINTSERVERS` parameter to an empty string in the `tps` system configuration file `/etc/rc.config.d/tps`

The following script will perform the above procedure:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.4 Disable the CDE GUI login, if possible (Level 1, Scorable)

Description:
CDE stands for "Common Desktop Environment," and is an environment for logging on to and interacting with your system via an X-windows type GUI interface from the console. Intended for use with workstation or desktop systems, this service is not commonly used with the server-class systems or in large enterprise environments.

The X Windows-based CDE GUI services were developed with a different set of security expecations from those expected in many enterprise deployments, and have had a history of security issues. Unless there is a mission-critical need for a CDE GUI login to the system, this service should not be run to further reduce opportunities for security attacks.

Rationale:
The X Windows-based CDE GUI on HP-UX systems has had a history of security issues, and should be disabled if unused.

Remediation:
Perform the following to disable the GUI login:

```
ch_rc -a -p DESKTOP="" /etc/rc.config.d/desktop
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.5 Disable email server, if possible (Level 1, Scorable)

Description:
Disable the sendmail daemon to avoid processing incoming email.

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 remediation below 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.

Rationale:
Avoid potential vulnerabilities in the sendmail server if incoming email service is not used.

Remediation:
Perform the following to disable the sendmail server:

1. Set the `SENDMAIL_SERVER` parameter to zero in the `mailservs` system configuration file.
2. Setup a `cron` job to run sendmail at regular intervals (e.g. every hour) in order to process queued, outgoing mail.

The following script will perform the above procedure:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

References:
More information is available at http://www.deer-run.com/~hal/dns-sendmail/DNSandSendmail.pdf and at http://www.sendmail.org/.

1.3.6 Disable SNMP and OpenView Agents, if remote management or monitoring are not needed. (Level 1, Scorable)

Description:
Disable SNMP and OpenView agents if they are not needed.

Note: If SNMP is used, it is recommended to change the default SNMP community string by modifying the `get-community` and `set-community` parameters in the SNMP configuration file `/etc/SnmpAgent.d/snmpd.conf`

Rationale:
If SNMP and OpenView agents are not needed, avoid potential security vulnerabilities in these programs by disabling them.

Remediation:
Perform the following to disable the SNMP and OpenView Agents:

```
cd /sbin/rc2.d
mv -f S570SnmpFddi .NOS570SnmpFddi

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
ch_rc –a –p OSPFMIB=0 \
  /etc/rc.config.d/netdaemons
ch_rc –a –p OPCAGT=0 \
  /etc/rc.config.d/opcagt
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.7 Disable rarely used standard boot services (Level 1, Scorable)

Description:
Disable other standard boot services.

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 remediation section below. 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.

Note: that HP-UX 11.31 was the first version to support disablement of the NFS core services. Disablement on earlier versions is possible by moving

`/sbin/rc2.d/S400nfs.core` to `/sbin/rc2.d/.NOS400nfs.core`, but there is some risk of system instability.

Rationale:
Avoid potential security vulnerabilities in infrequently used subsystems by disabling them.

Remediation:
Perform the following:

```
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 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 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 HPWS_APACHE_START=0 /etc/rc.config.d/hpws_apacheconf
ch_rc -a -p NFS_CORE=0 /etc/rc.config.d/nfsconf
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.8 Only enable Windows-compatibility server processes if absolutely necessary (Not scorable)

Description:
Re-enable CIFS Server (Samba) services.

HP-UX 11i includes the popular Open Source Samba server (HP-UX CIFS 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

Rationale:
This machine provides authentication, file sharing, or printer sharing services to systems running Microsoft Windows operating systems.

Remediation:
Perform the following to re-enable CIFS Server:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.9 Only enable Windows-compatibility client processes if absolutely necessary (Not scorable)

Description:
Re-enable the HP CIFS Client service.

Rationale:
This system requires access to file systems from remote servers via the Windows (SMB) file services.

Remediation:
Perform the following:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.10 Only enable NFS server processes if absolutely necessary (Not scorable)

Description:
Re-enable the NFS file service.

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 1.3.12 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 performing the following:

1. Temporarily set `NFS_SERVER=1, NUM_NFSD=1`, and `NUM_NFSIOD=1` in `/etc/rc.config.d/nfsconf`

2. Execute:

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

3. Install Oracle

4. Stop the NFS services:

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

5. Disable the NFS services by resetting NFS`_SERVER=0, NUM_NFSD=0,` and `NUM_NFSIOD=0` in `/etc/rc.config.d/nfsconf`.

Rationale:
This machine is a NFS file server.

Remediation:
Perform the following:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.11 Only enable NFS client processes if absolutely necessary (Not Scorable)

Description:
Re-enable the NFS Client service.

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.

Rationale:
This system must access file systems from remote servers via NFS.

Remediation:
Perform the following:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.12 Only enable RPC-based services if absolutely necessary (Not Scorable)

Description:
Re-enable RPC-based services.

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.

Rationale:
RPC-based services are used such as:

- 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)

Remediation:
Perform the following for 11.31 and later:

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

For 11.23 and prior:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.13 Only enable Web server if absolutely necessary (Not Scorable)

Description:
Re-enable the Web server suite.

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 runnin

Rationale:
There is a mission-critical reason why this system must run a Web server.

Remediation:
Perform the following:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.3.14 Only enable BIND DNS server if absolutely necessary (Not Scorable)

Description:
Re-enable the BIND DNS service.

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.

Rationale:
There exists a mission-critical reason why this system must run a DNS server.

Remediation:
Perform the following:

11.23 and prior:

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

11.31 and later:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.4 Kernel Tuning

1.4.1 Enable stack protection (Level 1, Scorable)

Description:
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.

Rationale:
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.

Remediation:
For 11i v2 and later:

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

For 11i v1:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.4.2 Network parameter modifications (Level 1, Scorable)

Description:
Modify the network parameter boot configuration file to meet current best practices.

Note: HP-UX 11.11 systems require patch PHNE_25644 for `ndd` to set `arp_cleanup_interval` from `/etc/rc.config.d/nddconf`

Bastille Note: Bastille performs a similar action but does not support the exact same changes.

Rationale:
Network parameter default values should align with current best practices unless there is a specific need to use other values.

Remediation:
Perform the following to update the default network parameter values:

1. Change to the `/etc/rc.config.d` directory
2. Open `nddconf` and review the comment lines on how to use the configuration file
3. Set each of the following network parameters to the recommended value. If a parameter does not have an entry in `nddconf` then add a new entry to the end of the file while properly incrementing the parameter index:

	TRANSPORT_NAME	NDD_NAME	NDD_VALUE
a.	tcp	tcp_syn_rcvd_max	4096
b.	arp	arp_cleanup_interval	60000
c.	ip	ip_forward_src_routed	0
d.	ip	ip_forward_directed_broadcasts	0
e.	ip	ip_respond_to_timestamp	0
f.	ip	ip_respond_to_timestamp_broadcast	0
g.	ip	ip_respond_to_address_mask_broadcast	0
h.	ip	ip_respond_to_echo_broadcast	0

4. Save `nddconf.`

If creating this file for the first time:

1. Set `root` as the owner of `nddconf`.
2. Set `sys` as the group owner of `nddconf.`
3. Restrict write access to `nddconf` to the file owner.
4. Remove the executable and sticky bit from `nddconf.`

If the existing `nddconf` file contains no entries, then the following script will perform the above procedure:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.4.3 Use more random TCP sequence numbers (Level 1, Scorable)

Description:
Generate initial TCP sequence numbers that comply with RFC1948.

Note: In HP-UX 11i v1 and later, an algorithm largely compliant with RFC1948 is already used. However, setting the isn passphrase closes the small remaining gap, and adds entropy to the seed.

Rationale:
Makes remote off-net session hijacking attacks more difficult.

Remediation:
Perform the following to use more random TCP sequence numbers upon system startup:

1. Create/open the file `/sbin/rc2.d/S999tcpisn`
2. Add the following line:
   ```
   ndd -set /dev/tcp tcp_isn_passprase=<random string>
   ```
   replacing `<random string>` with a string of random characters.
3. Save the file.
4. Set `root` as the owner and `bin` as the group owner of the file.
5. Restrict write access to the file.
6. Set the execution bit for the file.

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.4.4 Additional network parameter modifications (Level 1, Scorable)

Description:
Configure networking to NOT forward TCP/IP packets between multiple networks, even if the machine has multiple network adapters connected to multiple networks.

Rationale:
System is not going to be used as a firewall or gateway to pass network traffic between different networks.

Remediation:
Perform the following to disable forwarding TCP/IP packets between networks:

1. Change to the `/etc/rc.config.d` directory
2. Open `nddconf` and review the comment lines on how to use the configuration file
3. Set each of the following network parameters to the recommended value. If a parameter does not have an entry in `nddconf` then add a new entry to the end of the file while properly incrementing the parameter index:

	TRANSPORT_NAME	**NDD_NAME**	**NDD_VALUE**
a.	ip	ip_forwarding	0
b.	ip	ip_send_redirects	0

4. Save `nddconf`.

If creating this file for the first time:

5. Set `root` as the owner of `nddconf`.
6. Set `sys` as the group owner of `nddconf`.
7. Restrict write access to `nddconf` to the file owner.
8. Remove the executable and sticky bit from `nddconf`.

The following script will perform the above procedure properly if used as a follow-on from the script in item 1.4.2 :

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.5 File/Directory Permissions/Access

1.5.1 Set Sticky Bit on World Writable Directories (Level 1, Scorable)

Description:
Ensure that the sticky bit is set for all unexpected or exposed world writable directories

Rationale:
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.

Remediation:
Perform the following to set the sticky bit on all exposed world writable directories:

1. Execute the `checkperms` utility to generate a list of all world writable directories not registered as part of an HP-UX installed product.
2. For each directory on this list set the sticky bit:

```
chmod u+t  <directory>
```

Audit:
Execute the `checkperms` utility to generate a report of world writable directories without a sticky bit:

```
checkperms
```

1.5.2 Secure unauthorized world-writable files and SUID/SGID executables (Level 1)

Description:
Identify and remove write access for world-writable files and unauthorized SUID/SGID files on the system.

Rationale:
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.

Remediation:
Perform the following to identify world writable files and SUID/SGID executables:

1. Execute the `checkperms` utility to generate a list of all world writable files and unlisted SUID/SGID files.

2. For each listed world-writable file remove write access for “other” users:

```
chmod o-w <filename>
```

3. Review each listed SUID/SGID file and remove if unauthorized.

Note: generally removing write access for the "other" category is advisable, but always consult relevant vendor documentation in order to avoid breaking any application dependencies on a given file.

Audit:
Executing the checkperms script will flag unexpected world writable files and unauthorized SUID/SGID executables:

```
checkperms
```

Note: this script uses the HP-UX Installed-Product Database (IPD), 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.

1.5.3 Resolve “unowned” files and directories (Level 1, Scorable)

Description:
Evaluate ownership of any files that are not owned by a locally defined user, and consider reassignment to an active user.

Rationale:
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 (in this example, “bin”) as appropriate

Remediation:
Perform the following to identify “unowned” files and directories, and consider resetting ownership to a default owner and restricting access permissions:

1. Locate all local files that are owned by users or groups not listed in the system configuration files.

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

2. Consider resetting user and group ownership of these files to a default active user (e.g. bin)

```
chown bin:bin  <filename>
```

3. Consider restricting world-write permissions, and removing any SUID/SGID bits on these files.

```
chmod ug-s,o-w <filename>
```

Note: there is no reason for an application to require an unowned file, so these changes should be application-safe.

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6 System Access, Authentication, and Authorization

1.6.1 Enable Hidden Passwords (Level 1, Scorable)

Description:
Enable hidden passwords by converting the system to a Trusted System or to use Shadow Passwords.

Note: do not perform this if the system runs applications that read the encrypted password entries in `/etc/passwd` directly.

Rationale:
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 1.8.3) ensures that users change their passwords on a regular basis and helps stop the use of stolen passwords.

Remediation:
Perform one of the following to convert the system to trusted mode or shadowed mode:

A. Use the system management program `smh` or `sam` to convert to a trusted system –or-
B. Use the command `pwconv` to convert to shadowed passwords.

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.2 Restrict users who can access to FTP (Level 1, Scorable)

Description:
Configure FTP to prevent certain users from accessing the system via FTP.

The file `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.

Note: more fine-grained FTP access controls can be placed in `/etc/ftpd/ftpaccess`

Rationale:
Privileged users such as `root` and other "system" type accounts should *never* be transferring information via such an insecure service as FTP.

Remediation:
Perform the following to restrict default priviledged users from access to FTP:

1. Add the users `root daemon bin sys adm lp uucp nuucp nobody hpdb useradm` to the file `/etc/ftpd/ftpusers` (each user on a single line).
2. Set the file owner and group owner to the user `bin`.
3. Set the file permissions so that only the file owner has read or write perms and no user has execute permission (`600`).

The following script will create and populate the `ftpusers` file as described above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.3 Prevent Syslog from accepting messages from the network (Level 1, Scorable)

Description:
Prevent syslogd from accepting messages from the network.

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: Do not perform this action if this machine is a log server, or needs to receive Syslog messages via the network from other systems.

Note: 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.

Rationale:
Disabling unused network services will reduce the remote attack surfaces of the hosting system.

Remediation:
Disable the syslog network option by doing the following:

1. Open the syslogd startup configuration file `/etc/rc.config.d/syslogd`
2. Add the parameter “`-N`” to the `SYSLOGD_OPTS=` line if it is not already present
3. Save and close the file.

The following script will perform the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.4 Disable XDMCP port (Level 1, Scorable)

Description:
Disable the XDMCP port for remote login services.

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. This behavior can be overridden in the `/etc/dt/config/Xaccess` file.

Rationale:
XDMCP is an unencrypted protocol that may reduce the confidentiality and integrity of data that traverses it.

Remediation:
Perform the following to disable the XDMCP port:

1. Open the file `/etc/dt/config/Xconfig`. If it does not exist, copy it from `/usr/dt/config/Xconfig.`
2. Append the line `Dtlogin.requestPort:0` to the file and close.

The following script will perform the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.5 Set default locking screensaver timeout (Level 1, Scorable)

Description:
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. Uniformly reduce this default timeout value to 10 minutes (this setting can still be overridden by individual users in their own environment.)

Rationale:
Setting the inactivity timer to a low value will reduce the probability of a malicious entity compromising the system via the console.

Remediation:
Perform the following to set a default screensaver timeout for all environments:

1. For every `sys.resources` file in each directory in `/usr/dt/config/` create a corresponding `/etc/dt/config/*/sys.resources` file if it does not already exist.
2. Append the following lines to each `/etc/dt/config/*/sys.resources` file:
   ```
   dtsession*saverTimeout: 10
   dtsession*lockTimeout: 10
   ```

The following script will perform the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.6 Configure IPFilter to allow only select communication (Level 1, Scorable)

Description:
HP-UX IPFilter (B9901AA) is a stateful system firewall that controls IP packet flow in or out of a machine. It is installed by default on HP-UX 11iv2 (11.23) and later. On older systems, IPFilter can be obtained from http://www.hp.com/go/ipfilter.

The rules below will work in an otherwise-empty ipf.conf file, or, if there are rules already present, it will block all that were not passed earlier in the ruleset. This is less likely to break things, but will allow more traffic through. Alternatively, you can instead take the pass lines below (not using the block rule), and change them into “block in quick” rules, and place those at the top of the file. This will error on the side of blocking traffic. See ipf(5) for detail. Your ruleset can be tested using ipftest(1).

Bastille note: if using to change and monitor the IPFilter firewall, ensure that rules are added to /etc/opt/sec_mgmt/bastille/ipf.customrules, and that Bastille is rerun with the last config file, so they will not be overwritten in a subsequent lockdown.

Rationale:
Restricting incoming network traffic to explicitly allowed hosts will help prevent unauthorized access the system.

Remediation:
Perform the following to add enable ipfilter and install a default ruleset to block unauthorized incoming connections:

1. Enable ipfilter: `ipfilter -e`
2. Append the following lines to `/etc/opt/ipf/ipf.conf` :

```
block in all
pass in from <allowed net>/<mask>
pass in from <allowed net>/<mask>
```

   replacing each `<allowed net>/<mask>` with an authorized IP address and mask.

3. Flush the old rules and read in the updated rules:

```
ipf -Fa -f /etc/opt/ipf/ipf.conf
```

The following script can be used to as a template for creating your own script to perform the procedure above:

```
ipfilter -e

cat <<EOF >> /etc/opt/ipf/ipf.conf
block in all
pass in from <allowed net>/<mask>
pass in from <allowed net>/<mask>
EOF

ipf -Fa -f /etc/opt/ipf/ipf.conf
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.7 Restrict at/cron to authorized users (Level 1, Scorable)

Description:
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.

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.

Rationale:
On many systems, only the system administrator needs the ability to schedule jobs.

Remediation:
Perform the following to restrict at/cron to root only:

1. Change to the `/var/adm/cron` directory
2. Archive or delete any existing `cron.deny` and `at.deny` files
3. Create or replace the `cron.allow` and `at.allow` files with a single line file containing just `root`
4. Ensure that the files are owned by `root` and group owned by `sys`
5. Ensure that no users have write/execute permission to the files, and that only `root` has read access to the files.

The following script will perform the procedures above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.8 Restrict crontab file permissions (Level 1, Scorable)

Description:
The system `crontab` files are only accessed by the `cron` daemon (which runs with superuser privileges) and the `crontab` command (which is set-UID to `root`).

Rationale:
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.

Remediation:
Perform the following so that only `root` has access to the `crontab` files:

1. Change to the `/var/spool/cron/crontabs` directory
2. Change the file owner to `root` and file group owner to `sys`
3. Set file permissions so that only `root` has access to the files.

The following script will perform the procedure above:

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

chown root:sys *
chmod og-rwx *
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.9 Restrict root logins to system console (Level 1, Scorable)

Description:
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 a limited audit trail in the event of problems.

Rationale:
Anonymous `root` logins do not provide an audit trail, nor are subject to additional authorization provisions.

Remediation:
Perform the following to restrict root logins to the system console only:

1. Replace the file `/etc/securetty` with a single line file containing `console`
2. Change the file owner to `root` and file group owner to `sys`
3. Set file permissions so that only `root` has access to the file.

The following script will perform the procedure above:

```
echo console > /etc/securetty
chown root:sys /etc/securetty
chmod og-rwx /etc/securetty
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.10 Set retry limit for account lockout (Level 1, Scorable)

Description:
The commands below 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 1.8.4. 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 `/etc/default/security` setting below 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 Note: sets the retry limit to ten (10) only when converting a system to trusted mode.

Rationale:
Setting the retry limit to a reasonably low value helps discourage brute force password guessing attacks.

Remediation:

1. Ensure system is a trusted system.
2. Use the `/usr/lbin/modprpw` command to set the maximum retry limit to 10 for all current unlocked users except `root`.
3. Use the `/usr/lbin/modprdef` command to set the default max retry limit to 10
4. Append the line `AUTH_MAXTRIES=10` to `/etc/default/security` to set the default max retry limit to 10

The following script will perform the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.6.11 Disable nobody access for secure RPC (Level 1, Scorable)

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

Rationale:
The default "nobody" user should not be accessing information via secure RPC.

Remediation:
Perform the following to disable nobody access for secure RPC:

1. Add the "`-d`" option to the `KEYSERV_OPTIONS` parameter in the system startup configuration file `/etc/rc.config.d/namesvrs`

The following script will perform the procedure above:

```
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
```

Audit:

Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.7 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 Host Intrusion Detection System (HIDS) for HP-UX 11i 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

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.

1.7.1 Enable kernel-level auditing (Level 1, Scorable)

Description:
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 auditing has a prerequisite of either Standard Security Mode Extensions, or in the case of HP-UX 11iv1 and prior, Trusted Mode.
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.

Rationale:
By recording key system events in log files, kernel-level auditing provides a trail to detect and analyze security breaches. Moreover, this data can be used to detect potential security weakness, and also serves as a deterrent against system abuses.

Remediation:
Use the Systems Management Homepage (SMH) facility to configure and enable the type and level of auditing appropriate for your environment.

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.7.2 Enable logging from inetd (Level 1, Scorable)

Description:

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.

Rationale:

Logging information about the source of inetd network connections assists in the detection and identification of unusual activity that may be associated with security intrusions.

Remediation:

Perform the following:

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

Audit:

Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.7.3 Turn on additional logging for FTP daemon (Level 1, Scorable)

Description:

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.

Rationale:
Logging information about the source of ftp network connections assists in the detection and identification of unusual activity that may be associated with security intrusions.

Remediation:
Perform the following to enable logging for the FTP daemon:

1. Change directory to `/etc`.
2. Open the `inetd.conf` file and locate the `ftpd` configuration entry line.
3. Add the “`-L`” and “`-l`” flags to the `ftpd` entry if not already present.
4. Save and close file.

The following script will perform the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8 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 typically provided with this document, but are also 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.

1.8.1 Block system accounts (Level 1, Scorable)

Description:
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 actions below 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.

Rationale:
System accounts are not used by regular users, and almost never require direct access; thus, they should be locked to prevent accidental or malicious usage.

Remediation:
Perform the following to properly lock the following known system users:

```
www sys smbnull iwww owww sshd hpsmh named uucp nuucp
adm daemon bin lp nobody noaccess hpdb useradm
```

1. Lock the account:

```
passwd -l <user>
```

2. Set the login shell to an invalid program:

```
/usr/sbin/usermod -s /bin/false <user>
```

3. If a trusted system, set the adminstrator lock:

```
/usr/lbin/modprpw -m alock=YES <user>
```

The following script will perform the procedure above:

```
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 [[ -f /tcb ]]; then
        /usr/lbin/modprpw -m alock=YES "$user"
    fi
done
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.2 Verify that there are no accounts with empty password fields (Level 1, Scorable)

Description:
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*`"

Rationale:
User accounts should have passwords, or be locked.

Remediation:
Perform the following to ensure that no accounts have an empty password field:

1. Identify all user accounts with an empty password field:

```
logins -p
```

2. Lock each account:

```
 passwd -l <user>
```

3. If a trusted system, set the administrator lock:

```
/usr/lbin/modprpw -m alock=YES <user>
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.3 Set account expiration parameters on active accounts (Level 1, Scorable)

Description:
The commands below 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.

Rationale:
It is a good idea to force users to change passwords on a regular basis.

Remediation:
Perform the following to set password expiration parameters on all active accounts:

1. Identify all user accounts excluding root that are not locked, and for each:

2. Set password expiration parameters for the account (`logname)` by executing the following:

   ```
   passwd -x 91 -n 7 -w 28 <logname>
   ```

   for trusted systems, perform the following:

   ```
   /usr/lbin/modprpw -m exptm=90,mintm=7,expwarn=30 <logname>
   ```

3. Set the default account expiration parameters by appending the following lines to `/etc/default/security`:

   ```
   a. PASSWORD_MAXDAYS=91
   b. PASSWORD_MINDAYS=7
   c. PASSWORD_WARNDAYS=28
   ```

4. Set the default parameters for trusted systems with:

   ```
   /usr/lbin/modprdef -m exptm=90,mintm=7,expwarn=30
   ```

The following script will perform the procedure above.

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.4 Set strong password enforcement policies (Level 1, Scorable)

Description:
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 1.6.10). A password history depth of ten combined with passwords that expire four times per year (item 1.8.3) 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.

Note: 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 you local security standards before adopting the values given above.

Rationale:
All users should use strong passwords.

Remediation:
Perform the following to set strong password enforcement policies:

1. Change the following parameters in the `/etc/default/security` file to establish default password policies for new users:

   ```
   a. MIN_PASSORD_LENGTH=7
   b. PASSWORD_HISTORY_DEPTH=10
   c. PASSWORD_MIN_UPPER_CASE_CHARS=1
   d. PASSWORD_MIN_DIGIT_CHARS=1
   e. PASSWORD_MIN_SPECIAL_CHARS=1
   f. PASSWORD_MIN_LOWER_CASE_CHARS=1
   ```

2. If using a trusted system, issue the following `modprdef` commands to disallow null or trivial passwords:

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

The following script will perform the procedure above:

```
ch_rc –a -p MIN_PASSORD_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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.5 Verify no legacy '+' entries exist in passwd and group files (Level 1, Scorable)

Description:
`'+'` entries in various passwd and group files served as markers for systems to insert data from NIS maps at a certain point in a system configuration file. HP-UX does not use these markers, but they may exist in files that have been imported from other platforms. They should be deleted if they exist.

Rationale:
Legacy ‘+’ entries are no longer required on HP-UX systems, and may provide an avenue for attackers to gain privileged access on the system.

Remediation:
Perform the following to remove any legacy ‘+’ entries in passwd and group files:

1. Display legacy ‘+’ entries:

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

2. Remove any entries found from the passwd and group files.

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.6 No '.' or group/world-writable directory in root $PATH (Level 1, Scorable)

Description:
Remove the current working directory (`'.'`) or other world-writable directories from the root user’s execution path. To execute a file in the current directory when `‘.’` is not in the `$PATH`, use the format `“./filename”`.

Rationale:
Including these paths in the `root`'s executable path allows an attacker to gain superuser access if an administrator operating as root executes a Trojan horse program.

Remediation:
Remove the following path components if they exist in the root user’s $PATH:

1. current working directory ('.')
2. empty directories (‘::’)
3. a trailing path seperator at the end of the $PATH (‘:’)
4. any directory with world or group -write permissions set

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.7 Secure user home directories (Level 1, Scorable)

Description:
Remove group write and world access to all user home directories.
While the modifications below are relatively benign, making global modifications to user home directories without alerting your user community can result in unexpected outages and unhappy users.

Rationale:
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.

Remediation:
Perform the following to secure user home directories:

1. Identify all user accounts excluding root that are not locked, and for each of these user home directories:
2. Remove `group` write permission (`g-w`) and all `other` permissions (`o-rwx`)

The following script will perform the procedure above:

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

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.8 No user dot-files should be group/world writable (Level 1, Scorable)

Description:
Remove group and world write permissions from user dot-files.
While the modifications below are relatively benign, making global modifications to user dot-files without alerting your user community can result in unexpected outages and unhappy users.

Rationale:
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.

Remediation:
Perform the following:

1. Identify all user accounts excluding root that are not locked, and for each of these user home directories:
2. Remove `group`/`other` write permissions (`go-w`) from any files beginning with '.'

The following script performs the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.9 Remove user .netrc, .rhosts and .shosts files (Level 1, Scorable)

Description:
Remove user `.netrc`, `.rhosts`, and `.shosts` files.

Note that making global modifications to user security files in their home directories without alerting your user community can result in unexpected outages and unhappy users.

Rationale:
`.netrc` files may contain unencrypted passwords that may be used to attack other systems, while `.rhosts` and `.shosts` files used in conjunction with the BSD-style “r-commands” (`rlogin, remsh, rcp`) or SSH 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).

Remediation:
Perform the following to remove user .netrc, .rhosts, and .shosts files.

1. Identify all user accounts, and for each existing home directory:
2. Remove `.netrc, .rhosts,` and `.shosts` files

The following script performs the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.10 Set default umask for users (Level 1, Scorable)

Description:
Set the default `umask` to `077` so that files created by users will not be readable by any other user on the system. 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 Note: sets the default `umask`, but uses a `umask` of `027` rather than the `077`.

Rationale:
Restricting access to files and directories created by a user from any other user on the system reduces the possibility of an unauthorized account accessing that user’s files. 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.

Remediation:
Perform the following to set a default umask for users:

1. Change directory to `/etc`
2. Append the line `umask 077` to the following files:
   ```
   a. profile
   b. csh.login
   c. d.profile
   d. d.login
   ```
3. Update the `UMASK` parameter to `077` in the file `/etc/default/security`

The following script performs the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.8.11Set "mesg n" as default for all users (Level 1, Scorable)

Description:
Block the use of `write` or `talk` commands to contact the user at their terminal in order to slightly strengthen permissions on the user's `tty` device. Note that this setting is the default on HP-UX 11i.

Rationale:
Since `write` and `talk` are no longer widely used at most sites, the incremental security increase is worth the loss of functionality.

Remediation:
Perform the following:

1. Change directory to `/etc`
2. Append the line `mesg n` to the following files:
   ```
   a. profile
   b. csh.login
   c. d.profile
   d. d.login
   ```

The following script performs the procedure above:

```
cd /etc
for file in profile csh.login d.profile d.login
```

```
do  echo mesg n >> "$file"
done
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.9 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.

1.9.1 Create warning banners for terminal-session logins (Level 1, Scorable)

Description:
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.

Rationale:
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.

Remediation:
Perform the following to create warning banners for terminal-session logins:

1. Compose a default banner text string
2. Append this string to the files /etc/motd and /etc/motd
3. Change the owner to `root` and group owner to `sys` for the file `/etc/motd`
4. Change the owner to `root` and group owner to `root` for the file `/etc/issue`
5. Change file permissions to (`644`) for the files `/etc/motd` and `/etc/issue`

The following script performs the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.9.2 Create warning banners for GUI logins (Level 1, Scorable)

Description:
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 below 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 council about the specifics of any warning banners.

Rationale:
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.

Remediation:
Perform the following to install default warning banners for GUI logins:

1. Create a default banner text string ($banner)
2. For each directory in `/usr/dt/config` that contains a `Xresources` file, copy that `Xresources` file into a corresponding directory in `/etc/dt/config` (creating the directory if needed)
3. Append the following lines (replacing $banner with the string in step 1) to each `/etc/dt/config/*/Xresources` file:
    a. `Dtlogin*greeting.labelString:` $banner
    b. `Dtlogin*greeting.persLabelString:` $banner
4. Change the owner to `root` and group owner to `sys` for each `Xresource` file
5. Change the file permissions to `644` for each `Xresource` file

The following script performs the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

1.9.3 Create warning banners for FTP daemon (Level 1, Scorable)

Description:
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 1.2.1.

Rationale:
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.

Remediation:
Perform the following to install a default warning banner for the FTP daemon:

1. Ensure that an appropriate warning message exists in the `/etc/issue` file .
2. Append the line “`banner /etc/issue`” to the file `/etc/ftpd/ftpaccess`
3. Change file permissions to `600` for `/etc/ftpd/ftpaccess`
4. Change owner to `root` and group owner to `sys` for both /`etc/ftpd` and `/etc/ftpd/ftpaccess`

The following script performs the procedure above:

```
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
```

Audit:
Run Bastille to create an assessment report as shown:

```
/opt/sec_mgmt/bastille/bin/bastille --assessnobrowser
```

See Appendix D for question mapping.

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:

```
Install and use Nagios, available free from the internet express
bundle(software.hp.com).
```

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.

This information can shed light on the timing of certain DOS or resource-intensive breakins, but is also of value for regular system maintenance. HP-UX Capacity Adviser can also be used (for fee) as a more integrated solution.

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 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 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:
As an alternate mechanism to IPFilter, 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 6.6.

Appendix D: Summary of CIS compliance using HP-UX Bastille.

This table contains a single consolidated listing of the actions Bastille performs that are relevant to the CIS benchmark, and their alignment with the benchmark.

CIS ID#		Related Bastille Items	Comments / Exceptions
1.1	Patches and Additional Software		
1.1.1	Apply latest OS patches	Patches.spc_run	Manual Process, though Bastille can leverage SWA to provide a report and build a depot
1.1.2	Install and configure SSH	MiscellaneousDaemons.configure_ssh	Default installed on HP-UX 11.23 and subsequent
1.1.3	Install and Run Bastille	n/a	Manual
1.2	Minimize inetd network services		
1.2.1	Disable Standard Services	SecureInetd.inetd_general SecureInetd.deactivate_builtin SecureInetd.deactivate_finger SecureInetd.deactivate_ident SecureInetd.deactivate_ntalk SecureInetd.deactivate_recserv SecureInetd.deactivate_time SecureInetd.deactivate_uucp SecureInetd.deactivate_dttools SecureInetd.deactivate_printer SecureInetd.deactivate_telnet SecureInetd.deactivate_ftp SecureInetd.deactivate_rtools SecureInetd.deactivate_tftp SecureInetd.deactivate_printer SecureInetd.deactivate_ktools SecureInetd.deactivate_bootp SecureInetd.deactivate_rquotad	Bastille disables all of the inetd services listed that are on by default except registrar. The off-by-default services Bastille does not lock down are: instl, boots, rpc.rstatd, rpc.ruserd, rpc.rwalld, rpc.sprayd, rpc.cmsd, kcms_server, bootps, and rpc.ttdbserver
1.2.2	Only enable telnet if absolutely necessary	SecureInetd.deactivate_telnet	
1.2.3	Only enable FTP if absolutely necessary	SecureInetd.deactivate_ftp	
1.2.4	Only enable rlogin/remsh/rcp if absolutely necessary	SecureInetd.deactivate_rtools	
1.2.5	Only enable TFTP if absolutely necessary	SecureInetd.deactivate_tftp	
1.2.6	Only enable printer service if absolutely necessary	SecureInetd.deactivate_printer	
1.2.7	Only enable rquotad if	SecureInetd.deactivate_rquotad	

	absolutely necessary		
1.2.8	Only enable CDE-related daemons if absolutely necessary	SecureInetd.deactivate_dttools	
1.2.9	Only enable Kerberos-related daemons if absolutely necessary	SecureInetd.deactivate_ktools	
1.2.10	Only enable BOOTP/DHCP daemon if absolutely necessary	SecureInetd.deactivate_bootp	
1.3	Minimize boot services		
1.3.1	Disable login: prompts on serial ports	AccountSecurity.serial_port_login	
1.3.2	Disable NIS/NIS+ related processes, if possible	MiscellaneousDaemons.nis_client MiscellaneousDaemons.nis_server MiscellaneousDaemons.nisplus_server MiscellaneousDaemons.nisplus_client	
1.3.3	Disable printer daemons, if possible	Printing.xprintserver,	
1.3.4	Disable GUI login, if possible	AccountSecutity.gui_login	
1.3.5	Disable email server, if possible	Sendmail.sendmaildaemon Sendmail.sendmailcron	
1.3.6	Disable SNMP and OpenVIew, if possible	MiscellaneousDaemons.snmpd	
1.3.7	Disable other standard boot services	MiscellaneousDaemons.disable_rbootd MiscellaneousDaemons.nfs_server MiscellaneousDaemons.nfs_client MiscellaneousDaemons.disable_ptydaemon Apache.deactivate_hpws_apache MiscellaneousDaemons.snmpd MiscellaneousDaemons.license_server MiscellaneousDaemons.nfs_core	
1.3.8	Only enable Windows-compatibility server processes if absolutely necessary	MiscellaneousDaemons.disable_smbclient	
1.3.9	Only enable Windows-compatibility client processes if absolutely necessary	MiscellaneousDaemons.disable_smbsever	
1.3.10	Only enable NFS server processes, if absolutely necessary	MiscellaneousDaemons.nfs_server	
1.3.11	Only enable NFS client processes, if absolutely necessary	MiscellaneousDaemons.nfs_client	
1.3.12	Only enable RPC-based services, if absolutely necessary	MiscellaneousDaemons.nfs_core	HP does not recommend disabling this item prior to HP-UX 11iv3 due to OS interdependencies

1.3.13	Only enable Web server, if absolutely necessary	Apache.deactivate_hpws_apache	
1.3.14	Only enable BIND DNS server, if absolutely necessary	MiscellaneousDaemons.disable_bind	
1.4	Kernel Tuning		
1.4.1	Enable stack protection	HP_UX.stack_execute	
1.4.2	Network parameter modifications	HP_UX.ndd	Values vary between Bastille and HP-UX Benchmark
1.4.3	Use better TCP sequence numbers	HP_UX.tcp_isn	
1.4.4	Additional network parameter modifications	HP_UX.ndd	Bastille does not use the specified values
1.5	File/Directory Permissions/Access		
1.5.1	Set Sticky Bit on World Writable Directories	FilePermissions.world_writeable	Bastille creates a script to change these items
1.5.2	Find unauthorized world-writable files and SUID/SGID executables	Checkperms utility	
1.5.3	Find “unowned” files and directories	AccountSecurity.unowned_files	Note to Bastille_Team… consider this for checkperms, and making this question a general checkperms run
1.6	System Access, Authentication, and Authorization		
1.6.1	Enable Password Hiding	AccountSecurity.hidepasswords	
1.6.2	Create /etc[/ftpd]/ftpusers	FTP.ftpusers	
1.6.3	Prevent Syslog from accepting messages from the network	MiscellaneousDaemons.syslog_localonly	
1.6.4	Disable XDMCP port	MiscellaneousDaemons.xaccess	
1.6.5	Set default-lock screensaver timeout	HP_UX.screensaver_timeout	
1.6.6	Configure IPFilter to allow only select communication		
1.6.7	Restrict at/cron to authorized users	AccountSecurity.cronuser, AccountSecurity.atuser	
1.6.8	Restrict crontab file permissions	AccountSecurity.crontabs_file	
1.6.9	Restrict root logins to system console	AccountSecurity.create_securetty	
1.6.10	Set retry limit for account lockout	This occurs as a side-effect of trusted system conversion.	Bastille sets this only upon conversion to trusted mode.
1.6.11	Disable “nobody”	MiscellaneousDaemons.nobody_secur	

	access for secure RPC	e_rpc	
1.7	Logging		
1.7.1	Enable kernel-level auditing	AccountSecurity.system_auditing	
1.7.2	Enable logging from inetd	SecureInetd.log_inetd	
1.7.3	Turn on additional logging for FTP daemon		
1.8	User Accounts and Environment		
1.8.1	Block system accounts	AccountSecurity.block_system_accounts	
1.8.2	Verify that there are no accounts with empty password fields	AccountSecurity.lock_account_nopasswd	
1.8.3	Set account expiration parameters on active accounts	AccountSecurity. PASSWORD_MAXDAYS AccountSecurity. PASSWORD_MINDAYS AccountSecurity. PASSWORD_WARNDAYS	
1.8.4	Set strong password enforcement policies	AccountSecurity. PASSWORD_HISTORY_DEPTH AccountSecurity. MIN_PASSWORD_LENGTH	Does not enforce minimum number of special characters, numbers or upper/lower case.
1.8.5	Verify no legacy '+' entries exist in passwd and group files	MiscellaneousDaemons.nis_client	
1.8.6	No '.' or group/world-writable directory in root $PATH	AccountSecurity.root_path	
1.8.7	User home directories should be mode 750 or more restrictive	AccountSecurity.restrict_home	
1.8.8	No user dot-files should be group/world writable	AccountSecurity.user_dot_files	
1.8.9	Remove user .netrc, .rhosts and .shosts files	AccountSecurity.user_rc_files	
1.8.10	Set default umask for users	AccountSecurity.umask	027
1.8.11	Set "mesg n" as default for all users	AccountSecurity.mesgn	Default setting in at least 11iv2
1.9.0	Warning Banners		
1.9.1	Create warning banners for terminal-session logins	SecureInetd.banners	
1.9.2	Create warning banners for GUI logins	HP_UX.gui_banner	

Appendix E: HP-UX Bastille configuration entries

The following HP-UX Bastille configuration entries specify lockdown actions that align with the CIS recommendations as described in the CIS Compliance Summary table in the preceding appendix. The same items are included in a default config file (`CIS.config`) bundled with HP-UX Bastille version 3.1.01 and later. Note that users should always refer to the `CIS.config` file that comes with their version of HP-UX Bastille as implementation details may evolve.

```
AccountSecurity.ABORT_LOGIN_ON_MISSING_HOMEDIR="N"
AccountSecurity.MIN_PASSWORD_LENGTH="7"
AccountSecurity.NOLOGIN="N"
AccountSecurity.NUMBER_OF_LOGINS_ALLOWEDyn="N"
AccountSecurity.PASSWORD_HISTORY_DEPTH="10"
AccountSecurity.PASSWORD_HISTORY_DEPTHyn="Y"
AccountSecurity.PASSWORD_MAXDAYS="91"
AccountSecurity.PASSWORD_MINDAYS="7"
AccountSecurity.PASSWORD_WARNDAYS="28"
AccountSecurity.SU_DEFAULT_PATHyn="N"
AccountSecurity.atuser="Y"
AccountSecurity.block_system_accounts="Y"
AccountSecurity.create_securetty="Y"
AccountSecurity.crontabs_file="Y"
AccountSecurity.cronuser="Y"
AccountSecurity.gui_login="Y"
AccountSecurity.hidepasswords="Y"
AccountSecurity.lock_account_nopasswd="Y"
AccountSecurity.mesgn="Y"
AccountSecurity.passwordpolicies="Y"
AccountSecurity.restrict_home="Y"
AccountSecurity.root_path="Y"
AccountSecurity.serial_port_login="Y"
AccountSecurity.single_user_password="N"
AccountSecurity.system_auditing="Y"
AccountSecurity.umask="077"
AccountSecurity.umaskyn="Y"
AccountSecurity.unowned_files="Y"
AccountSecurity.user_dot_files="Y"
AccountSecurity.user_rc_files="Y"
Apache.chrootapache="N"
Apache.deactivate_hpws_apache="Y"
DNS.chrootbind="N"
FTP.ftpusers="Y"
FilePermissions.world_writeable="Y"
HP_UX.gui_banner="Y"
HP_UX.mail_config="N"
HP_UX.ndd="Y"
HP_UX.other_tools="N"
HP_UX.restrict_swacls="N"
HP_UX.scan_ports="N"
HP_UX.screensaver_timeout="Y"
HP_UX.stack_execute="Y"
HP_UX.tcp_isn="Y"
IPFilter.configure_ipfilter="N"
MiscellaneousDaemons.configure_ssh="Y"
MiscellaneousDaemons.diagnostics_localonly="N"
MiscellaneousDaemons.disable_bind="Y"
MiscellaneousDaemons.disable_ptydaemon="Y"
MiscellaneousDaemons.disable_pwgrd="N"
MiscellaneousDaemons.disable_rbootd="Y"
MiscellaneousDaemons.disable_smbclient="Y"
MiscellaneousDaemons.disable_smbserver="Y"
MiscellaneousDaemons.nfs_client="Y"
MiscellaneousDaemons.nfs_core="Y"
MiscellaneousDaemons.nfs_server="Y"
MiscellaneousDaemons.nis_client="Y"
MiscellaneousDaemons.nis_server="Y"
MiscellaneousDaemons.nisplus_client="Y"
MiscellaneousDaemons.nisplus_server="Y"
MiscellaneousDaemons.nobody_secure_rpc="N"
MiscellaneousDaemons.snmpd="Y"
MiscellaneousDaemons.syslog_localonly="Y"
MiscellaneousDaemons.xaccess="Y"
Patches.spc_cron_run="N"
Patches.spc_proxy_yn="N"
Patches.spc_run="Y"
Printing.printing="Y"
SecureInetd.banners="Y"
SecureInetd.deactivate_bootp="Y"
SecureInetd.deactivate_builtin="Y"
SecureInetd.deactivate_dttools="Y"
SecureInetd.deactivate_finger="Y"
SecureInetd.deactivate_ftp="Y"
SecureInetd.deactivate_ident="Y"
SecureInetd.deactivate_ktools="Y"
SecureInetd.deactivate_ntalk="Y"
SecureInetd.deactivate_printer="Y"
SecureInetd.deactivate_recserv="Y"
SecureInetd.deactivate_rquotad="Y"
SecureInetd.deactivate_rtools="Y"
SecureInetd.deactivate_swat="N"
SecureInetd.deactivate_telnet="Y"
SecureInetd.deactivate_tftp="Y"
SecureInetd.deactivate_time="Y"
SecureInetd.deactivate_uucp="Y"
SecureInetd.ftp_logging="N"
SecureInetd.inetd_general="Y"
SecureInetd.log_inetd="Y"
SecureInetd.owner="its owner"
Sendmail.sendmailcron="Y"
Sendmail.sendmaildaemon="Y"
Sendmail.vrfyexpn="N"
```

Appendix F: References

The Center for Internet Security

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

“Internet Express” Open-Source Software Collection (ex: 11iv2)
http://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUXIEXP1123

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 G: Change History

Version	Date	Changes
1.5.0	9/17/2009	- Added Bastille Configuration that represents Benchmark guidance to Appendix. - Updated format. - Updated to cover HP-UX 11i Update 4 - Resolved defects in audit/remediation scripts. - Added clarifying procedures for audit and remediation sections.
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	--	--