the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Solaris 10 11/06 through 10/09

Version 5.0.0
July 9th, 2010

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

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 Solaris 10 11/06 through 10/09,* was specifically designed to address the recommended security settings included in Solaris 10 11/06 (Update 3) through Solaris 10 10/09 (Update 8) running on *x86 or SPARC* platforms. The Solaris 10 operating system (Solaris 10 OS) was originally released in March 2005 and has since undergone several updates. While many of the controls discussed in this document were available in earlier versions of the Solaris OS, some of the functionality discussed may not be present in those older versions. This guide was tested against *Solaris 10 10/09* as installed using the SUNWCXall "Entire Distribution Plus OEM" software installation cluster. 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.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to 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 incorporate *Solaris 10* on a x86 or SPARC platform.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Authors
Carole Fennelly
Jonathan Klein

Maintainers
Carole Fennelly

Contributors and Reviewers
Wilfred Artman, *Independent Contractor*
Mike Bamford
Nelson Benitez
Vladimir Bogodist, *IT Security Specialist*
Glenn Brunette, *Oracle Corporation*
Chris Cook, CISSP, *Cable & Wireless Worldwide*
Blake Frantz, *Center for Internet Security*
Filip Francis
Ian J Hunt, *Global Crossing, GCTO*
John Jenkinson
Jason Mackanick, *DISA FSO*
David Pollard, *NASA DFRC*
Douglas J Schmidt
Damian Southard

The CIS community also extends thanks to the Defense Information Systems Agency (DISA) Field Security Office (FSO) for contributing their Solaris 10 Update 7 configuration baseline for use in the development of this benchmark.

The CIS community also extends thanks to those that contributed to previous versions of this Benchmark:

Adam Montville, Andrew Gilmore, John Banghart, Christopher Calabrese, Dave Shackleford, David A. Kennel, Glenn Brunette, Hal Pomeranz, Hoang Truong Dinh, Jason Mackanick, Jay Beale, Joel Kirch, Joe Wulf, John Traenkenschuh, Keith Buck, Larry Cole, Mark Phillips, Nancy Whitney, Ralph Durkee, Randy Young, Timothy Wood, Tom Maloy, Tom Rhodes, 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. Text that is typed by the user will appear in **`bold-face courier`** while responses from the system will be displayed in `non-bold courier`.
`Monospace font`	Used for inline code, commands, or examples. Interpret text 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
- do 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:

- are intended for environments or use cases where security is paramount
- acts as defense in depth measure
- may negatively inhibit the utility or performance of the technology

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.

Identification Table

The Identification Table identifies the areas to which an item applies. The identifiers for this table are as follows:

- Configuration Level. This identifier notes the configuration level associated with this benchmark item.
- Hardware Platform. This identifier is used to list all the hardware platforms to which the action applies.
- OS Default. This identifier specifies if the recommended action or setting corresponds to the default configuration as set by the vendor.
- Zone Support. This identifier specifies if the action applies to all zones (global and non-global) or the global zone only.
- Reboot Required. This identifier specifies whether a system restart is needed in order for the recommended setting to take effect.
- Solaris Security Toolkit. This identifier specifies how the Solaris Security Toolkit can be used to address implement the recommended action or setting.
- Scorable Item. This identifier denotes whether the CIS Scoring Tool should attempt to determine whether a system is compliant with an item.

Assumptions and Recommendations

OS Platform

The recommendations and actions described in this document are based upon a complete Solaris OS installation using the SUNWCXall ("Entire Distribution Plus OEM") software installation cluster. Therefore, some actions may not apply to systems that have been installed with other installation clusters or fewer software packages.

System State

It is recommended that all actions be applied when the system is in a "quiet" state – one in which application and third party software and services are not active. Hardening services that may be used by running applications can have unpredictable results. If possible perform the actions when the system is running in "single user mode".

Test Actions

It is strongly recommended that all actions be first executed on a test or non-critical system before being performed on a production server. While the actions described in this document have been tested, there is no way to predict with certainty how they will affect a given environment.

Shell Environment

The actions listed in this document are written with the assumption that they will be executed by the *root* user running the `/sbin/sh` shell and without `noclobber` set.

Order of Operations

The actions listed in this document are written with the assumption that they will be executed in the order presented here. Some actions may need to be modified if the order is changed. Actions are written so that they may be copied directly from this document into a *root* shell window with a "cut-and-paste" operation.
Organizations wanting a more structured and repeatable process are encouraged to consider the Solaris Security Toolkit, a freely available and supported tool for both configuring and validating the security configuration of the Solaris OS. Always be sure to download the most recent version of this tool, including any patches, to take advantage of the latest functionality.
For more information on this tool, see http://www.sun.com/software/security/jass/

Backup Key Files

Before performing the steps of this benchmark it is **strongly recommended** that administrators at least make backup copies their system configuration as critical files will be modified by recommended actions listed in this document. If this step is not performed, then the site may have no reasonable back-out strategy for reversing system modifications made as a result of this document. It is preferable to perform a complete system backup to ensure that nothing is missed.

Create `/opt/CIS` Directory (optional)

This benchmark includes a number of scripts to help the administrator implement the recommendations listed in this benchmark. These scripts are provided as-is with no implied warranty. It is strongly recommended that they be reviewed and modified to suit the organization's particular needs. The scripts are designed to be installed in a directory named /opt/CIS which must be created as follows (note the instruction to remove /opt/CIS if it already exists to ensure it contains only the latest files. This command will fail if it does not already exist):

```
# rm –rf /opt/CIS
# mkdir –m 700 /opt/CIS/
```

To install the scripts, copy the downloaded tar file to /opt/CIS and run the following command:

```
# tar xvf CIS_Sol10_scripts.tar
```

This will create two directories under /opt/CIS: audit and remediation.

Benchmark Items

1. Install Updates, Patches and Additional Software

Updating the operating system by applying software updates and patches is the first step for ensuring the security and reliability of the system. Vendors 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. Oracle's recommended patching strategy is covered in the document "Solaris Patch Management: Recommended Strategy" available from http://www.sun.com/bigadmin/patches/solaris/index.jsp

1.1 Use the Latest OS Release

Configuration Level	Level-I
Hardware Platform	All
OS Default	N/A
Zone Support	N/A
Reboot Required	Yes
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
Periodically, Oracle releases updates to the Solaris 10 operating system to support new hardware platforms, deliver new functionality as well as the bundle together a set of patches that can be tested as a unit.

Rationale:
Newer updates may contain security enhancements that would not be available through the standard patching process. As a result, it is recommended that the latest update of the Solaris 10 OS software be used to take advantage of the latest functionality. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

Remediation:
Obtain and install the latest update of the Solaris 10 OS software.

Audit:

1. Run the following command to determine the current OS level:

```
# head -1 /etc/release
```

References:

1. For more information on each of the Solaris 10 updates, see the "Solaris 10 What's New" documentation collection at: http://docs.sun.com/app/docs/doc/817-0547?l=en

1.2 Apply Latest OS Patches

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	Yes
Solaris Security Toolkit	Use the Finish script, install-recommended-patches.fin, to install the Solaris Recommended and Security Patch Cluster
Scorable Item	No

Description:
During the patch cluster installation process, administrators may ignore individual patches that fail to install returning either code 2 (indicates that the patch has already been installed on the system) or code 8 (the patch applies to an operating system package which is not installed on the machine). If a patch install fails with any other return code, consult the patch installation log in `/var/sadm/install_data`.
Note that in addition to installing the Patch Clusters as described above, administrators may wish to also check the `Solaris<osrel>.PatchReport` file (available from the same FTP site as the patch clusters) for additional security or functionality patches that may be required on the local system. Administrators are also encouraged to check the individual `README` files provided with each patch for further information and post-install instructions. Automated tools for maintaining current patch levels are also available, such as the Oracle Patch Manager tool ("`man smpatch`" for more info).

Note that best practices recommend verifying the integrity of downloaded software and patches using file or package signatures. Failure to do so may result in the system being compromised by a "Trojan Horse" created by an attacker with unauthorized access to the archive site. Oracle provides digital signatures for its patches.

Rationale:
Installing the latest available patches provides protection from exploitation of known vulnerabilities that have been patched.

Remediation:
Create a directory to extract the patches. Make sure this directory is owned by *root* and mode `755`, such as `/var/tmp/patches`. Obtain OraclePatch Cluster from http://sunsolve.sun.com/show.do?target=patches/patch-access and look for the Recommended Patch Clusters. The downloaded file will, by default, be named

<osrel>_Recommended.zip, where <osrel> is the Solaris OS release number. Download the Patch Cluster into /var/tmp/patches using the following commands:

```
# mkdir /var/tmp/patches
# chmod 755 /var/tmp/patches
# cd /var/tmp/patches
```

Once the patch cluster is downloaded, extract and install the patches using the following commands:

```
# unzip -qq *_Recommended.zip
# cd *_SunAlert_Patch_Cluster
# ./installcluster --<passcode>
# cd ..
# rm -rf *_Recommended*
```

The <passcode> may be found in the patch cluster README file and is required to ensure the README has been read.

Audit:
Automated tools for maintaining current patch levels are available, such as the Oracle Patch Manager tool ("man smpatch" for more info). There are also a number of auditing tools that are designed to check for patch levels.

References:

1. Solaris Patches and Updates
   http://sunsolve.sun.com/show.do?target=patches/patch-access

2. For more information on signed patches, see:
   http://sunsolve.sun.com/search/document.do?assetkey=1-9-229051-1.

3. Solaris Patch Management Strategy
   http://docs-pdf.sun.com/817-0574-12/817-0574-12.pdf
4. Solaris Patch Testing Overview
   http://sunsolve.sun.com/search/document.do?assetkey=1-9-81064-1

5. Oracle Software Update Entitlement Policy for Solaris
   http://sunsolve.sun.com/search/document.do?assetkey=1-9-203648-1

6. How to Use Solaris Live Upgrade to Install Patches
   http://www.sun.com/bigadmin/sundocs/articles/lu-patch.jsp

1.3 Install Solaris Encryption Kit

Configuration Level	Level-I

Hardware Platform	All
OS Default	Yes (Solaris 10 8/07 or newer only)
Zone Support	Global Zone Only
Reboot Required	Yes
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
The Solaris 10 Encryption Kit contains kernel modules that implement various encryption algorithms for IPsec and Kerberos, utilities that encrypt and decrypt files from the command line, and libraries with functions that application programs call to perform encryption. The Encryption Kit enables larger key sizes (> 128) of the following algorithms:

AES (128, 192, and 256-bit key sizes)
Blowfish (32 to 448-bit key sizes in 8-bit increments)
RCFOUR/RC4 (8 to 2048-bit key sizes)

Please see the documentation included with the package for more information.
Regulations on the export of encryption software are subject to change
This action is not needed for systems running Solaris 10 08/07 and newer as the Solaris 10 Encryption Kit is installed by default. Do not use this software download on systems running Solaris 10 08/07 or newer versions of the operating system.

Rationale:
Stronger encryption algorithms aid in protecting data from unauthorized access or disclosure.

Remediation:
For Solaris 10 11/06 or older versions of the Solaris OS, obtain the Solaris 10 Encryption Kit from https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_SMI-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=Sol10-GA-Encryption-G-F@CDS-CDS_SMI

After downloading the software, to implement this action, execute the following commands:

```
# unzip -qq sol-10-encrypt-GA-iso.zip
# lofiadm -a `pwd`/sol-10-encrypt-GA.iso /dev/lofi/1
# mount -F hsfs -o ro /dev/lofi/1 /mnt
```

Note that the device returned in the step above is the one to be used in the next step.

```
# mount -F hsfs -o ro /dev/lofi/1 /mnt
# cd /mnt/Encryption_10/`uname -p`/Packages
# pkgadd -d . all
[respond to pkgadd questions]
```

```
# cd
# umount /mnt
# lofiadm -d /dev/lofi/1
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# pkgchk SUNWcry
# pkgchk SUNWcryr
```

Note: If you are installing the Encryption Kit on Solaris 10 11/06 or older versions of the Solaris OS, the package will also install `SUNWcryman`. On newer versions, the manual pages are included in the system manual pages by default.

References:

1. For current information, please follow the links to Export Information at: http://www.sun.com/sales/its/index.html
2. This weblog describes strong encryption in Solaris 10: http://blogs.sun.com/bubbva/entry/strong_encryption_included_with_solaris

2. Restrict Services

While applying system updates and patches (see Items 1.1 and 1.2 above) helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited. The actions in this section of the document provide guidance on what services can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system.

2.1 Establish a Secure Baseline

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Implemented by the `sysidcfg/Solaris_10/sysidcfg` file along with the `install-local-syslog.fin` file.
Scorable Item	Yes

Description:
Starting with Solaris 10 11/06, Oracle has provided an option for new installations to install the system as "Secure By Default (SBD)." Use of this installation option provides a

secure system base in which the only network service that is enabled for remote access is Secure Shell (`ssh`) Some services, such as `sendmail`(1M) and `syslogd`(1M), are enabled for local connections only. Users who are upgrading to this release or who wish to establish a secure baseline may invoke the SBD settings by running the `netservices`(1M) command. SBD settings will not be reversed by applying patches.

Rationale:
The best defense against a service being exploited is to disable it. Disabling unnecessary services reduces the attack surface.

Remediation:
To establish a hardened OS baseline as recommended by Oracle, run the `netservices` (1M) command as follows:

```
# netservices limited
```

Note: At present, there is a known bug that prevents webconsole from refreshing after "`netservices limited`" is run:

6555726 svc:/system/webconsole SMF service doesn't have a refresh method

Until a patch is available, this bug requires that an extra step be performed to restart the webconsole as follows:

```
# svcadm restart svc:/system/webconsole:console
```

Audit:
To see what services are being listened on, type the following command and see if the listening services are bound to the Loopback interface:

```
# netstat –an | grep LISTEN
```

Portscanning tools also be used to verify that unnecessary TCP and UDP services have been disabled.

2.2 Disable Unnecessary Local Services

The "`netservices limited`" command reduces the network-accessible attack surface of Solaris by disabling the majority of services that listened for network connections in previous releases of the Solaris OS. Several services are not disabled, but rather are placed into a 'local only' mode where they will accept connections only if they originate from the local system itself. This was done to strike a balance between security and out of the box usability. If these services are not required, it is recommended that they too be disabled to guard against potential exploit by users and services that are operating locally on the system.

2.2.1 Disable Local CDE ToolTalk Database Server

Configuration Level	Level-I
Hardware Platform	All
OS Default	No (this is set to local only by section 2.1)
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the update-inetd-conf.fin Finish script with the default service list defined by the variable, JASS_SVCS_DISABLE (from finish.init).
Scorable Item	Yes

Description:
The ToolTalk service enables independent CDE applications to communicate with each other without having direct knowledge of each other. Applications create and send ToolTalk messages to communicate with each other. The ToolTalk service receives these messages, determines the recipients, and then delivers the messages to the appropriate applications.

Rationale:
Unless your organization is specifically using the ToolTalk service, disable it. The best defense against a service being exploited is to disable it.

Remediation:
To disable the ToolTalk service, run the following command:

```
# svcadm disable svc:/network/rpc/cde-ttdbserver:tcp
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/rpc/cde-ttdbserver:tcp
disabled
```

2.2.2 Disable Local CDE Calendar Manager

Configuration Level	Level-I
Hardware Platform	All
OS Default	No (this is set to local only by section 2.1)
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the update-inetd-conf.fin Finish script with the default service list defined by the variable, JASS_SVCS_DISABLE (from

	finish.init).
Scorable Item	Yes

Description:
CDE Calendar Manager is an appointment and resource scheduling tool. CDE Calendar Manager can help you schedule and keep track of your daily appointments. Upon request, Calendar Manager can send you reminders in advance of your appointments.
If you place the CDE Calendar Manager in local only mode, users on other computers will not be able to attach to the system calendar manager and look at the local user's calendar.

Rationale:
Unless your organization is specifically using the CDE Calendar Manager service, disable it.

Remediation:
To disable the CDE Calendar Manager service, run the following command:

```
# svcadm disable svc:/network/rpc/cde-calendar-manager:default
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/rpc/cde-calendar-manager:default
disabled
```

2.2.3 Disable Local Graphical Login Environment

Configuration Level	Level-I
Hardware Platform	All
OS Default	No (this is set to local only by section 2.1)
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-dtlogin.fin Finish script.
Scorable Item	Yes

Description:
The CDE login service provides the capability of logging into the system using an X-windows type interface from the console. If XDMCP remote session access to a machine is not required at all, but graphical login access for the console is required, leave the service in local-only mode. If there is no requirement for graphical services on the console, disable this service. Run this command from the command-line interface as disabling it will kill any active graphical sessions.
CDE login manager is just one of two available in the Solaris OS, the other being the GNOME Display Manager which is not enabled by default in Solaris.

Rationale:

Unless your organization specifically requires graphical login access from the console, disable it.

Remediation:
To disable graphical login access from the console, run the following command:

```
# svcadm disable svc:/application/graphical-login/cde-login
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/application/graphical-login/cde-login
disabled
# svcs -Ho state svc:/application/gdm2-login
disabled
```

2.2.4 Disable Local sendmail Service

Configuration Level	Level-I
Hardware Platform	All
OS Default	No (this is set to local only by section 2.1)
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-sendmail.fin Finish script.
Scorable Item	No

Description:
If `sendmail` is set to local only mode, users on remote systems cannot connect to the `sendmail` daemon. This eliminates the possibility of a remote exploit attack against `sendmail`. Leaving `sendmail` in local-only mode permits mail to be sent out from the local system. If the local system will not be processing or sending any mail, disable the `sendmail` service. If you disable `sendmail` for local use, messages sent to the `root` account, such as for `cron` job output or audit daemon warnings, will fail to be delivered properly. Another solution often used is to disable sendmail's local-only mode and to have a `cron` job process all mail that is queued on the local system and send it to a relay host that is defined in the `sendmail.cf` file. It is recommended that sendmail be left in local-only mode unless there is a specific requirement to disable it.

Rationale:
Most systems can safely keep sendmail in local-only mode, but those who do not want it to run in any capacity can disable it as described in this section.

Remediation:
To disable sendmail for local use, run the following command:

```
# svcadm disable svc:/network/smtp:sendmail
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/smtp:sendmail
disabled
```

References:

- Please refer to http://sendmail.org for more information on sendmail.

2.2.5 Disable Local Web Console

Configuration Level	Level-I
Hardware Platform	All
OS Default	No (this is set to local only by section 2.1)
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-smcwebserver.fin Finish script.
Scorable Item	Yes

Description:
The Java Web Console (`smcwebserver`(1M)) provides a common location for users to access web-based system management applications.

Rationale:
If there is no need to use web based management applications, disable this service**.**

Remediation:
Perform the following to disable the Java Web Console:

```
# svcadm disable svc:/system/webconsole:console
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/system/webconsole:console
disabled
```

2.2.6 Disable Local WBEM

Configuration Level	Level-I
Hardware Platform	All
OS Default	No (this is set to local only by section 2.1)
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-wbem.fin Finish script.

Scorable Item	Yes

Description:
Web-Based Enterprise Management (WBEM) is a set of management and Internet technologies. Solaris WBEM Services software provides WBEM services in the Solaris OS, including secure access and manipulation of management data. The software includes a Solaris platform provider that enables management applications to access information about managed resources such as devices and software in the Solaris OS. WBEM is used by the Solaris Management Console (SMC).

Rationale:
If your site does not use Web-Based Enterprise Management, disable this service.

Remediation:
To disable Web-Based Enterprise Management, run the following command:

```
# svcadm disable svc:/application/management/wbem
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/application/management/wbem
disabled
```

2.2.7 Disable Local BSD Print Protocol Adapter

Configuration Level	Level-I
Hardware Platform	All
OS Default	No (this is set to local only by section 2.1)
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-lp.fin Finish script.
Scorable Item	Yes

Description:
RFC 1179 describes the Berkeley system based line printer protocol. The service is used to control local Berkeley system based print spooling. It listens on port 515 for incoming print jobs. Secure by default limits access to the line printers by only allowing print jobs to be initiated from the local system. If the machine does not have locally attached printers, disable this service. Note that this service is not required for printing to a network printer.
Note:
In Solaris 10, Update 8, this service is disabled by `netservices limited` if the service `svc:/application/print/server` is disabled.

Rationale:
If your site does not use local Berkeley system based print spooling, disable this service.

Remediation:

To disable local Berkeley system based print spooling, run the following command:

```
# svcadm disable svc:/application/print/rfc1179
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/application/print/rfc1179
disabled
```

2.3 Disable Other Services

The "`netservices limited`" command disables a majority of services, but there are some not touched by the SBD setting that can be disabled if they are not required. It is also important to confirm that an unnecessary service has not been either explicitly or inadvertently enabled by a system administrator.

2.3.1 Disable RPC Encryption Key

Configuration Level	Level-I
Hardware Platform	All
OS Default	No, but disabled by Item "Establish a Secure Baseline"
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-rpc.fin Finish script.
Scorable Item	Yes

Description:
The `keyserv` process is only required for sites that are using Oracle's Secure RPC mechanism. The most common uses for Secure RPC on Solaris machines are NIS+ and "secure NFS", which uses the Secure RPC mechanism to provide higher levels of security than the standard NFS protocols. Do not confuse "secure NFS" with sites that use Kerberos authentication as a mechanism for providing higher levels of NFS security. "Kerberized" NFS does not require the `keyserv` process to be running.

Rationale:
The `keyserv` process is only required for sites that are using Oracle's Secure RPC mechanism. If you are not using Oracle's Secure RPC mechanism, disable this service.

Remediation:
To disable the `keyserv` process, run the following command:

```
# svcadm disable svc:/network/rpc/keyserv
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/rpc/keyserv
disabled
```

2.3.2 Disable NIS Server Daemons

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-nis-server.fin Finish script.
Scorable Item	Yes

Description:
These daemons are only required on systems that are acting as an NIS server for the local site. Typically there are only a small number of NIS servers on any given network. These services are disabled by default unless the system has been previously configured to act as a NIS server.

Rationale:
NIS server daemons are disabled by default and users are encouraged to use LDAP in place of NIS.

Remediation:
No action is necessary to disable NIS server daemons unless they have been specifically enabled by the administrator. If so, they may be disabled using the following commands:

```
# svcadm disable svc:/network/nis/server
# svcadm disable svc:/network/nis/passwd
# svcadm disable svc:/network/nis/update
# svcadm disable svc:/network/nis/xfr
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/nis/server
disabled
# svcs -Ho state svc:/network/nis/passwd
disabled
# svcs -Ho state svc:/network/nis/update
disabled
# svcs -Ho state svc:/network/nis/xfr
disabled
```

2.3.3 Disable NIS Client Daemons

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes, unless NIS was configured at or after system installation time.
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-nis-client.fin Finish script.
Scorable Item	Yes

Description:
If the local site is not using the NIS naming service to distribute system and user configuration information, this service may be disabled. This service is disabled by default unless the NIS service has been configured on the system.

Rationale:
NIS client daemons are disabled by default and users are encouraged to use LDAP in place of NIS.

Remediation:
No action is necessary to disable NIS client daemons unless they have been specifically enabled by the administrator. If so, they may be disabled using the following command:

```
# svcadm disable svc:/network/nis/client
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/nis/client
disabled
```

2.3.4 Disable NIS+ Daemons

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes, unless NIS+ was configured at or after system installation time.
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-nisplus-server.fin Finish script.
Scorable Item	Yes

Description:

NIS+ was designed to be a more secure version of NIS. However, the use of NIS+ has been deprecated by Oracle and customers are encouraged to use LDAP as an alternative naming service. This service is disabled by default unless the NIS+ service has been configured on the system.

Rationale:
NIS+ is disabled by default and users are encouraged to use LDAP in place of NIS+.

Remediation:
No action is necessary to disable NIS+ daemons unless they have been specifically enabled by the administrator. If so, they may be disabled using the following command:

```
# svcadm disable svc:/network/rpc/nisplus
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/rpc/nisplus
disabled
```

2.3.5 Disable LDAP Cache Manager

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes, unless LDAP was configured at or after system installation time.
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-ldap-client.fin Finish script.
Scorable Item	Yes

Description:
If the local site is not currently using LDAP as a naming service, there is no need to keep LDAP-related daemons running on the local machine. This service is disabled by default unless LDAP client services have been configured on the system. If a naming service is required, users are encouraged to use LDAP instead of NIS/NIS+.

Rationale:
Unless your organization specifically requires a naming service, disable it.

Remediation:
No action is necessary to disable the LDAP cache manager unless it has been specifically enabled by the administrator. To disable the LDAP cache manager, run the following command:

```
# svcadm disable svc:/network/ldap/client
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/ldap/client
disabled
```

2.3.6 Disable Kerberos TGT Expiration Warning

Configuration Level	Level-I
Hardware Platform	All
OS Default	No, but set to "local only" by Item "Establish a Secure Baseline"
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the update-inetd-conf.fin Finish script with the default service list defined by the variable, JASS_SVCS_DISABLE (from finish.init).
Scorable Item	Yes

Description:
While Kerberos can be a security enhancement, if the local site is not currently using Kerberos then there is no need to have the Kerberos TGT expiration warning enabled.

Rationale:
Unless your organization specifically requires uses Kerberos, disable it.

Remediation:
To disable the Kerberos TGT expiration warning, run the following command:

```
# svcadm disable svc:/network/security/ktkt_warn
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/security/ktkt_warn
disabled
```

2.3.7 Disable Generic Security Services (GSS) Daemons

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the update-inetd-conf.fin Finish script with the default service list defined by the variable, JASS_SVCS_DISABLE (from finish.init).
Scorable Item	Yes

Description:
The GSS API is a security abstraction layer that is designed to make it easier for developers to integrate with different authentication schemes. It is most commonly used in applications for sites that use Kerberos for network authentication, though it can also allow applications to interoperate with other authentication schemes.

Note:
Since this service uses Oracle's standard RPC mechanism, it is important that the system's RPC portmapper (`rpcbind`) also be enabled when this service is turned on. This daemon will be taken offline if `rpcbind` is disabled. For more information see Item 2.3.14.

Rationale:
GSS does not expose anything external to the system as it is configured to use TLI (protocol = `ticotsord`) by default. However, unless your organization is using the GSS API, disable it.

Remediation:
To disable the GSS API, run the following command:

```
# svcadm disable svc:/network/rpc/gss
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/rpc/gss
disabled
```

2.3.8 Disable Volume Manager

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone only
Reboot Required	No
Solaris Security Toolkit	Use the disable-vold.fin Finish script along with the update-inetd-conf.fin Finish script with the default service list defined by the variable, JASS_SVCS_DISABLE (from finish.init).
Scorable Item	Yes

Description:
The volume manager automatically mounts external devices for users whenever the device is attached to the system. These devices include CD-R, CD-RW, floppies, DVD, USB and 1394 mass storage devices. See the `vold` (1M) manual page for more details.
Note:

Since this service uses Oracle's standard RPC mechanism, it is important that the system's RPC portmapper (`rpcbind`) also be enabled when this service is turned on. For more information see Item 2.3.14 Disable Local RPC Port Mapping Service

Rationale:
Allowing users to mount and access data from removable media devices makes it easier for malicious programs and data to be imported onto your network. It also introduces the risk that sensitive data may be transferred off the system without a log record. Another alternative is to edit the `/etc/vold.conf` file and comment out any removable devices that you do not want users to be able to mount.

Remediation:
To disable `vold`, run the following command:

```
# svcadm disable svc:/system/filesystem/volfs
# svcadm disable svc:/network/rpc/smserver
```

Note:
`rmformat(1)` and the CDE Filemanager are `rpc.smserverd` clients. If you need to support these services, but still want to disable `vold`, then do not disable `smserver` in the action above.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/system/filesystem/volfs
disabled
# svcs -Ho state svc:/network/rpc/smserver
disabled
```

2.3.9 Disable Samba Support

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-samba.fin Finish script.
Scorable Item	Yes

Description:
Solaris includes the popular open source Samba server for providing file and print services to Windows-based systems. This allows a Solaris 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. Note that on Solaris releases prior to 11/06 the file `/etc/sfw/smb.conf` does not exist and the service will not be started by default even on newer releases.

Rationale:
Samba has been known to have security issues. If this functionality is not required by the site, disable this service.

Remediation:
To disable Samba, run the appropriate command for your Solaris OS level:

Solaris 10 <= 11/06

```
# /etc/init.d/samba stop
# mv /etc/sfw/smb.conf /etc/sfw/smb.conf.CIS
```

Solaris 10 >= 8/07

```
# svcadm disable svc:/network/samba
```

Audit:
Perform the following to determine if the system is configured as recommended:

Solaris 10 <= 11/06

```
# pgrep smbd
# ls -l /etc/sfw/smb.conf
/etc/sfw/smb.conf: No such file or directory
```

Solaris 10 >= 8/07

```
# svcs -Ho state svc:/network/samba
disabled
```

2.3.10 Disable `automount` Daemon

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-automount.fin Finish script
Scorable Item	Yes

Description:
The `automount` daemon is normally used to automatically mount NFS file systems from remote file servers when needed. However, the `automount` daemon can also be configured to mount local (loopback) file systems as well, which may include local user home directories, depending on the system configuration. Sites that have local home directories configured via the `automount` daemon in this fashion will need to ensure that this daemon is running for Oracle's Solaris Management Console administrative interface to function properly. If the `automount` daemon is not running, the mount points created by SMC will not be mounted.
Note:

Since this service uses Oracle's standard RPC mechanism, it is important that the system's RPC portmapper (`rpcbind`) also be enabled when this service is turned on. For more information see Item 2.3.14 Disable Local RPC Portmapping Service.

Rationale:
If there is no need to use `automount`, disable it.

Remediation:
To disable the `automount` daemon, run the following command:

```
# svcadm disable svc:/system/filesystem/autofs
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/system/filesystem/autofs
disabled
```

2.3.11 Disable Apache Services

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-apache2.fin Finish script.
Scorable Item	Yes

Description:
The action in this section describes disabling the Apache 1.x and 2.x web servers provided with Solaris 10. Both services are disabled by default. Run control scripts for Apache 1 and the NCA web servers still exist, but the services will only be started if the respective configuration files have been set up appropriately, and these configuration files do not exist by default.

Even if the system is a Web server, the local site may choose not to use the Web server provided with Solaris 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.

Rationale:
Unless your organization specifically requires Apache services, disable it.

Remediation:
To disable Apache, run the appropriate command for the version installed:

Apache 1.x:

```
# /etc/init.d/apache stop
# mv /etc/apache/httpd.conf /etc/apache/httpd.conf.CIS
```

Apache 2.x:

```
# svcadm disable svc:/network/http:apache2
```

Audit:
Perform the following to determine if the system is configured as recommended:

Apache 1.x:

```
# pgrep httpd
# ls /etc/apache/httpd.conf
/etc/apache/httpd.conf: No such file or directory
```

Apache 2.x:

```
# svcs -Ho state svc:/network/http:apache2
disabled
```

References:

1. Apache Benchmark and scoring tool from CIS, http://www.cisecurity.org/bench_apache.html,
2. Apache Foundation's "Security Tips" document http://httpd.apache.org/docs-2.0/misc/security_tips.html

2.3.12 Disable Solaris Volume Manager Services

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone only
Reboot Required	No

Solaris Security Toolkit	Use the update-inetd-conf.fin Finish script and add the following to the JASS_SVCS_DISABLE service list:
	`svc:/system/metainit:default`
	`svc:/platform/sun4u/mpxio-upgrade:default`
	`svc:/system/mdmonitor:default`
	This is included in the cis-secure.driver Toolkit driver.

Scorable Item	Yes

Description:
The Solaris Volume Manager, formerly known as Solstice DiskSuite, provides functionality for managing disk storage, disk arrays, etc. However, many systems without large storage arrays do not require that these services be enabled or may be using an alternate volume

manager rather than the bundled SVM functionality. This service is disabled by default in the OS.

Rationale:
Unless your organization specifically requires the Solaris Volume Manager, disable this service.

Remediation:
To disable the Solaris Volume Manager, run the following commands:

```
# svcadm disable svc:/system/metainit
# svcadm disable svc:/system/mdmonitor
```

In addition, run the appropriate command for the Solaris 10 level that you are running:

Solaris 10 <= 11/06

```
# svcadm disable svc:/platform/sun4u/mpxio-upgrade
```

Solaris 10 >= 8/07

```
# svcadm disable svc:/system/device/mpxio-upgrade
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/system/metainit
disabled
# svcs -Ho state svc:/system/mdmonitor
disabled
```

Solaris 10 <= 11/06

```
# svcs -Ho state svc:/platform/sun4u/mpxio-upgrade
disabled
```

Solaris 10 >= 8/07

```
# svcs -Ho state svc:/system/device/mpxio-upgrade
disabled
```

2.3.13 Disable Solaris Volume Manager GUI

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone only
Reboot Required	No
Solaris Security Toolkit	Use the update-inetd-conf.fin Finish script with the default service list defined by the

	variable, JASS_SVCS_DISABLE (from finish.init).
Scorable Item	Yes

Description:
The Solaris Volume Manager, formerly Solstice DiskSuite, provides software RAID capability for Solaris systems. This functionality can either be controlled via the GUI administration tools provided with the operating system, or via the command line. However, the GUI tools cannot function without several daemons listed in Item 2.3.12 Disable Solaris Volume Manager Services enabled. If you have disabled Solaris Volume Manager Services, also disable the Solaris Volume Manager GUI.
Note:
Since these services use Oracle's standard RPC mechanism, it is important that the system's RPC portmapper (`rpcbind`) also be enabled when these services are turned on. For more information see Item 2.3.14 Disable Local RPC Port Mapping Service.

Rationale:
Since the same functionality that is in the GUI is available from the command line interface, administrators are strongly urged to leave these daemons disabled and administer volumes directly from the command line.

Remediation:
To disable the GUI administration tools for the Solaris Volume Manager, run the following commands:

```
# svcadm disable svc:/network/rpc/mdcomm
# svcadm disable svc:/network/rpc/meta
# svcadm disable svc:/network/rpc/metamed
# svcadm disable svc:/network/rpc/metamh
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/rpc/mdcomm
disabled
# svcs -Ho state svc:/network/rpc/meta
disabled
# svcs -Ho state svc:/network/rpc/metamed
disabled
# svcs -Ho state svc:/network/rpc/metamh
disabled
```

2.3.14 Disable Local RPC Port Mapping Service

Configuration Level	Level-I
Hardware Platform	All
OS Default	No (this is set to local only by section 2.1)
Zone Support	All

Reboot Required	No
Solaris Security Toolkit	Use the disable-rpc.fin Finish script.
Scorable Item	Yes

Description:
Remote Procedure Calls (RPC) is used by many services within the Solaris 10 operating system. Some of these services allow external connections to use the service (e.g. NFS, NIS).

Rationale:
RPC-based services are typically deployed to use very weak or non-existent authentication and yet may share very sensitive information. Unless one of the services 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.

Remediation:
To disable local RPC port mapping service, run the following command:

```
# svcadm disable svc:/network/rpc/bind
```

If you want to restrict access to this service, but not disable it completely, consider using a host-based firewall such as `ipfilter(5)` to control what hosts are allowed to access this daemon. Alternatively, TCP Wrappers support can be enabled in the daemon with the commands:

```
# svccfg -s svc:/network/rpc/bind setprop \
      config/enable_tcpwrappers = true
# svcadm refresh rpc/bind
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/rpc/bind
disabled
```

2.4 Configure TCP Wrappers

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot required	No
Solaris Security Toolkit	Use the enable-tcpwrappers.fin Finish script and the file templates in Files/etc/hosts.allow and Files/etc/hosts.deny.
Scorable Item	Yes

Description:
TCP Wrappers is a host-based access control system that allows administrators to control who has access to various network services based on the IP address of the remote end of the connection. TCP Wrappers also provide logging information via `syslog` about both successful and unsuccessful connections. Rather than enabling TCP Wrappers for all services with "`inetadm -M ...`", the administrator has the option of enabling TCP Wrappers for individual services with "`inetadm -m` *<svcname>* `tcp_wrappers=TRUE`", where *<svcname>* is the name of the specific service that uses TCP Wrappers.

Rationale:

TCP Wrappers provides more granular control over which systems can access services which limits the attack vector. The logs show attempted access to services from non-authorized systems, which can help identify unauthorized access attempts.

Remediation:
To enable TCPWrappers, run the following commands:

1. Create `/etc/hosts.allow`:

```
# echo "ALL: <net>/<mask>, <net>/<mask>, …" \
>/etc/hosts.allow
```

where each *<net>/<mask>* combination (for example, "`192.168.1.0/255.255.255.0`") represents one network block in use by your organization that requires access to this system.

2. Create `/etc/hosts.deny`:

```
# echo "ALL: ALL" >/etc/hosts.deny
```

3. Update default policy with `inetadm`:

```
# inetadm -M tcp_wrappers=TRUE
```

Note that the above actions will only provide filtering on standard TCP-based services that are spawned by `inetd`. To protect UDP and RPC-based services that are spawned from `inetd`, consider implementing a host-based firewall such as ipfilter ("`man ipf`" for further information). The versions of SSH and `sendmail` that ship with Solaris 10 will automatically use TCP Wrappers to filter access if a hosts.allow or hosts.deny file exists. Also, the command "`svccfg -s rpc/bind setprop config/enable_tcpwrappers=true`" will enable TCP Wrappers for the `rpc/bind` service.

Audit:
To verify that tcp_wrappers is enabled, run the following command and verify that the value is set to TRUE:

```
# inetadm -p | grep tcp_wrappers
tcp_wrappers=TRUE
# ls /etc/hosts.deny
/etc/hosts.deny
```

```
# ls /etc/hosts.allow
/etc/hosts.allow
```

3. Kernel Tuning

This section describes additional measures that may be taken to provide protection on the kernel level.

3.1 Restrict Core Dumps to Protected Directory

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the enable-coreadm.fin Finish script.
Scorable Item	Yes

Description:
The action described in this section creates a protected directory to store core dumps and also causes the system to create a log entry whenever a regular process dumps core.

Rationale:
Core dumps, particularly those from set-UID and set-GID processes, may contain sensitive data.

Remediation:
To restrict core files to a protected directory, run the following commands:

```
# mkdir -p /var/cores
# chown root:root /var/cores
# chmod 700 /var/cores
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
        -e log -e global -e global-setid \
        -d process -d proc-setid
```

If the local site chooses, dumping of core files can be completely disabled with the following command:

```
# coreadm -d global -d global-setid -d process \
-d proc-setid
```

Audit:
Run the `coreadm` command to verify the settings match the output shown below:

```
# coreadm
```

```
     global core file pattern: /var/cores/core_%n_%f_%u_%g_%t_%p
     global core file content: default
       init core file pattern: core
       init core file content: default
            global core dumps: enabled
       per-process core dumps: disabled
      global setid core dumps: enabled
 per-process setid core dumps: disabled
     global core dump logging: enabled
```

3.2 Enable Stack Protection

Configuration Level	Level-I
Hardware Platform	SPARC, AMD (w/NX), Intel (w/XD)
OS Default	No
Zone Support	Global zone only
Reboot Required	Yes
Solaris Security Toolkit	Use the enable-stack-protection.fin Finish script.
Scorable Item	Yes

Description:
Buffer overflow exploits have been the basis for many highly publicized compromises and defacements of large numbers of Internet connected systems. Many of the automated tools in use by system attackers exploit well-known buffer overflow problems in vendor-supplied and third-party software.

Rationale:
Enabling stack protection prevents certain classes of buffer overflow attacks and is a significant security enhancement. However, this does not protect against buffer overflow attacks that do not execute code on the stack (such as `return-to-libc` exploits).

Remediation:
To enable stack protection, run the following commands to edit the /etc/system file:

```
# if [ ! "`grep noexec_user_stack= /etc/system`"]; then
    cat <<END_CFG >>/etc/system
* Attempt to prevent and log stack-smashing attacks
set noexec_user_stack=1
set noexec_user_stack_log=1

END_CFG
fi
```

Note:
A reboot is necessary for this change to take effect.

Audit:

Run the following command and ensure that the output is as shown:

```
# grep "^set noexec_user_stack=1" /etc/system
set noexec_user_stack=1
# grep "^set noexec_user_stack_log=1" /etc/system
set noexec_user_stack_log=1
# echo "noexec_user_stack/D" | mdb -k
noexec_user_stack:
noexec_user_stack:                  1
```

References:

1. Solaris Non-Executable Stack Overview (Part 1)
   http://blogs.sun.com/gbrunett/entry/solaris_non_executable_stack_overview
2. Solaris Non-Executable Stack Continues (Part 2)
   http://blogs.sun.com/gbrunett/entry/solaris_non_executable_stack_continued
3. Solaris Non-Executable Stack Concluded (Part 3)
   http://blogs.sun.com/gbrunett/entry/solaris_non_executable_stack_concluded

3.3 Enable Strong TCP Sequence Number Generation

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the enable-rfc1948.fin Finish script.
Scorable Item	Yes

Description:
The variable `TCP_STRONG_ISS` sets the mechanism for generating the order of TCP packets. If an attacker can predict the next sequence number, it is possible to inject fraudulent packets into the data stream to hijack the session. Solaris supports three sequence number methods:

0 = Old-fashioned sequential initial sequence number generation.
1 = Improved sequential generation, with random variance in increment.
2 = RFC 1948 sequence number generation, unique-per-connection-ID.

Rationale:
The RFC 1948 method is widely accepted as the strongest mechanism for TCP packet generation. This makes remote session hijacking attacks more difficult, as well as any other network-based attack that relies on predicting TCP sequence number information. It is theoretically possible that there may be a small performance hit in connection setup time when this setting is used, but there are no benchmarks that establish this.

Remediation:

Run the following commands to set `TCP_STRONG_ISS` to use RFC 1948 sequence number generation:

```
# cd /etc/default
# awk '/TCP_STRONG_ISS=/ { $1 = "TCP_STRONG_ISS=2" }; \
{ print }' inetinit > inetinit.new
# mv inetinit.new inetinit
# pkgchk -f -n -p /etc/default/inetinit
# ndd -set /dev/tcp tcp_strong_iss 2
```

Audit:
Run the following command and verify that the output is as shown:

```
# ndd -get /dev/tcp tcp_strong_iss
2
```

3.4 Modify Network Parameters

Network device drivers have parameters that can be set to provide stronger security settings, depending on environmental needs. This section describes modifications to network parameters for IP, ARP and TCP.

Note:
The items that are Solaris 10 defaults include:
`ip_forward_directed_broadcasts`
`ip_forward_src_routed`
`ip6_forward_src_routed`
`ip_respond_to_timestamp`
`ip_respond_to_timestamp_broadcast`
`ip_respond_to_address_mask_broadcast`
`ip6_send_redirects`
`tcp_rev_src_routes`

The items that are NOT Solaris 10 defaults include:
`arp_cleanup_interval`
`ip_ire_arp_interval`
`ip_ignore_redirect`
`ip6_ignore_redirect`
`ip_respond_to_echo_broadcast`
`ip_strict_dst_mutihoming`
`ip6_strict_dst_multihoming`
`ip_send_redirects`
`tcp_conn_req_max_q0`
`tcp_conn_req_max_q`
`tcp_extra_priv_ports_add`

The settings described in this section meet most functional needs while providing additional security against common network attacks. However, it is important to understand the needs of your particular environment to determine if these settings are appropriate for you.

Note that we are creating a new script that will be executed at boot time to reconfigure the network parameters described in this section. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. The `cis_netconfig.sh` script that follows is a compilation of all the network parameter settings in this section. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Oracle is moving away from legacy run control scripts in `/etc/init.d` in favor of using SMF services.

Remediation:

```
cat > cis_netconfig.sh << END
#!/sbin/sh
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip6_forward_src_routed 0
ndd -set /dev/tcp tcp_rev_src_routes 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/tcp tcp_conn_req_max_q0 4096
ndd -set /dev/tcp tcp_conn_req_max_q 1024
ndd -set /dev/ip ip_respond_to_timestamp 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
ndd -set /dev/ip ip6_respond_to_echo_multicast 0
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
ndd -set /dev/arp arp_cleanup_interval 60000
ndd -set /dev/ip ip_ire_arp_interval 60000
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip6_ignore_redirect 1
ndd -set /dev/tcp tcp_extra_priv_ports_add 6112
ndd -set /dev/ip ip_strict_dst_multihoming 1
ndd -set /dev/ip ip6_strict_dst_multihoming 1
ndd -set /dev/ip ip_send_redirects 0
ndd -set /dev/ip ip6_send_redirects 0


END
chmod +x cis_netconfig.sh
```

Place the script in `/lib/svc/method`.
Appendix B contains a script to create an SMF service to run all the network commands described in the following sub-sections. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
cp cis_netconfig.sh /lib/svc/method
chmod 750 /lib/svc/method/cis_netconfig.sh
svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date. A description for each network parameter seeting is included in the following sections.

Audit:
The following subsections have an audit point for each of these items. For convenience, they are summarized in this section. Run the following commands and verify that the output is as shown.

```
# ndd -get /dev/ip ip_forward_src_routed
0
# ndd -get /dev/ip ip6_forward_src_routed
0
# ndd -get /dev/tcp tcp_rev_src_routes
0
# ndd -get /dev/ip ip_forward_directed_broadcasts
0
# ndd -get /dev/tcp tcp_conn_req_max_q0
4096
# ndd -get /dev/tcp tcp_conn_req_max_q
1024
# ndd -get /dev/ip ip_respond_to_timestamp
0
# ndd -get /dev/ip ip_respond_to_timestamp_broadcast
0
# ndd -get /dev/ip ip_respond_to_address_mask_broadcast
0
# ndd -get /dev/ip ip_respond_to_echo_multicast
0
# ndd -get /dev/ip ip6_respond_to_echo_multicast
0
# ndd -get /dev/ip ip_respond_to_echo_broadcast
0
# ndd -get /dev/arp arp_cleanup_interval
60000
# ndd -get /dev/ip ip_ire_arp_interval
60000
# ndd -get /dev/ip ip_ignore_redirect
1
# ndd -get /dev/ip ip6_ignore_redirect
1
# ndd -get /dev/tcp tcp_extra_priv_ports
2049
# ndd -get /dev/ip ip_strict_dst_multihoming
1
# ndd -get /dev/ip ip6_strict_dst_multihoming
1
# ndd -get /dev/ip ip_send_redirects
0
# ndd -get /dev/ip ip6_send_redirects
0
```

3.4.1 Disable Source Packet Forwarding

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_forward_src_routed` and `ip6_forward_src_routed` parameters control whether IPv4/IPv6 forwards packets with source IPv4/IPv6 routing options
Rationale:
Keep this parameter disabled to prevent denial of service attacks through spoofed packets.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

IPv4:
```
# ndd -set /dev/ip ip_forward_src_routed 0
```

IPv6:
```
# ndd -set /dev/ip ip6_forward_src_routed 0
```

Note:
These settings will NOT persist between reboots.
Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following commands and verify that the output is as shown:

IPv4:

```
# ndd -get /dev/ip ip_forward_src_routed
0
```

IPv6:

```
# ndd -get /dev/ip ip6_forward_src_routed
0
```

3.4.2 Disable Broadcast Packet Forwarding

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_forward_directed_broadcasts` parameter controls whether or not Solaris forwards broadcast packets for a specific network if it is directly connected to the machine.

Rationale:
The default value of 1 causes Solaris to forward broadcast packets. An attacker could send forged packets to the broadcast address of a remote network, resulting in a broadcast flood. Setting this value to 0 prevents Solaris from forwarding these packets. Note that disabling this parameter also disables broadcast pings.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/ip ip_forward_directed_broadcasts 0
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/ip ip_forward_directed_broadcasts
0
```

3.4.3 Disable Response to ICMP Timestamp Requests

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_respond_to_timestamp` parameter controls whether or not to respond to ICMP timestamp requests.

Rationale:
Reduce attack surface by restricting a vector for host discovery.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots,

which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/ip ip_respond_to_timestamp 0
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/ip ip_respond_to_timestamp
0
```

Reference:
1. http://capec.mitre.org/data/definitions/295.html

3.4.4 Disable Response to ICMP Broadcast Timestamp Requests

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_respond_to_timestamp_broadcast` parameter controls whether or not to respond to ICMP broadcast timestamp requests.

Rationale:

Reduce attack surface by restricting a vector for bulk host discovery.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/ip ip_respond_to_timestamp_broadcast
0
```

Reference:
1. http://capec.mitre.org/data/definitions/295.html

3.4.5 Disable Response to ICMP Netmask Requests

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone and non-global zones configured with exclusive IP stacks

Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_respond_to_address_mask_broadcast` parameter controls whether or not to respond to ICMP netmask requests, typically sent by diskless clients when booting.

Rationale:
An attacker could use the netmask information to determine network topology. The default value is 0.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/ip ip_respond_to_address_mask_broadcast
0
```

3.4.6 Disable ICMPv6 Redirect Messages

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip6_send_redirects` parameter controls whether or not IPv6 sends out ICMPv6 redirect messages.

Rationale:
A malicious user can exploit the ability of the system to send ICMP redirects by continually sending packets to the system, forcing the system to respond with ICMP redirect messages, resulting in an adverse impact on the CPU and performance of the system.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/ip ip6_send_redirects 0
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/ip ip6_send_redirects
0
```

3.4.7 Disable Response to Broadcast ICMPv4 Echo Request

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_respond_to_echo_broadcast` parameter controls whether or not IPv4 responds to a broadcast ICMPv4 echo request.

Rationale:
Responding to echo requests verifies that an address is valid, which can aid attackers in mapping out targets. ICMP echo requests are often used by network monitoring applications.

Remediation:
If required, configure tcp_wrappers (section 2.4) to restrict host access.
Otherwise, see the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

Note:

These settings will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/ip ip_respond_to_echo_broadcast
0
```

3.4.8 Disable Response to Multicast Echo Request

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip6_respond_to_echo_multicast` and `ip_respond_to_echo_multicast` parameters control whether or not IPv6 or IPv4 responds to a multicast IPv6 or IPv4 echo request.

Rationale:
Responding to multicast echo requests verifies that an address is valid, which can aid attackers in mapping out targets.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once

imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

IPv4:

```
# ndd -set /dev/ip ip_respond_to_echo_multicast 0
```

IPv6:

```
# ndd -set /dev/ip ip6_respond_to_echo_multicast 0
```

Note:
These settings will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following commands and verify that the output is as shown:

IPv4:

```
# ndd -get /dev/ip ip_respond_to_echo_multicast
0
```

IPv6:

```
# ndd -get /dev/ip ip6_respond_to_echo_multicast
0
```

3.4.9 Set Interval for Scanning IRE_CACHE

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No

Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_ire_arp_interval` parameter determines the intervals in which Solaris scans the IRE_CACHE (IP Resolved Entries) and deletes entries that are more than one scan old. This interval is used for solicited arp entries, not un-solicited which are handled by arp_cleanup_interval.

Rationale:
This helps mitigate ARP attacks (ARP poisoning). Consult with your local network team for additional security measures in this area, such as using static ARP, or fixing MAC addresses to switch ports.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/ip ip_ire_arp_interval 60000
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/ip ip_ire_arp_interval
60000
```

3.4.10 Ignore ICMP Redirect Messages

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_ignore_redirect` and `ip6_ignore_redirect` parameters determine if redirect messages will be ignored. ICMP redirect messages cause a host to re-route packets and could be used in a DoS attack. The default value for this is 0. Setting this parameter to 1 causes redirect messages to be ignored.

Rationale:
IP redirects should not be necessary in a well-designed, well maintained network. Set to a value of 1 if there is a high risk for a DoS attack. Otherwise, the default value of 0 is sufficient.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

IPv4:
```
# ndd -set /dev/ip ip_ignore_redirect 1
```

IPv6:
```
# ndd -set /dev/ip ip6_ignore_redirect 1
```

Note:
These settings will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

IPv4:

```
# ndd -get /dev/ip ip_ignore_redirect
1
```

IPv6:

```
# ndd -get /dev/ip ip6_ignore_redirect
1
```

3.4.11 Set Strict Multihoming

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_strict_dst_multihoming` and `ip6_strict_dst_multihoming` parameters determines whether a packet arriving on a non -forwarding interface can be accepted for an IP address that is not explicitly configured on that interface. If ip_forwarding is enabled, or xxx:ip_forwarding (where xxx is the interface name) for the appropriate interfaces is enabled, then this parameter is ignored because the packet is actually forwarded.

Rationale:
Set this parameter to 1 for systems that have interfaces that cross strict networking domains (for example, a firewall or a VPN node) .

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

IPv4:
```
# ndd -set /dev/ip ip_strict_dst_multihoming 1
```

IPv6:
```
# ndd -set /dev/ip ip6_strict_dst_multihoming 1
```

Note:
These settings will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

IPv4:
```
# ndd -get /dev/ip ip_strict_dst_multihoming
1
```

IPv6:
```
# ndd -get /dev/ip ip6_strict_dst_multihoming
1
```

3.4.12 Disable ICMPv4 Redirect Messages

Configuration Level	Level-I

Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `ip_send_redirects` parameter controls whether or not IPv4 sends out ICMPv4 redirect messages.

Rationale:
A malicious user can exploit the ability of the system to send ICMP redirects by continually sending packets to the system, forcing the system to respond with ICMP redirect messages, resulting in an adverse impact on the CPU performance of the system.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/ip ip_send_redirects 0
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.
Audit:

To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/ip ip_send_redirects
0
```

3.4.13 Set ARP Cleanup Interval

Configuration Level	Level-I
Hardware Platform	All
OS Default	300000
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `arp_cleanup_interval` parameter controls the length of time, in milliseconds, that an unsolicited Address Resolution Protocal (ARP) request remains in the ARP cache.

Rationale:
If unsolicited ARP requests are allowed to remain in the ARP cache for long periods an attacker could fill up the ARP cache with bogus entries. Set this parameter to 60000 ms (1 minute) to reduce the effectiveness of ARP attacks. The default value is 300000.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/arp arp_cleanup_interval 60000
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
```

```
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following commands and verify that the output is as shown:

```
# ndd -get /dev/arp arp_cleanup_interval
60000
```

3.4.14 Disable TCP Reverse IP Source Routing

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `tcp_rev_src_routes` parameter determines if TCP reverses the IP source routing option for incoming connections. If set to 0, TCP does not reverse IP source. If set to 1, TCP does the normal reverse source routing. The default setting is 0.

Rationale:
If IP source routing is needed for diagnostic purposes, enable it. Otherwise leave it disabled.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/tcp tcp_rev_src_routes 0
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/tcp tcp_rev_src_routes
0
```

3.4.15 Set Maximum Number of Half-open TCP Connections

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `tcp_conn_req_max_q0` parameter determines how many half-open TCP connections can exist for a port. This setting is closely related with `tcp_conn_req_max_q.`

Rationale:
It is necessary to control the number of completed connections to the system to provide some protection against Denial of Service attacks. Note that the value of 4096 is a minimum to establish a good security posture for this setting. In environments where connections numbers are high, such as a busy webserver, this value may need to be increased.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file

cis_netconfig.xml is an SMF manifest for the cis_netconfig service. Once imported into the SMF database, the cis_netconfig.sh script will run on every system reboot to set the network parameters appropriately. Shown below is the ndd command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in /lib/svc/method.

```
# ndd -set /dev/tcp tcp_conn_req_max_q0 4096
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the cis_netconfig.sh script will be executed and the appropriate network parameters will be updated. Store the file in /var/svc/manifest/site if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following commands and verify that the output is as shown:

```
# ndd -get /dev/tcp tcp_conn_req_max_q0
4096
```

3.4.16 Set Maximum Number of Incoming Connections

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:

The tcp_conn_req_max_q parameter determines the maximum number of incoming connections that can be accepted on a port. This setting is closely related with tcp_conn_req_max_q0.

Rationale:
Restricting the number of "half open" connections limits the damage of DOS attacks where the attacker floods the network with "SYNs". Having this split from the tcp_conn_req_max_q parameter allows the administrator some discretion in this area. Note that the value of 1024 is a minimum to establish a good security posture for this setting. In environments where connections numbers are high, such as a busy webserver, this value may need to be increased.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file cis_netconfig.xml is an SMF manifest for the cis_netconfig service. Once imported into the SMF database, the cis_netconfig.sh script will run on every system reboot to set the network parameters appropriately. Shown below is the ndd command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in /lib/svc/method.

```
# ndd -set /dev/tcp tcp_conn_req_max_q 1024
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the cis_netconfig.sh script will be executed and the appropriate network parameters will be updated. Store the file in /var/svc/manifest/site if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/tcp tcp_conn_req_max_q
1024
```

3.4.17 Lock down `dtspcd(8)`

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.
Scorable Item	Yes

Description:
The `tcp_extra_priv_ports_add` parameter adds a non privileged port to the privileged port list.

Rationale:
Lock down `dtspcd(8)` (CDE Subprocess Control Service). This optional service is seldom used. It has historically been associated with malicious scans. Making it a privileged port prevents users from opening up the service on a Solaris machine.

Remediation:
See the notes in Item 3.4 Modify Network Parameters regarding a master script that will be executed at boot time to reconfigure various network parameters. The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` script will run on every system reboot to set the network parameters appropriately. Shown below is the `ndd` command that controls this particular parameter, but it does not persist between system reboots, which is the reason for creating the master script. Edit the script for the particular needs of your organization and place the script in `/lib/svc/method`.

```
# ndd -set /dev/tcp tcp_extra_priv_ports_add 6112
```

Note:
This setting will NOT persist between reboots.

Appendix B contains a script to create an SMF service to run the commands. If the SMF service is created as described in Appendix B execute the following command for it to take effect:

```
# cp cis_netconfig.sh /lib/svc/method
# chmod 750 /lib/svc/method/cis_arp_netconfig.sh
# svccfg import cis_netconfig.xml
```

When the service is enabled or system is rebooted, the `cis_netconfig.sh` script will be executed and the appropriate network parameters will be updated. Store the file in `/var/svc/manifest/site` if it has to be re-imported into the system at a later date.

Audit:
To verify the correct network parameter settings, run the following command and verify that the output is as shown:

```
# ndd -get /dev/tcp tcp_extra_priv_ports
2049
```

3.5 Disable Network Routing

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes if a default router was specified during or after system installation. If no default router was specified, then routing services are enabled by default.
Zone Support	Global zone and non-global zones configured with exclusive IP stacks
Reboot Required	No
Solaris Security Toolkit	Use the disable-routing.fin Finish script.
Scorable Item	Yes

Description:
The network routing daemon, `in.routed`, manages network routing tables. If enabled, it periodically supplies copies of the system's routing tables to any directly connected hosts and networks and picks up routes supplied to it from other networks and hosts.

Rationale:
Routing Internet Protocol (RIP) is a legacy protocol with a number of security issues (e.g. no authentication, no zoning, and no pruning).
Routing (in.routed) is disabled by default in all Solaris 10 systems, if there is a default router defined. If no default gateway is defined during system installation, network routing is enabled.

Remediation:
Run the following commands to disable routing. This action is unnecessary unless it was manually enabled by the administrator or the system was previously used as a network gateway.

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -d ipv4-routing -d ipv6-routing
# routeadm -u
```

Audit:
Run the following commands and compare the results with those shown below to determine if network routing has been enabled:

```
# routeadm -p |\
  egrep "^ipv[46]-routing |^ipv[46]-forwarding" |\
      awk '{ printf("%s %s\n", $1, $NF); }'
ipv4-routing current=disabled
ipv6-routing current=disabled
ipv4-forwarding current=disabled
ipv6-forwarding current=disabled
```

4. Logging

The items in this section describe enabling various different forms of system logging to track system activity. Tools such as Swatch (http://swatch.sourceforge.net/) can be used to automatically monitor logs for intrusion attempts and other suspicious system behavior. Note that these tools are not officially supported by Oracle and that log formats and messages used by these tools may be added or changed in patches, updates and new releases.

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 via an encrypted connection. 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). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized 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.sun.com/blueprints and http://www.ntp.org.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

If using the Solaris Security Toolkit, run the script `set-log-file-permissions.fin` to ensure appropriate permissions of log files.

4.1 Enable inetd Connection Logging

Configuration Level	Level-I
Hardware Platform	All
OS Default	No

Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the enable-inetd-syslog.fin Finish script.
Scorable Item	Yes

Description:
The inetd process starts Internet standard services and the "tracing" feature can be used to log information about the source of any network connections seen by the daemon.

Rationale:
Rather than enabling `inetd` tracing for all services with "`inetadm -M ...`", the administrator has the option of enabling tracing for individual services with "`inetadm -m` *<svcname>* `tcp_trace=TRUE`", where *<svcname>* is the name of the specific service that uses tracing.
This information is logged via `syslogd` (1M) and is deposited by default in `/var/adm/messages` with other system log messages. If the administrator wants to capture this information in a separate file, simply modify `/etc/syslog.conf` to log `daemon.notice` to some other log file destination. For further configuration information, see 4.3 Enable Debug Level Daemon Logging.

Remediation:
Run the following commands to enable inetd connection logging:

```
# inetadm -M tcp_trace=true
# svcadm refresh svc:/network/inetd
```

Audit:
Run the following command and compare the results to determine if `inetd` connection logging is enabled:

```
# svcprop -p defaults/tcp_trace svc:/network/inetd
true
```

4.2 Enable FTP daemon Logging

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the enable-ftp-debuglog.fin Finish script.
Scorable Item	Yes (if FTP is installed)

Description:

Information about FTP sessions will be logged via `syslogd` (1M), but the system must be configured to capture these messages.

Rationale:
If the FTP daemon is installed and enabled, it is recommended that the "debugging" (`-d`) and connection logging (`-l`) flags also be enabled to track FTP activity on the system. Note that enabling debugging on the FTP daemon can cause user passwords to appear in clear-text form in the system logs, if users accidentally type their passwords at the username prompt. For further configuration information, see 4.3 Enable Debug Level Daemon Logging.

Remediation:
Run the following command to enable FTP daemon logging:

```
# inetadm -m svc:/network/ftp \
    exec="/usr/sbin/in.ftpd -a -l -d"
```

Audit:
Run the following command to ensure that FTP daemon logging is enabled:

```
# svcprop -p inetd_start/exec svc:/network/ftp
/usr/sbin/in.ftpd\ -a\ -l\ -d
```

4.3 Enable Debug Level Daemon Logging

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the install-connlog.fin Finish script.
Scorable Item	Yes

Description:
If the FTP service is installed and enabled on the system, Item 4.2 Enable FTP daemon Logging enables the "debugging" (`-d`) and connection logging (`-l`) flags to track FTP activity on the system. Similarly, the tracing (`-t`) option to `inetd` was enabled in Item 4.1 Enable inetd Connection Logging.

Rationale:
All of this information is logged by `syslogd` (1M), but `syslogd` (1M) must be configured to capture this information to a separate file so it may be more easily reviewed.

Remediation:

The commands listed below direct `syslogd` (1M), to send the log information for these services to a log file named `connlog`. Review the `connlog` file on a regular basis. It is important to note that use of the debugging option can generate very large log files.

```
# if [ ! "`grep -v '^#' /etc/syslog.conf | \
        grep /var/log/connlog`" ]; then
    echo "daemon.debug\t\t\t/var/log/connlog" \
        >>/etc/syslog.conf
fi
# touch /var/log/connlog
# chown root:root /var/log/connlog
# chmod 600 /var/log/connlog
# logadm -w connlog -C 13 -a 'pkill -HUP syslogd' \
       /var/log/connlog
# svcadm refresh svc:/system/system-log
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/system/system-log
online
# grep -v "^#" /etc/syslog.conf | grep /var/log/connlog
daemon.debug                    /var/log/connlog
```

4.4 Capture `syslog` AUTH Messages

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the install-authlog.fin Finish script.
Scorable Item	Yes

Description:
By default, Solaris systems do not capture logging information that is sent to the `LOG_AUTH` facility.

Rationale:
A great deal of important security-related information is sent via the `LOG_AUTH` facility (e.g., successful and failed `su` attempts, failed login attempts, `root` login attempts, etc.).

Remediation:
The commands below will cause information generated by the `LOG_AUTH` facility to be captured in the `/var/log/authlog` file (which is only readable by the superuser).

```
# if [ ! "`grep -v '^#' /etc/syslog.conf | \
```

```
          grep /var/log/authlog`" ]; then
    echo "auth.info\t\t\t/var/log/authlog" \
        >>/etc/syslog.conf
fi
# logadm -w authlog -C 13 -a 'pkill -HUP syslogd' \
       /var/log/authlog
# pkgchk -f -n -p /var/log/authlog
# svcadm refresh svc:/system/system-log
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/system/system-log
online
# grep -v "^#" /etc/syslog.conf | grep /var/log/authlog
auth.info               /var/log/authlog
```

4.5 Enable Login Records

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the install-loginlog.fin Finish script.
Scorable Item	Yes

Description:
If the file `/var/adm/loginlog` exists, it will capture failed login attempt messages with the login name, tty specification, and time. This file does not exist by default and must be manually created.

Rationale:
Tracking failed login attempts is critical to determine when an attacker is attempting a brute force attack on user accounts. Note that this is only for login-based such as login, telnet, rlogin, etc. and does not include SSH. Review the `loginlog` file on a regular basis.

Remediation:
Perform the following to implement the recommended state:

```
# touch /var/adm/loginlog
# chown root:sys /var/adm/loginlog
# chmod 600 /var/adm/loginlog
# logadm -w loginlog -C 13 /var/adm/loginlog
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls –l /var/adm/loginlog
-rw------- 1 root sys    0 <date> <time> /var/adm/loginlog
```

```
# grep loginlog /etc/logadm.conf
loginlog -C 13 /var/adm/loginlog
```

4.6 Capture All Failed Login Attempts

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-failed-logins.fin Finish script.
Scorable Item	Yes

Description:
The `SYS_FAILED_LOGIN` variable is used to determine how many failed login attempts occur before a failed login message is logged. Setting the value to 0 will cause a failed login message on every failed login attempt.

Rationale:
The `SYSLOG_FAILED_LOGINS` parameter in the `/etc/default/login` file is used to control how many login failures are allowed before log messages are generated—if set to zero then all failed logins will be logged.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/SYSLOG_FAILED_LOGINS=/ \
   { $1 = "SYSLOG_FAILED_LOGINS=0" }; \
   { print }' login >login.new

# mv login.new login
# pkgchk -f -n -p /etc/default/login
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^SYSLOG_FAILED_LOGINS=0" /etc/default/login
SYSLOG_FAILED_LOGINS=0
```

4.7 Enable cron Logging

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All

Reboot Required	No
Solaris Security Toolkit	Use the enable-cronlog.fin Finish script.
Scorable Item	Yes

Description:
Setting the CRONLOG parameter to YES in the `/etc/default/cron` file causes information to be logged for every `cron` job that gets executed on the system. This setting is the default for Solaris.

Rationale:
A common attack vector is for programs that are run out of `cron` to be subverted to execute commands as the owner of the `cron` job. Log data on commands that are executed out of `cron` can be found in the `/var/cron/log` file. Review this file on a regular basis.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/CRONLOG=/ { $1 = "CRONLOG=YES" }; \
                { print }' cron > cron.new
# mv cron.new cron
# pkgchk -f -n -p /etc/default/cron
# chown root:root /var/cron/log
# chmod go-rwx /var/cron/log
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^CRONLOG=YES" /etc/default/cron
CRONLOG=YES
# ls /var/cron/log
/var/cron/log
```

4.8 Enable System Accounting

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the enable-sar.fin Finish script.
Scorable Item	Yes

Description:

System accounting gathers baseline system data (CPU utilization, disk I/O, etc.) every 20 minutes. The data may be accessed with the `sar` command, or by reviewing the nightly report files named `/var/adm/sa/sar*`.

Rationale:
Once a normal baseline for the system has been established, abnormalities can be investigated to detect unauthorized activity such as CPU-intensive jobs and activity outside of normal usage hours.

Note:
The sys id must be added to /etc/cron.allow to run the system accounting commands..

Remediation:
Perform the following to implement the recommended state:

```
# svcadm enable -r svc:/system/sar
# EDITOR=ed crontab -e sys << END_ENTRIES
\$a
0,20,40 * * * * /usr/lib/sa/sa1
45 23 * * * /usr/lib/sa/sa2 -s 0:00 -e 23:59 -i 1200 -A
.
w
q
END_ENTRIES
# chown sys:sys /var/adm/sa/*
# chmod go-wx /var/adm/sa/*
```

Note:
This data is only archived for one week before being automatically removed by the regular nightly `cron` job. Administrators may wish to archive the `/var/adm/sa` directory on a regular basis to preserve this data for longer periods.
The `sys` account must be permitted to use the `cron(1M)` facility for system accounting to function properly. See Item 6.9 Restrict at/cron to Authorized Users.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/system/sar
online
# ls -l /var/adm/sa
[verify that the directory is not empty]
# crontab -l sys | grep -v "^#" | egrep '(sa1|sa2)'
0,20,40 * * * * /usr/lib/sa/sa1
45 23 * * * /usr/lib/sa/sa2 -s 0:00 -e 23:59 -i 1200 -A
```

4.9 Enable Kernel Level Auditing

Configuration Level	Level-I

Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	Yes
Solaris Security Toolkit	Use the enable-bsm.fin Finish script.
Scorable Item	Yes

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 `praudit` command. Note that enabling kernel-level auditing on Solaris disables the automatic mounting of external devices via the Solaris volume manager daemon (`vold`).

Rationale:
Kernel-level auditing can consume a large amount of disk space and even cause system performance impact, particularly on heavily used machines. The consensus settings described in this section are an effort to log interesting system events without consuming excessive amounts of resources logging significant but usually uninteresting system calls. The document *Auditing in the Solaris™ Operating Environment* published by Oracle as part of the Blueprints On-Line series contains additional information on reducing the amount of logging produced by the administrative (`ad`) audit class (see http://www.sun.com/blueprints for more details).
Note that DoD installations have much more stringent auditing requirements than those listed here. DoD guidelines require `flags:lo,ad,cc,fw,-fc,-fd,-fr` to be set in the `audit_control` file. Note that "`-fr`" in particular can cause extremely large audit trails to be generated.

Remediation:
Perform the following to implement the recommended state:

```
if [ ! "`grep c2audit:audit_load /etc/system`" ]
then

# Turn on auditing
  echo y | /etc/security/bsmconv
  cd /etc/security

# Create a CIS custom class (cc) to audit_class. Apply this class to the
# following event types in audit_event:
#
#       fm - file attribute modify
#       ps - process start/stop
#       pm - process modify
#       pc - process (meta-class)

  echo "0x08000000:cc:CIS custom class" >>audit_class
  awk 'BEGIN { FS = ":"; OFS = ":" }
     ($4 ~ /fm/) && ! ($2 ~ /MCTL|FCNTL|FLOCK|UTIME/) \
{ $4 = $4 ",cc" }
```

```
     ($4 ~ /p[cms]/) && \
     ! ($2 ~ /FORK|CHDIR|KILL|VTRACE|SETGROUPS|SETPGRP/) \
{ $4 = $4 ",cc" }
     { print }' audit_event >audit_event.new

  mv audit_event.new audit_event
# Set Audit Control parameters
# Audit Control directory - /var/audit
# User attributable event flags - login/logout, old administrative (meta
class)
#     and CIS Custom class (cc)
# Non-user attributable (cannot determine user) event flags - login/logout,
#     old administrative (meta class), exec
# Set minimum space percentage to 20% to force an audit warning.
  cat <<END_PARAMS >audit_control
dir:/var/audit
flags:lo,ad,cc
naflags:lo,ad,ex
minfree:20
END_PARAMS
# Set up Audit to monitor root for login/logout and old administrative (meta
cla
ss). Do not audit invalid class (e.g. obsolete) events.
  echo root:lo,ad:no >audit_user

# Force /usr/sbin to be prepeneded to any naked auditconfig commands

  awk '/^auditconfig/ { $1 = "/usr/sbin/auditconfig" }; \
 { print }' audit_startup >audit_startup.new

# Set the audit policy to log exec argv and environment parameters to
# the audit file
  echo '/usr/sbin/auditconfig -setpolicy +argv,arge' \
  >>audit_startup.new
  mv audit_startup.new audit_startup

# Verify and set the appropriate permissions/owner/group to the event,
control
# and startup file

  pkgchk -f -n -p /etc/security/audit_event
  pkgchk -f -n -p /etc/security/audit_control
  pkgchk -f -n -p /etc/security/audit_startup

# Add the command to have cron close the current audit file at the start of
# each day.
  EDITOR=ed crontab -e root << END_CRON
\$a
0 * * * * /usr/sbin/audit -n
.
w
q
END_CRON
fi

# Set the owner/group/permissions to /var/audit
chown root:root /var/audit/*
```

```
chmod go-rwx /var/audit/*
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# auditconfig -getcond
audit condition = auditing
# auditconfig -getpolicy
audit policies = arge,argv,cnt
# ls -l /var/audit/*.not_terminated.*
[verify that the file size is not zero and is growing as events are audited]
```

5. File/Directory Permissions/Access

File and directory permission control is one of the greatest challenges of secure system administration. This section provides guidance on how to secure system files and directories and set secure defaults for users. Guidance for monitoring user and system files on an on-going basis is provided in Section 9 System Maintenance.

5.1 Set daemon umask

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	Yes
Solaris Security Toolkit	Use the set-system-umask.fin Finish script with the JASS_UMASK variable.
Scorable Item	Yes

Description:
The `umask (1)` utility overrides the file mode creation mask as specified by the CMASK value in the `/etc/default/init` file. The most permissive file permission is mode 666 (777 for executable files). The CMASK value subtracts from this value. For example, if CMASK is set to a value of 022, files created will have a default permission of 644 (755 for executables). See the `umask (1)` manual page for a more detailed description.

Rationale:
Set the system default file creation mask (`umask`) to at least `022` to prevent daemon processes from creating world-writable files by default. The NSA and DISA recommend a more restrictive `umask` values of `077` (Note: The execute bit only applies to executable files) . This may cause problems for certain applications— consult vendor documentation for further information. The default setting for Solaris is `022`.

Note:

There are some known bugs in the following daemons that are impacted by changing the `CMASK` parameter from its default setting: (Note: Current or future patches may have resolved these issues. Consult with your Oracle Support representative)

6299083 picld i initialise picld_door file with wrong permissions after JASS

4791006 ldap_cachemgr initialise i ldap_cache_door file with wrong permissions

6299080 nscd i initialise name_service_door file with wrong permissions after JASS

The `ldap_cachemgr` issue has been fixed but the others are still unresolved. While not directly related to this, there is another issue related to `077` `umask` settings:
2125481 in.lpd failed to print files when the umask is set 077

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/^CMASK=/ { $1 = "CMASK=022" }
               { print }' init >init.new
# mv init.new init
# pkgchk -f -n -p /etc/default/init
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^CMASK=022" /etc/default/init
CMASK=022
```

5.2 Restrict Set-UID on User Mounted Devices

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone only
Reboot Required	No
Solaris Security Toolkit	Use the set-rmmount-nosuid.fin Finish script.
Scorable Item	Yes

Description:
If the volume manager (`vold`) is enabled to permit users to mount external devices, the administrator can force these file systems to be mounted with the `nosuid` option to prevent users from bringing set-UID programs onto the system via CD-ROMs, floppy disks, USB drives or other removable media.

Rationale:

Removable media is one vector by which malicious software can be introduced onto the system. The risk can be mitigated by forcing use of the `nosuid` option. Note that this setting is included in the default `rmmount.conf` file for Solaris 8 and later.

Remediation:
Perform the following to implement the recommended state:

```
# if [ ! "`grep -v "^#" /etc/rmmount.conf |\
      grep -- '-o nosuid'`" ]; then
      fs=`awk '($1 == "ident") && ($2 != "pcfs") \

            { print $2 }' /etc/rmmount.conf`

      echo mount \* $fs -o nosuid >>/etc/rmmount.conf
fi
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep -v "^#" /etc/rmmount.conf | grep – "-o nosuid" \
      /etc/rmmount.conf
# mount * hsfs ufs udfs -o nosuid
```

5.3 Set Sticky Bit on World Writable Directories

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the check-world-writable-files.aud Audit script.
Scorable Item	No

Description:
When the so-called sticky bit (set with `chmod +t`) 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).

Rationale:
Setting the sticky bit prevents users from overwriting each others files, whether accidentally or maliciously, and is generally appropriate for most world-writable directories (e.g. /tmp). However, consult appropriate vendor documentation before blindly applying the sticky bit to any world writable directories found in order to avoid breaking any application dependencies on a given directory.

Remediation:
To set the sticky bit on a directory, run the following command:

```
# chmod +t [directory name]
```

Audit:
To generate a list of world writable directories that do not have the sticky bit set execute the following commands:

```
# find / \( -fstype nfs -o -fstype cachefs \
      -o -fstype autofs -o -fstype ctfs \
      -o -fstype mntfs -o -fstype objfs \
      -o -fstype proc \) -prune -o -type d \
      \( -perm -0002 -a ! -perm -1000 \) -print
```

6. System Access, Authentication, and Authorization

Access control is a huge security issue that relies on an organization's policies and procedures to manage. The actions described in this section are just a few measures that can be taken on a system level to control access to services. It is strongly advised that organizations have a process in place to authorize access privileges and to revoke authorizations when they are no longer required.

6.1 Disable `login:` Prompts on Serial Ports

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	Global zone only
Reboot Required	No
Solaris Security Toolkit	Use the disable-serial-login.fin Finish script.
Scorable Item	Yes

Description:
The `pmadm` command provides service administration for the lower level of the Service Access Facility hierarchy and can be used to disable the ability to login on a particular port.

Rationale:
By disabling the `login:` prompt on the system serial devices, unauthorized users are limited in their ability to gain access by attaching modems, terminals, and other remote access devices to these ports. Note that this action may safely be performed even if console access to the system is provided via the serial ports, because the `login:` prompt on the console device is provided through a different mechanism.

Remediation:
Perform the following to implement the recommended state:

```
# pmadm -d -p zsmon -s ttya
# pmadm -d -p zsmon -s ttyb
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# pmadm -L | awk -F: '($4 == "ux") { print $3 }'
ttya
ttyb
```

6.2 Disable "nobody" Access for RPC Encryption Key Storage Service

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-keyserv-uid-nobody.fin Finish script.
Scorable Item	Yes

Description:
The `keyserv` process, if enabled, stores user keys that are utilized with Sun's Secure RPC mechanism.

Rationale:
The action listed prevents keyserv from using default keys for the `nobody` user, effectively stopping this user from accessing information via Secure RPC.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/ENABLE_NOBODY_KEYS=/ \
        { $1 = "ENABLE_NOBODY_KEYS=NO" }
        { print }' keyserv >keyserv.new
# mv keyserv.new keyserv
# pkgchk -f -n -p /etc/default/keyserv
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^ENABLE_NOBODY_KEYS=NO" /etc/default/keyserv
ENABLE_NOBODY_KEYS=NO
```

6.3 Configure SSH

Configuration Level	Level-I
Hardware Platform	All

OS Default	See Notes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`.

Rationale:
It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network. Most of these settings are the default in Solaris 10 with the following exceptions:

`MaxAuthTries` (default is 6)
`MaxAuthTriesLog` (default is 3)
`Banner` (commented out)
`X11Forwarding` (default is "yes")

Remediation:
The individual SSH settings are described in the following subsections. For convenience, they are all consolidated in the following script. Edit this script based on your site's particular needs.

```
#!/sbin/sh
echo "Host *" >> /etc/ssh/sshd_config
/usr/bin/awk '/^Protocol/                { $2 = "2" };   \
     /^X11Forwarding/           { $2 = "no" }; \
     /^MaxAuthTries/            { $2 = "3" };   \
     /^MaxAuthTriesLog/         { $2 = "0" };   \
     /^IgnoreRhosts/            { $2 = "yes" }; \
     /^RhostsAuthentication/    { $2 = "no" };  \
     /^RhostsRSAAuthentication/ { $2 = "no" };  \
     /^PermitRootLogin/         { $2 = "no" };  \
     /^PermitEmptyPasswords/    { $2 = "no" };  \
     /^#Banner/                 { $1 = "Banner" } \
     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

6.3.1 Set SSH Protocol to 2

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All

Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.

Rationale:
Secure Shell version 2 (SSH2) is more secure than the legacy SSH1 version, which is being deprecated.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^Protocol/                { $2 = "2" }    \

     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^Protocol"
Protocol 2
```

References:
For more information on the status of the SSH1 protocol, see the SSH web site http://www.ssh.com/company/newsroom/article/210/.

6.3.2 Disable SSH X11Forwarding

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
The `X11Forwarding` parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

Rationale:
Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled that users can may be able to install their own forwarders.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^ X11Forwarding /                { $2 = "no" }   \
     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^X11Forwarding"
X11Forwarding no
```

6.3.3 Set SSH MaxAuthTries to 3

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
The `MaxAuthTries` paramener specifies the maximum number of authentication attempts permitted per connection. The default value is 6.

Rationale:

Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^ MaxAuthTries/                { $2 = "3" }    \

     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^MaxAuthTries"
MaxAuthTries 3
```

6.3.4 Set SSH MaxAuthTriesLog to 0

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
The `MaxAuthTriesLog` parameter specifies the maximum number of failed authorization attempts before a syslog error message is generated. The default value is 3.

Rationale:
Setting this parameter to 0 ensures that every failed authorization is logged.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^ MaxAuthTriesLog/                { $2 = "0" }    \

     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
```

```
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^MaxAuthTriesLog"
MaxAuthTriesLog 0
```

6.3.5 Set SSH IgnoreRhosts to yes

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
The `IgnoreRhosts` parameter specifies that .rhosts and .shosts files will not be used in `RhostsRSAAuthentication` or `HostbasedAuthentication`.

Rationale:
Setting this parameter forces users to enter a password when authenticating with SSH.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^ IgnoreRhosts/                { $2 = "yes" }    \

     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^IgnoreRhosts"
IgnoreRhosts yes
```

6.3.6 Set SSH RhostsAuthentication to no

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
The `RhostsAuthentication` parameter specifies if authentication using rhosts or `/etc/hosts.equiv` is permitted. The default is no.

Rationale:
Rhosts authentication is insecure and should not be permitted.
Note that this parameter only applies to SSH protocol version 1.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^RhostsAuthentication/                { $2 = "no" }    \

     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^RhostsAuthentication"
RhostsAuthentication no
```

6.3.7 Set SSH RhostsRSAAuthentication to no

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
The `RhostsRSAAuthentication` parameter specifies if rhosts or `/etc/hosts.equiv` authentication together with successful RSA host authentication is permitted. The default is no.

Note that this parameter only applies to SSH protocol version 1.

Rationale:
Rhosts authentication is insecure and should not be permitted, even with RSA host authentication.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^ RhostsRSAAuthentication/                { $2 = "no" }    \

     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^RhostsRSAAuthentication"
RhostsRSAAuthentication no
```

6.3.8 Disable SSH root login

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes

Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
The `PermitRootLogin` parameter specifies if the root user can log in using `ssh(1)`. The default is no.

Rationale:
The root user must be restricted from directly logging in from any location other than the console.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^ PermitRootLogin/                { $2 = "no" }    \

     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^PermitRootLogin"
PermitRootLogin no
```

6.3.9 Set SSH PermitEmptyPasswords to no

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:

The `PermitEmptyPasswords` parameter specifies if the server allows login to accounts with empty password strings.

Rationale:
All users must be required to have a password.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^PermitEmptyPasswords/                { $2 = "no" }   \

     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^PermitEmptyPasswords"
PermitEmptyPasswords no
```

6.3.10 Set SSH Banner

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.
Scorable Item	Yes

Description:
The `Banner` parameter specifies a file whose contents must sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale:
Banners are used to warn connecting users of the particular site's policy regarding connection. Consult with your legal department for the appropriate warning banner for your site.

Remediation:
Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
# awk '/^#Banner/                 { $2 = "Banner" }    \

     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Note:
If you will be editing all the SSH parameters, use the script in section 6.3 Configure SSH.

Audit:
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep -v "^#" sshd_config | grep "^Banner"
Banner /etc/issue
```

6.4 Disable .rhosts Support in /etc/pam.conf

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-rhosts.fin Finish script.
Scorable Item	Yes

Description:
Used in conjunction with the BSD-style "r-commands" (`rlogin`, `rsh`, `rcp`), `.rhosts` files 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).

Rationale:
Disabling `.rhosts` support helps prevent users from subverting the system's normal access control mechanisms.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc
# sed -e 's/^.*pam_rhosts_auth/#&/' < /etc/pam.conf > pam.conf.new
# mv pam.conf.new pam.conf
```

```
# pkgchk -f -n -p /etc/pam.conf
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^#" /etc/pam.conf | grep "pam_rhosts_auth"
#rlogin auth sufficient         pam_rhosts_auth.so.1
#rsh    auth sufficient         pam_rhosts_auth.so.1
```

6.5 Restrict FTP Use

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the install-ftpusers.fin Finish script.
Scorable Item	Yes, if FTP is installed

Description:
If FTP is permitted to be used on the system, the file `/etc/ftpd/ftpusers` is used to specify a list of users who *are not* allowed to access the system via FTP.

Rationale:
FTP is an old and insecure protocol that transfers files and credentials in clear text and is better replaced by using `sftp` instead. However, if it is permitted for use in your environment, it is important to ensure that the default "system" accounts are not permitted to transfer files via FTP, especially the *`root`* account. Consider also adding the names of other privileged or shared accounts that may exist on your system such as user `oracle` and the account which your Web server process runs under.

Remediation:
Add the system accounts to the `/etc/ftpd/ftpusers` file as shown below:

```
# cd /etc/ftpd
# for user in adm bin daemon gdm listen lp noaccess \
      nobody nobody4 nuucp postgres root smmsp svctag \
      sys uucp webservd
do
    echo $user >> ftpusers
done
# sort -u ftpusers > ftpusers.new
# mv ftpusers.new ftpusers
# pkgchk -f -n -p /etc/ftpd/ftpusers
```

If your site policy states that users have to be authorized to use FTP, consider placing all your users in the /etc/ftpusers file and then explicitly removing those who are permitted to use the service. For example:

```
# getent passwd | cut -f1 -d":" > /etc/ftpd/ftpusers
```

This prohibits any user on the system from using ftp unless they are explicitly removed from the file. Note that this file will need to be updated as users are added to or removed from the system.

Note that the above script adds users from the local password file. If a naming service such as LDAP is being used, modify the /etc/ftpd/ftpusers file to include those users (listed in the naming service) who are prohibited from using FTP.

More granular security settings can be specified through use of the ftpservers(4), ftpaccess(4), ftpgroups(4), ftphosts(4) and ftpconversions(4) files in the /etc/ftpd directory. For more details on these files, please refer to the respective manual pages.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# for user in `awk -F: '{ print $1 }' /etc/passwd`; do
      grep -w "${user}" /etc/ftpd/ftpusers >/dev/null 2>&1
      if [ $? != 0 ]; then
            echo "User ${user} not in /etc/ftpd/ftpusers."
      fi
done
```

6.6 Set Delay between Failed Login Attempts to 4

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-failed-logins.fin Finish script.
Scorable Item	Yes

Description:
The SLEEPTIME variable in the /etc/default/login file controls the number of seconds to wait before printing the "login incorrect" message when a bad password is provided.

Rationale:
Delaying the "login incorrect" message can help to slow down brute force password-cracking attacks.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/SLEEPTIME=/ { $1 = "SLEEPTIME=4" }
     { print }' login >login.new
# mv login.new login
# pkgchk -f -n -p /etc/default/login
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^SLEEPTIME=4" /etc/default/login
SLEEPTIME=4
```

6.7 Set Default Screen Lock for CDE Users

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the enable-xscreensaver.fin Finish script.
Scorable Item	Yes, if a graphical login environment is enabled.

Description:
The default timeout for keyboard/mouse inactivity is 30 minutes before a password-protected screen saver is invoked by the CDE session manager.

Rationale:
Many organizations prefer to set the default timeout value to 10 minutes, though this setting can still be overridden by individual users in their own environment.

Remediation:
Run the following commands to set the default inactivity timeout to a value appropriate for your environment.

```
# for file in /usr/dt/config/*/sys.resources; do

      dir=`dirname $file | sed s/usr/etc/`

      mkdir -m 755 -p $dir

      echo 'dtsession*saverTimeout: 10' >>$dir/sys.resources

      echo 'dtsession*lockTimeout: 10' >>$dir/sys.resources

      chown root:sys $dir/sys.resources
```

```
      chmod 444 $dir/sys.resources
done
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# for file in /usr/dt/config/*/sys.resources; do
      dir=`dirname $file | sed s/usr/etc/`
      egrep "dtsession\*saverTimeout:" \
            $dir/sys.resources /dev/null
done
/etc/dt/config/C/sys.resources:dtsesion*saverTimeout: 10

# for file in /usr/dt/config/*/sys.resources; do
      dir=`dirname $file | sed s/usr/etc/`
      egrep "dtsession\*lockTimeout:" \
            $dir/sys.resources /dev/null
done
/etc/dt/config/C/sys.resources:dtsesion*lockTimeout: 10
```

6.8 Set Default Screen Lock for GNOME Users

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the enable-xscreensaver.fin Finish script.
Scorable Item	Yes, if a graphical login environment is enabled.

Description:
The default timeout is 30 minutes of keyboard and mouse inactivity before a password-protected screen saver is invoked by the `Xscreensaver` application used in the GNOME windowing environment.

Rationale:
Many organizations prefer to set the default timeout value to 10 minutes, though this setting can still be overridden by individual users in their own environment.

Remediation:
Perform the following to implement the recommended state:

```
# cd /usr/openwin/lib/app-defaults
# awk '/^\*timeout:/     { $2 = "0:10:00" }
     /^\*lockTimeout:/ { $2 = "0:00:00" }
     /^\*lock:/        { $2 = "True" }
     { print }' xScreenSaver >xScreenSaver.new

# mv xScreenSaver.new xScreenSaver
```

```
# pkgchk -f -n -p /usr/openwin/lib/app-defaults/xScreenSaver
```

Note:
Presently, the file `/usr/openwin/lib/app-defaults/xScreenSaver` is not marked volatile, so the `pkgchk` command produces an error for this item. The following bug has been filed in relation to this:

6255740 xScreenSaver global property file should be marked as volatile

Audit:
Perform the following to determine if the system is configured as recommended:

```
# cd /usr/openwin/lib/app-defaults
# grep "^\*timeout:" xScreenSaver
timeout:                0:15:00

# grep "^\*lockTimeout:" xScreenSaver
*lockTimeout:           0:00:00
# grep "^\*lock:" xScreenSaver
*lock:                  True
```

6.9 Restrict at/cron to Authorized Users

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the install-at-allow.fin and update-cron-deny.fin Finish scripts.
Scorable Item	Yes

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.

Rationale:
On many systems, only the system administrator needs the ability to schedule jobs.
Note that even though a given user is not listed in `cron.allow`, `cron` jobs can still be run as that user. The `cron.allow` file only controls administrative access to the `crontab` command for scheduling and modifying `cron` jobs. Much more effective access controls for the `cron` system can be obtained by using Role-Based Access Controls (RBAC).
Note that if System Accounting is enabled in Item 4.8 Enable System Accounting, add the user `sys` to the `cron.allow` file in addition to the `root` account.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/cron.d
# mv cron.deny cron.deny.cis
# mv at.deny at.deny.cis
# echo root > cron.allow
# cp /dev/null at.allow
# chown root:root cron.allow at.allow
# chmod 400 cron.allow at.allow
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls /etc/cron.d/cron.deny
/etc/cron.d/cron.deny: No such file or directory
# ls /etc/cron.d/at.deny
/etc/cron.d/at.deny: No such file or directory
# cat /etc/cron.d/cron.allow
root
# cat /etc/cron.d/at.allow
[there should be no output]
```

References:

1. System Administration Guide: Security Services
   http://docs.sun.com/app/docs/doc/816-4557/prbac-1?a=view
2. RBAC in the Solaris Operating Environment
   http://www.sun.com/software/whitepapers/wp-rbac/wp-rbac.pdf

6.10 Restrict `root` Login to System Console

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-remote-root-login.fin Finish script.
Scorable Item	Yes

Description:
Privileged access to the system via the `root` account must be accountable to a particular user. The system console is supposed to be protected from unauthorized access and is the only location where it is considered acceptable to permit the `root` account to login directly, in the case of system emergencies. This is the default configuration for Solaris.

Rationale:

Use an authorized mechanism such as RBAC, the `su` command or the freely available `sudo` package to provide administrative access through unprivileged accounts. These mechanisms provide at least some limited audit trail in the event of problems.
Note that in addition to the configuration steps included here, there may be other login services (such as SSH in Item 6.3 Configure SSH) that require additional configuration to prevent `root` logins via these services.

A more secure practice is to make `root` a "role" instead of a user account. Role Based Access Control (RBAC) is similar in function to `sudo`, but provides better logging ability and additional authentication requirements. With `root` defined as a role, administrators would have to login under their account and provide `root` credentials to invoke privileged commands. This restriction also includes logging in to the console, except for single user mode.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/CONSOLE=/ { print "CONSOLE=/dev/console"; next }; \
                { print }' login >login.new
# mv login.new login
# pkgchk -f -n -p /etc/default/login
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^CONSOLE=/dev/console" /etc/default/login
CONSOLE=/dev/console
```

References:

1. SPOTD: The Guide Book to Solaris Role-Based Access Control http://blogs.sun.com/security/entry/spotd_the_guide_book_to
2. SPOTD: The 5 Cent Tour of Solaris Role-Based Access Control : http://blogs.sun.com/security/entry/slotd_the_5_cent_tour

6.11 Set Retry Limit for Account Lockout

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the enable-account-lockout.fin Finish script.
Scorable Item	Yes

Description:
The `RETRIES` parameter is the number of failed login attempts a user is allowed before being disconnected from the system and forced to reconnect. When

LOCK_AFTER_RETRIES is set in /etc/security/policy.conf, then the user's account is locked after this many failed retries (the account can only be unlocked by the administrator using the command:passwd -u *<username>*

Rationale:
Setting these values helps discourage brute force password guessing attacks.
The action specified here sets the lockout limit at 3, which complies with NSA and DISA recommendations. This may be too restrictive for some operations with large user populations.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/RETRIES=/ { $1 = "RETRIES=3" }
     { print }' login >login.new
# mv login.new login
# pkgchk -f -n -p /etc/default/login

# cd /etc/security
# awk '/LOCK_AFTER_RETRIES=/ \
        { $1 = "LOCK_AFTER_RETRIES=YES" }
     { print }' policy.conf >policy.conf.new
# mv policy.conf.new policy.conf
# pkgchk -f -n -p /etc/security/policy.conf
```

Be careful when enabling these settings as they can create a denial-of-service situation for legitimate users and applications. Account lockout can be disabled for specific users via the usermod command. For example, the following command disables account lock specifically for the oracle account:

```
# usermod -K lock_after_retries=no oracle
```

By default the root account is exempt from account lockout.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^RETRIES=3" /etc/default/login
RETRIES=3
# grep "^LOCK_AFTER_RETRIES=YES" /etc/security/policy.conf
LOCK_AFTER_RETRIES=YES
```

6.12 Set EEPROM Security Mode and Log Failed Access

Configuration Level	Level-I
Hardware Platform	SPARC only
OS Default	No

Zone Support	Global zone only
Reboot Required	No
Solaris Security Toolkit	Use the install-security-mode.fin Finish script.
Scorable Item	No

Description:
Oracle SPARC systems support the use of a EEPROM password for the console.

Rationale:
Setting the `EEPROM` password helps prevent attackers with physical access to the system console from booting off some external device (such as a CD-ROM or floppy) and subverting the security of the system.

Remediation:
Create a script and store it in a local directory (e.g. `/opt/local/bin`). In this example, `/opt/local/bin` will be used as the storage directory for the script. The script will be called `eeprom_badlogin.ksh`:

```
# /bin/ed /opt/local/bin/eeprom_badlogin.ksh
a
#!/bin/ksh
badCount=`eeprom security-#badlogins |\
      awk -F= '{ print $2 }'`
if [ -z "${badCount}" ]; then
   exit 0
elif [ ${badCount} != 0 ]; then
      logger -p auth.notice "EEPROM Security Bad Logins is ${badCount}."
fi
.
w
q
# chmod +x /opt/local/bin/eeprom_badlogin.ksh
# /opt/local/bin/eeprom_badlogin.ksh
# eeprom security-#badlogins=0
# if [ ! "`crontab -l | grep eeprom_badlogin`" ]; then
      cd /var/spool/cron/crontabs
      crontab -l > root.tmp
      echo "0 0,8,16 * * * /opt/local/bin/eeprom_badlogin.ksh" >> root.tmp
      crontab root.tmp
      rm -f root.tmp
fi
# eeprom security-mode=command
```

After entering the last command above, the administrator will be prompted for a password. This password will be required to authorize any future command issued at boot-level on the system (the `ok` or > prompt) *except* for the normal multi-user `boot` command (i.e., the system will be able to reboot unattended).

Write down the password and store it in a sealed envelope in a secure location (note that locked desk drawers are typically *not* secure). If the password is lost or forgotten, simply run the command:

```
# eeprom security-mode=none
```

This will erase the forgotten password. To set a new password, run the command:

```
# eeprom security-mode=command
```

Audit:
To check if a password has been set enter the following command:

```
# eeprom security-mode | awk -F= '{ print $2 }'
```

If a password has been set, the command will return `command or full.` If a password has not been set, the command will return `none`.

6.13 Secure the GRUB Menu

Configuration Level	Level-I
Hardware Platform	x86/x64 only
OS Default	No
Zone Support	Global zone only
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
GRUB is a boot loader for x86/x64 based systems that permits loading an OS image from any location. Oracle x86 systems support the use of a GRUB Menu password for the console.

Rationale:
The flexibility that GRUB provides creates a security risk if its configuration is modified by an unauthorized user. The failsafe menu entry needs to be secured in the same environments that require securing the systems firmware to avoid unauthorized removable media boots. Setting the `GRUB Menu` password helps prevent attackers with physical access to the system console from booting off some external device (such as a CD-ROM or floppy) and subverting the security of the system.

The actions described in this section will ensure you cannot get to failsafe or any of the GRUB command line options without first entering the password. Note that you can still boot into the default OS selection without a password.

Remediation:
Perform the following to implement the recommended state:

```
# /boot/grub/bin/grub
```

```
grub> md5crypt

Password: [enter desired boot loader password]
Encrypted: [enter md5 password string]
grub> [enter control-C (^C)]
```

The actual `menu.lst` file to be used varies depending upon whether ZFS or UFS is used as the root file system. If a ZFS filesystem is being used, then edit the file `/rpool/boot/grub/menu.lst`. Otherwise edit the file `/boot/grub/menu.lst`. Add the following line to the `menu.lst` file above the entries added by bootadm:

```
# password -md5 [enter md5 password string generated above]
```

Next, add the keyword lock to the Solaris failsafe boot entry as in the following example:

```
title Solaris failsafe
lock
```

Last, ensure the `menu.lst` file can only be read by the `root` user:

```
(UFS)   # chmod 600 /boot/grub/menu.lst
(ZFS)   # chmod 600 /rpool/boot/grub/menu.lst
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
(UFS)   # grep "^password -md5" /boot/grub/menu.lst
(ZFS)   # grep "^password -md5" /rpool/boot/grub/menu.lst
password -md5 [password string]
```

7. User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment. Guidance for monitoring these settings and others that may change over time is provided in Section 9 System Maintenance.

7.1 Disable System Accounts

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-system-accounts.fin Finish script with the JASS_ACCT_DISABLE variable.
Scorable Item	Yes

Description:

There are a number of accounts provided with the Solaris OS that are used to manage applications and are not intended to provide an interactive shell.

Rationale:
It is important to make sure that accounts that are not being used by regular users are locked to prevent them from logging in or running an interactive shell. By default, Solaris sets the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to "false." This prevents the account from potentially being used to run any commands.

Remediation:
Accounts that have been locked are prohibited from running commands on the system. Such accounts are not able to login to the system nor are they able to use scheduled execution facilities such as `cron`. To lock an account, use the command:

```
# passwd -l [username]
```

An example

```
# /usr/bin/passwd -l daemon
# for user in bin nuucp smmsp listen gdm webservd nobody noaccess nobody4
svctag; do
      /usr/bin/getent passwd $user > /dev/null 2>&1
      if [ $? -eq 0 ]
      then
            /usr/bin/passwd -l $user
            /usr/sbin/passmgmt -m -s /usr/bin/false $user
      fi
done

# passwd -N sys
# for user in postgresadm lp uucp; do
      /usr/bin/getent passwd $user > /dev/null 2>&1
      if [ $? -eq 0 ]
      then
            /usr/bin/passwd -N $user
            /usr/sbin/passmgmt -m -s /usr/bin/false $user
      fi
done
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# for user in daemon bin nuucp smmsp listen gdm webservd nobody noaccess
nobody4 svctag
do
      /usr/bin/getent passwd $user > /dev/null 2>/dev/null
      if [ $? -eq 0 ]
      then
            stat=`passwd -s ${user} | awk '{ print $2 }'`
            if [ "${stat}" != "LK" ]; then
                  echo "Account ${user} is not locked."
            fi
      fi
```

```
done
# for user in sys adm lp uucp postgres; do
      /usr/bin/getent passwd $user > /dev/null 2>/dev/null
      if [ $? -eq 0 ]
      then
            stat=`passwd -s ${user} | awk '{ print $2 }'`
            if [ "${stat}" != "NL" ]; then
                  echo "Account ${user} is not non-login."
            fi
      fi
done
```

References:

1. http://www.securitydocs.com/library/2636.
2. http://blogs.sun.com/gbrunett/entry/managing_non_login_and_locked

7.2 Set Password Expiration Parameters on Active Accounts

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-user-password-reqs.fin Finish script with the JASS_AGING_MINWEEKS, JASS_AGING_MAXWEEKS, JASS_AGING_WARNWEEKS variables.
Scorable Item	Yes

Description:
Many organizations require users to change passwords on a regular basis.

Rationale:
The commands for this item set all active accounts (except the *root* account) to force password changes every 91 days (13 weeks), and then prevent password changes for seven days (one week) thereafter. Users will begin receiving warnings 28 days (4 weeks) 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.

Notes:
Since `/etc/default/passwd` sets defaults in terms of number of weeks (even though the actual values on user accounts are kept in terms of days), it is probably best to choose interval values that are multiples of 7.

Actions for this item do not work on accounts stored on network directories such as LDAP.

Remediation:
Perform the following to implement the recommended state:

```
# logins -ox |\
      awk -F: '($1 == "root" || $8 == "LK" || $8 == "NL") { next } ; \
            { $cmd = "passwd" } ;\
            ($11 <= 0 || $11 > 91)  { $cmd = $cmd " -x 91" } \
            ($10 < 7)          { $cmd = $cmd " -n 7" } \
            ($12 < 28)               { $cmd = $cmd " -w 28" } \
            ($cmd != "passwd")             { print $cmd " " $1 }' \
            > /etc/CISupd_accounts
# /sbin/sh /etc/CISupd_accounts
# rm -f /etc/CISupd_accounts
# cd /etc/default
# /usr/bin/grep -v WEEKS passwd > passwd.new
# cat <<EODefaults >> passwd.new
MAXWEEKS=13
MINWEEKS=1
WARNWEEKS=4
EODefaults
# /usr/bin/mv passwd.new passwd
# /usr/sbin/pkgchk -f -n -p /etc/default/passwd
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# echo "The Output from the Audit of Control 7.2 - Set Password Expiration
Parameters on Active Accounts is"
# echo "/usr/bin/logins -ox | awk -F: '( $1 != "root" && $8 != \"LK\" && $8
!= \"NL\" \
            && ( $10 != \"7\" || $11 != \"91\" || $12 != \"28\" { print }'"
# /usr/bin/logins -ox | awk -F: '( $1 != "root" && $8 != "LK" && $8 != "NL")
\
            && ( $10 != "7" || $11 != "91" || $12 != "28")  { print }'
# echo "/usr/bin/grep \"MAXWEEKS=13\" /etc/default/passwd"
# /usr/bin/grep "MAXWEEKS=13" /etc/default/passwd
# echo "/usr/bin/grep \"MINWEEKS=1\" /etc/default/passwd"
# /usr/bin/grep "MINWEEKS=1" /etc/default/passwd
# echo "/usr/bin/grep \"WARNWEEKS=4\" /etc/default/passwd"
# /usr/bin/grep "WARNWEEKS=4" /etc/default/passwd
```

7.3 Set Strong Password Creation Policies

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-user-password-reqs.fin, set-strict-password-checks.fin and the enable-password-history.fin Finish scripts with the

	JASS_PASS_LENGTH, JASS_PASS_HISTORY, JASS_PASS_MAXREPEATS, JASS_PASS_MINALPHA, JASS_PASS_MINDIFF, JASS_PASS_MINNONALPHA, JASS_PASS_MINDIGIT, JASS_PASS_MINSPECIAL, JASS_PASS_MINUPPER, JASS_PASS_MINLOWER, JASS_PASS_NAMECHECK, JASS_PASS_WHITESPACE, JASS_PASS_DICTIONDB,and JASS_PASS_DICTIONLIS T variables.
Scorable Item	Yes

Description:
Password policies are designed to force users to make better password choices when selecting their passwords.

Rationale:
Administrators may wish to change some of the parameters in this remediation step (particularly `PASSLENGTH` and `MINDIFF`) if changing their systems to use MD5, SHA-256, SHA-512 or Blowfish password hashes ("`man crypt.conf`" for more information). Similarly, administrators may wish to add site-specific dictionaries to the `DICTIONLIST` parameter.

Sites often have differing opinions on the optimal value of the `HISTORY` parameter (how many previous passwords to remember per user in order to prevent re-use). The values specified here are in compliance with DISA requirements. If this is too restrictive for your site, you may wish to set a HISTORY value of 4 and a MAXREPEATS of 2. Consult your local security policy for guidance.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/PASSLENGTH=/   { $1 = "PASSLENGTH=8" };
     /NAMECHECK=/    { $1 = "NAMECHECK=YES" };
     /HISTORY=/      { $1 = "HISTORY=10" };
     /MINDIFF=/      { $1 = "MINDIFF=3" };
     /MINALPHA=/     { $1 = "MINALPHA=2" };
     /MINUPPER=/     { $1 = "MINUPPER=1" };
     /MINLOWER=/     { $1 = "MINLOWER=1" };
     /MINNONALPHA=/  { $1 = "MINNONALPHA=1" };
     /MAXREPEATS=/   { $1 = "MAXREPEATS=0" };
     /WHITESPACE=/   { $1 = "WHITESPACE=YES" };
     /DICTIONDBDIR=/ { $1 = "DICTIONDBDIR=/var/passwd" };
     /DICTIONLIST=/ \
        { $1 = "DICTIONLIST=/usr/share/lib/dict/words" };
```

```
    { print }' passwd > passwd.new
# mv passwd.new passwd
# pkgchk -f -n -p /etc/default/passwd
```

Audit:
Run the following commands and verify that the output is as shown:

```
# grep "^PASSLENGTH=8" /etc/default/passwd
PASSLENGTH=8
# grep "^NAMECHECK=YES" /etc/default/passwd
NAMECHECK=YES
# grep "^HISTORY=10" /etc/default/passwd
HISTORY=10
# grep "^MINDIFF=3" /etc/default/passwd
MINDIFF=3
# grep "^MINALPHA=3" /etc/default/passwd
MINALPHA=2
# grep "^MINUPPER=1" /etc/default/passwd
MINUPPER=1
# grep "^MINLOWER=1" /etc/default/passwd
MINLOWER=1
# grep "^MINNONALPHA=1" /etc/default/passwd
MINNONALPHA=1
# grep "^MAXREPEATS=0" /etc/default/passwd
MAXREPEATS=0
# grep "^WHITESPACE=YES" /etc/default/passwd
WHITESPACE=YES
# grep "^DICTIONDBDIR=/var/passwd" /etc/default/passwd
DICTIONDBDIR=/var/passwd
# grep "^DICTIONLIST=/usr/share/lib/dict/words" \
      /etc/default/passwd
DICTIONLIST=/usr/share/lib/dict/words
```

7.4 Set Default Group for *root* Account

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	Yes, to ensure GID is properly set on all root initiated services.
Solaris Security Toolkit	Use the set-root-group.fin Finish script.
Scorable Item	Yes

Description:
For Solaris 9 and earlier, the default group for the *root* account is the "other" group, which may be shared by many other accounts on the system. Solaris 10 has adopted GID 0 (group "*root*") as default group for the *root* account.

Rationale:

If your system has been upgraded from an earlier version of Solaris, the password file may contain the older group classification for the `root` user. Using GID 0 for the *`root`* account helps prevent *`root`*-owned files from accidentally becoming accessible to non-privileged users.

Remediation:
Perform the following to implement the recommended state:

```
# passmgmt -m -g 0 root
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep root /etc/passwd | cut -f4 -d:
0
```

7.5 Change Home Directory for *`root`* Account

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-root-home-dir.fin Finish script.
Scorable Item	Yes

Description:
By default, the Solaris OS *root* user's home directory is "/".

Rationale:
Changing the home directory for the *`root`* account provides segregation from the OS distribution and activities performed by the `root` user. A further benefit is that the *`root`* home directory can have more restricted permissions, preventing viewing of the *`root`* system account files by non-*`root`* users.

Remediation:
Perform the following to implement the recommended state:

```
# mkdir -m 700 /root
# mv -i /.?* /root/
# passmgmt -m -h /root root
```

Note:
If the user logs into GNOME, the directories "Desktop" and "Documents" will also be created under `/`. Move these directories into `/root`, if they exist.

Audit:

Perform the following to determine if the system is configured as recommended:

```
# grep root /etc/passwd | cut -f6 -d:
/root
```

7.6 Set Default umask for Users

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-user-umask.fin Finish script.
Scorable Item	Yes

Description:
The default `umask(1)` determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the `chmod(1)` 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.

Rationale:
Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of `077` causes files and directories created by users to 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.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/UMASK=/ { $1 = "UMASK=077" }
      { print }' login >login.new
# mv login.new login
# cd /etc
# for file in profile .login ; do
      if [ "`grep umask $file`" ]; then

            awk '$1 == "umask" { $2 = "077" }

                  { print }' $file > $file.new

            mv $file.new $file

      else
```

```
            echo umask 077 >> $file

      fi
done
# pkgchk -f -n -p /etc/default/login
# pkgchk -f -n -p /etc/profile
# pkgchk -f -n -p /etc/.login
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^UMASK=077" /etc/default/login
UMASK=077
# grep "^umask 077" /etc/.login
umask 077
# grep "^umask 077" /etc/profile
umask 077
```

7.7 Set Default umask for FTP Users

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-ftpd-umask.fin Finish script.
Scorable Item	Yes, if FTP is installed.

Description:
If FTP is permitted, set the `umask` value to apply to files created by the FTP server.

Rationale:
Many users assume that files transmitted over FTP inherit their system `umask` value when they do not. This setting ensures that files transmitted over FTP are protected. See Item 6.5 Restrict FTP Use for a more complete description of FTP and Item 7.6 Set Default `umask` for Users for a description of `umask`.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/ftpd

# if [ "`grep '^defumask' ftpaccess`" ]; then
      awk '/^defumask/ { $2 = "077" }

            { print }' ftpaccess > ftpaccess.new

      mv ftpaccess.new ftpaccess
```

```
else

      echo defumask 077 >>ftpaccess
fi
# pkgchk -f -n -p /etc/ftpd/ftpaccess
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^defumask 077" /etc/ftpd/ftpaccess
defumask 077
```

7.8 Set "mesg n" as Default for All Users

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-mesg.fin Finish script.
Scorable Item	Yes

Description:
The "`mesg n`" command blocks attempts to use the `write` or `talk` commands to contact users at their terminals, but has the side effect of slightly strengthening permissions on the user's tty device.

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 to implement the recommended state:

```
# cd /etc
# for file in profile .login; do
      if [ "`grep mesg $file`" ]; then
            awk '$1 == "mesg" { $2 = "n" }
                  { print }' $file > $file.new
            mv $file.new $file
      else
            echo mesg n >>$file
      fi
      pkgchk -f -n -p /etc/$file
done
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^mesg n" /etc/.login
mesg n
```

```
# grep "^mesg n" /etc/profile
mesg n
```

7.9 Lock Inactive User Accounts

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:
Guidelines published by the U.S. Department of Defense specify that user accounts must be locked out after 35 days of inactivity. This number may vary based on the particular site's policy.

Rationale:
Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Remediation:
Create a shell script as follows:

```
#!/bin/sh

if [ ! -f /usr/sadm/defadduser ]; then
      echo "Default inactivity lockout not set."
      echo "Run useradd -D -f 35 to create the file"
      exit 1
fi

x=`grep definact /usr/sadm/defadduser` 2>&1
if [ $? -ne 0 ]; then
      echo "Default lockout variable not set."
      echo "Run useradd -D -f 35 to set the lockout to 35 days"
      exit 1
fi

y=`echo $x | sed -e 's/.*=//'`
if [ $y -ne 35 ]; then

      echo "Default lock variable set to $y."
      echo "Run useradd -D -f 35 to set the lockout to 35 days"
fi

/bin/cp /etc/shadow /etc/shadow.$$
/bin/ed /etc/shadow.$$ << END
1,/nobody4/d
w
q
END
```

```
/bin/cat /etc/shadow.$$ | while : ; do
      x=`line`
      if [ "$x" = "" ]; then
            break
      fi
      num=`echo $x | cut -f7 -d":"`
      user=`echo $x | cut -f1 -d":"`
      if [ "$num" = "" ]; then
            echo "User $user lockout not set"
      else
            if [ $num -ne 35 ]; then
                  echo "User $user lockout set to $num instead of 35."
            fi
      fi
done
/bin/rm /etc/shadow.$$
```

Notes:
To set the default for creating user accounts to expire after 35 days of inactivity, use the command:

```
# useradd –D –f 35
```

This will create or modify the file `/usr/sadm/defadduser` with an entry `definact=35` (or whatever you set it to for your site's policy).

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep definact /usr/sadm/defadduser
definact=35
```

8. Warning Banners

Presenting a warning message prior to the normal user login 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 exploits 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. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at http://www.justice.gov/criminal/cybercrime/

Important Note: The text provided in the remediation actions for these items is intended as an example only. Please edit to include the specific text for your organization as approved by your legal department.

8.1 Create Warnings for Standard Login Services

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Add the Files/etc/motd and Files/etc/issue file templates to the JASS_FILES variable (to be used by install-templates.fin)
Scorable Item	Yes

Description:
The contents of the `/etc/issue` file are displayed prior to the login prompt on the system's console and serial devices, and also prior to logins via `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:
Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Consult with your organization's legal counsel for the appropriate wording for your specific organization.

Remediation:
Perform the following to implement the recommended state:

```
# echo "Authorized uses only. All activity may be \

monitored and reported." > /etc/motd
# echo "Authorized uses only. All activity may be \
monitored and reported." > /etc/issue
# pkgchk -f -n -p /etc/motd
# chown root:root /etc/issue
# chmod 644 /etc/issue
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls /etc/motd
/etc/motd
# ls /etc/issue
/etc/issue
```

The commands above simply validate the presence of the `/etc/motd` and `/etc/issue` files. Review the contents of these files with the "`cat`" command and ensure that it is appropriate for your organization.

8.2 Create Warning Banner for CDE Users

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-banner-dtlogin.fin Finish script
Scorable Item	Yes, if a graphical login (windowing) system is enabled.

Description:
The Common Desktop Environment (CDE) provides a uniform desktop environment for users across diverse Unix platforms.

Rationale:
Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Consult with your organization's legal counsel for the appropriate wording for your specific organization.

Remediation:
Perform the following to implement the recommended state:

```
# for file in /usr/dt/config/*/Xresources ; do
      dir=`dirname $file | sed s/usr/etc/`
      mkdir -m 755 -p $dir
      if [ ! -f $dir/Xresources ]; then
            cp $file $dir/Xresources
      fi
      echo "Dtlogin*greeting.labelString: \
Authorized uses only!" \
            >> $dir/Xresources

      echo "Dtlogin*greeting.persLabelString: \
All activity may be monitored and reported." \
            >> $dir/Xresources
done
# chown root:sys /etc/dt/config/*/Xresources
# chmod 644 /etc/dt/config/*/Xresources
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# for file in /usr/dt/config/*/Xresources ; do
      dir=`dirname $file | sed s/usr/etc/`
      if [ -f $dir/Xresources ]; then
            grep "^Dtlogin\*greeting\.labelString: \
Authorized uses only\!" $dir/Xresources
      fi
done
Dtlogin*greeting.labelString: Authorized uses only!

# for file in /usr/dt/config/*/Xresources ; do
      dir=`dirname $file | sed s/usr/etc/`
      if [ -f $dir/Xresources ]; then
            grep "^Dtlogin\*greeting\.persLabelString: \
All activity may be monitored and reported\." \
            $dir/Xresources
      fi
done
Dtlogin*greeting.persLabelString: All activity may be monitored and reported.
```

8.3 Create Warning Banner for GNOME Users

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-greeter-warning.fin Finish script.
Scorable Item	Yes, if a graphical login (windowing) system is enabled.

Description:
The GNOME Display Manager is used for login session management. See the manual page `gdm(1)` for more information.

Rationale:
The remediation action for this item sets a warning message for GDM users before they log in.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/X11/gdm
# awk '/^#?Greeter=/ \
      { print "Greeter=/usr/bin/gdmlogin"; next }
      /^#?Welcome=/ \
      { print "Welcome=Authorized uses only!\\n" \
            "All activity may be monitored " \
            "and reported."
            next }
 { print }' gdm.conf > gdm.conf.new
```

```
# mv gdm.conf.new gdm.conf
# pkgchk -f -n -p /etc/X11/gdm/gdm.conf
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# cd /etc/X11/gdm
# grep "Greeter=/usr/bin/gdmlogin" gdm.conf
Greeter=/usr/bin/gdmlogin
# grep "^Welcome=Authorized uses only\!" gdm.conf
Welcome=Authorized uses only!\nAll activity may be monitored and reported.
```

8.4 Create Warning Banner for FTP daemon

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-banner-ftp.fin Finish script.
Scorable Item	Yes, if FTP is installed.

Description:
The action for this item sets a warning message for FTP users before they log in.

Rationale:
Warning messages inform users who are attempting to access the system of their legal status regarding the system. Consult with your organization's legal counsel for the appropriate wording for your specific organization.

Remediation:
Perform the following to implement the recommended state:

```
# echo Authorized uses only.  All activity may \
be monitored and reported. > /etc/ftpd/banner.msg
# chown root:root /etc/ftpd/banner.msg
# chmod 444 /etc/ftpd/banner.msg
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "Authorized uses only. All activity may \
be monitored and reported." /etc/ftpd/banner.msg
Authorized uses only. All activity may be monitored and reported.
```

8.5 Check Banner Setting for `telnet` is Null

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-banner-telnetd.fin Finish script.
Scorable Item	Yes

Description:
The `BANNER` variable in the file `/etc/default/telnetd` can be used to display text before the telnet login prompt. Traditionally, it has been used to display the OS level of the target system.

Rationale:
The warning banner provides information that can be used in reconnaissance for an attack. By default, Oracle distributes this file with the `BANNER` variable set to null. It is not necessary to create a separate warning banner for `telnet` if a warning is set in the `/etc/issue` file.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
awk '/BANNER=/ { $1 = "BANNER=" }; \
                { print }' telnetd >telnetd.new
# mv telnetd.new telnetd
# pkgchk -f -n -p /etc/default/telnetd
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^BANNER=$" /etc/default/telnetd
BANNER=
```

See Item 8.1 Create Warning Banner for Standard Login Services.

9. System Maintenance

No matter how securely a system has been installed and hardened, administrator and user activity over time can introduce security exposures. The section describes tasks to be performed on a regular, ongoing basis—perhaps in an automated fashion via the `cron` utility. The automated host-based scanning tools provided from the Center for Internet Security can be used for this purpose. These scanning tools are typically provided with this document, but are also available for free download from http://www.CISecurity.org/

Note that, unlike other sections, the items in this section specify an Audit action followed by a Remediation action since it is necessary to determine what the current setting is before determining remediation measures, which will vary depending on the site's policy.

9.1 Check for Remote Consoles

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	Global zone only
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:
The `consadm` command can be used to select or display alternate console devices.

Rationale:
Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined. The "`consadm -p`" command displays any alternate consoles that have been defined as auxiliary across reboots. If no remote consoles have been defined, there will be no output from this command.

Remediation:
Perform the following to implement the recommended state:

```
# /usr/sbin/consadm [-d device...]
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# /usr/sbin/consadm -p
```

9.2 Verify System File Permissions

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the print-package-files.fin Finish script.
Scorable Item	No

Description:

The `pkgchk` command checks the accuracy of installed files as well as the integrity of directory structures and files.

Rationale:
It is important to ensure that system files and directories are maintained with the permissions they were intended to have from the OS vendor (Oracle).

Remediation:
To force the default setting, use the `-f` option as follows:

```
# pkgchk -f -n -p /etc/shadow
```

Audit:
Check the permissions of all Solaris packages installed on the system by executing the following command (the "-n" option excludes checking volatile or editable files):

```
# pkgchk –n
```

If the files are not in compliance, an error message similar to the following will be displayed:

```
ERROR: /etc/shadow
    group name <sys> expected <other> actual
```

Depending on the number of packages installed on the system, this command could take a long time to run and generate a lot of output to standard error. Not all of the errors generated reflect actual problems. You may want to save the output to a file for later review. You can also create a custom script to verify the integrity of critical files, such as the following:

```
# pkgchk -n -p /etc/passwd
# pkgchk -n -p /etc/shadow
```

9.3 Ensure Password Fields are Not Empty

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the check-null-passwords.aud Audit script.
Scorable Item	Yes

Description:
An account with an empty password field means that anybody may log in as that user without providing a password at all (assuming that PASSREQ=NO in /etc/default/login).

Rationale:
All accounts must have passwords or be locked.

Remediation:
Use the `passwd -l` command to lock accounts that are not permitted to execute commands (shown by `*LK*` in the password field). Use the `passwd -N` command for accounts that do not use a password to login but must execute commands (shown by `NP` in the password field).

Audit:
Run the following command and verify that no output is returned:

```
# logins -p
```

9.4 Verify No Legacy "+" Entries Exist in `passwd`, `shadow`, and `group` Files

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the check-include-nis-map.aud Audit script.
Scorable Item	Yes

Description:
The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on Solaris systems, but may exist in files that have been imported from other platforms.

Rationale:
These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:
Run the following command and verify that no output is returned:

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

Remediation:
Delete these entries if they exist.

9.5 Verify No UID 0 Accounts Exist Other than root

Configuration Level	Level-I

Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
SST Setting	Use the check-uids-unique.aud Audit script.
Scorable Item	Yes

Description:
Any account with UID 0 has superuser privileges on the system.

Rationale:
This access must be limited to only the default `root` account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 6.10 Restrict `root` Login to System Console.

Audit:
Run the following command and verify that only the word "root" is returned:

```
# logins -o | awk -F: '($2 == 0) { print $1 }'
root
```

Remediation:
Delete any other entries that are displayed.
Finer granularity access control for administrative access can be obtained by using Oracle's Role-Based Access Control (RBAC) system.

RBAC configurations can be monitored via the `/etc/user_attr` file to make sure that privileges are managed appropriately.

References:

1. *Oracle. " RBAC in the Solaris Operating Environment,"* http://www.sun.com/software/whitepapers/wp-rbac/wp-rbac.pdf
2. *OpenSolaris. "RBAC – Role Based Access Control"* http://www.opensolaris.org/os/community/security/projects/rbac/

9.6 Ensure root PATH Integrity

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the check-root-path.aud Audit script.
Scorable Item	Yes

Description:
The `root` user can execute any command on the system and could be fooled into executing programs unemotionally if the PATH is not set correctly.

Rationale:
Including the current working directory (`.`) or other writable directory in `root`'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a Trojan horse program.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# if [ "`echo $PATH | grep :: `" != "" ]; then
      echo "Empty Directory in PATH (::)"
 fi

# if [ "`echo $PATH | grep :$`"  != "" ]; then
      echo "Trailing : in PATH"
fi

# p=`echo $PATH | sed -e 's/::/:/' -e 's/:$//' -e 's/:/ /g'`
# set -- $p
# while [ "$1" != "" ]; do
      if [ "$1" = "." ]; then
            echo "PATH contains ."
            shift
            continue
      fi
      if [ -d $1 ]; then
            dirperm=`ls -ld $1 | cut -f1 -d" "`
            if [ `echo $dirperm | cut -c6 ` != "-" ]; then
                  echo "Group Write permission set on directory $1"
            fi
            if [ `echo $dirperm | cut -c9 ` != "-" ]; then
                  echo "Other Write permission set on directory $1"
            fi
      fi
      shift
done
```

Remediation:
Correct or justify any items discovered in the Audit step.

9.7 Check Permissions on User Home Directories

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the check-home-permissions.aud Audit

	script.
Scorable Item	Yes

Description:
While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

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.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# for dir in `logins -ox |\
      awk -F: '($8 == "PS" && $1 != "root") { print $6 }'`; do
            dirperm=`ls -ld $dir | cut -f1 -d" "`
            if [ `echo $dirperm | cut -c6 ` != "-" ]; then
                  echo "Group Write permission set on directory $dir"
            fi
            if [ `echo $dirperm | cut -c8 ` != "-" ]; then
                  echo "Other Read permission set on directory $dir"

            fi

            if [ `echo $dirperm | cut -c9 ` != "-" ]; then
                  echo "Other Write permission set on directory $dir"
            fi
            if [ `echo $dirperm | cut -c10 ` != "-" ]; then
                  echo "Other Execute permission set on directory $dir"
            fi
done
```

Remediation:
Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

9.8 Check User Dot File Permissions

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the check-hidden-files.aud Audit script.
Scorable Item	Yes

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

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.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# for dir in `logins -ox | awk -F: '($8 == "PS") { print $6 }'`; do
      for file in $dir/.[A-Za-z0-9]*; do

            if [ ! -h "$file" -a -f "$file" ]; then
                  fileperm=`ls -ld $file | cut -f1 -d" "`

                  if [ `echo $fileperm | cut -c6 ` != "-" ]; then
                        echo "Group Write permission set on file $file"
                  fi
                  if [ `echo $fileperm | cut -c9 ` != "-" ]; then
                        echo "Other Write permission set on file $file"
                  fi
            fi

      done

done
```

Remediation:
Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

9.9 Check Permissions on User `.netrc` Files

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes, no `.netrc` files are shipped by default in Solaris
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the check-netrc-files.aud Audit script.
Scorable Item	Yes

Description:
While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Rationale:

Users' `.netrc` files may contain unencrypted passwords that may be used to attack other systems.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# for dir in `logins -ox |\
      awk -F: '($8 == "PS") { print $6 }'`; do
      for file in $dir/.netrc; do
            if [ ! -h "$file" -a -f "$file" ]; then
                  fileperm=`ls -ld $file | cut -f1 -d" "`
                  if [ `echo $fileperm | cut -c5 ` != "-" ]
                  then
                        echo "Group Read set on $file"
                  fi
                  if [ `echo $fileperm | cut -c6 ` != "-" ]
                  then
                        echo "Group Write set on $file"
                  fi
                  if [ `echo $fileperm | cut -c7 ` != "-" ]
                  then
                        echo "Group Execute set on $file"
                  fi
                  if [ `echo $fileperm | cut -c8 ` != "-" ]
                  then
                        echo "Other Read  set on $file"
                  fi
                  if [ `echo $fileperm | cut -c9 ` != "-" ]
                  then
                        echo "Other Write set on $file"
                  fi
                  if [ `echo $fileperm | cut -c10 ` != "-" ]
                  then
                        echo "Other Execute set on $file"
                  fi
            fi
      done
done
```

Remediation:
Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` file permissions and determine the action to be taken in accordance with site policy.

9.10 Check for Presence of User .rhosts Files

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes, no `.rhosts` files are shipped by default in Solaris
Zone Support	All

Reboot Required	No
Solaris Security Toolkit	Use the print-rhosts.aud Audit script.
Scorable Item	Yes

Description:
While no `.rhosts` files are shipped with Solaris, users can easily create them.

Rationale:
This action is only meaningful if `.rhosts` support is permitted in the file `/etc/pam.conf`. Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.
Please see Item 6.4 Disable `.rhosts` support in `/etc/pam.conf` for more information.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# for dir in `logins -ox |\
      awk -F: '($8 == "PS") { print $6 }'`; do
      for file in $dir/.rhosts; do
            if [ ! -h "$file" -a -f "$file" ]; then
                  echo ".rhosts file in $dir"
            fi    done
done
```

Remediation:
It may be useful to run this audit check and, if any users have `.rhosts` files, determine why they have them.

9.11 Check Groups in /etc/passwd

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:
Over time, system administration errors and changes can lead to groups being defined in `/etc/passwd` but not in `/etc/group`.

Rationale:
Groups defined in the `/etc/passwd` file but not in the `/etc/group` file pose a threat to system security since group permissions are not properly managed.

Audit:
Create a script as shown below and run it:

```
#!/sbin/sh
defUsers="root daemon bin sys adm lp uucp nuucp smmsp listen gdm webservd
postgres svctag nobody noaccess nobody4"
/usr//bin/cat /etc/passwd | while :
do
        x=`line`
        if [ "$x" = "" ]
        then
                break
        fi
        userid=`echo "$x" | cut -f1 -d':'`
      found=0
      for n in $defUsers
      do
            if [ $userid = "$n" ]
            then
                  found=1
                  break
            fi
      done
      if [ $found -eq 1 ]
      then
            continue
      fi
            groupid=`echo "$x" | cut -f4 -d':'`
            /usr/bin/cat /etc/group | while :
            do
                  x=`line`
                  if [ "$x" = "" ]
                  then
                        echo "Groupid $groupid does not exist in /etc/group,
but is used by $userid"
                        break
                  fi
                  y=`echo $x | cut -f3 -d":"`
                  if [ $y -eq $groupid ]
                  then
                        break
                  fi
        done
done
```

Remediation:
Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

9.12 Check That Users Are Assigned Home Directories

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No

Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:
The `/etc/passwd` file defines a home directory that the user is placed in upon login. If there is no defined home directory, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Rationale:
All users must be assigned a home directory in the `/etc/passwd` file.

Audit:
This script checks to make sure a home directory is defined for each user in the `/etc/passwd` file.

```
#!/sbin/sh

 echo "The Output for the Audit of Control 9.12 - Check That Users Are
Defined Home Directories is"
defUsers="root daemon bin sys adm lp uucp nuucp smmsp \
      listen gdm webservd postgres svctag nobody noaccess \
      nobody4"
 cat /etc/passwd |\
      awk -F: '{ print $1 " " $6 }' |\
      while read user dir
      do
            found=0
            for n in $defUsers
            do
                  if [ "$user" = "$n" ]
                  then
                        found=1
                        break
                  fi
            done
            if [ $found -eq 0 ]
            then
                  if [ -z "$dir" ]
                  then
                        echo "User $user has no home directory."
                  fi
            fi
      done
```

Remediation:
Based on the results of the Audit script, perform the appropriate action for your environment (e.g. delete unneeded users or assign them a home directory).

9.13 Check That Defined Home Directories Exist

Configuration Level	Level-I
Hardware Platform	All
OS Default	No

Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:
Users can be defined to have a home directory in `/etc/passwd`, even if the directory does not actually exist.

Rationale:
If the user's home directory does not exist, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Audit:
This script checks to make sure that home directories assigned in the `/etc/passwd` file exist. You can also use the command `/usr/sbin/pwck` to check for inconsistencies in the `/etc/passwd` file, such as the presence of a valid home directory.

```
#!/sbin/sh

echo "The Output for the Audit of Control 9.13 - Check That Defined Home
Directories Exist is"
defUsers="root daemon bin sys adm lp uucp nuucp smmsp \
      listen gdm webservd postgres svctag nobody noaccess \
      nobody4"
 cat /etc/passwd |\
      awk -F: '{ print $1 " " $6 }' |\
      while read user dir; do
            found=0
            for n in $defUsers
            do
                  if [ "$user" = "$n" ]
                  then
                        found=1
                        break
                  fi
            done
            if [ $found -eq 0 ]
            then
                  if [ -z "${dir}" ]; then
                        echo "User $user has no home directory."
                  elif [ ! -d $dir ]; then
                        echo "User $user home directory not found"
                  fi
            fi
      done
```

Remediation:
If any users' home directories do not exist, create them and make sure the respective user owns the directory.

9.14 Check User Home Directory Ownership

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:
The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:
Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Audit:
This script checks to make sure users own the home directory they are assigned to in the `/etc/passwd` file.

```
#!/sbin/sh

echo "The Output for the Audit of Control 9.14 - Check User Home Directory
Ownership is"
defUsers="root daemon bin sys adm lp uucp nuucp smmsp \
      listen gdm webservd postgres svctag nobody noaccess \
      nobody4"
 /usr/bin/cat /etc/passwd |  \
      awk -F: '{ print $1 " " $6 }' |\
      while read user dir; do
            found=0
            for n in $defUsers
            do
                  if [ "$user" = "$n" ]
                  then
                        found=1
                        break
                  fi
            done
            if [ -z "${dir}" ]
            then
                  if [ -d ${dir} ]
                  then
                              owner=`ls -ld $dir | sed -e 's/  */ /g' | cut -
f3 -d" "`
                              if [ "$owner" != "$user" ]
                              then
                                    echo "Home directory for $user owned by
$owner"
                              fi
```

```
                fi
            fi
        done
```

Remediation:
Change the ownership any home directories that are not owned by the defined user to the correct user.

9.15 Check for Duplicate UIDs

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:
Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

Rationale:
Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:
This script checks to make sure all UIDs in the `/etc/passwd` file are unique.

```
#!/sbin/sh

echo "The Output for the Audit of Control 9.15 - Check for Duplicate UIDs is"
 cat /etc/passwd | cut -f3 -d":" | sort -n | uniq -c |\
      while read x ; do
      [ -z "${x}" ] && break
      set - $x
      if [ $1 -gt 1 ]; then
            users=`nawk -F: '($4 == n) { print $1 }' n=$2 \
                  /etc/passwd | xargs`
            echo "Duplicate UID ($2): ${users}"
      fi
done
```

Remediation:
Based on the results of the script, establish unique UIDs and review all files owned by the shared UID to determine which UID they are supposed to belong to.

9.16 Check for Duplicate GIDs

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:
Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

Rationale:
User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit:
This script checks to make sure all UIDs in the `/etc/group` file are unique. You can also use the `/usr/sbin/grpck` command to check for other inconsistencies in the `/etc/group` file.

```
#!/sbin/sh

 echo "The Output for the Audit of Control 9.16 - Check for Duplicate GIDs
is"
 cat /etc/group | cut -f3 -d":" | sort -n | uniq -c |\
      while read x ; do
      [ -z "${x}" ] && break
      set - $x
      if [ $1 -gt 1 ]; then
            grps=`nawk -F: '($3 == n) { print $1 }' n=$2 \
                  /etc/group | xargs`
            echo "Duplicate GID ($2): ${grps}"
      fi
done
```

Remediation:
Based on the results of the script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

9.17 Check That Reserved UIDs Are Assigned to System Accounts

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All

Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:
Traditionally, Unix systems establish "reserved" UIDs (0-99 range) that are intended for system accounts.

Rationale:
If a user is assigned a UID that is in the reserved range, even if it is not presently in use, security exposures can arise if a subsequently installed application uses the same UID.

Audit:
This script checks to make sure that "reserved" UIDs (0-99 range) are not assigned to non-system (default) accounts.

```
#!/sbin/sh

 echo "The Output for the Audit of Control 9.17 - Check That Reserved UIDS
Are Assigned to System Accounts is"
defUsers="root daemon bin sys adm lp uucp nuucp smmsp \
      listen gdm webservd postgres svctag nobody noaccess \
      nobody4"
cat /etc/passwd |\
      awk -F: '($3 < 100) { print $1" "$3 }' |\
      while read user uid; do
            found=0
            for tUser in ${defUsers}
            do
                  if [ ${user} = ${tUser} ]; then
                        found=1
                  fi
            done
            if [ $found -eq 0 ]; then
                  echo "User $user has a reserved UID ($uid)."
            fi
      done
```

Remediation:
Based on the results of the script, change any UIDs that are in the reserved range to one that is in the user range. Review all files owned by the reserved UID to determine which UID they are supposed to belong to.

9.18 Check for Duplicate User Names

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A

Scorable Item	Yes

Description:
Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the user name.

Rationale:
If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in /etc/passwd. For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

Audit:
This script checks to make sure all user names in the `/etc/passwd` file are unique.

```
#!/sbin/sh

echo "The Output for the Audit of Control 9.18 - Check for Duplicate User
Names is"
cat /etc/passwd | cut -f1 -d":" | sort -n | uniq -c |\
      while read x ; do
      [ -z "${x}" ] && break
      set - $x
      if [ $1 -gt 1 ]; then
            uids=`nawk -F: '($1 == n) { print $3 }' n=$2 \
                  /etc/passwd | xargs`
            echo "Duplicate User Name ($2): ${uids}"
      fi
done
```

Remediation:
Based on the results of the script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

9.19 Check for Duplicate Group Names

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	Yes

Description:

Although the `groupadd` program will not let you create a duplicate group name, it is possible for an administrator to manually edit the `/etc/group` file and change the group name.

Rationale:
If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in /etc/groups. Effectively, the GID is shared, which is a security problem.

Audit:
This script checks to make sure all group names in the `/etc/group` file are unique.

```
#!/sbin/sh

echo "The Output for the Audit of Control 9.19 - Check for Duplicate Group
Names is"
cat /etc/group | cut -f1 -d":" | sort -n | uniq -c |\
      while read x ; do
      [ -z "${x}" ] && break
      set - $x
      if [ $1 -gt 1 ]; then
            gids=`nawk -F: '($1 == n) { print $3 }' n=$2 \
                  /etc/group | xargs`
            echo "Duplicate Group Name ($2): ${gids}"
      fi
done
```

Remediation:
Based on the results of the script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

9.20 Check for Presence of User .netrc Files

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the print-rhosts.aud Audit script.
Scorable Item	Yes

Description:
The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

Rationale:
The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form.

Audit:

```
#!/sbin/sh
```

```
echo "The Output from the Audit of Control 9.20 - Check for Presence of User
.netrc Files is"
for dir in `logins -ox |\
      awk -F: '($8 == "PS") { print $6 }'`; do
      for file in $dir/.netrc; do
            if [ ! -h "$file" -a -f "$file" ]; then
                  echo ".netrc file $file exists"
            fi
      done
done
```

Remediation:
Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` files and determine the action to be taken in accordance with site policy.

9.21 Check for Presence of User .forward Files

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the print-rhosts.aud Audit script.
Scorable Item	Yes

Description:
The `.forward` file specifies an email address to forward the user's mail to.

Rationale:
Use of the `.forward` file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The `.forward` file also poses a risk as it can be used to execute commands that may perform unintended actions.

Audit:
This script checks for the presence of `.forward` files that may be in violation of the site security policy.

```
#!/sbin/sh

echo "The Output from the Audit of Control 9.21 - Check for Presence of User
.forward Files is"
for dir in `logins -ox |\
      awk -F: '($8 == "PS") { print $6 }'`; do
      for file in $dir/.forward; do
            if [ ! -h "$file" -a -f "$file" ]; then
                  echo ".forward file $file exists"
            fi
```

```
        done
done
```

Remediation:
Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.forward` files and determine the action to be taken in accordance with site policy.

9.22 Find World Writable Files

Configuration Level	Level-I
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the check-world-writable-files.aud Audit script.
Scorable Item	No

Description:
Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

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.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# find / \( -fstype nfs -o -fstype cachefs \
      -o -fstype autofs -o -fstype ctfs -o -fstype mntfs \
      -o -fstype objfs -o -fstype proc \) -prune \
      -o -type f -perm -0002 -print
```

Remediation:
Removing write access for the "other" category (`chmod o-w` *<filename>*) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

9.23 Find SUID/SGID System Executables

Configuration Level	Level-I
Hardware Platform	All
OS Default	No

Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the print-sgid-files.aud and print-suid-files.aud Audit scripts.
Scorable Item	No

Description:
The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID/SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

Rationale:
There are valid reasons for SUID/SGID programs, but it is important to identify and review such programs to ensure they are legitimate.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# find / \( -fstype nfs -o -fstype cachefs \
      -o -fstype autofs -o -fstype ctfs -o -fstype mntfs \
      -o -fstype objfs -o -fstype proc \) -prune \
      -o -type f \( -perm -4000 -o -perm -2000 \) -print
```

Remediation:
Ensure that no rogue set-UID programs have been introduced into the system. Digital signatures on Solaris set-UID binaries can be verified with the `elfsign` utility:

```
# elfsign verify -e /usr/bin/su
```

References:

1. For more information consult the `elfsign` manual page.
2. The Solaris Fingerprint Database also contains cryptographic checksums for these files (along with all other files in the Solaris OS): http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl
3. Oracle, "The Solaris Fingerprint Database" http://www.sun.com/blueprints/0306/816-1148.pdf

9.24 Find Un-owned Files and Directories

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the print-unowned-objects.aud Audit script.

Scorable Item	Yes

Description:
Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

Rationale:
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.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# find / \( -fstype nfs -o -fstype cachefs \
      -o -fstype autofs -o -fstype ctfs -o -fstype mntfs \
      -o -fstype objfs -o -fstype proc \) -prune \
      -o \( -nouser -o -nogroup \) -print
```

Remediation:
Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate. Note that the Solaris OS distribution is shipped with all files appropriately owned.

9.25 Find Files and Directories with Extended Attributes

Configuration Level	Level-I
Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the check-extended-file-attributes.aud Audit script.
Scorable Item	Yes

Description:
Extended attributes are implemented as files in a "shadow" file system that is not generally visible via normal administration commands without special arguments.

Rationale:
Attackers or malicious users could "hide" information, exploits, etc. in extended attribute areas. Since extended attributes are rarely used, it is important to find files with extended attributes set.

Audit:
Perform the following to determine if the system is configured as recommended:

```
# find / \( -fstype nfs -o -fstype cachefs \
      -o -fstype autofs -o -fstype ctfs -o -fstype mntfs \
```

```
      -o -fstype objfs -o -fstype proc \) -prune \
      -o -xattr -print
```

Remediation:
Investigate any files found. Note that Solaris does not ship with files that have extended attributes.

References:
For more information on extended attributes, "`man fsattr`" and see also http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf.

Appendix A: File Backup Script

```
#!/bin/sh

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

for file in /etc/.login             /etc/X11/gdm/gdm.conf   \
            /etc/cron.d/at.allow    /etc/cron.d/at.deny           \
            /etc/cron.d/cron.allow  /etc/cron.d/cron.deny   \
            /etc/default/cron       /etc/default/inetinit   \
            /etc/default/init       /etc/default/keyserv    \
            /etc/default/login     /etc/default/passwd            \
            /etc/default/syslogd                                  \
            /etc/dt/config/*/Xresources                           \
            /etc/dt/config/*/sys.resources                        \
            /etc/dt/config/Xconfig                                \
            /etc/dt/config/Xservers                         \
            /etc/ftpd/banner.msg    /etc/ftpd/ftpaccess           \
            /etc/ftpd/ftpusers                                    \
            /etc/hosts.allow        /etc/hosts.deny         \
            /etc/init.d/netconfig   /etc/issue              \
            /etc/mail/sendmail.cf   /etc/motd                     \
            /etc/pam.conf           /etc/passwd             \
            /etc/profile                  /etc/rmmount.conf       \
            /etc/security/audit_class                             \
            /etc/security/audit_control                           \
            /etc/security/audit_event                             \
            /etc/security/audit_startup                           \
            /etc/security/audit_user                              \
            /etc/security/policy.conf                             \
            /etc/shadow                                           \
            /etc/ssh/ssh_config     /etc/ssh/sshd_config    \
            /etc/syslog.conf        /etc/system             \
            /usr/openwin/lib/app-defaults/XScreenSaver
do
    [ -f $file ] && cp -p $file $file-preCIS-$ext
done

mkdir -p -m 0700 /var/spool/cron/crontabs-preCIS-$ext
cd /var/spool/cron/crontabs
tar cf - * | (cd ../crontabs-preCIS-$ext; tar xfp -)
```

Appendix B: Service Manifest for /lib/svc/method/cis_netconfig.sh

This script is to be used for the Action described in Item 3.4 Modify IP Parameters.

```
# cat > cis_netconfig.xml << END
<?xml version="1.0"?>
<!DOCTYPE service_bundle SYSTEM
"/usr/share/lib/xml/dtd/service_bundle.dtd.1">

<service_bundle type='manifest' name='CIS:cis_netconfig'>

<service
       name='site/cis_netconfig'
       type='service'
       version='1'>

       <create_default_instance enabled='true' />

       <single_instance />

       <dependency
              name='usr'
              type='service'
              grouping='require_all'
              restart_on='none'>
              <service_fmri value='svc:/system/filesystem/minimal' />
       </dependency>

<!-- Run ndd commands after network/physical is plumbed. -->
        <dependency
                name='network-physical'
                grouping='require_all'
                restart_on='none'
                type='service'>
                <service_fmri value='svc:/network/physical' />
        </dependency>

        <!-- but run the commands before network/initial -->
        <dependent
                name='ndd_network-initial'
                grouping='optional_all'
                restart_on='none'>
                <service_fmri value='svc:/network/initial' />
        </dependent>

       <exec_method
              type='method'
              name='start'
              exec='/lib/svc/method/cis_netconfig.sh'
              timeout_seconds='60' />

       <exec method
              type='method'
              name='stop'
```

```
                exec=':true'
                timeout_seconds='60' />

        <property_group name='startd' type='framework'>
                <propval name='duration' type='astring'
                        value='transient' />
        </property_group>

        <stability value='Unstable' />

        <template>
                <common_name>
                        <loctext xml:lang='C'>
                                CIS IP Network Parameter Set
                        </loctext>
                </common_name>

        </template>
</service>

</service_bundle>
END
```

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, compared to the other settings in this 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 at boot time

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the enable-process-accounting.fin Finish script.
Scorable Item	No

Description:
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.

Rationale:
While process accounting data would seem like useful information in the wake of a potential security incident on the system, kernel-level auditing with the "`+argv,arge`" policy (as enabled in Item 4.9 Enable Kernel Level Auditing) provides more information about each process execution in general (although kernel-level auditing does not capture system resource usage information). Both process accounting and kernel-level auditing can be a significant performance drain on the system, so enabling both seems excessive given the large amount of overlap in the information each provides.

Remediation:
Perform the following to implement the recommended state:

```
# ln -s /etc/init.d/acct /etc/rc3.d/S99acct
# /etc/init.d/acct start
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls /etc/rc3.d/S99acct
/etc/rc3.d/S99acct
```

SN.2 Use full path names in /etc/dfs/dfstab file

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
The commands in the `dfstab` file are executed via the `/usr/sbin/shareall` script at boot time, as well as by administrators executing the `shareall` command during the uptime of the machine.

Rationale:
It seems prudent to use the absolute pathname to the `share` command to protect against any exploits stemming from an attack on the administrator's `PATH` environment, etc. However, if an attacker is able to corrupt *root*'s path to this extent, other attacks seem more likely and more damaging to the integrity of the system.

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/dfs
# awk '($1 == "share") { $1 = "/usr/sbin/share" }; { print }' dfstab  \
>dfstab.new
# mv dfstab.new dfstab
# pkgchk -f -n -p /etc/dfs/dfstab
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep -v "^#" /etc/dfs/dfstab | grep "share" | grep -v "/usr/sbin/share"
[there should be no output]
```

SN.3 Restrict access to power management functions

Configuration Level	Level-II
Hardware Platform	All

OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-power-restrictions.fin Finish script.
Scorable Item	No

Description:
The settings in `/etc/default/power` control which users have access to the configuration settings for the system power management and checkpoint and resume features. By setting both values to –, configuration changes are restricted to only the `root` user.

Rationale:
Given that the benchmark document disables the power management daemon by default, the effect of these settings is essentially zero, but sites may wish to make this configuration change as a "defense in depth" measure.
At present, the file `/etc/default/power` is not marked as volatile in the package database, so the `pkgchk` command in this item returns an error. The following bug has been filed in relation to this:
4503253 several ON configuration files should be type `e', not `f'

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/^PMCHANGEPERM=/  { $1 = "PMCHANGEPERM=-" }
       /^CPRCHANGEPERM=/ { $1 = "CPRCHANGEPERM=-" }
                         { print }' power >power.new
# mv power.new power
# pkgchk -f -n -p /etc/default/power
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^PMCHANGEPERM=-" /etc/default/power
PMCHANGEPERM=-
# grep "CPRCHANGEPERM=-" /etc/default/power
CPRCHANGEPERM=-
```

SN.4 Restrict access to sys-suspend feature

Configuration Level	Level-II
Hardware Platform	All
OS Default	No

Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the set-sys-suspend-restrictions.fin Finish script.
Scorable Item	No

Description:
The `/etc/default/sys-suspend` settings control which users are allowed to use the `sys-suspend` command to shut down the system.

Rationale:
Bear in mind that users with physical access to the system can simply remove power from the machine if they are truly motivated to take the system off-line, and granting `sys-suspend` access may be a more graceful way of allowing normal users to shut down their own machines.

At present, the file `/etc/default/sys-suspend` is not marked as volatile in the package database, so the `pkgchk` command in this item returns an error. The following bug has been filed in relation to this:

6555732 /etc/default/sys-suspend is an editable file

Remediation:
Perform the following to implement the recommended state:

```
# cd /etc/default
# awk '/^PERMS=/ { $1 = "PERMS=-" }
                { print }' sys-suspend >sys-suspend.new
# mv sys-suspend.new sys-suspend
# pkgchk -f -n -p /etc/default/sys-suspend
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep "^PERMS=-" /etc/default/sys-suspend
PERMS=-
```

SN.5 Create symlinks for dangerous files

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No

Solaris Security Toolkit	N/A
Scorable Item	No

Description:
The `/.rhosts`, `/.shosts`, and `/etc/hosts.equiv` files enable a weak form of access control. 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).

Rationale:
The benchmark already disables `.rhosts`-style authentication in several ways, so the additional security provided by creating these symlinks is minimal.

Remediation:
Perform the following to implement the recommended state:

```
# for file in /.rhosts /.shosts /etc/hosts.equiv; do
      rm -f $file

      ln -s /dev/null $file
done
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls -l /.rhosts
[output needed]
# ls -l /.shosts
[output needed]
# ls -l /etc/hosts.equiv
[output needed]
```

SN.7 Remove Support for Internet Services (inetd)

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
If the actions in this section result in disabling all `inetd`-based services, then there is no point in running `inetd` at boot time.

Rationale:
If `inetd`-based services are ever re-enabled in the future it will be necessary to re-enable the `inetd` daemon as well ("`svcadm enable svc:/network/inetd:default`").

Remediation:
Perform the following to implement the recommended state:

```
# svcadm disable svc:/network/inetd
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# svcs -Ho state svc:/network/inetd
disabled
```

Appendix D: Application Notes

The items in this section are specific to applications that are not enabled by default. If you are using these applications, follow the guidance in this section.

AN.1 Samba: Enable SSH Port Forwarding in Web Admin Tool

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
Samba supports use of SSH to secure the client server connection.

Rationale:
The Samba Web Admin Tool (SWAT) must be utilized with SSH to ensure a secure connection between the client and the server. The SSH daemon on the server must be configured to allow port forwarding. If SWAT is being utilized to administer Samba on the server, perform the following command:

Remediation:
Perform the following to implement the recommended state:

```
# awk '/^AllowTcpForwarding/                { $2 = "yes" }    \
     { print }' /etc/ssh/sshd_config > /etc/ssh/sshd_config.new
# /usr/bin/mv /etc/ssh/sshd_config.new /etc/ssh/sshd_config
# /usr/sbin/pkgchk -f -n -p /etc/ssh/sshd_config
# /usr/sbin/svcadm restart svc:/network/ssh
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# grep -v "^#" /etc/ssh/sshd_config | grep "^AllowTcpForwarding"
AllowTcpForwarding yes
```

AN.2 Samba: Set Secure Permissions on `smb.conf` File

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No

Solaris Security Toolkit	N/A
Scorable Item	No

Description:
The `smb.conf` file is only to be writeable by root to prevent unauthorized changes of the configuration file

Rationale:
With root the only uid able to write the configuration file, the `smb.conf` will be protected from unauthorized changes.

Remediation:
The default location for smb.conf is `/usr/local/samba/lib`. However, the file can be installed in other places by samba installation packages. If the configuration is not placed in the `/usr/local/samba/lib` directory, change the remediation and audit commands to reflect the correct location.

```
# chmod 644 /usr/local/samba/lib/smb.conf
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls –l /usr/local/samba/lib/smb.conf
-rw-r—r--    1  root    root <size of file> <date>
/usr/local/samba/lib/smb.conf
```

AN.3 Samba: Set Group Ownership of `smb.conf` File

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
The owner smb.conf is to be set to root, so that root can properly control the file.

Rationale:
By setting root as the owner, only root can manipulate the permissions on the file, and thus, only root can alter the file.

Remediation:
Perform the following to implement the recommended state:

```
# chown root /usr/local/samba/lib/smb.conf
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls –l /usr/local/samba/lib/smb.conf
-rw-r—r--    1  root    root <size of file> <date>
/usr/local/samba/lib/smb.conf
```

AN.4 Samba: Set Secure Permissions on `smbpasswd` File

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
Set the permissions of the smbpasswd file to 600, so that the contents of the file can not be viewed by any user other than root

Rationale:
If the smbpasswd file were set to read access for other users, the lanman hashes could be accessed by an unauthorized user and cracked using various password cracking tools. Setting the file to 600 limits access to the file by users other than root.

Remediation:
Perform the following to implement the recommended state:

```
# chmod 600 /etc/sfw/private/smbpasswd
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls –l /etc/sfw/private/smbpasswd
-rw-------   1 root      root      <size of file> <date>
/etc/sfw/private/smbpasswd
```

AN.5 Samba: Set Group Ownership of `smbpasswd` File

Configuration Level	Level-II
Hardware Platform	All

OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
The `smbpasswd` file contains the encrypted passwords for Samba users.

Rationale:
It is important to protect the encrypted passwords from unauthorized access to prevent the use of password cracking tools to gain access.

Remediation:
Perform the following to implement the recommended state:

```
# chgrp root /etc/sfw/private/smbpasswd
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls –l /etc/sfw/private/smbpasswd
-rw-------   1 root      root      <size of file> <date>
/etc/sfw/private/smbpasswd
```

AN.6 Samba: Set Secure smb.conf File Options

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
The `smb.conf` file is the configuration file for the Samba suite and contains runtime configuration information for Samba.

Rationale:
All configuration files must be protected from tampering.
Remediation:
Perform the following to implement the recommended state:

```
# chmod 644 /etc/samba/smb.conf
```

```
# chown root /etc/samba/smb.conf
# chgrp root /etc/samba/smb.conf
```

Audit:
Run the following command and verify that the ownership and permissions:

```
# ls -l /etc/samba/smb.conf
-rw-r--r--    1 root     root         9643 Aug  6 02:59 smb.conf
```

AN.7 sendmail: Set Secure Logfile Ownership to the *root* User

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	N/A
Scorable Item	No

Description:
Set the ownership of the sendmail log file (by default on Solaris 10, /var/log/syslog) to be owned by root.

Rationale:
By setting the ownership of the sendmail log file to root, only root can change the permissions of the log file.

Remediation:
Perform the following to implement the recommended state:

```
# chown root /var/log/syslog
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls -l /var/log/syslog
-rw-r--r--   1    root   sys    <size of file> <date> /var/log/syslog
```

AN.8 sendmail: Set Secure Permissions on Log File

Configuration Level	Level-II
Hardware Platform	All
OS Default	No
Zone Support	All
Reboot Required	No

Solaris Security Toolkit	N/A
Scorable Item	No

Description:
The log file for sendmail (by default in Solaris 10, `/var/log/syslog`) is set to 644 so that sendmail (running as root) can write to the file and anyone can read the file.

Rationale:
Setting the log file `/var/log/syslog` to 644 allows sendmail (running as root) to create entries, but prevents anyone (other than root) from modifying the log file, thus rendering the log data worthless.

Remediation:
Perform the following to implement the recommended state:

```
# chmod 644 /var/log/syslog
```

Audit:
Perform the following to determine if the system is configured as recommended:

```
# ls –l /var/log/syslog
-rw-r--r--   1    root   sys    <size of file> <date> /var/log/syslog
```

Appendix E: References

The Center for Internet Security

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

Oracle

Oracle. " Patch and Updates,"
http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage

Oracle. " Data Center Practices,"
http://www.sun.com/blueprints/browsesubject.html#dcp

Oracle. " Solaris Security Toolkit,"
http://www.sun.com/security/jass/

Oracle. " Solaris Fingerprint Database,"
http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl

Oracle. " Kerberos,"
http://www.sun.com/software/security/kerberos/

Oracle. " RBAC in the Solaris Operating Environment,"
http://www.sun.com/software/whitepapers/wp-rbac/wp-rbac.pdf

Oracle. "OracleBluePrints Program,"
http://www.sun.com/blueprints/

Oracle. " OracleSecurity Community Security Blog,"
http://blogs.sun.com/security/

Oracle. " OpenSolaris Security Community,"
http://www.opensolaris.org/os/community/security

Oracle. " OpenSolaris Security Community Library,"
http://www.opensolaris.org/os/community/security/library/

Oracle. " OpenSolaris Security Presentations,"
http://www.opensolaris.org/os/community/security/preso/

Rotundo, Scott. " Secure By Default,"
http://www.opensolaris.org/os/community/security/projects/sbd/sbd_toi.pdf

Brunette, Glenn. "Glenn Brunette's Security Weblog,"
http://blogs.sun.com/gbrunett/?entry=solaris_secure_by_default_part

Oracle. " Solaris Service Management Facility,"
http://www.sun.com/bigadmin/content/selfheal/smf-quickstart.html

Oracle. " System Administration Guide: Security Services: Using Solaris SSH,"
http://docs.sun.com/app/docs/doc/816-4557/6maosrjj5?a=view

Other Miscellaneous Documentation

University of Waterloo. "Information Systems and Technology: How To Documents,"
http://ist.uwaterloo.ca/security/howto/

Pomeranz, Hal. "Solaris BSM Auditing,"
http://www.samag.com/documents/s=9427/sam0414c/0414c.htm

Brunette, Glenn. "Hiding Within the Trees,"
http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf

Brunette, Glenn. "Managing Non-Login and Locked Solaris 10 Accounts,"
http://www.securitydocs.com/library/2636

NTP Project."Network Tome Protocol Project Home Page,"
http://www.ntp.org/

Massachusetts Institute of Technology. " Kerberos: The Network Authentication Protocol,"
http://web.mit.edu/kerberos/www/

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

Josephes, Chris. "Using Solaris SMF," O'Reilly Media, Inc. (April, 2006)
http://www.oreillynet.com/pub/a/sysadmin/2006/04/13/using-solaris-smf.html

Software

Steven M. Christensen and Associates, Inc."SunFreeware.com Home Page,"
http://www.sunfreeware.com/

SourceFORGE, "Swatch (log monitoring tool),"
http://swatch.sourceforge.net/

Miller, Todd C. “sudo Main Page,”
http://www.courtesan.com/sudo/

Appendix F: Change History

Date	Version	Changes for this version
September 28th, 2007	4.0	Public Release
July 9th, 2010	5.0	Updated for Solaris 10, update 10/09 Global changes: - Edited text to be more accurate and readable - Added item to Identification table for Configuration Level - Format migrated to new CIS template that includes description, rationale, remediation and audit steps for each item. - Benchmark reorganized to include section 9 "System Maintenance" for items that require regular monitoring. Most of these items were previously in the section titled "File/Directory Permissions/Access". These are not system hardening items but items that can change over time, such as file permissions and belong in their own section. - Tested remediation and action items and updated text throughout document as needed based on results - Checked links and updated as needed - Removed section on "Enable Required Services" since this does not belong in a system hardening benchmark - Changed refererences to Sun to Oracle. Specific changes: - Changed header for Section 1 to "Install Updates, Patches and Additional Software" - Inserted Item 1.1 "Apply Latest OS Update" - For Item 1.3 "Install Solaris 10 Encryption Kit" noted that it is installed by default for Solaris 10 08/07 and newer - Item Restrict Core Dumps to Protected Directory" changed to /var/cores from /var/core to match the new directory implemented in OpenSolaris – will provide consistency as we move forward - Added Item "Check for Remote Consoles"

	- Added Item “Check Groups in /etc/passwd” - Added Item “Lock Inactive User Accounts” - Added Item “Check That Users Are Assigned Home Directories” - Added Item “Check User Home Directory Ownership” - Added Item “Check that Defined Home Directories Exist” - Added Item “Check for Duplicate UIDs” - Added Item “Check for Duplicate GIDs” - Added Item “Check that Reserved UIDS Are Assigned to System Accounts” - Added Item “Check for Duplicate User Names” - Added Item “Check for Duplicate Group Names” - Separated Item “Check for Presence of User .netrc and .forward Files” to two items - Broke up Item 3.4 Modify Network Settings into 3 subsections: IP, ARP and TCP. Added descriptions for settings. - Added Application Notes (Appendix F) to cover third party applications - Broke out Network Parameters into sub-items - Broke out SSH Parameters into sub-items.