Solaris 10 Benchmark v4.0

(Designed for Solaris 10 11/06 and 8/07)

Edited by: Carole Fennelly

Solaris 10 Benchmark v4.0
September 28, 2007

TERMS OF USE AGREEMENT

Background.

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

No Representations, Warranties, or Covenants.

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

User Agreements.

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

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

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

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

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

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

6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.

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

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

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

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

Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i)

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

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

Special Rules

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

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

Choice of Law; Jurisdiction; Venue

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

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

CIS Solaris 10 Benchmark

This document provides recommended security settings for systems running the Solaris 10 11/06 and Solaris 10 8/07 operating systems. 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.

The technical specifications described here have been defined through a consensus of user organizations, security professionals, auditors and software vendors. Security is about managing risk, and the risk for different organizations varies. This makes it difficult, if not impossible, to define a set of hard and fast rules for securing a system. It is important that organizations review their own security policies and use this benchmark as a guide in implementing the appropriate security measures for their sites.

Organization

Each section of this document has been organized in the following manner:

Section Header

This is the title of the section and describes a general area of concern, such as "Patches and Additional Software." Each section contains one or more items that cover specific security actions or settings.

Item Number & Description

This heading describes the specific issue of concern under the heading. An item number is a unique value identifying a specific security recommendation. Each item includes a brief description indicating the purpose of the item.

Identification Table

This table identifies areas the item applies to. The identifiers for this table are as follows:

- Lists all the hardware platforms to which the action applies
- This specifies if the recommended action or setting corresponds to the default value set by the vendor.
- This specifies if the action applies to all zones (global and non-global) or the global zone only.
- **Solaris Security Toolkit**
    - This specifies how the Solaris Security Toolkit can be used to address the item.

Action

This header details the recommended action to mitigate the security risk.

Reboot Required

This item specifies if a reboot is required for the action to take effect.

Notes

This section provides notes describing the issue in detail. This information helps organizations to better understand the benefits and risks associated with a given item.Armed with this information, organizations can make more informed decisions about which recommendations to use.

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 used by applications while they are active could have unpredictable results.

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/security/jass

Backup Key Files

Before performing the steps of this benchmark it is **strongly recommended** that administrators make backup copies of critical configuration files that may get modified by various benchmark items. 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. You may want to consider performing a complete system backup to ensure that nothing is missed.

1 Install Patches and Additional Software

Updating the operating system by applying software 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. Sun's recommended patching strategy is covered in the document "Solaris Patch Management: Recommended Strategy" available from http://www.sun.com/blueprints/browsesubject.html#dcp.

1.1 Apply Latest OS Patches

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the Finish script, install-recommended-patches.fin, to install the Solaris Recommended/Security Patch Cluster

Scoring Status: Not Scorable

Action:

Create a directory to extract the patches. This directory should be owned by *root* and mode *755*, such as `/var/tmp/patches`. Obtain Sun Patch Clusters from `http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage` and look for files named `<osrel>_SunAlert_Patch_Cluster.zip`, where `<osrel>` is the Solaris OS release number. Download the Sun Alert Patch Cluster into `/var/tmp/patches.`

To implement this action, execute the following commands:

```
mkdir /var/tmp/patches
chmod 755 /var/tmp/patches
cd /var/tmp/patches
unzip -qq *_SunAlert_Patch_Cluster.zip
cd *_SunAlert_Patch_Cluster
./install_cluster -q
cd ..
rm -rf *_SunAlert_Patch_Cluster*
```

Notes:

During the cluster installation process, administrators may ignore individual patch installs that fail with either return code 2 (indicates that the patch has already been

installed on the system) or return 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 Sun 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. Sun provides digital signatures for its patches. If possible, its is recommended that patches be applied while in single user mode.

Additional Resources:

Solaris Patches and Updates

http://sunsolve.sun.com/show.do?target=patchpage

Solaris Patch Management Strategy
http://docs-pdf.sun.com/817-0574-12/817-0574-12.pdf

Solaris Patch Testing Overview
http://sunsolve.sun.com/search/document.do?assetkey=1-9-81064-1

Sun Software Update (Patch) Access Policy
http://sunsolve.sun.com/search/document.do?assetkey=1-9-83061-1

(see http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/spfaq).

1.2 Install Solaris 10 Encryption Kit

Hardware Platform	All
OS Default	Yes (Solaris 10 8/07 or newer only)
Zone Support	Global Zone Only
Reboot Required	Yes
Solaris Security Toolkit	Not implemented

Action:

For Solaris 10 11/06 or older versions of the Solaris OS, obtain the Solaris 10 Encryption Kit from

http://javashoplm.sun.com/ECom/docs/Welcome.jsp?StoreId=8&PartDetailId=Sol10-GA-Encryption-G-F&TransactionId=try

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
```

Note that the device returned in the step above the 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
```

Notes:

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)
* ARCFOUR/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.

Additional Resources:

For current information, please follow the links to Export Information at:
http://www.sun.com/sales/its/index.html

This weblog describes strong encryption in Solaris:
http://blogs.sun.com/bubbva/entry/strong_encryption_included_with_solaris

2 Restrict Services

While applying system patches (see Item 1.1 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

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Implemented by the Sysidcfg/Solaris_10/sysidcfg file along with the install-local-syslog.fin.

Action:

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

```
# netservices limited
```

Notes:

Starting with Solaris 10 11/06, Sun 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`(8) and `syslogd`(8), 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.

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 webconsole
```

Note that, if you are running `netservices limited` from a GUI console, you will need to re-login to the system since the existing windowing session will be terminated.

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, however, 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 strike a balance between security and also out of the box functionality for ease of use. If these services are not required, it is recommended they 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

Hardware Platform	All
OS Default	Enabled Local-only by SBD
Zone Support	All
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).

Action:

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

Notes:

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.

Unless your organization is specifically using the Tool Talk service, disable it.

2.2.2 Disable Local CDE Calendar Manager

Hardware Platform	All
OS Default	Enabled Local-only by SBD
Zone Support	All

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).

Action:

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

Notes:

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 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 user's calendar.

Unless your organization is specifically using the CDE Calendar Manager service, it can be disabled.

2.2.3 Disable Local Common Desktop Environment (CDE)

Hardware Platform	All
OS Default	Enabled Local-only by SBD
Zone Support	All
Solaris Security Toolkit	Use the disable-dtlogin.fin Finish script.

Action:

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

Notes:

The CDE login service provides for 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, this service should be disabled. Note that you should 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. If no GUI is needed, users should also verify that `svc:/application/gdm2-login` (GNOME Display Manager) is also disabled. It is not enabled by default in Solaris.

2.2.4 Disable Local sendmail Service

Hardware Platform	All
OS Default	Enabled Local-only by SBD
Zone Support	All
Solaris Security Toolkit	Use the disable-sendmail.fin Finish script.

Recommendation: Leave sendmail in local-only mode

Scoring Status: Scorable

Action:

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

Notes:

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, then the `sendmail` service should be completely disabled. 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.

Additional References:

Please refer to the following site for more information on sendmail:
http://www.sendmail.org/

2.2.5 Disable Local Web Console

Hardware Platform	All
OS Default	Enabled Local-only by SBD
Zone Support	All
Solaris Security Toolkit	Use the disable-smcwebserver.fin Finish script.

Action:

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

Notes:

The Java Web Console (smcwebserver (1M)) provides a common location for users to access web-based system management applications. If there is no need to use web based management applications, disable this service**.**

2.2.6 Disable Local WBEM

Applicability	All
Hardware Platform	All
OS Default	Enabled Local-only by SBD
Zone Support	All
Solaris Security Toolkit	Use the disable-wbem.fin Finish script.

Action:

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

Notes:

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).

If your site does not use Web-Based Enterprise Management, this service should be disabled.

2.2.7 Disable Local BSD Print Protocol Adapter

Hardware Platform	All
OS Default	Enabled Local-only by SBD
Zone Support	All
Reboot Required	No
SST Setting	Use the disable-lp.fin Finish script.

Action:

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

Notes:

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 have locally attached printers, the service should be disabled. Note that this service is not required for printing to a network printer.

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

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Solaris Security Toolkit	Use the disable-rpc.fin Finish script.

Action:

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

Notes:

The `keyserv` process is only required for sites that are using Sun'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. Note that "secure NFS" here should not be confused 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.

2.3.2 Disable NIS Server Daemons

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Solaris Security Toolkit	Use the disable-nis-server.fin Finish script.

Action:

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

Notes:

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.

2.3.3 Disable NIS Client Daemons

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Solaris Security Toolkit	Use the disable-nis-client.fin Finish script.

Action:

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

Notes:

If the local site is not using the NIS naming service to distribute system and user configuration information, this service may be disabled.

2.3.4 Disable NIS+ daemons

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Solaris Security Toolkit	Use the disable-nisplus-server.fin Finish script.

Action:

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

Notes:

NIS+ was designed to be a more secure version of NIS. However, the use of NIS+ has been deprecated by Sun and customers are encouraged to use LDAP as an alternative naming service.

2.3.5 Disable LDAP Cache Manager

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-ldap-client.fin Finish script.

Action:

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

Notes:

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.

2.3.6 Disable Kerberos TGT Expiration Warning

Hardware Platform	All
OS Default	Enabled Local-only by SBD
Zone Support	All
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).

Action:

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

Notes:

While Kerberos can be a security enhancement, if the local site is not currently using Kerberos then there is no need to enable this service.

2.3.7 Disable Generic Security Services (GSS) daemons

Hardware Platform	All
OS Default	Enabled
Zone Support	All
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).

Action:

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

Notes:

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 that since this service uses Sun'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

Note that GSS does not expose anything external to the system as it is configured to use TLI (protocol = ticotsord) by default.

2.3.8 Disable Volume Manager

Hardware Platform	All
OS Default	Enabled by SBD
Zone Support	Global 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).

Action;

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

Notes:

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. 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 devices that you do not want users to be able to mount.

Note that since this service uses Sun'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.

Note that `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.

2.3.9 Disable Samba Support

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-samba.fin Finish script.

Action:

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:default
```

Notes:

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. However, if this functionality is not required by the site, the service should be disabled. Note that on Solaris releases prior to 11/06 the file /etc/sfw/smb.conf does not exist.

2.3.10 Disable automount daemon

Hardware Platform	All
OS Default	Enabled in SBD
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-automount.fin Finish script

Action:

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

Notes:

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 Sun'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. If there is no need to use `automount`, this can be disabled.

Note that since this service uses Sun'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.

2.3.11 Disable Apache services

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-apache2.fin Finish script.

Action:

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

Notes:

The action in this section describes disabling the Apache 2 web server provided with Solaris 10. This is disabled by default in the OS, but not by the SBD setting. Control scripts for Apache 1 and the NCA web servers still exist, but will only start the services if the respective configuration files have been set up appropriately.

Even if this machine 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. A good starting point is the Apache Benchmark and scoring tool from CIS, http://www.cisecurity.org/bench_apache.html, and the Apache Foundation's "Security Tips" document, http://httpd.apache.org/docs-2.0/misc/security_tips.html.

If you plan to use Apache v1.3.x, make sure the run control script exists in `/etc/rc3.d/S50apache` and that the configuration files called for in the control script are set up appropriately.

2.3.12 Disable Solaris Volume Manager Services

Hardware Platform	All
OS Default	Disabled
Zone Support	Global 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 , and svc:/system/mdmonitor:default. This is included in the cis-secure.driver Toolkit driver.

Action:

Solaris 10 <= 11/06

```
svcadm disable svc:/system/metainit:default
svcadm disable svc:/platform/sun4u/mpxio-upgrade:default
svcadm disable  svc:/system/mdmonitor:default
```

Solaris 10 >= 8/07

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

Notes:

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, but not by the SBD settings. Note that the `mpxio-upgrade` service does not exist on the x86 platform. For Solaris 10 8/07, this service has been changed to use a new FMRI, as listed in the action.

2.3.13 Disable Solaris Volume Manager GUI

Hardware Platform	All
OS Default	Disabled
Zone Support	Global 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).

Action:

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

Notes:

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 enabled in the action above. 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.

Note that since these services use Sun'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 2.2 above.

2.3.14 Disable Local RPC Port Mapping Service

Hardware Platform	All
OS Default	Enabled Local-only by SBD
Zone Support	All
Reboot Required	No
Solaris Security Toolkit	Use the disable-rpc.fin Finish script.

Action:

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

Notes:

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). 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.

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 rpc/bind setprop config/enable_tcpwrappers = true; svcadm refresh rpc/bind`".

2.4 Enable Required Services

Enabling services seems to be counter-productive in a system hardening benchmark. However, the following guidance is provided to assist administrators in identifying what services need to be enabled to support specific functions.
Enabling of these services assumes that the business need is greater than the risk associated with running the service or that other measures are taken to mitigate the risk. The services described in this section are assumed to be disabled by default or have been disabled by the `netservices` (1M) command.

2.4.1 Enable Kerberos server daemons

Hardware Platform	All
OS Default	Disabled in SBD
Zone Support	All
Reboot Required	No

Scoring Status: Not Scorable

Action:

```
svcadm enable -r svc:/network/security/kadmin:default
svcadm enable -r svc:/network/security/krb5kdc:default
svcadm enable -r svc:/network/security/krb5_prop:default
```

Notes:

Kerberos can be used to provide significantly higher levels of security than standard password-based authentication if the site is willing to make the effort to transition to a "Kerberized" environment. However, if the site is not using Kerberos and/or if this machine is not configured as one of the site's Kerberos servers, there is no reason to enable these services.

For more information on Kerberos, see Sun's Kerberos site, `http://www.sun.com/software/security/kerberos/` and the MIT Kerberos site `http://web.mit.edu/kerberos/www/`.

2.4.2 Enable NFS server processes

Hardware Platform	All

OS Default	Disabled in SBD
Zone Support	Global Only
Reboot Required	No

Scoring Status: Not Scorable

Action:

No action is required as NFS is automatically started when the `share` command is issued. SBD disables NFS services and they will remain disabled unless an administrator explicitly enables them or uses the `share` command.

Notes:

Inappropriate use of NFS can be leveraged to gain unauthorized access to files and systems. Clearly there is no need to run the NFS server-related daemons on hosts that are not NFS servers. If the system is an NFS server, the administrator should take reasonable precautions when exporting file systems, including restricting NFS access to a specific range of local IP addresses and exporting file systems "read-only" where appropriate. For more information consult the `share_nfs` manual page. Much higher levels of security can be achieved by combining NFS with secure RPC or Kerberos, although the transition to these more secure environments can be difficult.

NFSv4 provides better security protections for authentication, integrity and privacy - including support for RPCSEC_GSS mechanisms Kerberos V5, LIPKEY, and SPKM-3.

2.4.3 Enable NFS client processes

Hardware Platform	All
OS Default	Disabled in SBD
Zone Support	All
Reboot Required	No

Scoring Status: Not Scorable

Action:

No action is required as the NFS client is automatically started when the `mount` or `automount` commands are run. SBD disables NFS client services and they will remain disabled unless an administrator explicitly enables them or uses the `mount`or `automount` commands

Notes:

The administrator can completely disable NFS client access by removing the NFS client software packages, but these packages will have to be re-installed and re-patched if NFS is to be re-enabled at a later date.

Note that other file transfer schemes (such as `rdist` via SSH) can often be more secure than NFS for certain applications, although the use of secure RPC or Kerberos can significantly improve NFS security. Also note that if the machine will be an NFS client, then the `rpcbind` process must be running (see Item 3.1).

2.4.4 Enable `telnet` *access*

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Reboot Required	No

Scoring Status: Not Scorable

Action:

```
svcadm enable -r svc:/network/telnet:default
```

Notes:

`telnet` uses an unencrypted network protocol, which means data from the login session (such as passwords and all other data transmitted during the session) can be stolen by eavesdroppers on the network, and the session can be hijacked by outsiders to gain access to the remote system. SSH provides encrypted network logins and should be used instead. Sites that are already using Kerberos may take advantage of the various Kerberos-specific options to enable encryption and stronger authentication in the telnet daemon itself . See the `in.telnetd (1M)` manual page for more information. Use of `telnet` is strongly discouraged.

2.4.5 Enable FTP Access

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Reboot Required	No

Scoring Status: Not Scorable

Action:

```
svcadm enable -r svc:/network/ftp:default
```

Notes:

Use of `ftp` is strongly discouraged. Like `telnet`, the FTP protocol is unencrypted, which means passwords and other data transmitted during the session can be captured by sniffing the network, and the FTP session itself can be hijacked by an external attacker. SSH provides two different encrypted file transfer mechanisms—`scp` and `sftp`—and is a more secure alternative. Even if FTP is required because the local system is an anonymous FTP server, consider requiring non-anonymous users on the system to transfer files via SSH-based protocols. For further information on securing FTP on the system, see the following items:

4.2 Enable FTP daemon Logging

6.5 Restrict FTP Use

7.13 Set Default umask for ftp Users

8.4 Create Warning Banner for FTP daemon

2.4.6 Enable boot Services

Hardware Platform	All
OS Default	Disabled
Zone Support	Global Only
Reboot Required	No

Scoring Status: Not Scorable

Action*:*

```
svcadm enable -r svc:/network/rpc/bootparams:default
```

Notes:

The `/etc/bootparams` file contains a list of client entries used by clients for booting via the `rpc.bootparamd`(1M) program. For the service to run, a bootparams database must be created. Only enable this service if you need to support clients booting over the network..

2.4.7 Enable Reverse Address Resolution Protocol (RARP)

Hardware Platform	All
OS Default	Disabled by SBD
Zone Support	Global Only
Reboot Required	No

Scoring Status: Not Scorable

Action*:*

```
svcadm enable -r svc:/network/rarp:default
```

Notes:

`rarp` is used by diskless clients to retrieve their IP address. If there is no need to support diskless clients, `rarp` may be disabled.

2.4.8 Enable DHCP Server Support

Hardware Platform	All
OS Default	Disabled in SBD
Zone Support	All
Reboot Required	No

Scoring Status: Not Scorable

Action:

```
svcadm enable -r svc:/network/dhcp-server:default
```

Notes:

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

2.4.9 Enable Domain Name System (DNS) Server Support

Hardware Platform	All
OS Default	Disabled
Zone Support	All
Reboot Required	No

Scoring Status: Not Scorable

Action:

```
svcadm enable -r svc:/network/dns/server:default
```

Notes:

This service is not needed on most systems. There should be very few name servers running at any given site. For the service to run, a DNS server configuration must be created as /etc/resolv.conf.

2.4.10 Enable Trivial File Transfer Protocol (TFTP) Services

Hardware Platform	All
OS Default	Disabled in SBD
Zone Support	All
Reboot Required	No

Scoring Status: Not Scorable

Action:

```
if [ ! "`inetadm | grep tftp`" ]; then
        cd /var/svc/profile
        egrep '^(#tftp|tftp)' /etc/init.d/inetd.conf | sed
-e 's/^#//' > inetd-tftpd.tmp
        inetconv -n -i ./inetd-tftpd.tmp -o
/var/svc/profile
        sed 's#tftp/udp6#tftp#' tftp-udp6.xml >tftp.xml
        svccfg import tftp.xml
        rm -f inetd-tftpd.tmp tftp-udp6.xml tftp.xml
fi
```

Notes:

TFTP is typically used for network booting of diskless workstations, X-terminals, and other similar devices. TFTP is also used during network installs of systems via the Solaris Jumpstart facility. Routers and other network devices may copy configuration data to remote systems via TFTP for backup. By default, TFTP is not enabled or even configured in Solaris 10. It is commented out in `/etc/inetd.conf` and therefore never loaded into SMF. The instructions above create a new service for `tftp` and enable it. Unless this system is needed in one of these roles, it is best to leave the `tftp` service disabled. If, at a later time, it is determined the service is no longer needed, it can be manually disabled with the command:

```
svcadm disable svc:/network/tftp:default
```

2.4.11 Enable Printer Server Daemons

Hardware Platform	All
OS Default	Disabled in SBD
Zone Support	All
Reboot Required	No

Scoring Status: Not Scorable

Action:

```
svcadm enable -r svc:/application/print/cleanup:default
svcadm enable -r svc:/application/print/server:default
inetadm –m rfc1179 bind_addr=””
svcadm refresh svc:/application/print/rfc1179:default
svcadm enable –r svc:/application/print/ipp-
listener:default
```

Notes:

This service should only be enabled if it is necessary to print files from this system.

Note that the "`rfc1179`" service is a BSD-compatible print spooler, which only has to be enabled if the machine is being used as a network print server by machines that require a BSD-style remote printer interface. In most cases, this "`rfc1179`" service is not necessary and should not be enabled.

Enable the ipp-listener only if you wish to support Internet Printing Protocol (IPP) printing.

2.4.12 Enable Simple Network Management Protocol (SNMP)

Hardware Platform	All
OS Default	Disabled in SBD
Zone Support	All
Reboot Required	No

Scoring Status: Not Scorable

Action:

```
svcadm enable –r svc:/application/management/sma:default
```

Notes:

If you are using SNMP to monitor the hosts on your network, it is strongly recommended that the site changes the default community string used to access data via SNMP in order to prevent unauthorized information leakage. On Solaris systems, this parameter can be changed by modifying `/etc/snmp/conf/snmpd.conf` ("`man snmpd.conf`" for further information).

While the above is the preferred method, Sun also provides an alternate SNMP agent that can be enabled as follows:

```
svcadm enable -r
svc:/application/management/seaport:default
svcadm enable -r
svc:/application/management/snmpdx:default
```

2.5 Configure TCP Wrappers

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the enable-tcpwrappers.fin Finish script and the file templates in Files/etc/hosts.allow and Files/etc/hosts.deny.

Action:

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.

Create `/etc/hosts.deny`:

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

Update default policy with `inetadm`:

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

Notes:

TCP Wrappers is a host-based Access Control System (ACL) 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 should use TCP Wrappers.

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.

Additional References:

See the documentation provided with the TCP_Wrappers source code release for information on using TCP Wrappers style filtering with other stand-alone daemons that are not spawned out of `inetd`.

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

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the enable-coreadm.fin Finish script.

Action:

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

Notes:

Core dumps, particularly those from set-UID and set-GID processes, may contain sensitive data. The above action creates a protected directory to store core dumps from set-UID and set-GID processes and also causes the system to create a log entry whenever a regular process dumps core. 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`".

3.2 Enable Stack Protection

Hardware Platform	SPARC, AMD-64, Intel with NX bit
OS Default	Yes
Zone Support	Global Only
Solaris Security Toolkit	Use the enable-stack-protection.fin Finish script.

Action:

```
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
```

Notes:

Buffer overflow exploits have been the basis for many of the recent highly publicized compromises and defacements of large numbers of Internet connected systems. Many of the automated tools in use by system crackers exploit well-known buffer overflow problems in vendor-supplied and third-party software. Enabling stack protection prevents certain classes of buffer overflow attacks and is a significant security enhancement. However, this does not protect against buffer overflow attacks that do not execute code on the stack (such as `return-to-libc` exploits).

Additional Resources:

`Solaris Non-Executable Stack Overview (Part 1)`
http://blogs.sun.com/gbrunett/entry/solaris_non_executable_stack_overview

Solaris Non-Executable Stack Continues (Part 2)
http://blogs.sun.com/gbrunett/entry/solaris_non_executable_stack_continued

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

Hardware Platform	All

OS Default	No
Zone Support	Global Only
Solaris Security Toolkit	Use the enable-rfc1948.fin Finish script.

Action:

```
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
```

Notes:

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.

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.

3.4 Modify Network Parameters

Hardware Platform	All
OS Default	See Notes
Zone Support	Global Only
Solaris Security Toolkit	Use the install-nddconfig.fin Finish script.

Action:

```
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 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 1
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 the commands. If the SMF service is created as described in Appendix B, execute the following command for it to take effect:*

```
svccfg import cis_netconfig.xml
```

When the 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.

Notes:

Note that we are creating a new script that will be executed at boot time to reconfigure various network parameters. For a more complete discussion of these parameters and their effect on the security of the system, see: http://www.sun.com/security/blueprints/

The file `cis_netconfig.xml` is an SMF manifest for the `cis_netconfig` service. Once imported into the SMF database, the `cis_netconfig.sh` will run on every system reboot to set the network parameters appropriately. Sun is moving away from legacy run control scripts in `/etc/init.d` in favor of using SMF services.

The items that are Solaris 10 11/06 and Solaris 10 8/07 defaults include:

ip_forward_src_routed
ip6_forward_src_routed
tcp_rev_src_routes
ip_forward_directed_broadcasts
ip_respond_to_timestamp
ip_respond_to_timestamp_broadcast
ip_respond_to_address_mask_broadcast
ip6_send_redirects

The items that are NOT Solaris 10 11/06 or Solaris 10 8/07 defaults include:

tcp_conn_req_max_q0
tcp_conn_req_max_q
ip_respond_to_echo_broadcast
arp_cleanup_interval
ip_ire_arp_interval
ip_ignore_redirect
ip6_ignore_redirect
tcp_extra_priv_ports_add
ip_strict_dst_multihoming
ip6_strict_dst_multihoming
ip_send_redirects

3.5 Disable Network Routing

Hardware Platform	All
OS Default	Disabled* (See Notes)
Zone Support	Global Only
Solaris Security Toolkit	Use the disable-routing.fin Finish script.

Action:

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

Notes:

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. This action is unnecessary unless it was manually enabled by the administrator or the system was previously used as a network gateway.

4 Logging

The items in this section cover enabling various different forms of system logging in order to keep track of activity on the system. Tools such as Swatch (`http://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 Sun Microsystems 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/security/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 (SST) run the script set-log-file-permissions to ensure appropriate permissions of log files.

4.1 Enable `inetd` Connection Logging

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the enable-inetd-syslog.fin Finish script.

Action:

```
inetadm -M tcp_trace=true
```

Notes:

If `inetd` is running, the "tracing" feature can be used to log information about the source of any network connections seen by the daemon. 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 should use 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.

4.2 Enable FTP daemon Logging

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the enable-ftp-debuglog.fin Finish script.

Action:

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

Notes:

If the FTP daemon is 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.

Information about FTP sessions will be logged via `syslogd` (1M), but the system must be configured to capture these messages. For further configuration information, see 4.3 Enable Debug Level Daemon Logging.

4.3 Enable Debug Level Daemon Logging

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the install-connlog.fin Finish script.

Action:

```
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:default
```

Notes:

If the FTP service is enabled on the system, Item 4.2 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 above. All of this information is logged by `syslogd` (1M), but `syslogd` (1M) must be configured to capture this information to a file. The `connlog` file should be reviewed on a regular basis. It is important to note that use of the debugging option can generate very large log files.

4.4 Capture syslog AUTH Messages

Hardware Platform	All

OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the install-authlog.fin Finish script.

Action:

```
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:default
```

Notes:

By default, Solaris systems do not capture logging information that is sent to the `LOG_AUTH` facility. However, a great deal of important security-related information is sent via this channel (e.g., successful and failed `su` attempts, failed login attempts, *root* login attempts, etc.). The above action causes this information to be captured in the `/var/log/authlog` file (which is only readable by the superuser

4.5 Enable Login Records

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the install-loginlog.fin Finish script.

Action:

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

Notes:

If the file `/var/adm/loginlog` exists, it will capture failed login attempt messages. This file does not exist by default and must be manually created as described in the action.. The `loginlog` file should be reviewed on a regular basis.

4.6 Capture All Failed Login Attempts

Hardware Platform	All

OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the set-failed-logins.fin Finish script.

Action:

```
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
```

Notes:

The `SYSLOG_FAILED_LOGINS` parameter in `/etc/default/login` 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.

4.7 Enable `cron` Logging

Hardware Platform	All
OS Default	Yes
Zone Support	All
Solaris Security Toolkit	Use the enable-cronlog.fin Finish script.

Action:

```
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
```

Notes:

Setting the `CRONLOG` parameter to `YES` in `/etc/default/cron` causes information to be logged for every cron job that gets executed on the system. This setting is the default for Solaris. Log data can be found in `/var/cron/log` and this file should be reviewed on a regular basis.

4.8 Enable System Accounting

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the enable-sar.fin Finish script.

Action:

```
svcadm enable –r svc:/system/sar:default
EDITOR=vi 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/*
```

Notes:

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*`. Once a normal baseline for the system has been established, unauthorized activity (password crackers and other CPU-intensive jobs, and activity outside of normal usage hours) may be detected due to departures from the normal system performance curve.

Note that 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.

4.9 Enable Kernel Level Auditing

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

Action:

```
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/*
```

Notes:

Kernel-level auditing provides information on commands and system calls which 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`).

Kernel-level auditing can consume large amounts of disk space and even cause a system performance impact, particularly on heavily used machines. The consensus settings above 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 Sun Microsystems as part of their "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/security/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.

5 File/Directory Permissions/Access

File and directory permission control is one of the greatest challenges of secure system administration. The system administrator can and should monitor and secure permissions on system files and directories, but has little control over user-owned files and directories. This section provides guidance on how to secure system files and directories, set secure defaults for users and monitor file permissions.

5.1 Set daemon umask

Hardware Platform	All
OS Default	Yes

Zone Support	All
Solaris Security Toolkit	Use the set-system-umask.fin Finish script with the JASS_UMASK variable.

Action:

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

Notes:

The system default `umask` should be set to at least `022` in order to prevent daemon processes from creating world-writable files by default. The NSA and DISA recommend a more restrictive `umask` values of `077.` This may cause problems for certain applications—consult vendor documentation for further information. The default setting for Solaris is `022`.

Note that there are some known bugs in the following daemons:

6299083 picld initialises picld_door file with wrong permissions after JASS

4791006 ldap_cachemgr initialises ldap_cache_door file with wrong permissions

6299080 nscd initialises name_service_door file with wrong permissions after JASS

The LDAP CacheMgr issue has been fixed but the others are still open. 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

5.2 Restrict Set-UID on User Mounted Devices

Hardware Platform	All
OS Default	Yes
Zone Support	Global Only
Solaris Security Toolkit	Use the set-rmmount-nosuid.fin Finish script.

Action:

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

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

Notes:

Removable media is one vector by which malicious software can be introduced onto the system. If the volume manager (vold) is enabled to permit users to mount external devices, this action can mitigate the risk by forcing these file systems to be mounted with the "`nosuid`" option, the administrator prevents users from bringing set-UID programs onto the system via CD-ROMs and floppy disks. Note that this setting is included in the default `rmmount.conf` file for Solaris 8 and later.

5.3 Verify System File Permissions

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the print-package-files.fin Finish script.

Action:

It is recommended that all packages on the system be checked by executing the following command:

```
pkgchk –n
```

Notes:

This action will check the default owners and access permissions for all system packages and their associated files as well as the file contents. 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
```

To force the default setting, use the "-f" option as follows:

```
pkgchk -f -n -p /etc/shadow
```

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
```

5.4 Set Sticky Bit on World Writable Directories

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the check-world-writable-files.aud Audit script.

Action:

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

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

Notes:

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

Note that the system-supplied directory /var/webconsole/tmp is world-writable and lacks the sticky bit. The following bug has been filed in relation to this:

6407912 safe default permission violations in SUNWmconr for 04/03/2006 snv nightly build

5.5 Find World Writable Files

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the check-world-writable-files.aud Audit script.

Action:

Administrators who wish to obtain a list of the world-writable files currently on the system may run the following commands:

```
find / \( -fstype nfs -o -fstype cachefs –o –fstype ctfs –
o –fstype mntfs –o –fstype objfs –o –fstype proc \) -prune
-o \
       -type f -perm -0002 -print
```

Notes:

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

5.6 Find SUID/SGID System Executables

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the print-sgid-files.aud and print-suid-files.aud Audit scripts.

Action:

Administrators who wish to obtain a list of the set-UID and set-GID programs currently installed on the system may run the following commands:

```
find / \( -fstype nfs -o -fstype cachefs –o –fstype ctfs
–o –fstype mntfs –o –fstype objfs –o –fstype proc \) -
prune -o \
       -type f \
       \( -perm -04000 -o -perm -02000 \) -print
```

Notes:

The administrator should ensure that no rogue set-UID programs have been introduced into the system. Digital signatures on set-UID binaries can be verified with the `elfsign` utility, e.g. "`elfsign verify -e /usr/bin/su`" (for more information consult the `elfsign` manual page). The Solaris Fingerprint Database (see http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl) also contains cryptographic checksums for these files (along with all other files in the Solaris OS). Tools for interacting with the Fingerprint Database are available from http://www.sun.com/blueprints/tools/.

5.7 Find Un-owned Files and Directories

Hardware Platform	All
OS Default	Yes
Zone Support	All
Solaris Security Toolkit	Use the print-unowned-objects.aud Audit script.

Action:

Administrators who wish to locate files where the user or group owner of the file is not listed in the system password or group database on their system may run the following command:

```
find / \( -fstype nfs -o -fstype cachefs –o –fstype ctfs
–o –fstype mntfs –o –fstype objfs –o –fstype proc \) -
prune -o \
       \( -nouser -o -nogroup \) -print
```

Notes:

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

5.8 Find Files and Directories with Extended Attributes

Hardware Platform	All
OS Default	Yes
Zone Support	All
Solaris Security Toolkit	Use the check-extended-file-attributes.aud Audit script.

Action:

Administrators who wish to locate files which have extended attributes set on their system may run the following command:

```
find / \( -fstype nfs -o -fstype cachefs –o –fstype ctfs
–o –fstype mntfs –o –fstype objfs –o –fstype proc \) -
prune -o \
       -xattr -print
```

Notes:

Extended attributes are implemented as files in a "shadow" file system that is not generally visible via normal administration commands without special arguments. Attackers or malicious users could therefore "hide" information, exploits, etc. in

extended attribute areas. Since extended attributes are rarely used, finding files with extended attributes set could be cause for concern. For more information on extended attributes, start with "`man fsattr`" and see also http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf.

Note that Solaris does not ship with files that have extended attributes.

6 System Access, Authentication, and Authorization

Access Control is a huge security issue that relies on organization policies and procedures to manage. The actions describes 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 mechanism in place to authorized access privileges and to revoke that authorization.

6.1 Disable `login:` Prompts on Serial Ports

Hardware Platform	All
OS Default	No
Zone Support	Global Only
Solaris Security Toolkit	Use the disable-serial-login.fin Finish script.

Action:

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

Notes:

Disabling the `login:` prompt on the system serial devices makes it more difficult for unauthorized users to attach modems, terminals, and other remote access devices to these ports. Note that this action may safely be performed even if console access to the system is provided via the serial ports, because the `login:` prompt on the console device is provided through a different mechanism.

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

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the disable-keyserv-uid-nobody.fin Finish script.

Action:

```
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
```

Notes:

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

6.3 Configure SSH

Hardware Platform	All
OS Default	See Notes
Zone Support	All
Solaris Security Toolkit	Use the set-ssh-config.fin Finish script.

Action:

```
cd /etc/ssh
cat <<EOCliConfig >>ssh_config
Host *
Protocol 2
EOCliConfig
awk '/^Protocol/                { $2 = "2" };   \
     /^X11Forwarding/           { $2 = "no" }; \
     /^MaxAuthTries/            { $2 = "5" };   \
     /^MaxAuthTriesLog/         { $2 = "0" };   \
     /^IgnoreRhosts/            { $2 = "yes" }; \
     /^RhostsAuthentication/    { $2 = "no" };  \
     /^RhostsRSAAuthentication/ { $2 = "no" };  \
     /^PermitRootLogin/         { $2 = "no" };  \
     /^PermitEmptyPasswords/    { $2 = "no" };  \
     /^#Banner/                 { $1 = "Banner" } \
     { print }' sshd_config > sshd_config.new
mv sshd_config.new sshd_config
pkgchk -f -n -p /etc/ssh/sshd_config
```

Notes:

SSH is a secure, encrypted replacement for common login services such as telnet, FTP, rlogin, rsh, and rcp. It is strongly recommended that sites abandon these 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 11/06 and Solaris 10 8/07 with the following exceptions:

`MaxAuthTries` (default is 6)

`MaxAuthTriesLog` (default is 3)

`Banner` (commented out)

X11Forwarding (default is “yes”)

X11 forwarding should be disabled 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.

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

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the disable-rhosts.fin Finish script.

Action:

```
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
```

Notes:

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). Disabling `.rhosts` support helps prevent users from subverting the system’s normal access control mechanisms.

If `.rhosts` support is required for some reason, some basic precautions should be taken when creating and managing `.rhosts` files. Never use the "`+`" wildcard character in `.rhosts` files. In fact, `.rhosts` entries should always specify a specific trusted host name along with the user name of the trusted account on that system (e.g., "`trustedhost alice`" and not just "`trustedhost`"). Avoid establishing trust relationships with systems outside of the organization's security perimeter and/or systems not controlled by the local administrative staff and/or systems that are not physically secured.. Firewalls and other network security elements should actually block `rlogin`/`rsh`/`rcp` access from external hosts. Finally, make sure that `.rhosts` files are only readable by the owner of the file (i.e., these files should be mode `600`). It is strongly recommended that SSH be used as an alternative to the “r-commands”

6.5 Restrict FTP Use

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the install-ftpusers.fin Finish script.

Action:

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

Notes:

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

The file created by the action above is similar to the one that exists by default under Solaris. Consider also adding the names of other privileged or shared accounts which may exist on your system such as user `oracle` and the account which your Web server process runs under.

If your site policy states that users have to be authorized to use ftp, consider placing all your user ids in the `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 wil need to be updated as new users are added to the system.

6.6 Verify Delay between Failed Login Attempts Set to 4

Hardware Platform	All
OS Default	Yes
Zone Support	All
Solaris Security Toolkit	Use the set-failed-logins.fin Finish script.

Action:

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

6.7 Set Default Screen Lock for CDE Users

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the enable-xscreensaver.fin Finish script.

Action:

```
for file in /usr/dt/config/*/sys.resources; do
    dir=`dirname $file | sed s/usr/etc/`
    mkdir -p $dir
    echo 'dtsession*saverTimeout: 10' >>$dir/sys.resources
    echo 'dtsession*lockTimeout: 10' >>$dir/sys.resources
    chown root:sys $dir/sys.resources
    chmod 444 $dir/sys.resources
done
```

Notes:

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

6.8 Set Default Screen Lock for GNOME Users

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the enable-xscreensaver.fin Finish script.

Action:

```
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
```

Notes:

The default timeout is 30 minutes of keyboard/mouse inactivity before a password-protected screen saver is invoked by the `xscreensaver` application used in the GNOME windowing environment. The above action reduces the default timeout value to 10 minutes, though this setting can still be overridden by individual users in their own environment.

Note that presently, the file {\tt /usr/openwin/lib/app-defaults/XScreenSaver} is not marked volatile, so the `pkgchk` command in this item produces an error. The following bug has been filed in relation to this:

6255740 XScreenSaver global property file should be marked as volatile

6.9 Restrict `at`/`cron` to Authorized Users

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the install-at-allow.fin and update-cron-deny.fin Finish scripts.

Action:

```
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
```

Notes:

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

Note that even though a given user is not listed in `cron.allow`, `cron` jobs can still be run as that user (e.g., the `cron` jobs running as user `sys` for system accounting tasks—see Item 4.8 above). `cron.allow` 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).

Additional Resources:

System Administration Guide: Security Services
http://docs.sun.com/app/docs/doc/816-4557/prbac-1?a=view

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

Hardware Platform	All
OS Default	Yes
Zone Support	All
Solaris Security Toolkit	Use the disable-remote-root-login.fin Finish script.

Action:

```
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
```

Notes:

Anonymous *root* logins should never be allowed, except on the system console in emergency situations. This is the default configuration for Solaris. At all other times, the administrator should access the system via an unprivileged account and use some authorized mechanism (such as the `su` command, or the freely-available `sudo` package) to gain additional privilege. 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 above) that require additional configuration in order 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 loggin in to the console, except for single user mode.

Additional Resources:

SPOTD: The Guide Book to Solaris Role-Based Access Control

http://blogs.sun.com/security/entry/spotd_the_guide_book_to

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

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the enable-account-lockout.fin Finish script.

Action:

```
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
```

Notes:

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 "`passwd -u` <*username*>" command). 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 a large user base.

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, "`usermod -K lock_after_retries=no oracle`" would disable account lockout for the "`oracle`" account.

By default the root account is exempt from account lockout.

6.12 Set EEPROM Security Mode and Log Failed Access

Hardware Platform	SPARC only
OS Default	No
Zone Support	Global Only
Solaris Security Toolkit	Use the install-security-mode.fin Finish script.

Action:

Create a script and store it in a local bin 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`

```
eeprom_badlogin.ksh
/bin/ed /opt/local/bin/eeprom_badlogin.ksh
a
#!/bin/ksh
badCount=`eeprom security-#badlogins | awk -F= '{ print $2
}'`

[ $badCount != 0 ] && \

   logger -p auth.notice "EEPROM Security Bad Logins is
${badCount}."
.
w
q

chmod +x /opt/local/bin/eeprom_badlogin.ksh

/opt/local/bin/eeprom_badlogin.ksh
eeprom security-#badlogins=0
if [ ! "`crontab -l | grep security-#badlogins`" ]; then
    cd /var/spool/cron/crontabs
    crontab -l >root.tmp
    echo "0 0,8,16 * * * /usr/bin/logger -p auth.info \
      \`/opt/local/bin/eeprom_badlogin.ksh`" >>root.tmp
```

```
    crontab root.tmp
    rm -f root.tmp
fi
eeprom security-mode=command
```

Notes:

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). This 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.

Note that the administrator should write down this password and place the password 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`" as *root* to erase the forgotten password, and then set a new password with "`eeprom security-mode=command`".

6.13 Secure the GRUB Menu

Hardware Platform	x86/x64 only
OS Default	No
Zone Support	Global Only
Reboot Required	No
Solaris Security Toolkit	Not Implemented

Action:

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

grub> md5crypt

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

[edit /boot/grub/menu.lst and add the following line]:

```
password -md5 [enter md5 password string]
```

[add the lock command to the "Failsafe" section after the title line]:

```
title Solaris failsafe
lock
```

```
chmod 600 /boot/grub/menu.lst
```

Notes:

GRUB is a boot loader for x86/x64 based systems that permits loading an OS image from any location. 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.

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.

7 User Accounts and Environment

Note that the items in this section are tasks that the local administrator should undertake on a regular, ongoing basis—perhaps in an automated fashion via `cron`. 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/.

7.1 Disable System Accounts

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the disable-system-accounts.fin Finish script with the JASS_ACCT_DISABLE variable.

Action:

```
passwd -l daemon
for user in bin nuucp smmsp listen gdm webservd \
    nobody noaccess nobody4; do
  passwd -l $user
  /usr/sbin/passmgmt -m -s /usr/bin/false $user
done
passwd -N sys
for user in adm lp uucp; do
  passwd -N $user
  /usr/sbin/passmgmt -m -s /usr/bin/false $user
done
```

Notes:

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 (which is the default setting for these accounts under Solaris), 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.

All `cron` jobs are disabled for accounts blocked with the "`passwd -l`" command. In fact, any login that is locked via the "passwd –l" command is restricted from running commands.

Logins that do not have a password set but must be able to run commands (such as cron or any login using ssh keys) can have their password blocked with the "`passwd -N`" command.

Additional Resources:

http://www.securitydocs.com/library/2636.

http://blogs.sun.com/gbrunett/entry/managing_non_login_and_locked

7.2 Ensure Password Fields are Not Empty

Hardware Platform	All
OS Default	Yes
Zone Support	All
Solaris Security Toolkit	Use the check-null-passwords.aud Audit script.

Action:

Run the following command and verify that no output is returned:

```
logins -p
```

Notes:

An account with an empty password field means that anybody may log in as that user without providing a password at all. All accounts should have strong passwords or should be locked via the "passwd –l" command (locked accounts may not be used to execute commands, shown by *LK* in the password field) or via 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).

7.3 Set Password Expiration Parameters on Active Accounts

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the set-user-password-reqs.fin Finish script

	with the JASS_AGING_MINWEEKS, JASS_AGING_MAXWEEKS, JASS_AGING_WARNWEEKS variables.

Action:

```
logins -ox |awk -F: '($1 == "root" || $8 == "LK") { 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
grep -v WEEKS passwd >passwd.new
cat <<EODefaults >>passwd.new

MAXWEEKS=13
MINWEEKS=1
WARNWEEKS=4
EODefaults
mv passwd.new passwd
pkgchk -f -n -p /etc/default/passwd
```

Notes

It is a good idea to force users to change passwords on a regular basis. The commands above will set all active accounts (except the *root* account) to force password changes every 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. Note that due to the fact that `/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.

Note that the actions for this item do not work on accounts stored on network directories such as LDAP.

7.4 Set Strong Password Creation Policies

Hardware Platform	All
OS Default	No

Zone Support	All
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.

Action:

```
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
```

Notes:

The policies set here are designed to force users to make better password choices when changing their passwords. While the policy given here is a reasonable starting point, administrators may wish to change some of the above parameters (particularly `PASSLENGTH` and `MINDIFF`) if changing their systems to use MD5 or Blowfish password hashes ("`man crypt.conf`" for more information). Similarly, administrators may wish to add site-specific dictionaries to the `DICTIONLIST` parameter above.

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.

7.5 Verify No Legacy "+" Entries Exist in passwd, shadow, and group Files

Hardware Platform	All
OS Default	Yes
Zone Support	All
Solaris Security Toolkit	Use the check-include-nis-map.aud Audit script.

Action:

Run the following command and verify that no output is returned:

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

Notes:

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. These entries may provide an avenue for attackers to gain privileged access on the system, and should be deleted if they exist.

7.6 Verify No UID 0 Accounts Exist Other than root

Hardware Platform	All
OS Default	Yes
Zone Support	All
Reboot Required	No
SST Setting	Use the check-uids-unique.aud Audit script.

Action:

Run the following command and verify that only the word "root" is returned:

```
logins -o | awk -F: '($2 == 0) { print $1 }'
```

Notes:

Any account with UID 0 has superuser privileges on the system. The only superuser account on the machine should be the default *root* account, and it should be accessed by logging in as an unprivileged user and using the su command to gain additional privilege.

Finer granularity access control for administrative access can be obtained by using Sun's Role-Based Access Control (RBAC) system.

Note that sites using RBAC should also monitor the /etc/user_attr file to make sure that privileges are not be

ing incorrectly managed.

Additional Resources:

Sun Microsystems. " RBAC in the Solaris Operating Environment,"
http://www.sun.com/software/whitepapers/wp-rbac/wp-rbac.pdf
http://www.opensolaris.org/os/community/security/projects/rbac/

7.7 Set Default Group for root Account

Hardware Platform	All
OS Default	Yes
Zone Support	All
Solaris Security Toolkit	Use the set-root-group.fin Finish script.

Action:

```
passmgmt -m -g 0 root
```

Notes:

For Solaris 9 and earlier, the default group for the *root* account under Solaris 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 to help prevent *root*-owned files accidentally becoming accessible to non-privileged users.

7.8 Change Home Directory for root Account

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the set-root-home-dir.fin Finish script.

Action:

```
mkdir /root

mv –i /.?* /root/

passmgmt –m –h /root root

chmod 700 /root
```

Notes:

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.

Note that if the user logs into GNOME, the directories “Desktop” and “Documents” will also be created under “/”. If these exist, they should be moved into /root/.

7.9 Ensure root PATH Integrity

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the check-root-path.aud Audit script.

Action:

```
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
```

Notes:

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.

7.10 Check Permissions on User Home Directories

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the check-home-permissions.aud Audit script.

Action:

```
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
```

Notes:

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. Making global modifications to user home directories without alerting your 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.

7.11 Check User Dot File Permissions

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the check-hidden-files.aud Audit script.

Action:

```
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
```

Notes:

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. Making global modifications to user home directories without alerting your 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.

7.12 Check Permissions on User `.netrc` Files

Hardware Platform	All
OS Default	No

Zone Support	All
Solaris Security Toolkit	Use the check-netrc-files.aud Audit script.

Action:

```
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 permission set on directory $file"
        fi
        if [ `echo $fileperm | cut -c6 ` != "-" ]
        then
         echo "Group Write permission set on directory $file"
        fi
        if [ `echo $fileperm | cut -c7 ` != "-" ]
        then
           echo "Group Execute permission set on directory $file"
        fi
        if [ `echo $fileperm | cut -c8 ` != "-" ]
        then
           echo "Other Read permission set on directory $file"
        fi
        if [ `echo $fileperm | cut -c9 ` != "-" ]
        then
           echo "Other Write permission set on directory $file"
        fi
        if [ `echo $fileperm | cut -c10 ` != "-" ]
        then
           echo "Other Execute permission set on directory $file"
        fi
      fi
    done
done
```

Notes:

`.netrc` files may contain unencrypted passwords which may be used to attack other systems. Making global modifications to user home directories without alerting your 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.

7.13 Check for Presence of User .rhosts Files

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the print-rhosts.aud Audit script.

Action:

```
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
```

Notes:

This action is only meaningful if `.rhosts` support is permitted in the file `/etc/pam.conf`. Please see Item 6.4 more for more information.

7.14 Set Default umask for Users

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the set-user-umask.fin Finish script.

Action:

```
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
```

Notes:

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

7.15 Set Default umask for ftp Users

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the set-ftpd-umask.fin Finish script.

Action:

```
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
```

Notes:

Please see Item 7.14 for a discussion of different `umask` values.

7.16 Set "mesg n" as Default for All Users

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the disable-mesg.fin Finish script.

Action:

```
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
```

Notes:

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

8 Warning Banners

Presenting some sort of statutory warning message prior to the normal user logon may assist the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific attacks at a system.

Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. Clearly, the organization's local legal counsel and/or site security administrator should review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at http://www.usdoj.gov/criminal/cybercrime/s&sappendix2002.htm.

8.1 Create Warnings for Standard Login Services

Hardware Platform	All
OS Default	No
Zone Support	All
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)

Action:

```
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
```

Notes:

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.

8.2 Create Warning Banner for CDE Users

Hardware Platform	All
OS Default	No
Zone Support	All

Action:

```
for file in /usr/dt/config/*/Xresources
do
    dir=`dirname $file | sed s/usr/etc/`
    mkdir -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."\
>>$dir/Xresources
done
chown root:sys /etc/dt/config/*/Xresources
chmod 644 /etc/dt/config/*/Xresources
```

Notes:

The standard graphical login program for Solaris requires the user to enter their username in one dialog screen and their password in a second separate dialog. The `Dtlogin*greeting.labelString` is the message for the first dialog where the

user is prompted for their username, and ...`perslabelString` is the message on the second dialog box.

8.3 Create Warning Banner for GNOME Users

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the set-greeter-warning.fin Finish script.

Action:

```
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
```

Notes:

The GNOME Display Manager is used for login session management. See the manual page `gdm(1)` for more information. The action for this item sets a warning message for GDM users before they log in.

8.4 Create Warning Banner for FTP daemon

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the set-oem-banner.fin Finish script.

Action*:*

```
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
```

Notes:

The contents of the `/etc/ftpd/banner.msg` file are sent to clients before they log in.

8.5 Check Banner Setting for telnet is Null

Hardware Platform	All
OS Default	Yes
Zone Support	All
Solaris Security Toolkit	Use the set-banner-telnetd.fin Finish script.

Action:

```
if [ -f /etc/default/telnetd ]
 then
         grep "^BANNER=$" /etc/default/telnetd
         if [ $? -ne 0 ]
         then
                 /bin/ed /etc/default/telnetd << END >
/dev/null 2>&1
 g/^BANNER=/s//#&/
 \$a
 BANNER=
 .
 w
 q
 END
         fi
 fi
```

Notes:

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. This provides information that can be used in reconnaissance for an attack. By default, Sun 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 (see 8.1 Create Warnings for Standard Login Services).

8.6 Create Power On Warning

Hardware Platform	SPARC
OS Default	No
Zone Support	All

Action:

```
eeprom oem-banner="Authorized uses only. All activity \
may be monitored and reported."
eeprom oem-banner\?=true
```

Notes:

The OEM banner will be displayed only when the system is powered on. Setting this banner has the side effect of hiding the standard Sun power-on banner, which normally displays the system host ID, MAC address, etc.

8.7 Change Default Greeting String for Sendmail

Hardware Platform	SPARC
OS Default	No
Zone Support	All
Reboot Required	No
SST Setting	set-banner-sendmail.fin

Action:

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

Notes:

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

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 /var/svc/method/cis_netconfig.sh

This script is to be used for the Action described in section 3.4 Modify Network 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='/var/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 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, given the other settings in the benchmark document, the settings presented here provide relatively little incremental security benefit. Nevertheless, none of these settings should have a significant impact on the functionality of the system, and some sites may feel that the slight security enhancement of these settings outweighs the (sometimes minimal) administrative cost of performing them.

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

SN.1 Enable process accounting at boot time

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the enable-process-accounting.fin Finish script.

Action:

```
ln -s /etc/init.d/acct /etc/rc3.d/S99acct
```

Notes:

Process accounting logs information about every process that runs to completion on the system, including the amount of CPU time, memory, etc. consumed by each process. While this would seem like useful information in the wake of a potential security incident on the system, kernel-level auditing with the "`+argv,arge`" policy (as enabled in Item 0) provides more information about each process execution in general (although kernel-level auditing does not capture system resource usage information). Both process accounting and kernel-level auditing can be a significant performance drain on the system, so enabling both seems excessive given the large amount of overlap in the information each provides.

SN.2 Use full path names in `/etc/dfs/dfstab` file

Hardware Platform	All
OS Default	No
Zone Support	All

Reboot Required	No
SST Setting	None

Action:

```
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
```

Notes:

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. It seems prudent to use the absolute pathname to the `share` command to protect against an 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.

SN.3 Restrict access to power management functions

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the set-power-restrictions.fin Finish script.

Action:

```
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
```

Notes

The settings in `/etc/default/power` control which users have access to the configuration settings for the system power management and checkpoint/resume features. By setting both values to `"-"`, configuration changes are restricted to only the superuser. 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'

SN.4 Restrict access to sys-suspend feature

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Use the set-sys-suspend-restrictions.fin Finish script.

Action:

```
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
```

Notes:

The `/etc/default/sys-suspend` settings control which users are allowed to use the `sys-suspend` command to shut down the system. Setting `"PERMS=-"` means that only the superuser is granted this privilege. Bear in mind that a user 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

SN.5 Create symlinks for dangerous files

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Not Implemented

Action:

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

```
done
```

Notes

The `/.rhosts`, `/.shosts`, and `/etc/hosts.equiv` files enable a weak form of access control (see the discussion of `.rhosts` files in the item above). 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). However, the benchmark already disables `.rhosts`-style authentication in several ways, so the additional security provided by creating these symlinks is minimal.

SN.7 Remove Support for Internet Services (`inetd`)

Hardware Platform	All
OS Default	No
Zone Support	All
Solaris Security Toolkit	Not Implemented

Action:

```
svcadm disable svc:/network/inetd:default
```

Notes:

If the actions in this section result in all `inetd`-based services being disabled, then there is no point in running `inetd` at boot time. Of course, 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`").

References

The Center for Internet Security

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

Sun Microsystems

Sun Microsystems. " Patch and Updates,"
http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage

Sun Microsystems. " Data Center Practices,"
http://www.sun.com/blueprints/browsesubject.html#dcp

Sun Microsystems. " Solaris Security Toolkit,"
http://www.sun.com/security/jass/

Sun Microsystems. " Solaris Fingerprint Database,"
http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl

Sun Microsystems. " Kerberos,"
http://www.sun.com/software/security/kerberos/

Sun Microsystems. " RBAC in the Solaris Operating Environment,"
http://www.sun.com/software/whitepapers/wp-rbac/wp-rbac.pdf

Sun Microsystems. "Sun BluePrints Program,"
http://www.sun.com/blueprints/

Sun Microsystems. " Sun Security Community Security Blog,"
http://blogs.sun.com/security/

Sun Microsystems. " OpenSolaris Security Community,"
http://www.opensolaris.org/os/community/security

Sun Microsystems. " OpenSolaris Security Community Library,"
http://www.opensolaris.org/os/community/security/library/

Sun Microsystems. " 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

Sun Microsystems. " Solaris Service Management Facility,"
http://www.sun.com/bigadmin/content/selfheal/smf-quickstart.html

Sun Microsystems. " 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/

Tenable Network Security, "Nessus Vulnerability Scanner,"
http://www.nessus.org/