Solaris Benchmark v2.1.3

(Solaris 10)

Solaris Benchmark v2.1.3

June 26, 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.
The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

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

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that

the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

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

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

CIS Solaris Benchmark

Root Shell Environment Assumed

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

Executing Actions

The actions listed in this document are written with the assumption that they will be executed in the order presented here. Some actions may need to be modified if the order is changed. Actions are written so that they may be copied directly from this document into a root shell window with a "cut-and-paste" operation.

Reboot Required

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

Backup Key Files

Before performing the steps of this benchmark it is **strongly recommended** that administrators make backup copies of critical configuration files that may get modified by various benchmark items. 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. The script provided in Appendix A of this document will automatically back up all files that may be modified by the actions below, except for the boot scripts manipulated by the various items in Section 3 of this document, which are backed up automatically by the individual items in Section 3.

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

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

1 Patches and Additional Software

1.1 Apply latest OS patches

Action:

1. Download Sun Alert Patch Cluster into `/var/sadm` (obtain Sun Patch Clusters from `ftp://patches.sun.com/patchroot/clusters` and look for files named `<osrel>_SunAlert_Patch_Cluster.zip`, where `<osrel>` is the Solaris OS release number).

2. Execute the following commands:

```
cd /var/sadm
unzip -qq *_SunAlert_Patch_Cluster.zip
cd *_SunAlert_Patch_Cluster
./install_cluster -q
cd ..
rm -rf *_SunAlert_Patch_Cluster*
```

Discussion:

Keeping up-to-date with vendor patches is critical for 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*.

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

2 Minimize system 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. Should a vulnerability be discovered in one of these services in the future, attackers should not be able to exploit the vulnerability to gain access if the vulnerable service has been disabled. 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 secure baseline

Action:

Appendix B contains a script that will disable the majority of services that are enabled by default in the Solaris environment. Save this script as `/var/svc/profile/upgrade`*, and the script will be run when the system is rebooted. After being executed during the reboot, the script is automatically renamed so that it will not be run again on future reboots.*

A copy of this script is also provided in the archive containing the PDF version of this document and the CIS scoring tool. This archive creates a "`cis`*" subdirectory when unpacked, so assuming the administrator is in the directory where the archive has been unpacked, the command to copy the script into place would be:*

```
cp cis/upgrade-cis /var/svc/profile/upgrade
```

Discussion:

This action will effectively disable a wide variety of services at the next reboot. The actions in the rest of this section allow the administrator to modify the `/var/svc/profile/upgrade` script prior to the reboot to prevent critical services from being shut off.

2.2 Only enable RPC-based services if absolutely necessary

Question:

Are any of the following statements true?

- *This machine is an NFS client or server*
- *This machine is an NIS (YP) or NIS+ client or server*
- *The Kerberos security system is in use at this site*
- *Your site uses Sun's Solaris Management Console for system administration*
- *This machine runs a GUI or GUI-based administration tool*
- *This machine is a network boot server or Jumpstart server*
- *The system is running the Volume Manager daemon (`vold`)*
- *The system uses the Solaris Volume Manager for RAID storage management*
- *The machine runs a third-party software application which is dependent on RPC support (examples: FlexLM License managers, Veritas, etc.)*

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

Action:

```
awk '/rpc\/bind:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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

When enabling this service, consider using a host-based firewall such as `ipfilter(5)` in order 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`". For more information on configuring TCP Wrappers, see Item 6.10 below.

2.3 Only enable secure RPCs if absolutely necessary

Question:

Does this system require NIS+, secure NFS, or any other secure RPC-based service?

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

Action:

```
awk '/rpc\/keyserv:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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.

2.4 Only enable NIS server daemons if absolutely necessary

Question:

Is this machine an NIS server?

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

Action:

```
awk '/nis\/server:default/ { $2 = "enable -r" }
     /nis\/passwd:default/ { $2 = "enable -r" }
     /nis\/update:default/ { $2 = "enable -r" }
     /nis\/xfr:default/    { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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.

2.5 Only enable NIS client daemons if absolutely necessary

Question:

Is NIS in use at this site?

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

Action:

```
awk '/nis\/client:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

This service must be enabled if the local site is using the NIS naming service to distribute system and user configuration information.

2.6 Only enable NIS+ daemons if absolutely necessary

Question:

Is NIS+ in use at this site?

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

Action:

```
awk '/rpc\/nisplus:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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

2.7 Only enable the LDAP cache manager if absolutely necessary

Question:

Is the LDAP directory service in use at this site?

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

Action:

```
awk '/ldap\/client:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

Clearly, if the local site is not currently using LDAP as a naming service, then there is no need to keep LDAP-related daemons running on the local machine.

2.8 Only enable Kerberos server daemons if absolutely necessary

Question:

Is this system a Kerberos Key Distribution Center (KDC) for the site?

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

Action:

```
awk '/security\/kadmin:default/    { $2 = "enable -r" }
     /security\/krb5kdc:default/   { $2 = "enable -r" }
     /security\/krb5_prop:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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/ .

2.9 Only enable Kerberos client daemon if absolutely necessary

Question:

Is the Kerberos security system in use at this site?

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

Action:

```
awk '/security\/ktkt_warn:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

Again, 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.

2.10 Only enable GSS daemon if absolutely necessary

Question:

Is the Kerberos security system in use at this site, or some other security software that makes use of the GSS API?

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

Action:

```
awk '/rpc\/gss:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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. For more information see Item 2.2 above.

2.11 Only enable GUI if absolutely necessary

Question:

Is there a business need to run a GUI on this system?

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

Action:

```
awk '/rpc-100083/          { $2 = "enable -r" }
     $3 ~ /.NOS99dtlogin/  { $t = $2; $2 = $3; $3 = $t }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

Note that for the Solaris CDE GUI to function properly, it is also necessary to enable the `rpcbind` process (see Item 2.2). The X Windows-based CDE GUI on Solaris systems and the `rpc.ttdbserverd` process that supports it have had a history of security issues. Never run any GUI-oriented service or application on a system unless that machine is protected by a strong network security infrastructure, or a host-based firewall such as IPFilter.

Note that if the local site prefers the Gnome windowing environment, then enable the `gdm2-login` service instead of the services above ("`svcadm enable svc:/application/gdm2-login:default`").

2.12 Only enable Solaris Management Console if absolutely necessary

Question:

Is the Solaris Management Console used on this system for administrative tasks?

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

Action:

```
awk '$3 ~ /.NOS90wbem/       { $t = $2; $2 = $3; $3 = $t }
     $3 ~ /.NOS90webconsole/ { $t = $2; $2 = $3; $3 = $t }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

The Solaris Management Console provides an easy-to-use administrative interface for common tasks. However, there is usually a trade-off between administrative

convenience and security, so sites should consider disabling SMC and using the standard command-line administrative interfaces instead.

Sites that are interested in simplified administration tools may also wish to investigate the Open Source Webmin administrative interface, which is now provided in `/usr/sfw` (see `webmin(1M)` in the `/usr/sfw/man` directory for more information).

2.13 Only enable the volume manager if absolutely necessary

Question:

Is there a business case why CD-ROMs and floppy disks should be automatically mounted when inserted into system drives?

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

Action:

```
awk '/rpc\/smserver:default/ { $2 = "enable -r" }
     $3 ~ /.NOS81volmgt/     { $t = $2; $2 = $3; $3 = $t }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

The Solaris volume manager automatically mounts CD-ROMs and floppy disks for users whenever a disk is inserted in the local system's drive (the `mount` command is normally a privileged command). Be aware that allowing users to mount and access data from removable media drives makes it easier for malicious programs and data to be imported onto your network.

2.14 Only enable Windows-compatibility servers if absolutely necessary

Question:

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

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

Action:

```
awk '$3 ~ /.NOS90samba/ { $t = $2; $2 = $3; $3 = $t }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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.

2.15 Only enable NFS server processes if absolutely necessary

Question:

Is this machine an NFS file server?

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

Action:

```
awk '/nfs\/server:default/   { $2 = "enable -r" }
     /nfs\/nlockmgr:default/ { $2 = "enable -r" }
     /nfs\/status:default/   { $2 = "enable -r" }
     /nfs\/mapid:default/    { $2 = "enable -r" }
     /nfs\/cbd:default/      { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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.

Note that if the system is an NFS server then the `rpcbind` process must also be running (see Item 2.2 above). Also, the `nfs/mapid` and `nfs/cbd` services are only required for the new NFSv4 protocol. If the local site is not using NFSv4, then these services need not be enabled.

2.16 Only enable `rquotad` if absolutely necessary

Question:

Is this system an NFS file server with disk quotas enabled?

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

Action:

```
awk '/nfs\/rquota:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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

2.17 Only enable NFS client processes if absolutely necessary

Question:

Is there a business need for the machine to access file systems from remote file servers via NFS?

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

Action:

```
awk '/nfs\/client:default/   { $2 = "enable -r" }
     /nfs\/nlockmgr:default/ { $2 = "enable -r" }
     /nfs\/status:default/   { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

While the `upgrade` script in Item 2.1 disables the standard NFS client processes, it is important to note that it is still possible for the superuser to mount remote file systems on the local machine via NFS. 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 again the use of secure RPC or

Kerberos can significantly improve NFS security. Also note that if the machine will be an NFS client, then the `rpcbind` process must be running (see Item 2.2 above).

2.18 Only enable automount daemon if absolutely necessary

Question:

Are any of the following statements true?

- *The system requires an automount daemon to automatically mount local and/or NFS file systems as needed.*
- *The site uses Sun's SMC graphical administrative interface for system management.*

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

Action:

```
awk '/filesystem\/autofs:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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 SMC administrative interface to function properly.

2.19 Only enable `telnet` if absolutely necessary

Question:

Is there a business need that requires users to access this system via `telnet`, rather than the more secure SSH protocol?

If the answer to this question is yes, proceed with the action below.

Action:

```
awk '/network\/telnet:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

`telnet` uses an unencrypted network protocol, which means data from the login session (such as passwords and all other data transmitted during the session) can be stolen by eavesdroppers on the network, and also that the session can be hijacked by outsiders to gain access to the remote system. 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 ("`man telnetd`" for more information).

2.20 Only enable FTP if absolutely necessary

Question:

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

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

Action:

```
awk '/network\/ftp:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

Like `telnet`, the FTP protocol is unencrypted, which means passwords and other data transmitted during the session can captured by sniffing the network, and that the FTP session itself can be hijacked by an external attacker. SSH provides two different encrypted file transfer mechanisms—`scp` and `sftp`—and should be used instead. Even if FTP is required because the local system is an anonymous FTP server, consider requiring non-anonymous users on the system to transfer files via SSH-based protocols. For further information on restricting FTP access to the system, see Item 6.5 below.

2.21 Only enable `rlogin`/`rsh`/`rcp` if absolutely necessary

Question:

Is there any business reason why `rlogin`/`rsh`/`rcp` must be used instead of the more secure `ssh`/`scp`?

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

Action:

```
awk '/network\/login:rlogin/  { $2 = "enable -r" }
     /network\/shell:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

SSH was designed to be a drop-in replacement for these protocols. It seems unlikely that there is ever a case where these tools cannot be replaced with SSH. Note that sites that are using the Kerberos security system may wish to look into using the "Kerberized" versions of rlogin/rsh that are provided with Solaris (`eklogin`, `klogin`, and `kshell`)

If these protocols are left enabled, please also see Item 7.4 for additional security-related configuration settings.

2.22 Only enable boot services if absolutely necessary

Question:

Is this machine a network boot server or Jumpstart server?

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

Action*:*

```
awk '/network\/rarp:default/   { $2 = "enable -r" }
     /rpc\/bootparams:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

These services are designed to assist machines and devices that need to download their boot images over the network from some central server. However, these services should only be enabled if the machine is actually going to be acting as a boot server.

2.23 Only enable DHCP server if absolutely necessary

Question:

Does this machine act as a DHCP server for the network?

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

Action:

```
awk '/network\/dhcp-server:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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.

2.24 Only enable DNS name server if absolutely necessary

Question:

Is this machine a DNS name server?

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

Action:

```
awk '/network\/dns\/server:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

This service is not needed on most systems. There should be very few name servers running at any given site.

2.25 Only enable TFTP if absolutely necessary

Question:

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

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

Action:

```
awk '/network\/tftp:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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

2.26 Only enable the printer daemons if absolutely necessary

Question:

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

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

Action:

```
awk '/print\/server:default/  { $2 = "enable -r" }
     /print\/cleanup:default/ { $2 = "enable"; $3 = "-r" }
     /print\/rfc1179:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

If users will never print files from this machine and the system will never be used as a print server by other hosts on the network, then it is safe to disable these services. 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.

2.27 Only enable Web server if absolutely necessary

Question:

Is there a business reason why this system must run a Web server?

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

Action:

```
awk '/network\/http:apache2/ { $2 = "enable -r" }
     $3 ~ /.NOS42ncakmod/    { $t = $2; $2 = $3; $3 = $t }
     $3 ~ /.NOS94ncalogd/    { $t = $2; $2 = $3; $3 = $t }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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*.

Note that the above action enables the Apache v2.x server provided with Solaris. If the local site prefers Apache v1.3.x then disable the `apache2` service ("`svcadm disable svc:/network/http:apache2`") and enable the v1.3.x server via the `/etc/rc3.d/S50apache` legacy run control script ("`mv /etc/rc3.d/.NOS50apache /etc/rc3.d/S50apache`").

2.28 Only enable SNMP if absolutely necessary

Question:

Are hosts at this site remotely monitored by a tool (e.g., HP OpenView, MRTG, Cricket) that relies on SNMP?

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

Action:

```
awk '$3 ~ /.NOS82initsma/  { $t = $2; $2 = $3; $3 = $t }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

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).

Note that Sun also provides an alternate SNMP agent that can be enabled via the `/etc/rc3.d/S75seaport` and `/etc/rc3.d/S76snmpdx` legacy run control scripts. However, the "Net SNMP" agent enabled in the action above is preferred for most applications.

2.29 Only enable Solaris Volume Manager services if absolutely necessary

Question:

Is the Solaris Volume Manager (SVM) used to manage storage on this machine?

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

Action:

```
awk '/system\/metainit:default/  { $2 = "enable -r" }
     /mpxio-upgrade:default/     { $2 = "enable -r" }
     /system\/mdmonitor:default/ { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

The Solaris Volume Manager 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 the site may be using an alternate volume manager (such as Veritas) rather than the bundled SVM functionality.

2.30 Only enable Solaris Volume Manager GUI if absolutely necessary

Question:

Is the Solaris Volume Manager GUI administration tool required for the administration of this system?

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

Action:

```
awk '/rpc\/mdcomm:default/  { $2 = "enable -r" }
     /rpc\/meta:default/    { $2 = "enable -r" }
     /rpc\/metamed:default/ { $2 = "enable -r" }
     /rpc\/metamh:default/  { $2 = "enable -r" }
     { print }' /var/svc/profile/upgrade \
     >/var/svc/profile/upgrade.new
mv /var/svc/profile/upgrade.new /var/svc/profile/upgrade
```

Discussion:

The Solaris Volume Manager (formerly Solaris 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.

2.31 Disable `inetd` if possible

Action:

The code in the `/var/svc/profile/upgrade` script will automatically detect whether or not the `inetd` service needs to be active and take appropriate action.

Discussion:

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`").

3 Kernel Tuning

3.1 Restrict core dumps to protected directory

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
```

Discussion:

Core dumps, particularly those from set-UID and set-GID processes, may contain sensitive data. The above action disables 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 Compatibility:

This action only applies to SPARC and AMD64-based systems.

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
```

Discussion:

Buffer overflow exploits have been the basis for many of the recent highly publicized compromises and defacements of large numbers of Internet connected systems. Many of the automated tools in use by system crackers exploit well-known buffer overflow problems in vendor-supplied and third-party software. Enabling stack protection prevents certain classes of buffer overflow attacks and is a significant security enhancement.

3.3 Restrict NFS client requests to privileged ports

Action:

```
if [ ! "`grep nfssrv:nfs_portmon /etc/system`" ]; then
   cat <<END_CFG >>/etc/system
* Require NFS clients to use privileged ports
set nfssrv:nfs_portmon = 1

END_CFG
fi
```

Discussion:

Setting this parameter causes the NFS server process on the local system to ignore NFS client requests that do not originate from the privileged port range (ports less than 1024). This should not hinder normal NFS operations but may block some automated NFS attacks that are run by unprivileged users.

3.4 Use better TCP sequence numbers

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
```

Discussion:

Setting this parameter in `/etc/default/inetinit` causes the system to use a better randomization algorithm for generating initial TCP sequence numbers. This makes remote session hijacking attacks more difficult, as well as any other network-based attack that relies on predicting TCP sequence number information.

3.5 Network Parameter Modifications

Action:

```
if [ ! -f /etc/init.d/netconfig ]; then
    cat <<END_SCRIPT >/etc/init.d/netconfig
#!/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
END_SCRIPT
    chown root:root /etc/init.d/netconfig
    chmod 744 /etc/init.d/netconfig
    ln -s /etc/init.d/netconfig /etc/rc2.d/S05netconfig
fi
```

Discussion:

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/

3.6 Additional network parameter modifications

Question:

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

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

Action:

```
routeadm -d ipv4-forwarding -d ipv6-forwarding
if [ ! "`grep redirects /etc/init.d/netconfig`" ]
then
    cat <<END_SCRIPT >>/etc/init.d/netconfig
ndd -set /dev/ip ip_strict_dst_multihoming 1
ndd -set /dev/ip ip6_strict_dst_multihoming 1
ndd -set /dev/ip ip_send_redirects 0
ndd -set /dev/ip ip6_send_redirects 0
END_SCRIPT
fi
```

Discussion:

For a more complete discussion of these parameters and their effect on the security of the system, see the URL noted in the previous item.

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://www.oit.ucsb.edu/~eta/swatch/) and Logcheck (http://sourceforge.net/projects/sentrytools/) 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.

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

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

4.1 Turn on `inetd` tracing

Action:

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

Discussion:

If `inetd` is running, it is a good idea to make use of the "tracing" feature of the Solaris `inetd` that logs 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 Syslog and by default Solaris systems deposit this logging information in `/var/adm/messages` with other system log messages. Should the administrator wish to capture this information in a separate file, simply modify `/etc/syslog.conf` to log `daemon.notice` to some other log file destination (see Item 4.3 below).

4.2 Turn on additional logging for FTP daemon

Action:

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

Discussion:

If the FTP daemon is left on, 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 the user accidentally types their password at the username prompt.

Information about FTP sessions will be logged via Syslog, but the system must be configured to capture these messages. For further configuration information, see Item 4.3 below.

4.3 Capture FTP and `inetd` Connection Tracing Info

Action:

```
if [ ! "`grep -v '^#' /etc/syslog.conf | \
         grep /var/log/connlog`" ]; then
    echo -e "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
```

Discussion:

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 to Syslog, but the Syslog daemon must be configured to capture this information to a file. The `connlog` file should be reviewed on a regular basis.

4.4 Capture messages sent to syslog AUTH facility

Action:

```
if [ ! "`grep -v '^#' /etc/syslog.conf | \
         grep /var/log/authlog`" ]; then
    echo –e "auth.info\t\t\t/var/log/authlog" \
        >>/etc/syslog.conf
fi
logadm -w authlog -C 13 -a 'pkill -HUP syslogd' \
       /var/log/authlog
```

Discussion:

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). The `authlog` file should be reviewed on a regular basis.

4.5 Create /var/adm/loginlog

Action:

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

Discussion:

If it exists, the file `/var/adm/loginlog` will capture failed login attempt messages (this file does not exist by default). Administrators may also modify the `SYSLOG_FAILED_LOGINS` parameter in `/etc/default/login` to control how many login failures are allowed before log messages are generated—if set to zero then all failed logins will be logged. The `loginlog` file should be reviewed on a regular basis.

4.6 Turn on `cron` logging

Action:

```
cd /etc/default
awk '/CRONLOG=/ { $1 = "CRONLOG=YES" }; \
                { print }' cron > cron.new
mv cron.new cron
pkgchk -f -n -p /etc/default/cron
```

Discussion:

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.

4.7 Enable system accounting

Action:

```
svcadm enable svc:/system/sar:default
/usr/bin/su sys -c crontab <<END_ENTRIES
0,20,40 * * * * /usr/lib/sa/sa1
45 23 * * * /usr/lib/sa/sa2 -s 0:00 -e 23:59 -i 1200 -A
END_ENTRIES
```

Discussion:

System accounting gathers baseline system data (CPU utilization, disk I/O, etc.) every 20 minutes. 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.

4.8 Enable kernel-level auditing

Action:

```
if [ ! "`grep c2audit:audit_load /etc/system`" ]
then
  echo y | /etc/security/bsmconv
  cd /etc/security
  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
  cat <<END_PARAMS >audit_control
dir:/var/audit
flags:lo,ad,cc
naflags:lo,ad,ex
minfree:20
END_PARAMS
  echo root:lo,ad:no >audit_user
  awk '/^auditconfig/ { $1 = "/usr/sbin/auditconfig" }; \
    { print }' audit_startup >audit_startup.new
  echo '/usr/sbin/auditconfig -setpolicy +argv,arge' \
     >>audit_startup.new
  mv audit_startup.new audit_startup
  pkgchk -f -n -p /etc/security/audit_event
  pkgchk -f -n -p /etc/security/audit_control
  pkgchk -f -n -p /etc/security/audit_startup
  cd /var/spool/cron/crontabs
  crontab -l >root.tmp
  echo '0 * * * * /usr/sbin/audit -n' >>root.tmp
  crontab root.tmp
  rm -f root.tmp
fi
```

Discussion:

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 CD-ROMs and floppy disks 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. A more detailed discussion of the various auditing flags and their meaning can be found in *http://www.samag.com/documents/s=9427/sam0414c/0414c.htm*. 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.

4.9 Confirm permissions on system log files

Action:

```
pkgchk -f -n -p /var/log/syslog
pkgchk -f -n -p /var/log/authlog
pkgchk -f -n -p /var/adm/utmpx
pkgchk -f -n -p /var/adm/wtmpx
chown root:sys /var/adm/loginlog
chown root:root /var/cron/log /var/adm/messages \
  /var/log/connlog
chmod go-wx /var/adm/messages
chmod go-rwx /var/adm/loginlog /var/cron/log \
  /var/log/connlog
chown sys:sys /var/adm/sa/*
chmod go-wx /var/adm/sa/*
dir=`awk -F: '($1 == "dir") { print $2 }' \
   /etc/security/audit_control`
chown root:root $dir/*
chmod go-rwx $dir/*
```

Discussion:

It's critical to protect system log files from being modified by unauthorized individuals. Also, certain logs contain sensitive data that should only be available to the system administrator. Most of the settings enforced here reflect the standard Solaris default permissions.

5 File/Directory Permissions/Access

5.1 *Set daemon umask*

Action:

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

Discussion:

The system default `umask` should be set to at least `022` in order to prevent daemon processes from creating world-writable files by default. More restrictive `umask` values (such as `077`) can be used but may cause problems for certain applications—consult vendor documentation for further information. `022` is the default setting for Solaris.

5.2 Add 'nosuid' option to `/etc/rmmount.conf`

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
```

Discussion:

Removable media is one vector by which malicious software can be introduced onto the system. 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 `passwd`, `shadow`, and `group` file permissions

Action:

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

Discussion:

This action will enforce the default owners and access permissions for these files.

5.4 World-writable directories should have their sticky bit set

Action:

The automated tool supplied with this benchmark will flag world-writable directories that do not have the sticky bit set.

Administrators who wish to obtain a list of these directories may execute the following commands

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

Discussion:

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

5.5 Find unauthorized world-writable files

Action:

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

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

```
find / \( -fstype nfs -o -fstype cachefs \) -prune -o \
       -type f -perm -0002 -print
```

Discussion:

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

5.6 Find unauthorized SUID/SGID system executables

Action:

The automated testing tool supplied with this benchmark will flag unexpected set-UID and set-GID applications on the system.

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 / \( -fstype nfs -o -fstype cachefs \) -prune -o \
       -type f \
       \( -perm -04000 -o -perm -02010 \) -print
```

Discussion:

The administrator should take care to ensure that no rogue set-UID programs have been introduced into the system. Checksums 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/. Information on the set-UID and set-GID applications that normally ship with Solaris systems can be found at http://ist.uwaterloo.ca/security/howto/.

5.7 Find "Unowned" Files and Directories

Action:

The automated testing tool supplied with this benchmark will flag files and directories where the user or group owner of the file is not listed in the system password or group database.

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

```
find / \( -fstype nfs -o -fstype cachefs \) -prune -o \
       \( -nouser -o -nogroup \) -print
```

Discussion:

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.

5.8 Find Files and Directories with Extended Attributes

Action:

The automated testing tool supplied with this benchmark will flag files and directories which have extended attributes set.

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

```
find / \( -fstype nfs -o -fstype cachefs \) -prune -o \
       -xattr -print
```

Discussion:

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*.

6 System Access, Authentication, and Authorization

6.1 Disable `login:` prompts on serial ports

Action:

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

Discussion:

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

6.2 Disable "nobody" access for secure RPC

Action:

```
cd /etc/default
awk '/ENABLE_NOBODY_KEYS=/ \
        { $1 = "ENABLE_NOBODY_KEYS=NO" }
        { print }' keyserv >keyserv.new
cp –p keyserv keyserv.old
```

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

Discussion:

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

Action:

```
cd /etc/ssh
cat <<EOCliConfig >>ssh_config
Host *
Protocol 2
EOCliConfig
awk '/^Protocol/                { $2 = "2" };   \
     /^X11Forwarding/           { $2 = "yes" }; \
     /^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
```

Discussion:

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.

For more information on building the current OpenSSH distribution from source, see `www.openssh.com`. Sun also publishes information on building OpenSSH for Solaris (see `http://www.sun.com/security/blueprints/`).

6.4 Remove `.rhosts` support in `/etc/pam.conf`

Action:

```
cd /etc
grep -v rhosts_auth pam.conf > pam.conf.new
mv pam.conf.new pam.conf
pkgchk -f -n -p /etc/pam.conf
```

Discussion:

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. 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`).

6.5 Create `/etc/ftpd/ftpusers`

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
```

Discussion:

`ftpusers` contains a list of users who *are not* allowed to access the system via FTP. Generally, only normal users should ever access the system via FTP—there should be

no reason for “system” type accounts to be transferring information via this mechanism. Certainly the `root` account should *never* be allowed to transfer files directly via FTP.

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.

6.6 Prevent email server from listening on external interfaces

Question:

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

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

Action:

```
cd /etc/mail
awk '/DaemonPortOptions=/ && /inet6/ \
         { print "#" $0; next };
     /DaemonPortOptions=/ && !/inet6/ \
         { print $0 ", Addr=127.0.0.1"; next };
     { print }' sendmail.cf >sendmail.cf.new
mv sendmail.cf.new sendmail.cf
pkgchk -f -n -p /etc/mail/sendmail.cf
```

Discussion:

By default, the Sendmail daemon on Solaris systems listens on port 25/tcp for incoming email messages. However, if the machine is not acting as an email server, then there should never be a reason for this system ever to receive incoming email messages from other hosts on the network. The above configuration changes will tell the Sendmail daemon to listen only on the internal "loopback" network for outgoing messages generated on the local system, preventing direct access to the Sendmail daemon from external network devices and greatly reducing the impact of future Sendmail vulnerabilities on the local machine.

6.7 Prevent Syslog from accepting messages from network

Question:

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

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

Action:

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

Discussion:

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

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

6.8 Disable XDMCP port

Action:

```
if [ ! -f /etc/dt/config/Xconfig ]; then
    mkdir -p /etc/dt/config
    cp /usr/dt/config/Xconfig /etc/dt/config
fi
cd /etc/dt/config
awk '/Dtlogin.requestPort:/ \
     { print "Dtlogin.requestPort: 0"; next }
     { print }' Xconfig > Xconfig.new
mv Xconfig.new Xconfig
chown root:root Xconfig
chmod 444 Xconfig
cd /etc/X11/gdm
awk '/^\[xdmcp\]/, /^Enable=/ \
         { if ($1 ~ /^Enable=/) $1 = "Enable=false" }
     { print }' gdm.conf > gdm.conf.new
mv gdm.conf.new gdm.conf
pkgchk -f -n -p /etc/X11/gdm/gdm.conf
```

Discussion:

The standard GUI login provided on most Unix systems can act as a remote login server to other devices (including X terminals and other workstations). Setting `Dtlogin.requestPort` to zero in the `Xconfig` file and/or disabling XDMCP in `gdm.conf` prevents these login GUIs from even hearing requests for remote login services.

6.9 Prevent X server from listening on port 6000/tcp

Action:

```
if [ -f /etc/dt/config/Xservers ]; then
    file=/etc/dt/config/Xservers
else
    file=/usr/dt/config/Xservers
fi
awk '/Xserver/ && !/^#/ && !/-nolisten tcp/ \
       { print $0 " -nolisten tcp"; next }; \
       { print }' $file > $file.new
mkdir -p /etc/dt/config
mv $file.new /etc/dt/config/Xservers
chown root:sys /etc/dt/config/Xservers
chmod 444 /etc/dt/config/Xservers
cd /etc/X11/gdm
awk '/^command=/ && !/-nolisten tcp/ \
       { print $0 " -nolisten tcp"; next }; \
       { print }' gdm.conf > gdm.conf.new
mv gdm.conf.new gdm.conf
pkgchk -f -n -p /etc/X11/gdm/gdm.conf
```

Discussion:

X servers listen on port 6000/tcp for messages from remote clients running on other systems. However, X Windows uses a relatively insecure authentication protocol—an attacker who is able to gain unauthorized access to the local X server can easily compromise the system. Invoking the "`-nolisten tcp`" option causes the X server not to listen on port 6000/tcp by default.

This does prevent authorized remote X clients from displaying windows on the local system as well. However, the forwarding of X events via SSH will still happen normally. This is the preferred and more secure method transmitting results from remote X clients in any event.

6.10 Configure TCP Wrappers

Action:

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

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

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

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

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

3. Update default policy with `inetadm`:

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

Discussion:

TCP Wrappers allow the administrator 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, Sendmail, and `rpcbind` that ship with Solaris 10 can also use TCP Wrappers to filter access. For example, the command "`svccfg -s rpc/bind setprop config/enable_tcpwrappers=true`" will enable TCP Wrappers for the `rpc/bind` service. 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`.

6.11 Set default locking screensaver timeout

Action:

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

Discussion:

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

6.12 Remove empty crontab files and restrict file permissions

Action:

```
cd /var/spool/cron/crontabs
for file in *
do
   lines=`grep -v '^#' $file | wc -l | sed 's/ //g'`
   if [ "$lines" = "0" ]; then
       crontab -r $file
   fi
done
chown root:sys *
chmod 400 *
```

Discussion:

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

Allowing unprivileged users to read or (even worse) modify system crontab files can create the potential for a local user on the system to gain elevated privileges.

6.13 Restrict `at`/`cron` to authorized users

Action:

```
cd /etc/cron.d
rm -f cron.deny at.deny
echo root >cron.allow
cp /dev/null at.allow
chown root:root cron.allow at.allow
chmod 400 cron.allow at.allow
```

Discussion:

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

Note that even though a given user is not listed in `cron.allow`, `cron` jobs can still be run as that user (e.g., the `cron` jobs running as user `sys` for system accounting tasks—see Item 4.7 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).

6.14 Restrict root logins to system console

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
```

Discussion:

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.

6.15 Set retry limit for account lockout

Action:

```
cd /etc/default
awk '/RETRIES=/ { $1 = "RETRIES=5" }
     { 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
```

Discussion:

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.

Note that while the actions above set the lockout limit at 5, the US Department of Defense standard is even more restrictive, allowing only 3 failures. Users at DoD facilities are required to use this more restrictive setting.

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.

6.16 Set EEPROM `security-mode` and log failed access

Hardware Compatibility:

This action only applies to SPARC-based systems (not Solaris x86 or AMD64).

Action:

```
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 \
      \`/usr/sbin/eeprom security-#badlogins\`" >>root.tmp
    crontab root.tmp
    rm -f root.tmp
fi
eeprom security-mode=command
```

Discussion:

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`".

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 Block system accounts

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 /dev/null $user
done
passwd -N sys
for user in adm lp uucp; do
  passwd -N $user
  /usr/sbin/passmgmt -m -s /dev/null $user
done
```

Discussion:

Accounts that are not being used by regular users should be locked. Not only should the password field for the account be set to an invalid string (which is the default setting for these accounts under Solaris), but also the shell field in the password file should contain an invalid shell. `/dev/null` is a good choice because it is not a valid login shell, and should an attacker attempt to replace it with a copy of a valid shell the system will not operate properly.

All `cron` jobs are disabled for accounts blocked with the "`passwd –l`" command. Normal system maintenance `cron` jobs can still function for accounts blocked with "`passwd –N`". For more information see http://www.securitydocs.com/library/2636.

7.2 Verify that there are no accounts with empty password fields

Action:

The command

```
logins -p
```

should return no lines of output.

Discussion:

An account with an empty password field means that anybody may log in as that user without providing a password at all. All accounts should have strong passwords or should be locked by using a password string like "NP" or "*LK*".

7.3 Set account expiration parameters on active accounts

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
```

Discussion:

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

7.4 Set strong password enforcement policies

Action:

```
cd /etc/default
awk '/PASSLENGTH=/   { $1 = "PASSLENGTH=6" };
     /NAMECHECK=/    { $1 = "NAMECHECK=YES" };
     /HISTORY=/      { $1 = "HISTORY=4" };
     /MINDIFF=/      { $1 = "MINDIFF=3" };
     /MINALPHA=/     { $1 = "MINALPHA=2" };
     /MINUPPER=/     { $1 = "MINUPPER=1" };
     /MINLOWER=/     { $1 = "MINLOWER=1" };
     /MINNONALPHA=/  { $1 = "MINNONALPHA=1" };
     /MAXREPEATS=/   { $1 = "MAXREPEATS=2" };
     /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
```

Discussion:

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). A `HISTORY` value of 4, combined with passwords that expire every 91 days (see Item 7.3 above) means that users will not be able to re-use the same password within any given year. However, DISA requirements mandate a longer `HISTORY` period for US DoD installations (`HISTORY=10`), so be sure to consult your local security policies before adopting any of the values given above.

7.5 Verify no legacy '+' entries exist in `passwd`, `shadow`, and `group` files

Action:

The command

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

should return no lines of output.

Discussion:

'+' entries in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on 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 that no UID 0 accounts exist other than `root`

Action:

The command

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

should return only the word "`root`".

Discussion:

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 the freely-available `sudo` program (http://www.courtesan.com/sudo/) or Sun's own Role-Based Access Control (RBAC) system. For more information on Solaris RBAC, see http://wwws.sun.com/software/whitepapers/wp-rbac/. Note that sites using RBAC should also monitor the `/etc/user_attr` file to make sure that privileges are not being incorrectly managed.

7.7 Set default group for root account

Action:

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

Discussion:

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

Action:

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

Discussion:

Including the current working directory ('.') or other writable directory in root's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program.

7.9 User home directories should be mode 750 or more restrictive

Action:

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

Discussion:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges. Disabling "read" and "execute" access for users who are not members of the same group (the "other" access category) allows for appropriate use of discretionary access control by each user. While the above modifications are relatively benign, making global modifications to user home directories without alerting your user community can result in unexpected outages and unhappy users.

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

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 "$file" ]; then
            chmod go-w "$file"
        fi
    done
done
```

Discussion:

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

7.11 Remove user `.netrc` files

Action:

```
for dir in `logins -ox | \
    awk -F: '($8 == "PS") { print $6 }'`
do
    rm -f $dir/.netrc
done
```

Discussion:

`.netrc` files may contain unencrypted passwords which may be used to attack other systems. While the above modifications are relatively benign, making global modifications to user home directories without alerting your user community can result in unexpected outages and unhappy users.

7.12 Set default umask for users

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
```

Discussion:

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

7.13 Set default umask for FTP users

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
```

Discussion:

The Solaris FTP daemon is derived from the Washington University FTP daemon, so the default umask value is set in `/etc/ftpd/ftpaccess`. Please see previous item for a discussion of different umask values.

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

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
```

Discussion:

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

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

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
```

Discussion:

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 warnings for GUI-based logins

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
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
```

Discussion:

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. Settings for the Gnome windowing environment are found in the `gdm.conf` file.

8.3 Create warnings for FTP daemon

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
```

Discussion:

The Solaris FTP daemon is based on the popular Washington University FTP daemon (WU-FTPD), which is an Open Source program widely distributed on the Internet.

8.4 Create power-on warning

Hardware Compatibility:

This action only applies to SPARC-based systems (not Solaris x86 or AMD64).

Action:

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

Discussion:

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.

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: /var/svc/profile/upgrade Script

Note that this script extends over several pages. When copying it from this document, make sure to capture the entire script

```
# Item 2.2, rpcbind
svcadm disable svc:/network/rpc/bind:default

# Item 2.3, secure RPC
svcadm disable svc:/network/rpc/keyserv:default

# Item 2.4, NIS server
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

# Item 2.5, NIS client
svcadm disable svc:/network/nis/client:default

# Item 2.6, NIS+
svcadm disable svc:/network/rpc/nisplus:default

# Item 2.7, LDAP cache mgr
svcadm disable svc:/network/ldap/client:default

# Item 2.8, Kerberos server
svcadm disable svc:/network/security/kadmin:default
svcadm disable svc:/network/security/krb5kdc:default
svcadm disable svc:/network/security/krb5_prop:default

# Item 2.9, Kerberos client
svcadm disable svc:/network/security/ktkt_warn:default

# Item 2.10, GSS
svcadm disable svc:/network/rpc/gss:default

# Item 2.11, GUI
mv /etc/rc2.d/S99dtlogin /etc/rc2.d/.NOS99dtlogin 2> /dev/null
svcadm disable svc:/network/rpc-100083_1/rpc_tcp:default

# Item 2.12, Solaris Management Console
mv /etc/rc2.d/S90wbem /etc/rc2.d/.NOS90wbem 2> /dev/null
mv /etc/rc2.d/S90webconsole /etc/rc2.d/.NOS90webconsole 2> /dev/null

# Item 2.13, volume manager
svcadm disable svc:/network/rpc/smserver:default
mv /etc/rc3.d/S81volmgt /etc/rc3.d/.NOS81volmgt 2> /dev/null

# Item 2.14, SAMBA
mv /etc/rc3.d/S90samba /etc/rc3.d/.NOS90samba 2> /dev/null
```

```
# Item 2.15, NFS server
svcadm disable svc:/network/nfs/server:default
svcadm disable svc:/network/nfs/cbd:default
svcadm disable svc:/network/nfs/mapid:default

# Item 2.16, rquota
svcadm disable svc:/network/nfs/rquota:default

# Item 2.17, NFS client
svcadm disable svc:/network/nfs/client:default

# Both NFS servers and clients need these (see 2.16 and 2.18 above)
svcadm disable svc:/network/nfs/status:default
svcadm disable svc:/network/nfs/nlockmgr:default

# Item 2.18, auto mounter
svcadm disable svc:/system/filesystem/autofs:default

# Item 2.19, telnet server
svcadm disable svc:/network/telnet:default

# Item 2.20, FTP server
svcadm disable svc:/network/ftp:default

# Item 2.21, rlogin/rsh servers
svcadm disable svc:/network/login:rlogin
svcadm disable svc:/network/shell:default

# Item 2.22, boot services
svcadm disable svc:/network/rpc/bootparams:default
svcadm disable svc:/network/rarp:default

# Item 2.23, DHCP server
svcadm disable svc:/network/dhcp-server:default

# Item 2.24, DNS server
svcadm disable svc:/network/dns/server:default

# Set up TFTP server entry if necessary
if [ ! "`inetadm | grep tftp`" ]; then
        cd /var/svc/profile
        echo 'tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd
/tftpboot' >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

# Item 2.25, TFTP server
svcadm disable svc:/network/tftp:default
```

```
# Item 2.26, print servers
# Use -s for print/cleanup because it has already been started
# before upgrade script is read
svcadm disable -s svc:/application/print/cleanup:default
svcadm disable svc:/application/print/server:default
svcadm disable svc:/application/print/rfc1179:default

# Item 2.27, Web servers
# Apache 2.x (the first line below) is preferred.  If you would
# rather run Apache 1.3.x, then disable the Apache 2.x service and
# move the /etc/rc3.d/S50apache script back into place.
#
svcadm disable svc:/network/http:apache2
mv /etc/rc3.d/S50apache /etc/rc3.d/.NOS50apache 2> /dev/null
mv /etc/rc2.d/S42ncakmod /etc/rc2.d/.NOS42ncakmod 2> /dev/null
mv /etc/rc2.d/S94ncalogd /etc/rc2.d/.NOS94ncalogd 2> /dev/null

# Item 2.28, SNMP server (initsma is net-snmp)
mv /etc/rc3.d/S82initsma /etc/rc3.d/.NOS82initsma 2> /dev/null

# Item 2.29, Solaris Volume Manager (software RAID) services
svcadm disable svc:/system/metainit:default
svcadm disable svc:/platform/sun4u/mpxio-upgrade:default
svcadm disable svc:/system/mdmonitor:default

# Item 2.30, Solaris Volume Manager GUI services
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

# The following services are not frequently used.  It is unlikely that
# you will need to modify any of the lines below this point.
#
svcadm disable svc:/network/chargen:dgram
svcadm disable svc:/network/chargen:stream
svcadm disable svc:/network/daytime:dgram
svcadm disable svc:/network/daytime:stream
svcadm disable svc:/network/discard:dgram
svcadm disable svc:/network/discard:stream
svcadm disable svc:/network/echo:dgram
svcadm disable svc:/network/echo:stream
svcadm disable svc:/network/time:dgram
svcadm disable svc:/network/time:stream
svcadm disable svc:/network/rpc/rex:default
svcadm disable svc:/network/rexec:default
svcadm disable svc:/network/uucp:default
svcadm disable svc:/network/comsat:default
svcadm disable svc:/network/rpc/spray:default
svcadm disable svc:/network/rpc/wall:default
svcadm disable svc:/network/tname:default
svcadm disable svc:/network/talk:default
svcadm disable svc:/network/finger:default
svcadm disable svc:/network/rpc/rstat:default
svcadm disable svc:/network/rpc/rusers:default
svcadm disable svc:/network/rpc/ocfserv:default
svcadm disable svc:/network/login:eklogin
```

```
svcadm disable svc:/network/login:klogin
svcadm disable svc:/network/shell:kshell
# Use -s for system/power because it has already been started
# before upgrade script is read
svcadm disable -s svc:/system/power:default
svcadm disable svc:/network/slp:default
svcadm disable svc:/application/management/webmin:default
svcadm disable svc:/system/consadm:default
svcadm disable svc:/application/gdm2-login:default
svcadm disable svc:/application/print/ipp-listener:default
# Use -s for system/name-service-cache because it has already
# been started before upgrade script is read
svcadm disable -s svc:/system/name-service-cache:default
svcadm disable svc:/network/apocd/udp:default
svcadm disable svc:/application/x11/xfs:default
svcadm disable svc:/application/font/stfsloader:default
svcadm disable svc:/network/rpc-100068_2-5/rpc_udp:default
svcadm disable svc:/network/rpc-100235_1/rpc_ticotsord:default
mv /etc/rc2.d/S40llc2 /etc/rc2.d/.NOS40llc2 2> /dev/null
mv /etc/rc2.d/S47pppd /etc/rc2.d/.NOS47pppd 2> /dev/null
mv /etc/rc2.d/S70uucp /etc/rc2.d/.NOS70uucp 2> /dev/null
mv /etc/rc2.d/S72autoinstall /etc/rc2.d/.NOS72autoinstall 2> /dev/null
mv /etc/rc2.d/S73cachefs.daemon /etc/rc2.d/.NOS73cachefs.daemon \
       2> /dev/null
mv /etc/rc2.d/S89bdconfig /etc/rc2.d/.NOS89bdconfig 2> /dev/null
mv /etc/rc2.d/S89PRESERVE /etc/rc2.d/.NOS89PRESERVE 2> /dev/null
mv /etc/rc3.d/S16boot.server /etc/rc3.d/.NOS16boot.server 2> /dev/null
mv /etc/rc3.d/S52imq /etc/rc3.d/.NOS52imq 2> /dev/null
mv /etc/rc3.d/S84appserv /etc/rc3.d/.NOS84appserv 2> /dev/null
mv /etc/rc3.d/S75seaport /etc/rc3.d/.NOS75seaport 2> /dev/null
mv /etc/rc3.d/S76snmpdx /etc/rc3.d/.NOS76snmpdx 2> /dev/null
mv /etc/rc3.d/S77dmi /etc/rc3.d/.NOS77dmi 2> /dev/null
mv /etc/rc3.d/S80mipagent /etc/rc3.d/.NOS80mipagent 2> /dev/null

# Item 2.31, inetd
if [ "`inetadm | grep '^enable'`" ]; then
    svcadm enable svc:/network/inetd:default
else
    svcadm disable svc:/network/inetd:default
fi
```

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

Action:

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

Discussion:

Process accounting logs information about every process that runs to completion on the system, including the amount of CPU time, memory, etc. consumed by each process. While this would seem like useful information in the wake of a potential security incident on the system, kernel-level auditing with the "`+argv,arge`" policy (as enabled in Item 4.8) 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

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
```

Discussion:

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

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
```

Discussion:

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.

SN.4 Restrict access to sys-suspend feature

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
```

Discussion:

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.

SN.5 Create symlinks for dangerous files

Action:

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

Discussion:

The `/.rhosts`, `/.shosts`, and `/etc/hosts.equiv` files enable a weak form of access control (see the discussion of `.rhosts` files in 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.6 Change default greeting string for Sendmail

Action:

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

Discussion:

The default SMTP greeting string displays the version of the Sendmail software running on the remote system. Hiding this information is generally considered to be good practice, since it can help attackers target attacks at machines running a vulnerable version of Sendmail. However, the actions in the benchmark document prevent Sendmail from 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.

References

The Center for Internet Security

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

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

Sun Microsystems

Patch clusters and related documentation:
ftp://patches.sun.com/patchroot/clusters/

Patch management recommendations:
http://www.sun.com/blueprints/browsesubject.html#dcp

Solaris Security Toolkit:
http://www.sun.com/security/jass/

Solaris Fingerprint Database:
http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl

Sun's Kerberos Information
http://www.sun.com/software/security/kerberos/

Role-Based Access Control (RBAC) white paper:
http://wwws.sun.com/software/whitepapers/wp-rbac/

OpenSSH white paper, NTP white paper, information on kernel (ndd) settings, et al:
http://www.sun.com/security/blueprints/

Other Misc Documentation

Various documentation on Solaris security issues:
http://ist.uwaterloo.ca/security/howto/

On BSM Audit flags:
http://www.samag.com/documents/s=9427/sam0414c/0414c.htm

On hiding information in Solaris extended attributes:
http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf

Discussion of "locked" vs. "blocked" accounts:
http://www.securitydocs.com/library/2636

Primary source for information on NTP – http://www.ntp.org/

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

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

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

Software

Pre-compiled software packages for Solaris:
http://www.sunfreeware.com/
ftp://ftp.cisecurity.org/

OpenSSH (secure encrypted network logins):
www.openssh.org

Logcheck log monitoring tool:
http://sourceforge.net/projects/sentrytools/

Swatch (log monitoring tool):
http://www.oit.ucsb.edu/~eta/swatch/

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

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

Revision History

Version 2.1: August 18, 2005:

- Updated document date, version numbers, etc…
- Item 4.8: added missing backticks around grep command in “if” statement so that check functions properly.
- Item 5.4 through 5.8: replaced “-local” option to find command (which doesn’t work as expected) with:
    - “\(-fstype nfs –o –fstype cachefs \) –prune –o”
- Item 5.6: SGID check is now “-02010” (SGID bit + group execute) since the original “-02000” check would match files with mandatory locking set (SGID bit w/o group execute)

Version 2.1.1: February, 21 2006:

- Item 4.3: added “-e” to the echo command to enable interpretation of backslash escapes. Prior to that the “\t”s were not being interpreted as tabs.
- Item 4.4: added “-e” to the echo command to enable interpretation of backslash escapes. Prior to that the “\t”s were not being interpreted as tabs.
- Item 4.5: changed “connlog” to “logadm” to address conflicting benchmark items.
- Item 8.2: changed double quotes to single quotes to address processing of “!”. Single quotes don’t like being broken up across lines with “\” so those strings were changed to be on one line. One line in the “awk” command had “\\n” - changed it to “\n”.

Version 2.1.2: March 8, 2007:

- Item 4.5: changed "connlog" to "loginlog" in the final line of the script.

Version 2.1.3: June 26, 2007

- Added the lines “cp –p keyserv keyserv.old” and “mv keyserv.new keyserv” in section 6.2.