the CENTER for
INTERNET SECURITY

Solaris Benchmark v1.3.0

(for Solaris 2.5.1 and later releases)

Solaris Benchmark v1.3.0

June 17, 2004

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

1 Patches and Additional Software 2
1.1 Apply latest OS patches 2
1.2 Install TCP Wrappers 3
1.3 Install SSH 5

2 Minimize `inetd` network services 7
2.1 Disable standard services 7
2.2 Only enable `telnet` if absolutely necessary 8
2.3 Only enable FTP if absolutely necessary 8
2.4 Only enable `rlogin`/`rsh`/`rcp` if absolutely necessary 9
2.5 Only enable TFTP if absolutely necessary 9
2.6 Only enable printer service if absolutely necessary 10
2.7 Only enable `rquotad` if absolutely necessary 10
2.8 Only enable CDE-related daemons if absolutely necessary 11
2.9 Only enable Solaris Volume Manager daemons if absolutely necessary 11
2.10 Only enable removable media daemon if absolutely necessary 12
2.11 Only enable Kerberos-related daemons if absolutely necessary 13
2.12 Only enable GSS daemon if absolutely necessary 13

3 Minimize boot services 14
3.1 Disable `login:` prompts on serial ports 14
3.2 Set daemon umask 14
3.3 Disable `inetd` if possible 15
3.4 Disable email server, if possible 16
3.5 Disable boot services if possible 17
3.6 Disable other standard boot services 18
3.7 Only enable Windows-compatibility servers if absolutely necessary 19
3.8 Only enable NFS server processes if absolutely necessary 19
3.9 Only enable NFS client processes if absolutely necessary 20
3.10 Only enable automount daemon if absolutely necessary 20
3.11 Only enable other RPC-based services if absolutely necessary 21
3.12 Only enable Kerberos server daemons if absolutely necessary 22
3.13 Only enable directory server if absolutely necessary 22
3.14 Only enable the LDAP cache manager if absolutely necessary 23
3.15 Only enable the printer daemons if absolutely necessary 23
3.16 Only enable the volume manager if absolutely necessary 24
3.17 Only enable GUI login if absolutely necessary 24
3.18 Only enable Web server if absolutely necessary 25
3.19 Only enable SNMP if absolutely necessary 25
3.20 Only enable DHCP server if absolutely necessary 26

4 Kernel Tuning 26
4.1 Restrict core dumps to protected directory 26
4.2 Enable stack protection 27
4.3 Restrict NFS client requests to privileged ports 27
4.4 Network Parameter Modifications 28
4.5 Additional network parameter modifications 30
4.6 Use better TCP sequence numbers 31

5 Logging 31
5.1 Turn on `inetd` tracing 32
5.2 Turn on additional logging for FTP daemon 33
5.3 Capture FTP and `inetd` Connection Tracing Info 33
5.4 Capture messages sent to syslog `AUTH` facility 34
5.5 Create `/var/adm/loginlog` 34
5.6 Turn on `cron` logging 35
5.7 Enable system accounting 35
5.8 Enable kernel-level auditing 36
5.9 Confirm permissions on system log files 37

6 File/Directory Permissions/Access 38
6.1 Add '`logging`' option to root file system 38
6.2 Add '`nosuid`' option to `/etc/rmmount.conf` 39
6.3 Verify `passwd`, `shadow`, and `group` file permissions 39
6.4 World-writable directories should have their sticky bit set 39
6.5 Find unauthorized world-writable files 40
6.6 Find unauthorized SUID/SGID system executables 41
6.7 Find "Unowned" Files and Directories 41
6.8 Run `fix-modes` 42

7 System Access, Authentication, and Authorization 42
7.1 Set higher security level for `sadmind` service 42
7.2 Disable "nobody" access for secure RPC 43
7.3 Remove `.rhosts` support in `/etc/pam.conf` 44
7.4 Create `/etc[/ftpd]/ftpusers` 45
7.5 Prevent Syslog from accepting messages from network 46
7.6 Disable XDMCP port 47
7.7 Prevent X server from listening on port 6000/tcp 47
7.8 Set default locking screensaver timeout 48
7.9 Restrict `at/cron` to authorized users 48
7.10 Remove empty crontab files and restrict file permissions 49
7.11 Restrict root logins to system console 49
7.12 Limit number of failed login attempts 50
7.13 Set EEPROM `security-mode` and log failed access 50

8 User Accounts and Environment 51
8.1 Block system accounts 51
8.2 Verify that there are no accounts with empty password fields 52
8.3 Set account expiration parameters on active accounts 52
8.4 Verify no legacy '+' entries exist in `passwd`, `shadow`, and `group` files 53
8.5 Verify that no UID 0 accounts exist other than `root` 53
8.6 Set default group for root account 53
8.7 No '.' or group/world-writable directory in `root $PATH` 54
8.8 User home directories should be mode 750 or more restrictive 54
8.9 No user dot-files should be group/world writable 55
8.10 Remove user `.netrc` files 55
8.11 Set default umask for users 56
8.12 Set default umask for FTP users 57
8.13 Set "`mesg n`" as default for all users 58

9 Warning Banners 59
9.1 Create warnings for physical access services 59
9.2 Create warnings for GUI-based logins 60
9.3 Create warnings for telnet daemon 61
9.4 Create warnings for FTP daemon 61

Appendix A: File Backup Script 62

Appendix B: Log Rotation Script 63

Appendix C: Additional Security Notes 64

References 68

CIS Solaris Benchmark

A Word about Shaded Items

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

Root Shell Environment Assumed

The actions listed in this document are written with the assumption that they will be executed by the `root` user running the `/sbin/sh` shell 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

Note that the items in this section involve downloading vendor patches and third-party security software from external archive sites. It is critical to always verify the integrity of such software using file or package signatures (if provided) or at least MD5 checksums. 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.

When downloading software packages and patches, always download the files to a non-world-writable directory. Do not use a directory such as `/tmp` or `/var/tmp` which might allow another user on the system to corrupt or interfere with the files being downloaded.

1.1 Apply latest OS patches

Action *(Solaris 7 and later)*:

1. Download Sun Recommended Patch Cluster into `/var/sadm` (obtain Sun Patch Clusters from `ftp://sunsolve.sun.com/pub/patches/` -- look for files named *`<osrel>`*`_Recommended.zip`, where *`<osrel>`* is the Solaris OS release number).

2. Execute the following commands:

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

Action *(Solaris 2.6 and earlier)*:

1. Download Sun Recommended Patch Cluster into `/var/sadm` (obtain Sun Patch Clusters from `ftp://sunsolve.sun.com/pub/patches/` -- look for files named *`<osrel>`*`_Recommended.tar.Z`, where *`<osrel>`* is the Solaris OS release number).

3. Execute the following commands:

```
cd /var/sadm
zcat *_Recommended.tar.Z | tar xf -
cd *_Recommended
./install_cluster -q
cd ..
rm -rf *_Recommended*
```

Discussion:

Developing a procedure for 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. Note that in addition to installing the Solaris Recommended 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, Y2K, 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 Solaris Patch Manager tool (for more info, see http://www.sun.com/service/support/sw_only/patchmanager.html). As an additional security feature, Sun also provides digital signatures for its patches (for more information see http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/spfaq).

During the cluster installation process, administrators may ignore patch 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`.

1.2 Install TCP Wrappers

Action (Solaris 9):

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 `/etc/default/inetd`:

   ```
   cd /etc/default
   awk '/ENABLE_TCPWRAPPERS=/ \
       { $1 = "ENABLE_TCPWRAPPERS=YES" }
       { print }' inetd >inetd.new
   mv inetd.new inetd
   chown root:sys inetd
   chmod 444 inetd
   ```

Action (Solaris 8 and earlier):

1. Download pre-compiled TCP Wrappers software package from `ftp://ftp.sunfreeware.com/pub/freeware/<proc>/<osrel>/` (here *<proc>* is the processor type—"`sparc`" or "`intel`"— and *<osrel>* is the Solaris version number of your system, e.g. "`5.8`", etc.). The file name will be slightly different depending on the version of the software and the OS release, e.g. `tcp_wrappers-7.6-sol8-sparc-local.gz`

   Note that the `gzip` compression utilities must be installed in order to install the TCP Wrappers software package. The `gzip` utilities are included with the Solaris OS as of Solaris 8 (though the local site may have chosen not to install these utilities as part of their standard install image). Pre-compiled binaries for various Solaris releases may be obtained from the URL given above, where the package name would again be something like `gzip-1.3.5-sol7-sparc-local` (depending on the current version number of the `gzip` software and the OS revision). Use the command "`pkgadd -d gzip-*-local all`" to install the `gzip` software from this package file after downloading.

2. Install package:

```
gunzip tcp_wrappers-*-local.gz
pkgadd -d tcp_wrappers-*-local all
```

3. Remove package file after installation:

```
rm -f tcp_wrappers-*-local
```

4. 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.

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

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

6. Modify `inetd.conf`:

```
cd /etc/inet
awk '($3 ~ /^tcp/) && ($6 !~ /(internal|tcpd)$/) \
     { $7 = $6; $6 = "/usr/local/bin/tcpd" }; \
     { print }' inetd.conf > inetd.conf.new
mv inetd.conf.new inetd.conf
chown root:sys inetd.conf
chmod 444 inetd.conf
```

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. Solaris 9 now includes the TCP Wrappers distribution as part of the operating system (assuming the administrator has installed the `SUNWtcpd` software package). The software downloads from `sunfreeware.com` are not officially supported by Sun Microsystems.

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 Sun's SunScreen software, which is available for free to Solaris 8 users and bundled into the operating system as of Solaris 9. See the documentation provided with the TCP Wrappers source code release for information on using TCP Wrappers style filtering with stand-alone daemons that are not spawned out of `inetd`.

1.3 Install SSH

Action (Solaris 9 systems):

```
cd /etc/ssh
cat <<EOCliConfig >>ssh_config
Host *
Protocol 2
EOCliConfig
awk '/^Protocol/                { $2 = "2" };   \
     /^X11Forwarding/           { $2 = "yes" }; \
     /^MaxAuthTries/            { $2 = "3" };   \
     /^MaxAuthTriesLog/         { $2 = "0" };   \
     /^IgnoreRhosts/            { $2 = "yes" }; \
     /^RhostsAuthentication/    { $2 = "no" };  \
     /^RhostsRSAAuthentication/ { $2 = "no" };  \
     /^PermitRootLogin/         { $2 = "no" };  \
     /^PermitEmptyPasswords/    { $2 = "no" };  \
     /^#Banner/                 { $1 = "Banner" } \
     { print }' sshd_config > sshd_config.new
mv sshd_config.new sshd_config
chown root:sys sshd_config
chmod 600 sshd_config
```

Action (Solaris 8 and earlier):

1. Download OpenSSH software from
   http://www.sunfreeware.com/indexsparc8.html
   or
   http://www.sunfreeware.com/indexintel8.html
2. Follow Sun's instructions for installation and configuration.

Discussion:

OpenSSH is a popular free distribution of the standards-track SSH protocols, which allow secure encrypted network logins and file transfers. However, compilation of OpenSSH is complicated by the fact that it is dependent upon several other freely-available software libraries which also need to be built before OpenSSH itself can be compiled. In order to simplify the installation process for Solaris 8 and earlier, we make use of a pre-compiled version of OpenSSH, which is available in Solaris package format (the package contains 32-bit executables that should run on all releases of Solaris from 2.5.1 onwards). This package is not required on Solaris 9 systems, since Sun is now distributing OpenSSH with the Solaris operating system as of this release.

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

2 Minimize `inetd` network services

2.1 Disable standard services

Action:

```
cd /etc/inet
for svc in time echo discard daytime chargen fs dtspc \
           exec comsat talk finger uucp name xaudio \
           netstat ufsd rexd systat sun-dr uuidgen \
           krb5_prop; do
    awk "(\$1 == \"$svc\") { \$1 = \"#\" \$1 }; {print}" \
        inetd.conf >inetd.conf.new
    mv inetd.conf.new inetd.conf
done
for svc in 100068 100146 100147 100150 100221 100232 \
           100235 kerbd rstatd rusersd sprayd walld; do
    awk "/^$svc\\// { \$1 = \"#\" \$1 }; { print }" \
        inetd.conf >inetd.conf.new
    mv inetd.conf.new inetd.conf
done

for svc in printer shell login telnet ftp tftp; do
    awk "(\$1 == \"$svc\") { \$1 = \"#\" \$1 }; {print}" \
        inetd.conf >inetd.conf.new
    mv inetd.conf.new inetd.conf
done
for svc in 100083 100229 100230 100242 \
           100234 100134 100155 rquotad; do
    awk "/^$svc\\// { \$1 = \"#\" \$1 }; { print }" \
        inetd.conf >inetd.conf.new
    mv inetd.conf.new inetd.conf
done
chown root:sys inetd.conf
chmod 444 inetd.conf
```

Discussion:

The stock `/etc/inet/inetd.conf` file shipped with Solaris contains many services which are rarely used, or which have more secure alternatives. Indeed, after enabling SSH (see Item 1.3) it may be possible to completely do away with all `inetd`-based services, since SSH provides both a secure login mechanism and a means of transferring files to and from the system. In fact, the actions above will disable all standard services normally enabled in the Solaris `inetd.conf` file.

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

"**Action**" section above. Rather than disabling and then re-enabling these services, experienced administrators may wish to simply disable only those services that they know are unnecessary for their systems.

2.2 *Only enable `telnet` if absolutely necessary*

Question:

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

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

Action:

```
sed 's/^#telnet/telnet/' inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

Discussion:

`telnet` uses an unencrypted network protocol, which means data from the login session (such as passwords and all other data transmitted during the session) can be stolen by eavesdroppers on the network, and also that the session can be hijacked by outsiders to gain access to the remote system. The freely-available SSH utilities (see `http://www.openssh.com/`) provide encrypted network logins and should be used instead.

2.3 *Only enable FTP if absolutely necessary*

Question:

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

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

Action:

```
sed 's/^#ftp/ftp/' inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

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 7.4 below.

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

Question:

Is there a mission-critical 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:

```
sed 's/^#shell/shell/; s/^#login/login/' \
    inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

Discussion:

SSH was designed to be a drop-in replacement for these protocols. Given the wide availability of free SSH implementations, it seems unlikely that there is ever a case where these tools cannot be replaced with SSH (again, see http://www.openssh.com/).

If these protocols are left enabled, please also see Item 7.1 for additional security-related configuration settings.

2.5 Only enable TFTP if absolutely necessary

Question:

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

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

Action:

```
sed 's/^#tftp/tftp/' inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
mkdir -p /tftpboot
chown root:root /tftpboot
chmod 711 /tftpboot
```

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.

2.6 Only enable printer service if absolutely necessary

OS Revisions:

This item only applies to Solaris 2.6 and later systems.

Question:

Is this machine a print server for your network?

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

Action:

```
sed 's/^#printer/printer/' inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

Discussion:

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

2.7 Only enable `rquotad` if absolutely necessary

Question:

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

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

Action:

```
sed 's/^#rquotad/rquotad/' inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

Discussion:

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

2.8 Only enable CDE-related daemons if absolutely necessary

Question:

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

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

Action:

```
sed 's/^#100083/100083/' inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

Discussion:

The `rpc.ttdbserverd` process supports many tools and applications in Sun's CDE windowing environment, but has historically been a major security issue for Solaris systems. If you do plan to leave this service enabled, not only is it vital to keep up to date on vendor patches, but also *never* enable this service on any system which is not well protected by a complete network security infrastructure (including network and host-based firewalls, packet filters, and intrusion detection infrastructure).

Note that since this service uses 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 3.11 below.

2.9 Only enable Solaris Volume Manager daemons if absolutely necessary

OS Revisions:

This item only applies to Solaris 9 systems (or systems which have the Solaris Volume Manager or Solaris DiskSuite products installed).

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:

```
sed "s/^#100229/100229/; \
     s/^#100230/100230/; \
     s/^#100242/100242/" inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

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 `inetd.conf`. 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 3.11 below.

2.10 Only enable removable media daemon if absolutely necessary

OS Revisions:

This item only applies to Solaris 9 and later systems.

Question:

Is there a mission-critical reason 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:

```
sed 's/^#100155/100155/' inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

Discussion:

This item re-enables the `rpc.smserverd` process that works with the volume manager (see Item 3.16 below) and the CDE file manager application to automatically mount CD-ROMs and floppies when the user inserts new media into the system's drives (the `mount` command is normally a privileged command that can only be performed by the superuser). 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.

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 3.11 below.

2.11 Only enable Kerberos-related daemons if absolutely necessary

OS Revisions:

This item only applies to Solaris 8 and later systems.

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:

```
sed 's/^#100134/100134/' inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

Discussion:

With the release of Solaris 8, Kerberos support has been added to Solaris (see Sun's Kerberos site, `http://wwws.sun.com/software/security/kerberos/` and the MIT Kerberos site `http://web.mit.edu/kerberos/www/`). However, Kerberos may not be in use at all sites.

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 3.11 below.

2.12 Only enable GSS daemon if absolutely necessary

OS Revisions:

This item only applies to Solaris 7 and later systems.

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:

```
sed 's/^#100234/100234/' inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
```

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 3.11 below.

3 Minimize boot services

3.1 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.

3.2 *Set daemon umask*

Action *(Solaris 8 and later)*:

```
cd /etc/default
awk '/^CMASK=/ { $1 = "CMASK=022" }
               { print }' init >init.new
mv init.new init
chown root:sys init
chmod 444 init
```

Action *(Solaris 7 and earlier)*:

```
echo "umask 022" >/etc/init.d/umask.sh
chown root:sys /etc/init.d/umask.sh
chmod 744 /etc/init.d/umask.sh
for dir in /etc/rc?.d
do
        ln -s ../init.d/umask.sh $dir/S00umask.sh
done
```

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.

3.3 Disable inetd if possible

Action:

```
cd /etc/init.d
if [ ! -f newinetsvc ]; then
    cp inetsvc newinetsvc
fi
LINE=`awk '/\/usr\/sbin\/inetd/ && \
           !/\[/ { print }' newinetsvc`
if [ -n "$LINE" ]; then
    grep -v /usr/sbin/inetd newinetsvc >newinetsvc.new
    cat <<'EONewInetd' >>newinetsvc.new
lines=`grep -v '^#' /etc/inet/inetd.conf 2>/dev/null | \
       wc -l | sed 's/ //g'`
EONewInetd
    echo '[ "$lines" != "0" ] && \c' >>newinetsvc.new
    echo $LINE >>newinetsvc.new
    mv newinetsvc.new newinetsvc
fi
chown root:sys newinetsvc
chmod 744 newinetsvc
rm -f /etc/rc2.d/S72inetsvc
ln -s /etc/init.d/newinetsvc /etc/rc2.d/S72inetsvc
```

Discussion:

If the actions in Section 2 result in all inetd-based services being disabled, then there is no point in running inetd at boot time. The code added to the newinetsvc boot script will result in inetd automatically being restarted at boot time if services are ever enabled in inetd.conf. However, it may be necessary to manually start inetd if the administrator wishes to enable some of these services without rebooting the system.

3.4 Disable email server, if possible

Question:

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

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

Action *(Solaris 8 and later)*:

```
cd /etc/default
cat <<END_DEFAULT >sendmail
MODE=
QUEUEINTERVAL="15m"
END_DEFAULT
chown root:sys sendmail
chmod 744 sendmail
```

Action *(Solaris 7 and earlier)*:

```
mv /etc/rc2.d/S88sendmail /etc/rc2.d/.NOS88sendmail
if [ ! "`crontab -l | grep 'sendmail -q'`" ]; then
    cd /var/spool/cron/crontabs
    crontab -l >root.tmp
    echo '0 * * * * /usr/lib/sendmail -q' >>root.tmp
    crontab root.tmp
    rm -f root.tmp
fi
```

Discussion:

It is possible to run a Unix system with the Sendmail daemon disabled and still allow users on that system to send email out from that machine. Running Sendmail in *"daemon mode"* (with the `-bd` command-line option) is only required on machines that act as *mail servers*, receiving and processing email from other hosts on the network.

Note that after disabling the `-bd` option on the local mail server on Solaris 9 (or any system running Sendmail v8.12 or later) it is also necessary to modify the `/etc/mail/submit.cf` file. Find the line that reads "`D{MTAHost}localhost`" and change `localhost` to the name of some other local mail server for the organization. This will cause email generated on the local system to be relayed to that mail server for further processing and delivery.

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

3.5 Disable boot services if possible

Question:

Is this machine a network boot server or Jumpstart server?

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

Action *(Solaris 9):*

```
mv /etc/rc3.d/S16boot.server /etc/rc3.d/.NOS16boot.server
```

Action *(Solaris 8 and earlier):*

```
cd /etc/init.d
awk '/tftpboot/,/;;/ { if ($1 != ";;") next }
     { print }' nfs.server >newnfs.server
chown root:sys newnfs.server
chmod 744 newnfs.server
rm -f /etc/rc3.d/S15nfs.server
ln -s /etc/init.d/newnfs.server /etc/rc3.d/S15nfs.server
```

Discussion:

If the `/tftpboot` directory exists (see Item 2.5 above), the `in.rarpd` and `rpc.bootparamd` services will be enabled. These services are designed to assist machines and devices that need to download their boot images over the network from some central server. However, the system may be running TFTP and have a `/tftpboot` directory but not be acting as a boot server (for example, many sites use TFTP to back up configuration files from their network routers). `in.rarpd` and `rpc.bootparamd` should only be enabled if the machine is actually going to be acting as a boot server.

3.6 Disable other standard boot services

Action:

```
cd /etc/rc2.d
for file in S72autoinstall S85power S89bdconfig \
  S73cachefs.daemon S93cacheos.finish S40llc2 S47pppd \
  S47asppp S70uucp S72slpd S75flashprom S80PRESERVE \
  S89PRESERVE S94ncalogd S95ncad S96ab2mgr; do
  [ -s $file ] && mv $file .NO$file
done
cd /etc/rc3.d
for file in S77dmi S80mipagent; do
  [ -s $file ] && mv $file .NO$file
done

cd /etc/rc2.d
for file in S73nfs.client S74autofs S71rpc \
  S72directory S71ldap.client S80lp S80spc S92volmgt \
  S99dtlogin S42ncakmod; do
  [ -s $file ] && mv $file .NO$file
done
cd /etc/rc3.d
for file in S90samba S15nfs.server S13kdc.master S14kdc \
  S50apache S76snmpdx S34dhcp; do
  [ -s $file ] && mv $file .NO$file
done
```

Discussion:

Renaming these scripts in the system boot directories will effectively disable a wide variety of infrequently used subsystems. The scripts are merely renamed (rather than removed outright) so that the local administrator can easily "restore" any of these files if they discover a mission-critical need for one of these services. Not all of the scripts listed above will exist on all systems (some are only valid for certain releases, others only exist if certain OEM vendor software is installed). Note also that vendor patches may restore some of the original entries in the `/etc/rc*.d` directories—it is always a good idea to check these boot directories and remove any scripts that may have been added by the patch installation process.

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

3.7 Only enable Windows-compatibility servers if absolutely necessary

OS Revisions:

This item only applies to Solaris 9 systems.

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:

```
mv /etc/rc3.d/.NOS90samba /etc/rc3.d/S90samba
```

Discussion:

Solaris 9 now 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.

3.8 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:

```
mv /etc/rc3.d/.NOS15nfs.server /etc/rc3.d/S15nfs.server
```

Discussion:

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

Note that if the system is an NFS server than the `rpcbind` process must also be running (see Item 7.2 below).

3.9 Only enable NFS client processes if absolutely necessary

Question:

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

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

Action:

```
mv /etc/rc2.d/.NOS73nfs.client /etc/rc2.d/S73nfs.client
```

Discussion:

While this action disables the standard NFS client processes (statd and lockd), it is important to note that it is still possible for the superuser to mount remote file systems on the local machine via NFS. Starting with Solaris 9, the administrator can completely disable NFS client access by removing the NFS client software packages (SUNWnfscr, SUNWnfscu, and SUNWnfscx), but these packages will have to be re-installed 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 3.11 below).

3.10 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:

```
mv /etc/rc2.d/.NOS74autofs /etc/rc2.d/S74autofs
```

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 graphical administrative interface to function properly.

3.11 Only enable other 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*
- *Your site uses Sun's admintool application for system administration*
- *The Kerberos security system is in use at this site*
- *This machine runs a GUI or GUI-based administration tool*
- *This machine is a network boot server or Jumpstart server*
- *The system is running Solaris 9 and requires the Volume Manager (`vold`)*
- *The machine runs a third-party software application which is dependent on RPC support (examples: FlexLM License managers, Veritas, Solaris DiskSuite)*

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

Action:

```
mv /etc/rc2.d/.NOS71rpc /etc/rc2.d/S71rpc
```

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, 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.

3.12 Only enable Kerberos server daemons if absolutely necessary

OS Revisions:

This item only applies to Solaris 9 systems.

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:

```
mv /etc/rc3.d/.NOS13kdc.master /etc/rc3.d/S13kdc.master
mv /etc/rc3.d/.NOS14kdc /etc/rc3.d/S14kdc
```

Discussion:

Solaris 9 includes greater support for the Kerberos authentication system. In particular, the Kerberos server daemons have been bundled with the core operating system. However, if the site is not using Kerberos or if this machine is not configured as one of the site's Kerberos servers, there is no reason to enable this service.

3.13 Only enable directory server if absolutely necessary

OS Revisions:

This item only applies to Solaris 9 systems.

Question:

Is this system an LDAP directory server for this site?

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

Action:

```
mv /etc/rc2.d/.NOS72directory /etc/rc2.d/S72directory
```

Discussion:

Solaris 9 has included the iPlanet Directory Server product as part of the operating system. However, this service only needs to be running on the machines that have been designated as LDAP servers for the organization. If the machine is an LDAP server, the administrator is encouraged to search the Web for additional documentation on LDAP security issues.

3.14 Only enable the LDAP cache manager if absolutely necessary

OS Revisions:

This item only applies to Solaris 8 and later systems.

Question:

Is the LDAP directory service in use at this site, and is this machine an LDAP client?

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

Action:

```
mv /etc/rc2.d/.NOS71ldap.client /etc/rc2.d/S71ldap.client
```

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.

3.15 Only enable the printer daemons if absolutely necessary

Question:

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

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

Action:

```
mv /etc/rc2.d/.NOS80lp /etc/rc2.d/S80lp
mv /etc/rc2.d/.NOS80spc /etc/rc2.d/S80spc
```

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. The Unix print service has generally had a poor security record—be sure to keep up-to-date on vendor patches. The administrator may wish to consider converting to the LPRng print system (see `http://www.lprng.org/`), which was designed with security in mind and is widely portable across many different Unix platforms. Note, however, that LPRng is not supported by Sun Microsystems.

3.16 Only enable the volume manager if absolutely necessary

Question:

Is there a mission-critical reason 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:

```
mv /etc/rc2.d/.NOS92volmgt /etc/rc2.d/S92volmgt
```

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 which can only be performed by the superuser). 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.

Note that if the machine is running Solaris 9 or later, it is also necessary to re-enable the `rpc.smserverd` process for the volume manager to function (see Item 2.10 above).

3.17 Only enable GUI login if absolutely necessary

OS Revisions:

This item only applies to Solaris 2.6 and later releases.

Question:

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

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

Action:

```
mv /etc/rc2.d/.NOS99dtlogin /etc/rc2.d/S99dtlogin
```

Discussion:

Note that for the Solaris CDE GUI to function properly, it is also necessary to enable the `rpcbind` process (see Item 3.11) and the `rpc.ttdbserverd` process (see Item 2.8). The X Windows-based CDE GUI on Solaris systems, as well as the `rpcbind` and `rpc.ttdbserverd` processes 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.

3.18 Only enable Web server if absolutely necessary

OS Revisions:

This item only applies to Solaris 8 and later systems.

Question:

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

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

Action:

```
mv /etc/rc3.d/.NOS50apache /etc/rc3.d/S50apache
mv /etc/rc2.d/.NOS42ncakmod /etc/rc2.d/S42ncakmod
```

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 http://httpd.apache.org/docs-2.0/misc/security_tips.html.

3.19 Only enable SNMP if absolutely necessary

OS Revisions:

This item only applies to Solaris 2.6 and later systems.

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:

```
mv /etc/rc3.d/.NOS76snmpdx /etc/rc3.d/S76snmpdx
```

Discussion:

If you are using SNMP to monitor the hosts on your network, experts recommend changing the default community string used to access data via SNMP. On Solaris systems, this parameter can be changed by modifying the `system-group-read-community` parameter in `/etc/snmp/conf/snmpd.conf`

3.20 Only enable DHCP server if absolutely necessary

OS Revisions:

This item only applies to Solaris 9 systems.

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:

```
mv /etc/rc3.d/.NOS34dhcp /etc/rc3.d/S34dhcp
```

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.

4 Kernel Tuning

4.1 Restrict core dumps to protected directory

OS Revisions:

The configuration steps below may only be applied on Solaris 7 and later systems.

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 \
        -i /var/core/core_%n_%f_%u_%g_%t_%p \
        -e log \
        -e global -e global-setid -e process -e proc-setid
```

Discussion:

By default core dump files are world-readable. Yet core dumps, particularly those from set-UID and set-GID processes, may contain sensitive data that should not be viewed by all users on the system. The above action causes all core dumps on the system to be written to a special directory that is only accessible by the superuser. Note that on development workstations, this may make it difficult for developers to obtain core files for debugging without administrative intervention.

Core dumps tend to be large files and the contents of the `/var/core` directory can end up rapidly consuming large amounts of disk space and possibly causing a denial of service attack on the system. It is a good idea to monitor this directory on a regular basis and remove any unneeded core files. 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`". Note that there is a bug in Solaris 7 and 8 that automatically re-enables per-process core dumps during the reboot process. The only work-around at this time is to add a script to the system boot sequence that explicitly runs "`coreadm –d process`".

4.2 Enable stack protection

OS Revisions:

The configuration steps below may only be applied on Solaris 2.6 and later 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.

4.3 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.

4.4 Network Parameter Modifications

Action (for Solaris 8 and later):

```
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/S69netconfig
fi
```

Action *(for Solaris 2.6 and 7)*:

```
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 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_flush_interval 60000
ndd -set /dev/ip ip_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/S69netconfig
fi
```

Action *(for Solaris 2.5.1)*:

```
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 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_flush_interval 60000
ndd -set /dev/ip ip_ignore_redirect 1
END_SCRIPT
    chown root:root /etc/init.d/netconfig
    chmod 744 /etc/init.d/netconfig
    ln -s /etc/init.d/netconfig /etc/rc2.d/S69netconfig
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/

4.5 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 *(for Solaris 8 and later)*:

```
if [ ! "`grep ip_forwarding /etc/init.d/netconfig`" ]
then
    cat <<END_SCRIPT >>/etc/init.d/netconfig
ndd -set /dev/ip ip_forwarding 0
ndd -set /dev/ip ip6_forwarding 0
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
```

Action *(for Solaris 7 and earlier)*:

```
if [ ! "`grep ip_forwarding /etc/init.d/netconfig`" ]
then
    cat <<END_SCRIPT >>/etc/init.d/netconfig
ndd -set /dev/ip ip_forwarding 0
ndd -set /dev/ip ip_strict_dst_multihoming 1
ndd -set /dev/ip ip_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.

4.6 Use better TCP sequence numbers

OS Revisions:

Required for Solaris 2.6 and later, not supported in earlier releases

Action:

```
cd /etc/default
awk '/TCP_STRONG_ISS=/ { $1 = "TCP_STRONG_ISS=2" }; \
   { print }' inetinit > inetinit.new
mv inetinit.new inetinit
chown root:sys inetinit
chmod 444 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.

5 Logging

The items in this section cover enabling various different forms of system logging in order to keep track of activity on the system. Tools such as Swatch (http://www.oit.ucsb.edu/~eta/swatch/) 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.

5.1 Turn on `inetd` tracing

Action (Solaris 9):

```
cd /etc/default
if [ "`grep ENABLE_CONNECTION_LOGGING= inetd`" ]; then
    awk '/ENABLE_CONNECTION_LOGGING=/
                { $1 = "ENABLE_CONNECTION_LOGGING=YES" }
                { print }' inetd >inetd.new
    mv inetd.new inetd
else
    echo ENABLE_CONNECTION_LOGGING=YES >>inetd
fi
chown root:sys inetd
chmod 444 inetd
```

Action (Solaris 8 and earlier):

```
cd /etc/init.d
if [ ! -f newinetsvc ]; then
    cp inetsvc newinetsvc
fi
awk '/\/usr\/sbin\/inetd/ && !/-t/ { $NF = "-t " $NF }
     { print }' newinetsvc >newinetsvc.new
mv newinetsvc.new newinetsvc
chown root:sys newinetsvc
chmod 744 newinetsvc
rm -f /etc/rc2.d/S72inetsvc
ln -s /etc/init.d/newinetsvc /etc/rc2.d/S72inetsvc
```

Discussion:

If `inetd` is running, it is a good idea to make use of the "tracing" (`-t`) feature of the Solaris `inetd` that logs information about the source of any network connections seen by the daemon. 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 5.3 below).

In addition to the information provided by `inetd` tracing, the popular free PortSentry tool (http://sourceforge.net/projects/sentrytools/) can be used to monitor access attempts on unused ports. Note that running PortSentry may result in the CIS testing tools reporting "false positives" for "active" ports that are actually being held by the PortSentry daemon. Note that PortSentry is not officially supported by Sun Microsystems.

5.2 Turn on additional logging for FTP daemon

Action:

```
cd /etc/inet
awk '/in.ftpd/ && !/-d/ { $NF = $NF " -d" }
     /in.ftpd/ && !/-l/ { $NF = $NF " -l" }
     { print }' inetd.conf > inetd.conf.new
mv inetd.conf.new inetd.conf
chown root:sys inetd.conf
chmod 444 inetd.conf
```

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 5.3 below.

5.3 Capture FTP and `inetd` Connection Tracing Info

Action:

```
if [ ! "`grep -v '^#' /etc/syslog.conf | \
         grep /var/log/connlog`" ]; then
    echo "daemon.debug\t\t\t/var/log/connlog" \
        >>/etc/syslog.conf
fi
touch /var/log/connlog
chown root:root /var/log/connlog
chmod 600 /var/log/connlog
```

Discussion:

If the FTP service is enabled on the system, Item 5.2 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 5.1 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 and archived on a regular basis. A sample script for archiving log files is provided as Appendix B to this document. Solaris 9 systems include the `logadm` utility for archiving log files.

5.4 Capture messages sent to syslog `AUTH` facility

Action:

```
if [ ! "`grep -v '^#' /etc/syslog.conf | \
         grep /var/log/authlog`" ]; then
    echo "auth.info\t\t\t/var/log/authlog" \
        >>/etc/syslog.conf
fi
touch /var/log/authlog
chown root:sys /var/log/authlog
chmod 600 /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 and archived on a regular basis. A sample script for archiving log files is provided as Appendix B to this document. Solaris 9 systems include the `logadm` utility for archiving log files.

5.5 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
chown root:sys login
chmod 444 login
```

Discussion:

If it exists, the file `/var/adm/loginlog` will capture failed login attempt messages (this file does not exist by default). Starting with Solaris 8, 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 and archived on a regular basis. A sample script for archiving log files is provided as Appendix B to this document. Solaris 9 systems include the `logadm` utility for archiving log files.

5.6 Turn on `cron` logging

Action:

```
cd /etc/default
awk '/CRONLOG=/ { $1 = "CRONLOG=YES" }; \
                { print }' cron > cron.new
mv cron.new cron
chown root:sys cron
chmod 444 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.

5.7 Enable system accounting

Action:

```
cat <<END_SCRIPT >/etc/init.d/newperf
#!/sbin/sh
/usr/bin/su sys -c \
  "/usr/lib/sa/sadc /var/adm/sa/sa\`date +%d\`"
END_SCRIPT
chown root:sys /etc/init.d/newperf
chmod 744 /etc/init.d/newperf
rm -f /etc/rc2.d/S21perf
ln -s /etc/init.d/newperf /etc/rc2.d/S21perf
/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 CPUintensive 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.

5.8 *Enable kernel-level auditing*

Action:

```
if [ ! -f /etc/security/audit_startup ]; 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 ~ /pc/) && \
     ! ($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
  chown root:sys audit_event audit_control audit_startup
  chmod 640 audit_event audit_control
  chmod 740 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`). The `<Stop>-A` keyboard abort sequence is also disabled via an entry in the `/etc/system` file.

Kernel-level auditing can consume large amounts of disk space and even cause a system performance impact, particularly on heavily used machines. The consensus settings above are an effort to log "interesting" system events without consuming excessive amounts of resources logging "significant but usually uninteresting" system calls. The document *Auditing in the Solaris™ Operating Environment* published by Sun Microsystems as part of their "Blueprints On-Line" series contains additional information on reducing the amount of logging produced by the "administrative" (`ad`) audit class (see `http://www.sun.com/security/blueprints/` for more details).

Note that DoD installations have much more stringent auditing requirements than those listed here. DoD guidelines require "`flags:lo,ad,cc,fw,-fc,-fd,-fr`" to be set in the `audit_control` file. Note that "`-fr`" in particular can cause extremely large audit trails to be generated.

5.9 Confirm permissions on system log files

Action:

```
chown root:sys /var/log/syslog /var/log/authlog \
   /var/adm/loginlog
chown root:root /var/cron/log /var/adm/messages
chmod go-wx /var/log/syslog /var/adm/messages
chmod go-rwx /var/log/authlog /var/adm/loginlog \
   /var/cron/log
cd /var/adm
chown root:bin utmpx
chown adm:adm wtmpx
chmod 644 utmpx wtmpx
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.

Note that sites using the `runacct` script for generating billing reports and other data from the system process accounting logs will notice that the script incorrectly sets the mode on the `wtmpx` file to `664` (adds the "group writability" bit). The local site may wish to "`chmod g-w /var/adm/wtmpx`" after running the `runacct` script.

6 File/Directory Permissions/Access

6.1 *Add '`logging`' option to root file system*

OS Revisions:

This step may only be performed on Solaris 8 and later systems

Action:

```
awk '($4 == "ufs" && $3 == "/" && $7 == "-") \
     { $7 = "logging" }; \
     ($4 == "ufs" && $3 == "/" && $7 !~ /logging/) \
     { $7 = $7 ",logging" }; \
     { print }' /etc/vfstab >/etc/vfstab.new
mv /etc/vfstab.new /etc/vfstab
chown root:sys /etc/vfstab
chmod 664 /etc/vfstab
```

Discussion:

A corrupted root file system is one mechanism that an attacker with physical access to the system console can use to compromise the system. By enabling the "`logging`" option on the root file system, it is much more difficult for the root file system to become corrupted at all, thwarting this particular type of attack. However, other sorts of attacks are possible if the attacker has unrestricted physical access to the system. Be sure to keep critical systems in limited access data centers or other restricted facilities.

Note that the administrator may also wish to add the "`logging`" option to other `ufs` type file systems in `/etc/vfstab`. This will help the system to reboot faster in the event of a crash at the cost of some disk overhead (up to a maximum of 64MB per partition) for the file system transaction log file.

6.2 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 on Solaris 8 and later.

6.3 Verify passwd, shadow, and group file permissions

Action:

```
cd /etc
chown root:sys passwd shadow group
chmod 644 passwd group
chmod 400 shadow
```

Discussion:

These are the default owners and access permissions for these files.

6.4 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

```
for part in `awk '($4 == "ufs" || $4 == "tmpfs") \
                  { print $3 }' /etc/vfstab`
do
     find $part -xdev -type d \
          \( -perm -0002 -a ! -perm -1000 \) -print
done
```

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.

6.5 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:

```
for part in `awk '($4 == "ufs" || $4 == "tmpfs") \
                  { print $3 }' /etc/vfstab`
do
     find $part -xdev -type f -perm -0002 -print
done
```

Discussion:

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

6.6 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:

```
for part in `awk '($4 == "ufs" || $4 == "tmpfs") \
                  { print $3 }' /etc/vfstab`
do
     find $part -xdev -type f \
          \( -perm -04000 -o -perm -02000 \) -print
done
```

Discussion:

The administrator should take care to ensure that no rogue set-UID programs have been introduced into the system. 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/. Cryptographic checksums of these files (along with all standard files in the Solaris operating system) can be obtained from the Solaris Fingerprint Database (see http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl). Tools for interacting with the Fingerprint Database are available from http://www.sun.com/blueprints/tools/.

6.7 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 `/etc/passwd` or `/etc/group` files.

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

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

6.8 *Run `fix-modes`*

Action:

1. Download the pre-compiled `fix-modes` software from

   http://www.sun.com/blueprints/tools/index.html

2. Unpack and install the software

   ```
   uncompress SUNBEfixm.pkg.Z
   pkgadd -d SUNBEfixm.pkg all
   ```

3. Run the `fix-modes` program

   ```
   /opt/SUNBEfixm/fix-modes
   ```

Discussion:

The `fix-modes` software corrects various ownership and permission issues with files throughout the Solaris OS file systems. This program should be re-run every time packages are added to the system, or patches are applied. Administrators may wish to run the tool periodically out of `cron`.

Note that the actions below recommend using a pre-compiled version of `fix-modes` supplied by Sun for use with their Solaris Security Toolkit framework. The source code for the tool is also available from the same URL. Note that Sun's version of the tool has been specifically modified to avoid well-known problems when running `fix-modes` on SSP systems for the E10K and E15K products.

7 System Access, Authentication, and Authorization

7.1 Set higher security level for `sadmind` service

Action:

```
cd /etc/inet
awk '/sadmind/ && !/-S/ { $7 = $7 " -S 2" }
                        { print }' \
                        inetd.conf >inetd.conf.new
mv inetd.conf.new inetd.conf
chown root:sys inetd.conf
chmod 444 inetd.conf
```

Discussion:

The `sadmind` service is the primary daemon that enables the Solaris remote administration framework for distributed system administration tasks. Since the operations allowed by this daemon are extremely powerful, it is best to use the highest security setting available for authorizing client connections. Note that given the history of significant security issues with sadmind, the items in Section 2 of this document actually disable the sadmind service, so this setting will only take effect if the service is re-enabled in inetd.conf.

7.2 Disable "nobody" access for secure RPC

Action (Solaris 9):

```
cd /etc/default
awk '/ENABLE_NOBODY_KEYS=/ \
        { $1 = "ENABLE_NOBODY_KEYS=NO" }
        { print }' keyserv >keyserv.new
mv keyserv.new keyserv
chown root:sys keyserv
chmod 444 keyserv
```

Action (Solaris 8 and earlier):

```
awk '$1 ~ /keyserv/ && !/-d/ { $1 = $1 " -d" }; \
     { print }' /etc/init.d/rpc >/etc/init.d/newrpc
chown root:sys /etc/init.d/newrpc
chmod 744 /etc/init.d/newrpc
if [ -f /etc/rc2.d/S71rpc ]; then
    file=/etc/rc2.d/S71rpc
else
    file=/etc/rc2.d/.NOS71rpc
fi
rm -f $file
ln -s /etc/init.d/newrpc $file
```

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.

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

OS Revisions:

Required for Solaris 2.6 and later, not supported in earlier releases

Action:

```
cd /etc
grep -v rhosts_auth pam.conf > pam.conf.new
mv pam.conf.new pam.conf
chown root:sys pam.conf
chmod 644 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`).

7.4 Create /etc[/ftpd]/ftpusers

Action:

```
if [ -d /etc/ftpd ]; then
    file=/etc/ftpd/ftpusers
else
    file=/etc/ftpusers
fi
for user in root daemon bin sys adm lp uucp nuucp \
            smmsp listen nobody noaccess nobody4
do
    echo $user >>$file
done
sort -u $file >$file.new
mv $file.new $file
chown root:root $file
chmod 600 $file
```

Discussion:

`ftpusers` contains a list of users who *are not* allowed to access the system via FTP. For Solaris 8 and earlier, this file is `/etc/ftpusers`, but has been moved to `/etc/ftpd/ftpusers` as of Solaris 9.

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 8 and later. 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.

7.5 Prevent Syslog from accepting messages from network

OS Revisions:

This item only applies to Solaris 8 and later systems.

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 (Solaris 9):

```
cd /etc/default
if [ "`grep LOG_FROM_REMOTE= syslogd`" ]; then
    awk '/LOG_FROM_REMOTE=/ \
                { $1 = "LOG_FROM_REMOTE=NO" }
                { print }' syslogd >syslogd.new
    mv syslogd.new syslogd
else
    echo LOG_FROM_REMOTE=NO >>syslogd
fi
chown root:sys syslogd
chmod 444 syslogd
```

Action (Solaris 8):

```
awk '$1 ~ /syslogd/ && !/-(t|T)/ { $1 = $1 " -t" }; \
     { print }' /etc/init.d/syslog >/etc/init.d/newsyslog
chown root:sys /etc/init.d/newsyslog
chmod 744 /etc/init.d/newsyslog
rm -f /etc/rc2.d/S74syslog
ln -s /etc/init.d/newsyslog /etc/rc2.d/S74syslog
```

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.

7.6 Disable XDMCP port

OS Revisions:

This action is only required on Solaris 2.6 and later releases.

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
```

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 prevents the login GUI from even hearing requests for remote login services.

7.7 Prevent X server from listening on port 6000/tcp

OS Revisions:

This action is only required on Solaris 9 systems.

Action:

```
if [ -f /etc/dt/config/Xservers ]; then
    file=/etc/dt/config/Xservers
else
    file=/usr/dt/config/Xservers
fi
awk '/Xsun/ && !/^#/ && !/-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
```

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.

7.8 Set default locking screensaver timeout

OS Revisions:

This action is only required on Solaris 2.6 and later releases.

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
```

Discussion:

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

7.9 Restrict `at/cron` to authorized users

Action:

```
cd /etc/cron.d
rm -f cron.deny at.deny
echo root >cron.allow
echo root >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 5.7 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) in Solaris 8 and later.

7.10 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
       rm $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.

7.11 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
chown root:sys login
chmod 444 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.

7.12 Limit number of failed login attempts

Action:

```
cd /etc/default
if [ "`grep RETRIES= login`" ]; then
    awk '/RETRIES=/ { $1 = "RETRIES=3" }
                { print }' login >login.new
    mv login.new login
    chown root:sys login
    chmod 444 login
else
    echo RETRIES=3 >>login
fi
```

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. Setting this number to a reasonably low value helps discourage brute force password guessing attacks.

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

Hardware Compatibility:

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

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".

8 User Accounts and Environment

Note that the items in this section are tasks that the local administrator should undertake on a regular, ongoing basis—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/.

8.1 Block system accounts

Action:

```
passwd -l daemon
for user in adm bin lp smmsp nobody noaccess \
            uucp nuucp smtp listen nobody4; do
  passwd -l $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.

8.2 Verify that there are no accounts with empty password fields

Action:

The command

```
logins -p
```

should return no lines of output.

Discussion:

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

8.3 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
cat <<EO_DefPass >/etc/default/passwd
MAXWEEKS=13
MINWEEKS=1
WARNWEEKS=4
PASSLENGTH=6
EO_DefPass
```

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.

8.4 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.

8.5 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/`.

8.6 Set default group for root account

Action:

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

Discussion:

The default group for the `root` account under Solaris is the "`other`" group, which may be shared by many other accounts on the system. Changing the default group for the `root` account helps prevent `root`-owned files accidentally becoming accessible to non-privileged users.

8.7 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.

8.8 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.

8.9 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.

8.10 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.

8.11 Set default umask for users

Action:

```
cd /etc/default
if [ "`grep UMASK= login`" ]; then
    awk '/UMASK=/ { $1 = "UMASK=077" }
                  { print }' login >login.new
    mv login.new login
else
    echo UMASK=077 >>login
fi
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
chown root:sys /etc/default/login /etc/profile /etc/.login
chmod 444 /etc/default/login /etc/profile /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.

8.12 Set default umask for FTP users

OS Revisions:

This action is only required on Solaris 2.6 and later releases.

Action *(Solaris 9):*

```
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
chown root:sys ftpaccess
chmod 444 ftpaccess
```

Action *(Solaris 8 and earlier):*

```
cd /etc/default
if [ "`grep UMASK= ftpd`" ]; then
    awk '/UMASK=/ { $1 = "UMASK=077" }
                  { print }' ftpd >ftpd.new
    mv ftpd.new ftpd
else
    echo UMASK=077 >>ftpd
fi
chown root:sys ftpd
chmod 444 ftpd
```

Discussion:

The Solaris 9 FTP daemon is derived from the Washington University FTP daemon, so the default umask value is set in `/etc/ftpd/ftpaccess`. Earlier releases (at least as far back as Solaris 2.6) set this value in `/etc/default/ftpd`. Please see previous item for a discussion of different umask values.

8.13 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
    chown root:sys $file
    chmod 444 $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.

9 Warning Banners

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

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

9.1 Create warnings for physical access services

Action:

```
eeprom oem-banner="Authorized uses only. All activity \
may be monitored and reported."
eeprom oem-banner\?=true
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
chown root:sys /etc/motd
chown root:root /etc/issue
chmod 644 /etc/motd /etc/issue
```

Discussion:

The contents of the /etc/issue file are displayed prior to the login prompt on the system's console and serial devices. /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.

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.

9.2 Create warnings for GUI-based logins

OS Revisions:

This action is only required on Solaris 2.6 and later releases.

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 $dir/Xresources
    fi
    echo "Dtlogin*greeting.labelString: Authorized uses \
only.  All activity may be monitored and reported."     \
>>$dir/Xresources
    echo "Dtlogin*greeting.persLabelString: Authorized \
uses only. All activity may be monitored and reported."\
>>$dir/Xresources
done
chown root:sys /etc/dt/config/*/Xresources
chmod 644 /etc/dt/config/*/Xresources
```

Discussion:

The standard graphical login program for Solaris requires the user to enter their username in one dialog box and their password in a second separate dialog. The commands above set the warning message on both to be the same message, but the site has the option of using different messages on each screen. The `Dtlogin*greeting.labelString` is the message for the first dialog where the user is prompted for their username, and ...`perslabelString` is the message on the second dialog box.

9.3 Create warnings for telnet daemon

OS Revisions:

This action is only required on Solaris 2.6 and later releases.

Action:

```
cd /etc/default
if [ ! "`grep BANNER= telnetd`" ]; then
echo "BANNER=\"Authorized uses only.  All activity may \
be monitored and reported.\\\n\\\n\"" >telnetd
chown root:sys telnetd
chmod 444 telnetd
fi
```

Discussion:

Setting this banner has the side effect of hiding the default telnet banner, which advertises the version of Solaris running on the system.

9.4 Create warnings for FTP daemon

OS Revisions:

This action is only required on Solaris 2.6 and later releases.

Action *(Solaris 9):*

```
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
```

Action *(Solaris 8 and earlier):*

```
if [ ! "`grep BANNER= /etc/default/ftpd`" ]; then
echo "BANNER=\"Authorized uses only.  All activity may \
be monitored and reported.\"" >>/etc/default/ftpd
chown root:sys /etc/default/ftpd
chmod 444 /etc/default/ftpd
fi
```

Discussion:

The FTP daemon in Solaris 9 is based on the popular Washington University FTP daemon (WU-FTPD), which is an Open Source program widely distributed on the Internet. This is why the procedure for setting the warning banner on Solaris 9 differs from previous releases.

Appendix A: File Backup Script

```
#!/bin/sh

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

for file in /etc/.login            /etc/coreadm.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/ftpd        \
            /etc/default/inetd     /etc/default/inetinit    \
            /etc/default/init      /etc/default/keyserv     \
            /etc/default/login     /etc/default/passwd      \
            /etc/default/sendmail  /etc/default/syslogd     \
            /etc/default/telnetd                            \
            /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/ftpusers            \
            /etc/hosts.allow       /etc/hosts.deny          \
            /etc/inet/inetd.conf                            \
            /etc/init.d/netconfig  /etc/init.d/newinetsvc   \
            /etc/init.d/newnfs.server                       \
            /etc/init.d/newperf    /etc/init.d/newrpc       \
            /etc/init.d/newsyslog  /etc/init.d/umask.sh     \
            /etc/issue             /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/shadow            /etc/ssh/ssh_config      \
            /etc/ssh/sshd_config   /etc/syslog.conf         \
            /etc/system            /etc/vfstab
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: Log Rotation Script

```
#!/bin/ksh

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

FILE=$1
MODE=${2:-644}
DEPTH=${3:-4}

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

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

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

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

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

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

Appendix C: Additional Security Notes

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

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

SN.1 Enable process accounting 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 5.8) 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
chown root:sys dfstab
chmod 644 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

OS Revisions:

This action is only required on Solaris 2.6 and later releases.

Action:

```
cd /etc/default
awk '/^PMCHANGEPERM=/  { $1 = "PMCHANGEPERM=-" }
     /^CPRCHANGEPERM=/ { $1 = "CPRCHANGEPERM=-" }
                       { print }' power >power.new
mv power.new power
chown root:sys power
chmod 444 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

OS Revisions:

This action is only required on Solaris 2.6 and later releases.

Action:

```
cd /etc/default
awk '/^PERMS=/ { $1 = "PERMS=-" }
               { print }' sys-suspend >sys-suspend.new
mv sys-suspend.new sys-suspend
chown root:sys sys-suspend
chmod 444 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
chown root:bin sendmail.cf
chmod 444 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 completely disable Sendmail on the system, 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

Patches and related documentation:
ftp://sunsolve.sun.com/pub/patches/

Sun Patch Manager tool:
http://www.sun.com/service/support/sw_only/patchmanager.html

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

Pre-compiled `fix-modes` *software:*
http://wwws.sun.com/software/security/downloads.html

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

Sun's Kerberos Information
http://wwws.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/

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

TCP Wrappers source distribution:
ftp.porcupine.org

PortSentry and Logcheck (port and log monitoring tools):
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/

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

`fix-modes` *(free tool to correct permissions and ownerships in the Solaris OS):*
ftp://ftp.science.uva.nl/pub/solaris/fix-modes.tar.gz

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