AIX Benchmark v1.0.1

http://www.CISecurity.org/

CIS AIX Benchmark

AIX Benchmark v1.01

October 19, 2005

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

Table of Contents

CIS AIX Benchmark

Applicability

This benchmark was developed and tested on AIX 4.3.2, 4.3.3 and AIX 5L version 5.1.

Conventions

The following typographical conventions are used in this document:

Roman font	normal text
`Courier`	used to indicate either a command or a standard Unix parameter or a file
Italics	used for a question that you must evaluate before continuing

Root Shell Environment Assumed

The actions in this document are written with the assumption that they will be executed by the root user running the `/bin/ksh` shell and without `noclobber` set. Also, the following directories are assumed to be in root's path:

```
/usr/bin:/etc:/usr/sbin:/usr/ucb:/sbin
```

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.

Vulnerabilities

In addition to any specific issues presented by a particular service or protocol, ***every*** service has the potential of being an entry point into a system if a vulnerability is found. This is why we recommend that some services are disabled even though there is no clear way to exploit them, and there has never been a problem with the service. If you are running an unneeded service, you could have a problem if a hole is found.

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.ksh
```

`mksysb` is the best way of performing a backup of your system prior to making the changes in this Benchmark. If `mksysb` is not available to you for whatever reason, the `do-backup.ksh` script is provided to backup files that are changed in this Benchmark. It does not make a backup of the AIX object repository – use SMIT to remove installed software packages.

Software Package Removal

There is considerable debate over the maintenance of unused software packages. Some people feel that as long as the software is not being used, leaving it installed poses no appreciable risk. Others feel that unused software presents another attack vector and increases the maintenance effort for the administrators. This Benchmark makes no recommendation for the removal of unused software. If vulnerable software is present on a system, that vulnerability may be exploitable by a local attacker, and the reader is advised to consider the effort in either its removal or maintenance and the risks thereof.

Software Package Installation

Throughout this Benchmark, you may be directed to enable software package init scripts using the `chrctcp` command. This assumes you already installed said package(s). If the `chrctcp` command fails, verify you actually installed the software required.

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:

Update system per your Enterprise Update procedures. (Small sites, see discussion.)

Verify that all patches are properly configured with

```
lppchk -c
lppchk -l
lppchk -v
```

After applying patches, double-check that services that were previously disabled have remained disabled. Patches will occasionally re-enable services that you may have already disabled.

Discussion:

Installing up-to-date vendor patches and developing a procedure for keeping up-to-date with vendor patches is critical for the security and reliability of the system. The vast majority of successful attacks on systems use exploits against known vulnerabilities that have patches available. Vendors will issue operating system updates when they become aware of security vulnerabilities and other serious functionality issues, but it is up to their customers to actually download and install these patches.

Note that **`lppchk`** was designed to catch accidental breakage of software – it was not designed to resist intentional attack. `lppchk -c` checks only the size and checksums of files – it does not check file permissions. As a result, it will not notice a binary that is set-UID or set-GID that should not be, or a modified file that has been tailored to have the "correct" checksum. If `lppchk -c` reports an unexpected value, you do have a problem – the lack of errors does not guarantee that all is well. You may wish to consider installing packages such as TripWire or AIDE, which are designed to resist attempts to deceive it.

Also – it is normal for **lppchk -c** to flag files that have been updated by an emergency fix, as those fixes are not packaged to update the LPP database.

To check if a a specific LPP level is installed (for example, bos.rte.shell):

```
# lslpp -L bos.rte.shell
Fileset Level State Type Description (Uninstaller)
--------------------------------------------------------------
bos.rte.shell 5.1.0.16 A F Shells (bsh, ksh, csh)
```

To check if a specific APAR is installed (for example, IY25437):

```
# instfix -ivk IY25437
IY25437 Abstract: SECURITY: Buffer overflow in CDE dtspcd
Fileset X11.Dt.lib:5.1.0.16 is applied on the system.
All filesets for IY25437 were found.
```

You should also subscribe to IBM's Security Bulletins Digest, which directs you to install specific security patches as they come out. Information on subscribing to the Security Bulletins Digest is available from https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs

Small sites that do not have an Enterprise Update process

To download recommended maintenance levels or individual PTFs for AIX:

http://www.ibm.com/servers/eserver/support/pseries/aixfixes.html

and follow the instructions that IBM presents on the web site.

1.2 Validate your system before making changes

Ensuring your system is functioning properly before you make a change is a prudent system administration best practice and will save you hours of aggravation. Applying this Benchmark to a system that already has issues makes troubleshooting very difficult and may lead you to believe the Benchmark is at fault.

Examine the system and application logs using `errpt -a` or using `smit` to view them. ***Resolve all issues before continuing.***

1.3 Configure SSH

Action:

1. Install SSH (see discussion for sources).
2. Modify `/usr/local/etc/sshd_config` (may be `/etc/sshd_config`, depending on version installed) – the script below will find the correct location for you:

```
unalias cp rm mv
case `find /usr /etc -type f | grep -c ssh_config$` in
  0) echo "Cannot find ssh_config"
     ;;
  1) DIR=`find /usr /etc -type f 2>/dev/null | \
       grep ssh_config$ | sed -e "s:/ssh_config::"`
     cd $DIR
     cp ssh_config ssh_config.tmp
     awk '/^#? *Protocol/ { print "Protocol 2"; next };
    { print }' ssh_config.tmp > ssh_config
     if [ "`grep -El ^Protocol ssh_config`" = "" ]; then
         echo 'Protocol 2' >> ssh_config
     fi
     rm ssh_config.tmp
     chmod 600 ssh_config
     ;;
  *) echo "You have multiple sshd_config files.  Resolve"
     echo "before continuing."
     ;;
esac
```

Manually edit `$DIR/ssh_config` to put “`Protocol 2`” under the “`Host *`” entry. Because of the substantially different `ssh_config` files in the various versions of SSH, a manual edit is required.

Note: The required entry may already be in place.

```
cd $DIR
cp sshd_config sshd_config.tmp
awk '/^#? *Protocol/ { print "Protocol 2"; next };
    /^#? *X11Forwarding/ \
        { print "X11Forwarding yes"; next };
    /^#? *IgnoreRhosts/ \
        { print "IgnoreRhosts yes"; next };
    /^#? *RhostsAuthentication/ \
        { print " RhostsAuthentication no"; next };
    /^#? *RhostsRSAAuthentication/ \
        { print "RhostsRSAAuthentication no"; next };
    /^#? *HostbasedAuthentication/ \
        { print "HostbasedAuthentication no"; next };
    /^#? *PermitRootLogin/ \
        { print "PermitRootLogin no"; next };
    /^#? *PermitEmptyPasswords/ \
        { print "PermitEmptyPasswords no"; next };
    /^#? *Banner/ \
        { print "Banner /etc/motd"; next };
    {print}' sshd_config.tmp > sshd_config
rm sshd_config.tmp
chmod 600 sshd_config
```

Discussion:

OpenSSH is a popular free distribution of the standards-track SSH protocols, which allow secure encrypted network logins and file transfers. 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. However, we feel it is necessary to put forth this extra effort in order to stay current with OpenSSH releases and patches. Additionally, pre-compiled versions are often not compiled with the options you might find necessary, such as Kerberos support. For more information on OpenSSH, see http://www.openssh.org.

If you feel that you need to use a pre-compiled package for OpenSSH, you have several options:

1. An AIX version is supplied on the AIX Bonus Pack CD's.
2. IBM maintains an `installp` image for AIX5L at http://publib16.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixbman/security/openssh.htm. This site also includes instructions for compiling OpenSSH on AIX.
3. Bull maintains a very large repository of Open Source software for AIX, and may be more current than the software on the Bonus Pack CD's. Bull's web site is http://www.bullfreeware.com/. Install and configure SSH using the IBM Redbook at http://www.redbooks.ibm.com/redbooks/pdfs/sg246873.pdf, section 5.2.

The settings in this section attempt to ensure safe defaults for both the client and the server. Specifically, both the `ssh` client and the `sshd` server are configured to use only SSH protocol 2, as security vulnerabilities have been found in the first SSH protocol. This may cause compatibility issues at sites still using the vulnerable SSH protocol 1 these sites should endeavor to configure all systems to use only SSH protocol 2.

Note: If you installed the SSH package in this step, there will be no `-preCIS` backup of the configuration files. If SSH was previously existing, the `do-backup.ksh` script will capture a backup of the configuration files.

Note: Ensure `sshd` is working properly (including ability to start automatically on reboot) before proceeding with this Benchmark. Failure to do so could lock you out of your machine if `sshd` is not running and you disable `telnetd`.

1.4 Install TCP wrappers package

Action:

1. Download pre-compiled TCP Wrappers from

    http://www.bullfreeware.com/download/aix43/tcp_wrappers-7.6.1.0.exe

While the package is named aix43 it has been installed and tested on all versions up to AIX 5.2.

2. Install software.

Discussion:

TCP Wrappers is installed in this section and configured in section 2.2. This step is optional if you already have TCP Wrappers installed.

2 Minimize inetd network services

You will need to unalias the mv, rm and cp commands as some commands overwrite files and you may be prompted numerous times about overwriting these files:

```
unalias mv rm cp
```

2.1 Disable standard services

Action:

```
for SVC in ftp telnet shell kshell login klogin exec \
  echo discard chargen daytime time ttdbserver dtspc; do
    echo "Disabling $SVC TCP"
    chsubserver -d -v $SVC -p tcp
done

for SVC in ntalk rstatd rusersd rwalld sprayd pcnfsd \
  echo discard chargen daytime time cmsd; do
    echo "Disabling $SVC UDP"
    chsubserver -d -v $SVC -p udp
done
refresh -s inetd
```

Discussion:

The stock /etc/inetd.conf file shipped with AIX 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. Using the above commands effectively disables all inetd-based network services. You will need to re-enable any service you find absolutely necessary to your organization. By disabling all inetd-based services and only re-enabling what is necessary you avoid a common mistake of simply overlooking a service which may be vulnerable.

We strongly recommend that you implement local procedures to ensure that unwanted services remain disabled. This will ensure that an operating system patch doesn't re-enable a service.

2.2 Configure TCP wrappers to limit access

Question:

Is there a reason to allow unlimited network access to this server?

If the answer to this question is ***no***, then perform the action below.

Action:

1. Create `/etc/hosts.allow` and `/etc/hosts.deny` per available documentation and to suit your particular environment. Configuring TCP Wrappers is beyond the scope of this Benchmark.

Note: Do not deny access to your system without allowing access.

2. Modify `/etc/inetd.conf`:

```
cd /etc
awk '($3 ~ /^tcp/) && ($6 !~ /(internal|tcpd)$/) \
  { $7 = $6; $6 = "/usr/local/bin/tcpd" }; \
  { print }' inetd.conf > inetd.conf.with_tcp_wrappers
cp inetd.conf.with_tcp_wrappers inetd.conf
chown root:system inetd.conf
chmod 644 inetd.conf inetd.conf.with_tcp_wrappers
```

Test your configuration now by using the `/usr/local/bin/tcpdchk` command and by logging in remotely.

Discussion:

By limiting access to the server, you reduce your exposure to threats from attackers on remote systems. For Internet-connected servers that provide service to the whole Internet, limiting access may not make sense. Intranet servers, limited-access servers, and workstations should limit access to only authorized networks.

TCP Wrappers allows 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 provides logging information via Syslog about both successful and unsuccessful connections. TCP Wrappers are generally triggered out of `/etc/inetd.conf` but other options exist for "wrappering" non-`inetd`-based software (see the documentation provided with the source code release).

If you would rather download and compile TCP Wrappers instead of using the pre-compiled version, the source code is available at http://www.porcupine.org.

IPv6 Note: The TCP Wrappers binary referenced above does not support IPv6. If you need IPv6 support, please see http://www-aix.gsi.de/~bio/DOCS/tcpwrapperinstall.html for instructions on compiling TCP Wrappers for IPv6 support.

Many daemons (SSH for example) are compiled with TCP Wrapper support, so you can use `/etc/hosts.allow` and `/etc/hosts.deny` to limit SSH access to your systems.

It is important to note that TCP wrappers looks at `hosts.allow` first, then `hosts.deny`, and controls access based on the first match. If you omit entries in `hosts.allow` and deny access to ALL in `hosts.deny`, you will block network access to all network clients.

2.3 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 actions below.

Action:

```
chsubserver -a -v telnet -p tcp
refresh -s inetd
```

Discussion:

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

To aid in the migration to SSH, there is a freely available SSH client for Windows called putty, which is available from Simon Tatham (see http://www.chiark.greenend.org.uk/~sgtatham/putty/). There are numerous commercially supported SSH clients as well – check to see if your Enterprise already has an Enterprise SSH client.

Some Enterprises are using telnet over SSL, however, the simpler and more standard solution is to use SSH. Configuring telnet over SSL is beyond the scope of a Level 1 Benchmark and will not be addressed here.

It is understood that large Enterprises deeply entrenched in using `telnet` may take considerable effort in migrating from `telnet` to `ssh`, so `telnet` may have to be enabled. When it can be disabled, disable `telnetd` and refresh `initd`.

Note: Ensure you have tested an alternate remote access method for your servers before leaving `telnet` disabled. Failure to do so may result in being denied remote access.

2.4 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 an FTP server, rather than `sftp` or `scp`?

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

Action

```
chsubserver -a -v ftp -p tcp
refresh -s inetd
```

Discussion:

Like `telnet`, the FTP protocol is unencrypted, which means passwords and other data transmitted during the session can be captured by sniffing the network, and that the FTP session itself can be hijacked by an external attacker. SSH provides two 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 section 7.2 below.

Note: Any directory writable by an anonymous FTP server should have its own partition. This helps prevent an FTP server from filling a hard drive used by other services.

To aid in the migration away from FTP, there are a number of freely available `scp` and `sftp` client for Windows, such as WinSCP (available from http://winscp.sourceforge.net/eng/index.php) for a Graphical interface to putty, and pscp, which is a part of the previously mentioned putty package.

Some Enterprises are using FTP over SSL, however, the simpler and more standard solution is to use SSH. Configuring FTP over SSL is beyond the scope of a Level 1 Benchmark and will not be addressed here.

2.5 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:

```
chsubserver -a -v shell -p tcp
chsubserver -a -v login -p tcp
refresh -s inetd
```

Discussion:

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

2.6 Only enable TFTP Server 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:

```
chsubserver -a -v tftp -p udp
refresh -s inetd
```

Discussion:

TFTP is typically used for network booting of diskless workstations, X-terminals, and other similar devices. Also, ***IBM RS/6000 SP systems require tftp to operate.*** 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.

Note: The tftp-server software is not installed by default. You will have to install it if you need to use it. After installing it, perform the actions above.

2.7 Only enable Kerberos-related daemons if absolutely necessary

Question:

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

If the answer to these questions is ***yes***, proceed with the actions below.

Action:

```
chsubserver -a -v klogin -p tcp
chsubserver -a -v kshell -p tcp
refresh -s inetd
```

Discussion:

Kerberized `rlogin` offers a higher degree of security than traditional `rlogin` or `telnet` by eliminating many clear-text password exchanges from the network. However, it is still not as secure as SSH, which encrypts all traffic. For instance, if you use `klogin` to login to a system, that password isn't sent in the clear – but if you '`su`' to another userid, that password is fair game for any network-sniffing programs.

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.org).

2.8 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:

```
chsubserver -a -v rquotad -p udp
refresh -s inetd
```

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.

2.9 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:

```
chsubserver -a -v 100083 -p tcp
refresh -s inetd
```

Discussion:

The `rpc.ttdbserverd` process supports many tools and applications in the CDE windowing environment, but has historically been a major security issue for Unix-based 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.

3 Minimize Daemon Services

3.1 Disable login prompts on serial ports

Action – AIX5L only:

```
for i in `grep ^tty /etc/inittab | cut -f1 -d:`; do
    echo "Disabling login from port /dev/$i"
    chitab "$i:2:off:/usr/sbin/getty /dev/$i"
done
```

Discussion:

By disabling the `getty` process on the system serial ports, 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 system console's `getty` process uses `/dev/console` rather than a `/dev/tty`.

3.2 Disable `inetd`, if possible

Action:

```
if [ `grep -Evc '^[ \t]*(#|$)' /etc/inetd.conf` -eq 0 ]; then
    echo "Turning off inetd"
    chrctcp -d inetd
    stopsrc -s inetd
fi
```

Discussion:

If the actions in Section 2 of this benchmark resulted in all `inetd`-based services being disabled, 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.

3.3 Disable email server, if possible

Question:

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

Perform the appropriate action below.

Action – No, this machine does not process mail:

```
stopsrc -s sendmail
chrctcp -d sendmail
cd /var/spool/cron/crontabs
crontab -l > root.tmp
if [ `grep -c "sendmail -q" root.tmp` -eq 0 ]; then
    echo "0 * * * * /usr/sbin/sendmail -q" >> root.tmp
    crontab root.tmp
fi
rm -f root.tmp
```

This will make `sendmail` run the queue once an hour, sending out any mail that may have accumulated on the machine (from `cron` jobs, etc).

Action – Yes, this machine processes mail:

Sendmail is preconfigured to allow relaying from outside your domain. CIS is preparing a Sendmail Benchmark that will replace this section and address other Sendmail issues. In the interim, please follow the guidelines presented by Sandor Sklar at http://www.securitymap.net/sdm/docs/system-sec/Securing%20AIX%20Network%20Services.htm.

Discussion:

It is possible to run a Unix system with the Sendmail daemon disabled and still allow users (and programs such as 'cron') 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 AIX 5L (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.

Closing AIX Sendmail Open Relay

The default behavior of Sendmail in AIX 4.3.3 allows open relaying - the mail server will accept and process mail sent from outside your organization to addresses that are also outside your organization. This defect is commonly used by "spammers" to send e-mail to thousands of addresses, all originating from your mail server.

Before enabling sendmail in daemon mode, the sendmail configuration file must be modified to prevent this misuse of your system. The above steps explain how to update the `sendmail.cf` configuration file.

3.4 Disable NIS Server processes if possible

Question:

Is this machine an NIS (Network Information Service) server?

If the answer to this question is ***no***, then perform the action below.

Action:

Use the SMIT fast-path

```
smit remove
```

to remove the `bos.net.nis.server` fileset or use the command:

```
[ `lslpp -L bos.net.nis.server 2>&1 | \
  grep -c "not installed"` -eq 0 ] && \
  /usr/lib/instl/sm_inst installp_cmd -u \
  -f'bos.net.nis.server'
```

Discussion:

This service must be enabled if the local site is using the NIS naming service to distribute system and user configuration information.
NIS services are a convenient method to manage user accounts and home directories across a large network of servers, however they are also a favored entry point for attackers. If the NIS software is installed but not configured, an attacker can cripple a machine by starting NIS. In addition, tools like `ypsnarf` allow an attacker to grab the contents of your NIS maps, providing large amounts of information about your site. Use the `/etc/yp/securenets` file to restrict what machines your NIS server will talk to. Also utilize secure NIS to encrypt communication between the client and server.

3.5 Disable NIS Client processes if possible

Question:

Is this machine an NIS (Network Information Service) client?

If the answer to this question is ***no***, then perform the action below.

Action:

Use the SMIT fast-path

```
smit remove
```

to remove the `bos.net.nis.client` fileset or use the command:

```
[ `lslpp -L bos.net.nis.client 2>&1 | \
  grep -c "not installed"` -eq 0 ] && \
  /usr/lib/instl/sm_inst installp_cmd -u \
  -f'bos.net.nis.client'
```

Discussion:

NIS services are a convenient method to manage user accounts and home directories across a large network of servers, however they are also a favored entry point for attackers. For this reason, many organizations choose not to use NIS. If you do not need NIS, remove it from the system.

3.6 Disable NFS Server processes if possible

Question:

Is this machine an NFS file server?

If the answer to this question is ***no***, then perform the action below.

Action:

```
[ -f /etc/exports ] && rm -f /etc/exports
```

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 machine is an NFS server, the administrator should take reasonable precautions when exporting file systems, including restricting NFS access to a specific range of local

IP addresses and exporting file systems "read-only" and "nosuid" where appropriate. Also, you must ensure that all of the UID/GID on the server and clients systems are unique. NFS file access is based on the UID/GID pair so if there are conflicting UID/GID pairs between the servers and clients, there is a possibility of unauthorized file access. You should also strongly consider using the AIX Secure NFS facility. This facility uses DES encryption and public key cryptography to identify users and servers.

3.7 Disable NFS Client processes if possible

Question:

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

If the answer to this question is ***no***, then perform the action below.

Action:

```
    rmnfs -B
```

Discussion:

While this action disables the standard NFS client processes, it is important to note that it is still possible for the superuser to mount remote file systems on the local machine via NFS. The administrator can completely disable NFS client access by removing the NFS client software packages, but these packages will have to be re-installed and repatched 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 preferable to NFS for certain applications. The use of secure RPC or Kerberos can significantly improve NFS security. NIS is also started in `/etc/rc.nfs`, so do not run `rmnfs` if your site uses NIS.

3.8 Disable GUI login if possible

Question:

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

If the answer to this question is ***no***, then perform the action below.

Action:

```
chmod ug-s /usr/dt/bin/dtaction \
    /usr/dt/bin/dtappgather /usr/dt/bin/dtprintinfo
    /usr/dt/bin/dtsession
/usr/dt/bin/dtconfig -d
```

Discussion:

Note that for the 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 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.

3.9 Turn off services which are not commonly used

Action (AIX 4.3.3):

```
for SVC in routed gated named timed rwhod \
  snmpd dpid2 lpd portmap ndpd-router ndpd-host; do
    echo "Turning off $SVC"
    stopsrc -s $SVC
    chrctcp -d $SVC
done

for SVC in piobe httpdlite pmd writesrv; do
    echo "Turning off $SVC"
    rmitab $SVC
done
```

Action (AIX 5):

```
for SVC in routed gated named timed rwhod mrouted \
  snmpd hostmibd dpid2 lpd portmap autoconf6 \
  ndpd-router ndpd-host; do
    echo "Turning off $SVC"
    stopsrc -s $SVC
    chrctcp -d $SVC
done

for SVC in piobe i4ls httpdlite pmd writesrv; do
    echo "Turning off $SVC"
    stopsrc -s $SVC
    rmitab $SVC
done
```

Discussion:

Disabling these services in the System Resource Controller will disable a wide variety of infrequently used subsystems. The resources are made inoperative (rather than removed outright) so that the local administrator can easily "restore" any of these resources if they discover a mission-critical need for one of these services. Note also that vendor patches may restore some of the original entries in the System Resource Controller - it is always a good idea to check the System Resource Controller using `lssrc -a` for any resources 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. 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.

3.10 Only enable 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 the question is ***yes***, then perform the action below.

Action:

```
mkitab -i cron \
    "piobe:2:wait:/usr/lib/lpd/pio/etc/pioinit >/dev/null 2>&1"
chrctcp -a lpd
```

Discussion:

PIOBE stands for Printer IO Back End. If users will never print files from this machine and the system will never be used as a print server by other hosts on the network, then it is safe to disable these services. Note that the RFC 1179 service is a BSD-compatible print spooler, which only has to be enabled if the machine is being used as a network print server by machines that require a BSD-style remote printer interface. In most cases, this RFC 1179 service is not necessary and should not be enabled.

3.11 Only enable SNMP if absolutely necessary

Question:

Does a tool (e.g., IBM OpenView, MRTG, Cricket) that relies on SNMP remotely monitor this system?

If the answer to the question is ***yes***, then perform the action below.

Action:

```
chrctcp -a snmpd
chrctcp -a dpid2
chrctcp -a hostmibd
```

Discussion:

If you are using SNMP to monitor the hosts on your network, it is prudent to change the default community string used to access data via SNMP. Use the `community` and `view` statements in `/etc/snmpd.conf` to change the community strings. In addition, use the `address/netmask` and `permissions` parameters on the `community` statement to restrict SNMP access to only your management stations.

3.12 Only enable `portmap` 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;*
- *This machine runs the CDE GUI;*
- *The machine runs a third-party software application which is dependent on RPC support;*

If any of the answers to these questions is ***yes***, then proceed with the actions below.

Action:

```
chrctcp -a portmap
```

Discussion:

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

3.13 Only enable IPv6 if absolutely necessary

Question:

Does the system in question use the IPv6 protocol?

If the answer is ***yes***, then perform the following action.

Action:

```
chrctcp -a autoconf6
chrctcp -a ndpd-router
chrctcp -a ndpd-host
```

Discussion:

Although IPv6 is being deployed at many sites, it is still not widespread. Unless your network already has IPv6 support, running the IPv6 daemons is pointless (and can allow other hosts on the same physical subnet to connect via IPv6 even when the network doesn't support it). AIX's support of IPv6 (for instance, in `inetd`) does not require these daemons to be running unless you want to communicate with another machine using IPv6 – the IPv6-aware software works just fine in IPv4-only or standalone mode without these daemons.

3.14 Only enable DHCP if absolutely necessary

Question:

Does the system in question function as a DHCP client, server, or relay agent?

For each of the three cases, if the answer is ***yes***, then perform the applicable action below (shown in the comment to the right of the command).

Action:

DHCP client

```
     chrctcp -a dhcpcd # client daemon
```

DHCP server

```
     chrctcp -a dhcpsd # server daemon
```

DHCP relay agent

```
     chrctcp -a dhcprd # relay daemon
```

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, a DHCP client, or a DHCP relay agent, there is no need to be running this service.

3.15 Only enable `i4ls` and NCS if absolutely necessary

Question:

Does the system require the `i4ls` licensing software?

If the answer is ***yes***, then perform the following action.

Action:

```
mkitab -i cron "i4ls:2:wait:/usr/bin/startsrc -swritesrv"
chrctcp -a writesrv
```

Discussion:

As a particular special-case, the IBM VisualAge compilers can be installed with a nodelocked license in `/var/ifor/nodelock`, eliminating the requirement for the `i4ls` daemons. This in turn will probably result in the Network Computing System (NCS) daemons not being started either, as `i4ls` is one of the few products that uses NCS.

3.16 Only enable `writesrv`, `pmd`, `httpdlite` if absolutely necessary

Question:

Are the `writesrv`, `pmd`, or `httpdlite` services required?

If the answer is ***yes***, then perform the corresponding action below.

Action:

writesrv

```
mkitab -i cron "writesrv:2:wait:/usr/bin/startsrc -swritesrv"
chrctcp -a writesrv
```

pmd

```
mkitab -i cron "pmd:2:wait:/usr/bin/pmd > /dev/console 2>&1 #
Start PM daemon"
chrctcp -a pmd
```

httpdlite

```
mkitab -i cron
"httpdlite:2:once:/usr/IMNSearch/httpdlite/httpdlite -r
/etc/IMNSearch/httpdlite/httpdlite.conf & >/dev/console 2>&1"
chrctcp -a httpdlite
```

Discussion:

These services are started from the `/etc/inittab` file. The `rmitab` command removes a specified service. The following services are started by `inittab` and can be removed if not needed:

- `writesrv` – allows users to chat using the system write facility on a terminal.
- `pmd` – Power management service that turns your machine off if it has been idle a specific amount of time.
- `httpdlite` – Lite NetQuestion Web server software for online documentation. This is only needed for the “search” function for web-browsable documentation. The ‘man’ command does not need this to work correctly.

4 Kernel tuning

4.1 Disable core dumps

Action:

Edit `/etc/security/limits` and change the core value in the default stanza to:

```
core 0
```

Add the following line below it:

```
core_hard = 0
```

Execute these commands:

```
echo "# Added by CISecurity Benchmark" >> /etc/profile
echo "ulimit -c 0" >> /etc/profile
chdev -l sys0 -a fullcore=false
```

Discussion:

Some vulnerabilities attempt to cause a core dump. Since applications can dump the entire contents of that application's memory at the time of the fault, sensitive information can be contained in the core file and be extracted by attackers.

4.2 Network parameter modifications

Action:

```
cat <<EOF > /etc/rc.net-tune
#!/bin/ksh
# Deal with SYN-flood attacks as best we can.
/usr/sbin/no -o clean_partial_conns=1
# Do not allow SMURF broadcast attacks.
/usr/sbin/no -o directed_broadcast=0
# Don't allow other machines to reset our netmask
/usr/sbin/no -o icmpaddressmask=0
# Ignore redirects, don't send them ourselves.
# ICMP Redirect is a poor excuse for a routing protocol.
/usr/sbin/no -o ipignoreredirects=1
/usr/sbin/no -o ipsendredirects=0
# Refuse to have anything to do with source-routed packets.
/usr/sbin/no -o ipsrcrouteforward=0
/usr/sbin/no -o ipsrcrouterecv=0
```

```
/usr/sbin/no -o ipsrcroutesend=0
/usr/sbin/no -o nonlocsrcroute=0
EOF
chmod +x /etc/rc.net-tune
mkitab -i rctcpip "rcnettune:2:wait:/etc/rc.net-tune > \
    /dev/console 2>&1"
```

Discussion:

We are creating a new script that will be executed at boot time to reconfigure various network parameters, to be in line with current best practices.

Note also that support for source-routed packets is needed in some cluster configurations, so the four '`srcroute`' options should be omitted in those environments.

4.3 Restrict NFS Client requests to privileged ports

Action:

```
cat <<EOF >> /etc/rc.net-tune
# Require NFS to use privileged ports
/usr/sbin/nfso -o portcheck=1 -o nfs_use_reserved_ports=1
EOF
```

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 NFS attacks that are run by unprivileged users.

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 'logcheck' from http://www.logcheck.org/, 'logwatch' from http://www.psionic.com/, 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: These tools are not officially supported by IBM.

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). It also has the more mundane benefit of ensuring that you still have access to a copy of the logs for debugging system crashes as the local copy may not be accessible if the system is refusing to boot or the buffers were not flushed first.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) we 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://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/cmds/aixcmds6/xntpd.htm and http://www.ntp.org.

5.1 Capture messages sent to `syslog` (especially the AUTH facility)

Action:

```
printf "### Following lines added by CISecurity \
AIX Benchmark Section 5.1\n\
auth.info\t\t/var/adm/authlog\n\
*.info;auth.none\t\t/var/adm/syslog\n" \
    >> /etc/syslog.conf
touch /var/adm/authlog /var/adm/syslog
chown root:system /var/adm/authlog
chmod 600 /var/adm/authlog
chmod 640 /var/adm/syslog
stopsrc -s syslogd
startsrc -s syslogd
```

Discussion:

By default, AIX systems do not capture logging information sent to syslogd. This is unfortunate, since a great deal of important security-related information (successful and failed su attempts, failed login attempts, *root* login attempts, etc.) is sent via the LOG_AUTH channel. If this data is not logged, you don't have any way of knowing what is going on.

The above action causes this information to be captured in the /var/adm/authlog file, which is only readable by the superuser. This file should be reviewed and archived on a regular basis. In addition, messages sent to syslog channels other than LOG_AUTH are sent to /var/adm/syslog (which should also be reviewed).

Note: Some AIX administrators prefer to log syslog events to /var/log – if this is your preference, change the above script to reflect /var/log instead of /var/adm.

5.2 Configure syslogd to send logs to a remote loghost

Action:

In the script below, replace loghost with the proper name (FQDN, if necessary) of your loghost.

```
printf "### Following lines added by CISecurity \
AIX Benchmark Section 5.2\n\
auth.info\t\t@loghost
*.info;auth.none\t\t@loghost
*.emerg\t\t@loghost\n\
local7.*\t\t@loghost\n" >> /etc/syslog.conf
stopsrc -s syslogd
startsrc -s syslogd
```

Discussion:

Remote logging is essential in detecting intrusion and monitoring several servers operating in concert. An intruder – once he/she has obtained root – can edit the system logs to remove all traces of the attack. If the logs are stored off the machine, those logs can be analyzed for anomalies and used for prosecuting the attacker.

5.3 Prevent Syslog from accepting messages from the network

Question:

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

If the answer to this question is ***no***, then perform the action below.

Action:

```
chssys -s syslogd -a "-r"
stopsrc -s syslogd
startsrc -s syslogd
```

Discussion:

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

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

5.4 Enable `sar` accounting

Action:

Install the `bos.acct` fileset as it is required when making use of the `sar` utility.

Note: The following `crontab` entries are an example only. You need to adjust the times of the report and the period the data is collected. Refer to `sar` documentation.

```
lslpp -i bos.acct >/dev/null 2>&1
if [ "$?" != 0 ]; then
    echo "bos.acct not installed, cannot proceed"
else
    su - adm -c "crontab -l > /tmp/crontab.adm"
    cat << EOF >> /tmp/crontab.adm
0 8-17 * * 1-5 /usr/lib/sa/sa1 1200 3 &
0 * * * 0,6 /usr/lib/sa/sa1 &
0 18-7 * * 1-5 /usr/lib/sa/sa1 &
5 18 * * 1-5 /usr/lib/sa/sa2 -s 8:00 -e 18:01 -i 3600 -A &
EOF
    mkdir -p /var/adm/sa
    chown adm:adm /var/adm/sa
    chmod 755 /var/adm/sa
    su - adm -c "crontab /tmp/crontab.adm"
fi
```

Discussion:

System accounting gathers baseline system data (CPU utilization, disk I/O, etc.) every few minutes. The data may be accessed with the `sar` command, or by reviewing the nightly report files named `/var/adm/sa/sar*`. Once a normal baseline for the system has been established, unauthorized activity (password crackers and other CPU-intensive jobs, and activity outside of normal usage hours) may be detected due to departures from the normal system performance curve. Note that this data is only archived for one week before being automatically removed by the regular nightly cron job. Administrators may wish to archive the `/var/adm/sa/` directory on a regular basis to preserve this data for longer periods.

Note: The above `crontab` entries are an example only. You need to adjust the times of the report and the period the data is collected. Refer to `sar` documentation.

5.5 Enable kernel-level auditing

Action:

To activate auditing:

```
audit on
```

To start auditing automatically at next boot:

```
mkitab -i cron "audit:2:once:/usr/sbin/audit start 2>&1  >
/dev/console"
telinit q
echo "audit shutdown" >> /usr/sbin/shutdown
```

Discussion:

For information on auditing, see http://www.redbooks.ibm.com/redbooks/pdfs/sg246020.pdf, note chapter 2. Quote from chapter of note:

> An audit is defined as an examination of a group, individual account, or activity. Thus, the auditing subsystem provides a means of tracing and recording what is happening on your system.

> By default, auditing is not activated in AIX. When you start the audit subsystem, it gathers information depending on your configuration file. It may be unnecessary for you to start auditing if you just let the files sit in your busy system. What is important is for you to be able to interpret an auditing record. Depending on your environment, it may or may not be necessary for auditing to run every time. It is a decision you have to make.

We recommended that you explore kernel level auditing before implementing it in your startup scripts.

5.6 Confirm Permissions On System Log Files

Action:

```
for FILE in \
  /smit.log \
  /var/adm/cron/log \
  /var/tmp/dpid2.log \
  /var/tmp/hostmibd.log \
  /var/tmp/snmpd.log \
  /var/adm/ras/*
  /var/ct/RMstart.log
do
    if [ -f $FILE ]; then
        echo "Fixing log file permissions on $FILE"
        chmod o-rw $FILE
    fi
done
```

Discussion:

It is 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.

If you should add any of the services that affect the above logs, please revisit this section to ensure the logs have the correct/secure permissions.

6 File/directory permissions/access

6.1 Verify `passwd` and `group` file permissions

Action:

```
chown -R root:security /etc/passwd /etc/group /etc/security
chown -R root:audit /etc/security/audit
chmod 644 /etc/passwd /etc/group
chmod 750 /etc/security
chmod -R go-w,o-r /etc/security
```

Discussion:

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

6.2 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 `mount | grep dev | awk '{print $2}' | \
  grep -Ev 'cdrom|nfs'`; do
  echo "Searching $part"
  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.

6.3 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 installed on the system may run the following commands:

```
for part in `mount | grep dev | awk '{print $2}' | \
    egrep -v 'cdrom|nfs'`; do
    echo "Searching $part"
    find $part -xdev -type f \
    \( -perm -0002 -a ! -perm -1000 \) -print
done
```

There should be no entries returned.

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.

6.4 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 `mount | grep dev | awk '{print $2}' | \
    egrep -v 'cdrom|nfs'`; do
    echo "Searching $part"
    find $part \( -perm -04000 -o -perm -02000 \) \
    -type f -xdev -ls
done
```

Discussion:

The administrator should take care to ensure that no rogue set-UID programs have been introduced into the system. In addition, if possible, the administrator should attempt a Set-UID audit and reduction.

6.5 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 / \( -nouser -o -nogroup \) -ls
```

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.

7 System access, authentication, and authorization

7.1 Remove /etc/hosts.equiv

Action:

```
[ -f /etc/hosts.equiv ] && rm -f /etc/hosts.equiv
```

Discussion:

The /etc/hosts.equiv file provides total trust in any machines listed. If a machine listed is compromised, the attacker can immediately get full access to your machine. /etc/hosts.equiv sets up global trust relationships for all accounts on the system, which work in an analogous fashion to .rhosts files in user home directories. See the discussion of .rhosts files in the items below.

7.2 Create /etc/ftpusers

Action:

```
lsuser -c ALL | grep -v ^#name | cut -f1 -d: | while read NAME; do
  if [ `lsuser -f $NAME | grep id | cut -f2 -d=` -lt 200 ]; then
    echo "Adding $NAME to /etc/ftpusers"
    echo $NAME >> /etc/ftpusers.new
  fi
done
sort -u /etc/ftpusers.new > /etc/ftpusers
rm /etc/ftpusers.new
chown root:system /etc/ftpusers
chmod 600 /etc/ftpusers
```

Discussion:

/etc/ftpusers contains a list of users who are not allowed to access the system via FTP. Consider also adding the names of other privileged or shared accounts which may exist on your system such as user oracle and the account under which your Web server process runs.

Generally, only normal users should ever access the system via FTP – there should be no reason for “system” type accounts to transfer information via this mechanism. If a system userid is allowed to FTP files into the system, that userid can be used to upload malicious software and store it with the system userid’s permissions (which are probably higher than a normal user’s). Certainly, the root account should never be allowed to transfer files directly via FTP. (Of course, there is probably no reason for FTP to be enabled at all – this is mostly “defense in depth” in case FTP accidentally becomes re-enabled, or if it’s required for some function that is unable to use SSH instead).

The above script places all users those user id is less than 200 in the `/etc/ftpusers` file, which blocks all system account from being used for FTP

7.3 Disable XDMCP port

Action:

```
if [ ! -f /etc/dt/config/Xconfig ]; then
    mkdir -p /etc/dt/config
    cp /usr/dt/config/Xconfig /etc/dt/config
fi
cd /etc/dt/config
awk '/Dtlogin.requestPort:/ \
    { print "Dtlogin.requestPort: 0"; next } \
    { print }' Xconfig > Xconfig.new
mv Xconfig.new Xconfig
chown root:bin 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 ever hearing requests for remote login services.

7.4 Prevent X Server from listening on port 6000/tcp

Action:

```
if [ -f /etc/dt/config/Xservers ]; then
    file=/etc/dt/config/Xservers
else
    file=/usr/dt/config/Xservers
fi
awk '/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:bin /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.

7.5 Set default locking screensaver timeout

Action:

```
for file in /usr/dt/config/*/sys.resources; do
    dir=`dirname $file | sed -e s/usr/etc/`
    mkdir -p $dir
    echo 'dtsession*saverTimeout: 10' >> $dir/sys.resources
    echo 'dtsession*lockTimeout: 10' >> $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, although this setting can still be overridden by individual users in their own environment.

7.6 Remove empty `crontab` files and restrict file permissions

Action:

```
cd /var/spool/cron/crontabs
for file in *; do
    lines=`grep -Ev '^[ \t]*#' $file | wc -l | sed 's/
//g'`
    if [ $lines -eq 0 ]; then
```

```
        echo "Removing $file"
        rm $file
    fi
done
chgrp -R cron /var/spool/cron/crontabs
chmod -R o= /var/spool/cron/crontabs
chmod 770 /var/spool/cron/crontabs
```

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.

7.7 Restrict `at` and `cron` to authorized users

Action:

```
cd /var/adm/cron
rm -f cron.deny at.deny
echo root > cron.allow
echo root > at.allow
ls /var/spool/cron/crontabs | grep -v root >> cron.allow
ls /var/spool/cron/atjobs | grep -v root >> at.allow
chown root:sys cron.allow at.allow
chmod 400 cron.allow at.allow
cat at.allow
cat cron.allow
cat at.deny cron.deny # this should fail
```

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 with `cron.deny` or `at.deny` removed, if a given user is not listed in `cron.allow` or `at.allow`, their cron jobs will not be executed. This includes administrative accounts – all users will be denied until explicitly defined in `cron.allow` or `at.allow`.

To prevent an unintentional impact to the existing system, the above script adds the currently existing users to cron.allow and at.allow. These users and their jobs are found in

`/var/spool/cron/atjobs` and `/var/spool/cron/cronjobs`. You should review these users and jobs before adding them to your at.allow and cron.allow files.

7.8 Restrict `root` logins to system console

Action:

```
chuser rlogin=false login=true su=true sugroups=system root
```

Discussion:

Anonymous root logins should never be allowed, except on the system console in emergency situations. At all other times, the administrator should access the system via an unprivileged account and use some authorized mechanism (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. The command above additionally restricts '`su`' to root to members of the 'system' group, making it harder for an attacker to use a stolen root password (as they will first have to get access to a 'system' userid).

Note: Ensure you have at least one user account in the system group that can log in remotely. Failure to do so will prevent any remote user from becoming root.

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:

```
for user in daemon bin sys adm uucp nuucp printq guest
nobody lpd sshd; do
    chuser rlogin=false login=false "$user"
done
```

Discussion:

These accounts are non-human system accounts that should be made less useful to an attacker by locking them. They can even be deleted if the machines does not use the daemon/service that each is responsible for, though it is safest to simply deactivate them as is done here. To deactivate them, use `chuser` to disable remote and local logins.

8.2 Set password and account expiration on active accounts

Action (AIX 4.3.3):

```
chsec -f /etc/security/user -s default -a maxage=13
chsec -f /etc/security/user -s default -a minlen=6
chsec -f /etc/security/user -s default -a minage=1
chsec -f /etc/security/user -s default -a pwdwarntime=28
```

Discussion:

The above command adds a number of restrictions to enforce password changing and the use of more complicated passwords.

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. A complete list of the options can be found in `/etc/security/passwd` file.

8.3 Verify there are no accounts with empty password fields

Action:

```
pwdck -n ALL
```

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 "*".

The `pwdck` command will verify a number of other items for correctness. The '`-n`' flag will tell it to report errors but not change anything (running with '`-t`' instead will prompt you for each proposed fix – the '`-y`' and '`-p`' flags are dangerous). Note that `pwdck` won't flag null passwords unless the `minlen` attribute is set to a non-zero value.

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

Action:

The command:

```
     grep ^+: /etc/passwd /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 may provide an avenue for attackers to gain privileged access on the system, and should be deleted if they exist.

8.5 Verify no UID 0 accounts exist other than root

Action:

The command:

```
     lsuser -a id ALL | grep "id=0" | awk '{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 root account, and it should be accessed by logging in as an unprivileged user and using the `su` command (or equivalent) 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/).

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

Action:

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

To find '.' in $PATH:

```
     echo $PATH | grep -E '(^|:)(\.|:|$)'
```

To find group- or world-writable directories in $PATH:

```
     find `echo $PATH | tr ':' ' '` -type d \
         \( -perm -002 -o -perm -020 \) -ls
```

These commands should produce no output.

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.

8.7 User home directories should be mode 750 or more restrictive

Action:

```
NEW_PERMS=750
lsuser -c ALL | grep -v ^#name | cut -f1 -d: | while read NAME; do
  if [ `lsuser -f $NAME | grep id | cut -f2 -d=` -ge 200 ]; then
```

```
    HOME=`lsuser -a home $NAME | cut -f 2 -d =`
    echo "Changing $NAME homedir $HOME"
    chmod $NEW_PERMS $HOME
  fi
done
if [ `grep -c "chmod $NEW_PERMS $1" \
  /usr/lib/security/mkuser.sys` -eq 0 ]; then
  sed -e "s/mkdir \$1/mkdir \$1 \&\& chmod $NEW_PERMS \$1/g" \
  /usr/lib/security/mkuser.sys > /tmp/mkuser.tmp
  mv /tmp/mkuser.tmp /usr/lib/security/mkuser.sys
  chmod 750 /usr/lib/security/mkuser.sys
fi
```

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.

If you need more restrictive permissions on the home directories, set the appropriate permissions in the variable `NEW_PERMS`.

While the above modifications are relatively benign, making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users.

8.8 No user dot-files should be world-writable

Action:

```
lsuser -a home ALL |cut -f2 -d= | while read HOMEDIR; do
    echo "Examining $HOMEDIR"
    if [ -d $HOMEDIR ]; then
        ls -a $HOMEDIR | grep -Ev "^.$|^..$" | \
          while read FILE; do
            if [ -f $FILE ]; then
                echo "Adjusting $FILE"
                chmod go-w $FILE
            fi
        done
    else
        echo "No home dir for $HOMEDIR"
    fi
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 the user community can result in unexpected outages and unhappy users.

Note: `/usr/lib/security/mkuser.sys` issues a `chmod go-w $1/.login` upon creation of accounts with `csh` as default shell, so no additional work is needed after a new account is created.

8.9 Remove user `.netrc` and `.rhosts` files

Action:

```
find / -name .netrc
find / -name .rhosts
```

Stop!!! Read the discussion before proceeding.

```
lsuser -a home ALL |cut -f2 -d= | while read HOME; do
    if [ -e "$HOME/.netrc" ]; then
        echo "Removing $HOME/.netrc"
        rm -f "$HOME/.netrc"
    fi
    if [ -e "$HOME/.rhosts" ]; then
        echo "Removing $HOME/.rhosts"
        rm -f "$HOME/.rhosts"
    fi
done
```

Discussion:

`.netrc` files may contain unencrypted passwords that may be used to attack other systems, while `.rhosts` files used in conjunction with the BSD-style “r-commands” (`rlogin`, `remsh`, `rcp`) 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). 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. If the first command returns any results, carefully evaluate the ramifications of removing those files before executing the remaining commands as you may end up impacting an application that has not had time to revise its architecture to a more secure design.

8.10 Set Default `umask` for users

Action:

Change existing users

```
lsuser -a home ALL | awk '{print $1}' | while read user; do
    chuser umask=077 $user
done
```

Change default profile

To set a system-wide default, edit the file `/etc/security/user` and replace the default `umask` value in the `umask` line entry for the `default` stanza with `077`.

Discussion:

The above actions change the default umask for existing users, and then it changes the default profile, which applies to all newly created users.

With a default `umask` setting of `077` – a setting agreed to as part of the consensus process with DISA and NSA – 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.

Note: This is been shown to cause problems with the installation of software packages where the installation script uses the default `umask` – the directories are owned by root with `700` permissions, and then the application and/or daemon cannot read its files. A simple fix to this problem is to manually issue a less restrictive `umask` (such as `umask 022`) for the shell session doing the installation, or place such a `umask` command (in the beginning of the installation script) to a less restrictive value before the installation, or in the beginning of the installation script.

8.11 Set default `umask` for the FTP daemon

Action:

```
chsubserver -c -v ftp -p tcp "ftpd -l -u077"
refresh -s inetd
```

Discussion:

This command changes the `umask` of the FTP user to 077. The `umask` should be set to at least 027 in order to prevent the FTP daemon process from creating world-writable files by default.

Note: If `ftpd` is disabled, you will receive the following error:

```
chsubserver: ftp not in /etc/inetd.conf
```

Note: If `inetd` is disabled, you will receive the following error:

```
0513-036 The request could not be passed to the inetd subsystem.
Start the subsystem and try your command again.
```

8.12 Set “`mesg n`” as the default for all users

Action:

```
echo "mesg n" >> /etc/profile
echo "mesg n" >> /etc/csh.login
```

Discussion:

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

8.13 Removing unnecessary default user accounts

Action:

Note: Read discussion first!!!

```
# Remove users
LIST="uucp nuucp lpd guest printq"
for USERS in $LIST; do
    rmuser -p $USERS
    rmgroup $USERS
done
# Remove groups
LIST="uucp printq"
for USERS in $LIST; do
    rmgroup $USERS
done
```

Discussion:

Removing the users that your system does not need is a prudent security precaution. The AIX 5L Version 5.3 Security Guide (http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/aixbman/security/security.htm) lists these accounts as candidates for removal:

User ID	Description
uucp, nuucp	Owner of hidden files used by uucp protocol. The uucp user account is used for the UNIX-to-UNIX Copy Program, which is a group of commands, programs, and files, present on most AIX systems, that allows the user to communicate with another AIX system over a dedicated line or a telephone line.
lpd	Owner of files used by printing subsystem
guest	Allows access to users who do not have access to accounts

In addition, these group ID's may be removed if your system does not need them:

Group ID	Description
uucp	Group to which uucp and nuucp users belong
printq	Group to which lpd user belongs

Note: You may get one or more errors stating the group or user does not exist. This is harmless and may be ignored.

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 (though there are other mechanisms available for acquiring this information). 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 network and physical access services

Action:

Edit the banner currently in `/etc/motd` as required by your Enterprise. The following script is a template taken from the Bastille Linux project:

Important: You need to change "The Company" in the text below to an appropriate value for your organization

```
cd /etc
# Remember to enter name of your company here:
COMPANYNAME="its owner"
cat <<EOM \
    | sed -e "s/its owner/${COMPANYNAME}/g" > /etc/motd
***************************************************************************
                            NOTICE TO USERS

This computer system is the private property of its owner, whether
individual, corporate or government.  It is for authorized use only.
Users (authorized or unauthorized) have no explicit or implicit
expectation of privacy.

Any or all uses of this system and all files on this system may be
intercepted, monitored, recorded, copied, audited, inspected, and
disclosed to your employer, to authorized site, government, and law
enforcement personnel, as well as authorized officials of government
agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring,
recording, copying, auditing, inspection, and disclosure at the
discretion of such personnel or officials.  Unauthorized or improper use
of this system may result in civil and criminal penalties and
administrative or disciplinary action, as appropriate. By continuing to
use this system you indicate your awareness of and consent to these terms
and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the
conditions stated in this warning.
****************************************************************************
EOM
chown bin:bin /etc/motd
chmod 644 /etc/motd
```

Discussion:

The contents of `/etc/motd` is displayed after all successful logins, no matter where the user is logging in from. Recall that we edited `sshd_conf` to display the `/etc/motd` banner, so it will appear before and after login.

9.2 Create warnings for GUI-based logins

Action:

```
for file in /usr/dt/config/*/Xresources; do
  dir=`dirname $file | sed s/usr/etc/`
  mkdir -p $dir
  if [ ! -f $dir/Xresources ]; then
      cp $file $dir/Xresources
  fi
  WARN="Authorized uses only. All activity may be monitored and
reported."
  echo "Dtlogin*greeting.labelString: $WARN" >>$dir/Xresources
  echo "Dtlogin*greeting.persLabelString: $WARN" >>$dir/Xresources
done
chown root:sys /etc/dt/config/*/Xresources
chmod 644 /etc/dt/config/*/Xresources
```

Discussion:

The standard graphical login program for AIX 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

Action:

```
chsec -f /etc/security/login.cfg -s default -a
herald="Authorized uses only. All activity may be monitored
and reported\n\r\nlogin: "
```

Discussion:

This item configures `telnetd`'s "authorized users only" banner message.

9.4 Create warnings for FTP daemon

Action:

```
dspcat -g /usr/lib/nls/msg/en_US/ftpd.cat > /tmp/ftpd.tmp
sed "s/\"\%s FTP server (\%s) ready.\"/\"\%s Authorized
uses only. All activity may be monitored and reported\"/" \
/tmp/ftpd.tmp > /tmp/ftpd.msg
gencat ftpd.cat /tmp/ftpd.msg
```

Additional Action (AIX 5.1 and later):

```
echo “herald: /etc/ftpmotd” >> /etc/ftpaccess.ctl
cat << EOF >> /etc/ftpmotd
Authorized uses only. All activity may be monitored and
reported
EOF
```

Discussion:

This item configures `ftpd`'s "authorized users only" banner messages by replacing the default “FTP server ready” message. AIX 5.1 and later gives you the option of editing `/etc/ftpmotd` with the text of your choice.

10 Reboot

Action:

```
shutdown -Fr
```

Discussion:

Whenever you make substantial changes to a system, reboot. Some System Administrators believe any change to the init scripts warrant a reboot to ensure the system comes up as expected. Hours of lost productivity with extensive troubleshooting (not to mention lost revenue) have occurred because a system did not start up as expected. The root cause was an init problem that would have been detected had the reboot taken place while the change was fresh in the mind of the administrator.

Appendix A File backup script

```
#!/bin/ksh

# Create date-specific backup timestamp extension
EXT=`date '+%Y%m%d-%H:%M:%S'`

# Backup individual files
for FILE in \
  /etc/ssh_config /etc/sshd_config \
  /etc/openssh/ssh_config /etc/openssh/sshd_config \
  /etc/inetd.conf /etc/hosts.deny /etc/hosts.allow \
  /etc/sendmail.cw /etc/sendmail.cf \
  /etc/exports /etc/inittab \ /etc/profile \
  /etc/rc.net-tune /etc/syslog.conf \
  /usr/sbin/shutdown /etc/passwd /etc/group \
  /etc/hosts.equiv /etc/ftpusers \
  /etc/dt/config/Xconfig /etc/dt/config/Xservers \
  /usr/dt/config/Xservers \
  /usr/lib/security/mkuser.sys \
  /etc/motd /etc/csh.login /etc/profile \
  /etc/ftpd.cat \
  /etc/rc.tcpip \
  /etc/syslog.conf
  do
    if [ -f ${FILE} ]; then
        echo Making backup of file ${FILE}
        cp -p ${FILE} ${FILE}-preCIS-${EXT}
        chmod 700 ${FILE}-preCIS-${EXT}
    fi
done
# Backup directories that are changed
for DIR in \
  /etc/security /var/spool/cron/crontabs
  do
    echo Making backup of directory ${DIR}
    mkdir -p -m 0700 ${DIR}-preCIS-${EXT}
    cd ${DIR}
    tar cpf - * | (cd ${DIR}-preCIS-${EXT}; tar xpf -)
done
```

Appendix B 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 Create symlinks for dangerous files

Action:

```
for FILE in /.rhosts /.shosts /etc/hosts.equiv \
    /etc/shosts.equiv; do
    [ -e $FILE ] && 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 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).

SN.2 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 -f 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.

SN.3 Install and configure `sudo`

Action:

Using your Enterprise process, install `sudo`.

Discussion:

`sudo` is a package that allows the System Administrator to delegate activities to groups of users. These activities are normally beyond the administrative capability of that user – restarting the web server, for example. If frequent web server configuration changes are taking place (or you have a bug and the web server keeps crashing), it becomes very cumbersome to continually engage the SysAdmin just to restart the web server. `sudo` allows the Administrator to delegate just that one task using root authority without allowing that group of users any other root capability.

Once `sudo` is installed, configure it using `visudo` – do not vi the config file. `visudo` has error checking built in. Experience has shown that if `sudoers` gets botched (from using `vi` without `visudo`'s error checking feature), recovery may become very difficult.

Note: The `visudo` command is located in `/usr/local/sbin`. For convenience, you may want to update root's profile `$PATH` with this new directory.

Note: The `sudo` command is located in `/usr/local/bin`. For convenience, you may want to update your global profile `$PATH` (`/etc/profile`, `/etc/environment`, `/etc/tsh_profile` – please follow your site's policies) with this new directory. To make the change take effect for all new users, update `/etc/security/.profile`, or ensure `/etc/security/.profile` includes the existing `$PATH` vice defining a new `$PATH`.

SN.4 Limit number of failed login attempts

Action:

```
chsec -f /etc/security/user -s default -a loginretries=3
```

Discussion:

A system policy of locking out an account that fails several successive authentication attempts is an industry best practice, and is easily implemented in this Benchmark. The above value (`loginretries=3`) will cause the account to be locked out after 3 successive failed login attempts. This value is chosen as it is a common value used in some Federally-regulated industries – you are free to increase it if desired.

Appendix C: Revision History

Version 1.01:

- Item 3.16: removed text from title of item
- Formatting and style changes
- Added revision history

References

The Center for Internet Security

Free benchmark documents and security tools for various OS platforms and applications:

http://www.cisecurity.org/

AIX Software

Patches and related documentation:

http://www.ibm.com/servers/eserver/support/pseries/aixfixes.html

http://techsupport.services.ibm.com/server/aix.efixmgmt/

ftp://aix.software.ibm.com/aix/efixes/security/

https://techsupport.services.ibm.com/server/pseries.subscriptionSvcs

AIX 5L Version 5.3 Security Guide

http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/aixbman/security/security.htm

Other Misc Documentation

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

OpenSSH (secure encrypted network logins):

http://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/

sudo (provides fine-grained access controls for superuser activity):

http://www.courtesan.com/sudo/

Tripwire – file modification utility

http://www.tripwire.org