Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

This practical makes the following assumptions:

- The server will be connected to an isolated private network for the hardening process before it is deployed to the production network. This private network is only accessible from one secure server that has two network interfaces. The interface connected to the isolated private network has IP address of 192.168.1.100. The interface that faces the building production network has IP address of 192.168.2.100. The secure server is only accessible using SSH.
- These instructions are applicable to the F series, G series and J series servers.
- A central application development team supplies any software packages that the system administrator needs to install in AIX installp format. If there is no development team, then the system administrator will need access to a system with a compiler to build the needed software packages.
- This server will be used as general user workstation.
- There will be no compilers installed on this system, so users will not be able to compile software on this system, but will be able to execute their own shell scripts and pre-compiled binaries loaded under their home directory.
- This server will not accept mail, but users will be able to send mail.

Install the AIX 4.3.3 Base Operating System (BOS)

___ If you have a team that performs server OS installations, request that they build a server with the AIX 4.3.3 Base Operating System (BOS) installed on it, perform a TCP/IP minimum configuration to assign an IP address to it, install the AIX 4.3 manual pages and connect the server to the isolated private network for your hardening process.

___ If you do not have a team that performs server OS installations, you will need to install the AIX 4.3.3 BOS, perform the TCP/IP minimum configuration to assign the IP address, install the manual pages, and connect the server to server to the isolated private network for the hardening process. You will need to have access to the AIX BOS installation CDs and the AIX 4.3 Documentations CDs. You will also need to obtain an IP address for the server from the group who assigns network addresses.

You will need to refer to the documentation for the type of server type that you are installing AIX 4.3.3 to determine how to perform the BOS installation from CD because there are different procedures for booting from the CD drive depending on the server type.

Once you have received the server with the AIX BOS installed on it from the server installation team or you have performed the AIX BOS installation on the new server, you may proceed with the section **Access new system for the first time**.

Access new system for the first time

© SANS Institute 2000 - 2005 Author retains full rights.

Telnet to the server using the IP address

- provided by the server installation team
  or
- provided by the networking group to you for your AIX BOS installation

- Login as **root** using the password supplied by the server installation team or the password you set when you installed the OS on the server.

Update system time zone variable

___ Verify that the time zone for the server is set to CUT by issuing the following command:

/usr/bin/grep TZ /etc/environment

___ If the time zone is set to **CUT**, you should receive the following response:

TZ=CUT

___ If the time zone variable is set to CUT, you can skip to **Modify default profiles and environment files**

___ If the time zone variable is not set to CUT, you will need to update the TZ variable by issuing the following command:

/usr/bin/chtz CUT

___ If you needed to update the time zone variable, you will need to reboot the server to ensure that all processes running on the system have the correct time zone associated with it. To reboot the server issue the following command:

/usr/sbin/shutdown –Fr now

___ If you had to reboot the server, you will need to wait for the server to come back up again and log back in as the **root** user before continuing with **System microcode and maintenance levels**.

System microcode and maintenance levels

From the time the AIX 4.3.3 CD was created until the time a server is built with the CD, IBM AIX support has discovered non-security and security related bugs with the operating system and related software. Additionally, from the time a device was created until the time the device is installed for use in a system, IBM has created microcode updates to resolve non-security and

© SANS Institute 2000 - 2005 Author retains full rights.

security related issues or to enhance device functionality.

You will need to determine what microcode level the system devices are at and what the maintenance level the operating system is at and upgrade the microcode and system software as appropriate.

IBM provides a website at URL http://techsupport.services.ibm.com/rs6000/support, which the system administrator can use to determine what microcode and software levels are installed on the system and download the appropriate updates to bring the system to a current level.

The following sections provide the steps needed to ensure that the device microcode and system maintenance levels are at the latest available level and all available security APARs are installed.

Ensure system device microcode is at latest level

IBM has a facility named Microcode Discovery Service that facilitates determining whether an RS/6000 system is at the latest microcode level. IBM provides a software package named Inventory Scout that is used to determine what the current microcode level is for all of the devices on a system. The following URL http://techsupport.services.ibm.com/rs6k/mds.html provides more information regarding the Microcode Discovery Service. There should be a link on this page that will take you to the Inventory Scout User's Guide. The following URL http://techsupport.services.ibm.com/rs6k/invscout/invreadme.html will bring you directly to the Inventory Scout User's Guide

There are two different methods for running Inventory Scout. The first method of running Inventory is by invoking Java applets and the second is by running from the command line. Since the server that is being hardened does not have Internet access, the Java applet method cannot be used. The instructions for running Inventory Scout from the command will need to be followed.

Follow the instructions provided on the Inventory Scout User's Guide page for downloading and installing the Inventory Scout software. After the Inventory Scout software has been installed, follow the instructions for running Inventory Scout from the command line. Once Inventory Scout has been run on the server, the upload file will need to be transferred to a system that has Internet access. Once this file has been transferred, follow the instructions for using the Microcode Discovery Service to upload the data file to create a report showing the microcode level for this system.

___ If there are any devices that show up in the report as needing the microcode level updated, you will need to follow the instructions in the README document that will be provided for each device identified as having back level microcode to download and install the microcode update.

© SANS Institute 2000 - 2005 Author retains full rights.

___ If there are no devices that need to have the microcode updated or you have completed updating the microcode, you may continue with the next section **Ensure AIX maintenance level is up to date**.

Ensure AIX maintenance level is up to date

The following link http://techsupport.services.ibm.com/rs6k/ml.fixes.html provides instructions on determining the full maintenance level of your system. Follow the instructions provided at this link to determine the full maintenance level for an AIX 4.3.3 system. If your system is at the latest maintenance level, you will not need to download the latest maintenance level fix package.

If your system is not at the latest maintenance level, follow the instructions provided on the site to download the latest maintenance level fix package for AIX 4.3.3. The site will also provide instructions on how to install the packages that you have downloaded.

___ Since the server that is being hardened does not have Internet access, you will first have to download the maintenance level fix package to a system that has Internet access. You will then need to get the fix package loaded onto the system you are hardening. Follow the instructions provided at the web site to install the maintenance level fix package to the system.

___ If the system is already at the latest maintenance level or you have completed installing the latest maintenance level fix package, you may continue with the next section **Ensure all AIX 4.3 security APARs are installed**.

Ensure all AIX 4.3 security APARs are installed

After the system is brought to the latest maintenance level, you will need to ensure that the latest AIX security updates are installed.

___ To determine what the latest available security PTFs are, send an email to **aixserv@austin.ibm.com** with a subject of **security_apars**. You will receive a return email with a listing of security related APARs for current releases of AIX. To facilitate the ordering of all security APARs for AIX 4.3, the email will also contain a packaging APAR number.

To download the security packaging APAR:

- you can use the URL http://techsupport.services.ibm.com/rs6k/fixdb.html to download the security APAR package.
- you can use an AIX system that has Internet access and has the **FixDist** package installed on it to download the security APAR package.
- if you do not have access to system that already has **FixDist** installed on it, you can install **FixDist** on an AIX system that has Internet access and use it to download the security APAR package.

© SANS Institute 2000 - 2005 Author retains full rights.

For information on general AIX software fixes, go to the following link: http://techsupport.services.ibm.com/rs6k/fixes.html.

For more information on **FixDist** read the FixDist User's Guide at URL http://service.boulder.ibm.com/aix/tools/fixdist/fixdist.html.

To download FixDist go to the following URL ftp://service.boulder.ibm.com/aix/tools/fixdist/.

___ Once you have downloaded the security APAR package to the Internet accessible server, you will need to get the fix package loaded onto the system you are hardening. Depending on how large the fix package is you may need to create a temporary file system to store it in. A suggested name for the directory or file system to store the package in is **/tmp/ptfs.**

___ Once you have put the fix package into **/tmp/ptfs** you can issue the following commands to install the fix package:

___ The following command will update the table of contents file **.toc** for the fixes in **/tmp/ptfs**.

/usr/bin/inutoc /tmp/ptfs

___ To start the fix installation process, issue the following command

/usr/bin/smitty update_all

___ For the field **INPUT device / directory for software** enter **/tmp/ptfs** and press the enter key. You will receive another screen with more options with values that you will not change. Press enter twice to start the installation.

___ Once the fixes have been installed, review the messages returned during the installation and resolve any problems that may have been indicated. Reboot the system if a reboot is indicated in the messages as being necessary for the changes to take effect.

___ If you had to reboot the server, you will need to wait for the server to come back up again and log back in as the **root** user before continuing with **Modify default profiles and environment files**.

Modify default profiles and environment files

Edit **/etc/security/.profile** to update the **PATH** statement. This is the profile that is installed when new userids are created on the system using the **mkuser** command with a shell other than **csh**.

© SANS Institute 2000 - 2005 Author retains full rights.

___ Make a backup copy of **/etc/security/.profile** using the following command:

**/usr/bin/cp –p /etc/security/.profile **
/etc/security/.profile.backup.`date +"%Y%m%d-%T"``

___ Modify the file using the following command:

/usr/bin/vi /etc/security/.profile

The default PATH as it comes from the default OS installation is as follows:

PATH=/usr/bin:/etc:/usr/sbin:/usr/ucb:$HOME/bin:/usr/bin/X11:/sbin:.

There is no reason why a regular user would need to run programs which are located in /etc, /usr/sbin, or /sbin. Unless all home directories are created with a bin directory, **$HOME/bin** should not be included in the default path statement.

One also should never have "." (period or dot) in the search path. This will be discussed below.

___ Replace the PATH statement in **/etc/security/.profile** with the following PATH statement:

PATH=/usr/local/bin:/usr/bin:/usr/ucb:/usr/bin/X11

___ Ensure that the **PATH** statement in **/.profile**, **/etc/profile** and **/etc/environment** do not contain the "**.**" (period or dot) in the search path.

An entry of a period (or dot) in the PATH means to search the current directory. This is not a good practice, especially for root. As an example, a malicious user could place a script named **ls** in a directory such as **/tmp** which looks like the following:

```
#!/bin/sh
/usr/bin/cp /bin/sh /tmp/.mystuff > /dev/null 2> /dev/null
/usr/bin/chown root /tmp/.mystuff > /dev/null 2> /dev/null
/usr/bin/chmod 4555 /tmp/.mystuff > /dev/null 2> /dev/null
/usr/bin/rm –f $0 > /dev/null 2> /dev/null
exec /usr/bin/ls "$@"
```

The above script is based on a shell script from a section that discusses path attacks in the book "Practical Unix Security" by Simson Garfinkel and Gene Spafford, (O'Reilly and Associates, Inc., 1991)

© SANS Institute 2000 - 2005 Author retains full rights.

What the above script does is to create a shell which runs setuid to root in /tmp with a "hidden" name. It will then delete itself and then execute the real **ls** program with the arguments given by the user.

Because the permission for the directory **/tmp** has the "sticky" bit turned on, only the owner of this file or the root user can delete a file in **/tmp**. If any other user executes this script the script will not be deleted.

If the root user has "dot" in the PATH before either /bin or /usr/bin, has changed the working directory to **/tmp**, and runs "ls", the ls script in /tmp will run instead of the real ls command in /usr/bin. The script will create a shell that is setuid to root, delete itself and then it will run the real **ls** command. There is now a setuid to root shell that the malicious user can use to compromise the system at a later date.

Because of this danger it is highly recommended that you do not rely on the PATH variable and always type the full pathname of commands when running as the root user. This way you always know exactly what program you are running. This is why all commands that are listed in this document are invoked using the full pathname.

Modify settings in /etc/security/user

___ Modify/ensure the following settings under the **default:** section of **/etc/security/user**.

___ Make a backup copy of **/etc/security/user** using the following command:

**/usr/bin/cp –p /etc/security/user **
/etc/security/user.backup.`date +"%Y%m%d-%T"``

___ Modify this file by issuing the following command:

/usr/bin/vi /etc/security/user

- **admin = false** (Defines the administrative status of the user)
- **umask = 077** (Sets the default umask for the user)
- **pwdwarntime = 14** (Number of days before a forced password change that a warning will be given to the user informing them of the impending password change)
- **loginretries = 5** (The number of invalid login attempts before is userid is locked out. The root user will need to reset the user's failed login count before the user will be able to login)
- **histexpire = 26** (Number of weeks that a user will not be able to reuse a password)

© SANS Institute 2000 - 2005 Author retains full rights.

- **histsize = 5** (Number of previous passwords which can not be reused)
- **minage = 2** (Minimum number of weeks between password changes)
- **maxage = 13** (Maximum number of weeks a password is valid)
- **minalpha = 1** (Minimum number of alphabetic characters)
- **minother = 2** (Minimum number of non-alphabetic characters)
- **mindiff = 3** (Minimum number of characters in the new password that were not in the old password)
- **minlen = 8** (Minimum length of a password
- **maxrepeats = 2** (Maximum number of times a given character can appear in a password)

___ Change the root password by issuing the following command:

/usr/bin/passwd root

___ Set the maximum password age for **root** to be 5 weeks (35 days):

/usr/bin/chuser maxage=5 root

___ Create the group **sysadmin** using the following command:

/usr/bin/mkgroup sysadmin

The above group will be used as the primary group when creating userids for system administrators on this server

___ Create the group **users** using the following command:

/usr/bin/mkgroup users

The above group will be the default primary and secondary group for new userids that are created on the server.

Updates to files controlling the creation of new userids

___ Update the **/usr/lib/security/mkuser.default** to set the default primary and secondary group to **users** when creating new userids with the **mkuser** command.

___ Create a backup copy of **/usr/lib/security/mkuser.default** using the following command:

**/usr/bin/cp –p /usr/lib/security/mkuser.default **
/usr/lib/security/mkuser.default.backup.`date +"%Y%m%d-%T"``

© SANS Institute 2000 - 2005 Author retains full rights.

___ Modify the file **/usr/lib/security/mkuser.default** using the following command:

/usr/bin/vi /usr/lib/security/mkuser.default

The file **/usr/lib/security/mkuser.default** has a **user:** section that is similar to the following:

```
user:
        pgrp = staff
        groups = staff
        shell = /usr/bin/ksh
        home = /home/$USER
```

___ Change the pgrp and groups lines to look like the following:

```
user:
        pgrp = users
        groups = users
        shell = /usr/bin/ksh
        home = /home/$USER
```

___ Update the file **/usr/lib/security/mkuser.sys** to ensure:

- the home directory of new userids created using the **mkuser** command has mode 0700.
- the user's **.profile** or **.login** has mode 0700

___ Create a backup copy of **/usr/lib/security/mkuser.sys** using the following command:

**/usr/bin/cp –p /usr/lib/security/mkuser.sys **
/usr/lib/security/mkuser.sys.backup.`date +"%Y%m%d-%T"`

___ Modify the file **/usr/lib/security/mkuser.sys** using the following command:

/usr/bin/vi /usr/lib/security/mkuser.sys

___ Locate the section where the user's home directory is created. It will look similar to the following:

```
#
# Create the named directory if it does not already exist
# and set the file ownership and permission
#
if [ ! -d $1 ]
then
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
        mkdir $1
        chgrp $3 $1
        chown $2 $1
fi
```

___ Add the following line after the **mkdir** command, which will ensure that the permission of the directory has the permission of 0700:

chmod 0700 $1

___ The section would then look like the following:

```
if [ ! -d $1 ]
then
        mkdir $1
        chmod 0700 $1
        chgrp $3 $1
        chown $2 $1
fi
```

___ Locate the section where the file **/etc/security/.profile** is copied to the newly created home directory. It will look similar to the following:

```
cp /etc/security/.profile $1/.profile
chmod u+rwx,go-w $1/.profile
chgrp $3 $1/.profile
chown $2 $1/.profile
```

___ Change the line **chmod u+rwx,go-w $1/.profile** to **chmod u+rwx,go= $1/.profile**

___ Locate the section where the file **/etc/security/.login** is created in the newly created home directory. It will contain something similar to the following:

```
chmod u+rwx,go-w $1/.login
chgrp $3 $1/.login
chown $2 $1/.login
```

___ Change the line **chmod u+rwx,go-w $1/.login** to **chmod u+rwx,go= $1/.login**

___ Locate the "set path" line and ensure that is does not include "dot" in the path setting. Here is what the "set path" line looks like in the stock **/etc/security/mkuser.sys**.

**echo "set path = (/usr/bin /etc /usr/sbin /usr/ucb \$HOME/bin /usr/bin/X11 /sbin . **

© SANS Institute 2000 - 2005 Author retains full rights.

)" >> "$1"/.login

___ The "dot" needs to be removed which will result in the following line:

**echo "set path = (/usr/bin /etc /usr/sbin /usr/ucb \$HOME/bin /usr/bin/X11 /sbin **
)" >> "$1"/.login

See the discussion about why "dot" should not be in the search path under the section "Modify default profiles and environment files"

Create a userid for the system administrator performing the hardening process

___ Create a userid for the system administrator using the following command:

**/usr/bin/mkuser <userid> pgrp=sysadmin groups=sysadmin **
gecos="<sysadmin's name>"

___ Set the password for the userid that was just created:

/usr/bin/passwd <userid>

For example:

**/usr/bin/mkuser joeadmin pgrp=sysadmin groups=sysadmin **
gecos="Joe Admin"

/usr/bin/passwd joeadmin

___ Logout of the server and log back into the server using the userid that was just created

___ Become the root user by issuing the following command:

/usr/bin/su - root

___ Modify the user characteristics for the root userid to disable both console logins and logins over the network by issuing the following command:

/usr/bin/chuser rlogin=false login=false root

This will ensure that the root userid cannot login to the server either at the console or over a network connection.

The only way to become the root user on the server with be to login as a normal user and then

© SANS Institute 2000 - 2005 Author retains full rights.

issuing the following command:

/usr/bin/su - root

Modify /etc/security/login.cfg

___ Make a backup copy of **/etc/security/login.cfg** using the following command:

**/usr/bin/cp –p /etc/security/login.cfg **
/etc/security/login.cfg.backup.`date +"%Y%m%d-%T"``

___ Modify **/etc/security/login.cfg** by issuing the following command:

/usr/bin/vi /etc/security/login.cfg

___ Configure the system herald. This is the prompt that the user will see when they attempt to login to the server. This is configured by modifying the **herald** line under the **default:** section. Update the herald to the following:

herald = "UNAUTHORIZED USE OF THIS SYSTEM IS PROHIBITED\n\nSystem access may be monitored\n\nlogin: "

___ Add **/bin/false** as a shell to the **shells** entry under the **usw:** section, which looks similar to the following:

usw:
shells =
/bin/sh,/bin/bsh,/bin/csh,/bin/ksh,/bin/tsh,/usr/bin/sh,/usr/bin/bsh,/usr/bin/csh,/usr/bin/ksh,/usr/bin/tsh,/usr/sbin/sliplogin

This is what the above would look like after adding **/bin/false**

usw:
shells =
/bin/sh,/bin/bsh,/bin/csh,/bin/ksh,/bin/tsh,/usr/bin/sh,/usr/bin/bsh,/usr/bin/csh,/usr/bin/ksh,/usr/bin/tsh,/usr/sbin/sliplogin,/bin/false

Update /etc/motd

___ Make a backup copy of **/etc/motd** using the following command:

/usr/bin/cp –p /etc/motd /etc/motd.backup.`date +"%Y%m%d-%T"``

© SANS Institute 2000 - 2005 Author retains full rights.

___ Modify **/etc/motd** to show the following information using the following command:

/usr/bin/vi /etc/motd

```
**************************************************************************
**
*
*
* XYZ's internal systems must only be used for conducting XYZ's business or
*
* for purposes authorized by XYZ management. Use is subject to audit or
*
* monitoring at any time by XYZ management.
*
*
*
**************************************************************************
**
```

Update system limits

___ Make a backup copy of **/etc/security/limits** using the following command:

**/usr/bin/cp –p /etc/security/limits **
/etc/security/limits.backup.`date +"%Y%m%d-%T"``

___ Modify **/etc/security/limits** using the following command:

/usr/bin/vi /etc/security/limits

___ Update the **default:** section to include the following line:

core_hard = 0

The above entry will disallow the writing of core files on the system. Only the root user can increase a hard limit. By setting the hard limit to the value zero, normal users cannot increase the hard limit and thus cannot enable the writing of core files on the system.

Core files, which are named **core**, usually contain a complete image of the memory that was allocated to the program at the time of its crash. Running the **strings** command against the core file, **/usr/bin/strings core**, can reveal interesting information. Depending on when a program core dumps, it is possible that there could be sensitive information in the core file, which can be examined with the **strings** command.

Core files are generally world-readable which is why it is a good idea to restrict its creation on

© SANS Institute 2000 - 2005 Author retains full rights.

non-development systems since there is normally no reason why normal users would have a need to examine a core file for a process that dumps.

Another reason why you may want to restrict the creation of core files or limit core file sizes is that core files can be very large. If your system is tight on disk space, a core dump could be used to cause a denial of service.

Configure xntp daemon

___ Create **/etc/ntp.conf** using the following commands:

echo "driftfile /etc/ntp.drift" > /etc/ntp.conf
echo "server timeserver1.mycom.com" >> /etc/ntp.conf
echo "server timeserver2.mycom.com" >> /etc/ntp.conf
echo "server timeserver3.mycom.com" >> /etc/ntp.conf

___ Update **/etc/rc.tcpip** to start the xntpd daemon at boot time.

___ Make a backup copy of **/etc/rc.tcpip** using the following command:

/usr/bin/cp –p /etc/rc.tcpip /etc/rc.tcpip.backup.`date +"%Y%m%d-%T"``

___ Modify **/etc/rc.tcpip** using the following command:

/usr/bin/vi /etc/rc.tcpip

___ Search for the following lines and uncomment the line which starts the daemon
 # Start up Network Time Protocol (NTP) daemon
#start /usr/sbin/xntpd "$src_running"

Update /etc/inittab and /etc/rc.tcpip files

___ Issue the following commands to prevent unneeded and forbidden services from being starting at system boot time from **/etc/inittab**:

/usr/sbin/rmitab piobe	Print job manager for the printer backend
/usr/sbin/rmitab qdaemon	Schedules printing jobs enqueued by the enq command
/usr/sbin/rmitab writesrv	Allows users to send messages to and receive messages from a remote system
/usr/sbin/rmitab pmd	power management
/usr/sbin/rmitab rcnfs	NFS subsystems

© SANS Institute 2000 - 2005 Author retains full rights.

/usr/dt/bin/dtconfig '-d'	Sets the default user interface to command line and removes the call to /etc/rc.dt from /etc/inittab

___ Modify **/etc/rc.tcpip** using the following command:

/usr/bin/vi /etc/rc.tcpip

___ Remove all lines that start daemons that are commented out. This will make it easier to determine if any authorized updates have been made to the file. Here is an example of lines that should be commented out:

 # Start up the DHCP Server
#start /usr/sbin/dhcpsd "$src_running"

___ Ensure that you have removed the following lines relating to the portmapper daemon since we do not allow portmapper to be run on the server.

 # Start up Portmapper
#start /usr/sbin/portmap "$src_running"

___ Remove the section of lines which is related to the starting of sendmail and add the following line to the end of the file

 # Start sendmail, but not bound to port 25 (flushes mail queue only)
/usr/lib/sendmail -q15m

___ Update the line where the syslog daemon gets started:

start /usr/sbin/syslogd "$src_running"

to include the "-r" parameter which tells syslogd not to log messages from remote systems. The line should look like the following:

start /usr/sbin/syslogd "$src_running" -r

Configure syslog daemon

By default the syslog daemon is not configured to log anything even though the daemon gets started automatically at boot time.

___ Modify **/etc/syslog.conf** using the following command:

© SANS Institute 2000 - 2005 Author retains full rights.

/usr/bin/vi /etc/syslog.conf

___ Add the following two lines to the end of the file

***.debug /var/adm/messages**
auth,mark.info /var/adm/authlog

___ Issue the following command to create the log files:

/usr/bin/touch /var/adm/messages
/usr/bin/touch /var/adm/authlog

___ Issue the following commands to set the file permission for the log files so that only the root user can read them:

/usr/bin/chmod 600 /var/adm/messages
/usr/bin/chmod 600 /var/adm/authlog

___ Get syslogd to re-read **/etc/syslog.conf** by issuing the following command so that it starts logging to the files we just created:

/usr/bin/refresh –s syslogd

Create /etc/ftpusers file

The **/etc/ftpusers** file contains a list of the users who are not allowed to use FTP to access any files.

Even though we will not allow inbound ftp access to this server we will still create and populate the **/etc/ftpusers** file. We do this so that if ftp access to this server is accidentally enabled or if ftp access is requested in the future, this server will already have a list of userids to deny ftp access to.

___ The following userids must be added to **/etc/ftpusers**:

root
daemon
bin
sys
adm
uucp
nuucp

© SANS Institute 2000 - 2005 Author retains full rights.

lpd
guest
nobody
operator
system
boot
gateway
sccs
notes
news
sendmail

Cleanup /etc/inetd.conf

/etc/inetd.conf will be modified to only have the telnet service active. All lines that are commented out and all lines for other services will be removed from the file. The **inetd.conf** file should only consist of a single line. This will make it easy to notice if any new services are added to **inetd.conf**.

___ Make a backup copy of **/etc/inetd.conf** using the following command:

/usr/bin/cp –p /etc/inetd.conf /etc/inetd.conf.backup.`date +"%Y%m%d-%T"``

___ Modify **/etc/inetd.conf** using the following command:

/usr/bin/vi /etc/inetd.conf

___ Remove all lines from the file except for the line that defines the telnet service. This is a line that starts with the string "telnet stream".

___ Get the **inetd** daemon to re-read the **inetd.conf** file by issuing the following command:

/usr/bin/refresh –s inetd

This will ensure that the only service that the **inetd** daemon will be listening for is the telnet service.

Userid maintenance

Remove the userid **guest** from the system along with its home directory.

___ First determine the home directory of the userid guest using the following command:

© SANS Institute 2000 - 2005 Author retains full rights.

/usr/sbin/lsuser –a home guest

___ The home directory should be **/home/guest**. If the home directory is not **/home/guest**, replace /home/guest with the home directory returned by the previous command. Remove the home directory of guest using the following command:

/usr/bin/rm –r /home/guest

___ Now remove the userid **guest** from the system using the following command:

/usr/sbin/rmuser –p guest

The following userids: **uucp, nuucp, lpd, daemon, bin, sys, adm, and nobody,** need to have their shell set to **/bin/false**. Setting the shell for these userids to **/bin/false** effectively disables the use of these userids for running processes on the on the system.

___ Issue the following commands to set the shell for these userids:

/usr/sbin/chuser shell=/bin/false uucp
/usr/sbin/chuser shell=/bin/false nuucp
/usr/sbin/chuser shell=/bin/false lpd
/usr/sbin/chuser shell=/bin/false daemon
/usr/sbin/chuser shell=/bin/false bin
/usr/sbin/chuser shell=/bin/false sys
/usr/sbin/chuser shell=/bin/false adm
/usr/sbin/chuser shell=/bin/false nobody

Remove empty and unneeded crontab files

___ Remove the crontab files for userids sys, adm and uucp using the following commands:

/usr/bin/rm /var/spool/cron/crontabs/sys
/usr/bin/rm /var/spool/cron/crontabs/adm
/usr/bin/rm /var/spool/cron/crontabs/uucp

Install the tcpwrapper and ssh packages

___ Obtain the latest AIX installp images for the tcpwrapper and ssh software packages from the internal software development group.

___ Create the directory **/tmp/install** and download the tcpwrapper and ssh installation

© SANS Institute 2000 - 2005 Author retains full rights.

images into this directory

___ Install these packages by issuing the following command:

/usr/bin/smitty install_latest

For the "INPUT device / directory for software", enter the name of directory where you downloaded the packages into, which would be **/tmp/install** and then press the enter key. The screen will update to list a number of installation parameters, which you can leave with the defaults. To install the software, press the enter key again.

If the software installed without any problems, you should see "Command: OK" in the upper left hand corner of the screen, otherwise you will see "Command: Failed". If the installation failed, you will need to review the messages to determine what caused the problem so that you can fix it and re-run the installation.

Configure tcpwrapper

Set the default action of tcpwrapper to deny all connections.

___ Create the file **/etc/hosts.deny** with the following command:

/usr/bin/echo "ALL : ALL" > /etc/hosts.deny

Configure tcpwrapper to:

- allow system with IP 192.168.1.100 telnet access
- allow system with IP 192.168.1.100 ssh access
- allow systems in IP range 192.168.128.0 through 192.168.131.255 ssh access

The first two bullet items will allow the secure server on the private network with IP address 192.168.100 either telnet or ssh access. Once the server is deployed on the production network, the two entries allowing access to the server with IP 192.168.1.100 will need to be removed.

The last bullet item will allow systems in that IP range access via ssh.

___ Issue the following commands to create the **/etc/hosts.allow** file:

/usr/bin/echo "telnet: 192.168.1.100" > /etc/hosts.allow
/usr/bin/echo "ssh: 192.168.1.100" >> /etc/hosts.allow
/usr/bin/echo "ssh: 192.168.128.0/255.255.252.0" >> /etc/hosts.allow

___ Issue the following command to set the file permission for the **hosts.allow** and

© SANS Institute 2000 - 2005 Author retains full rights.

hosts.deny files:

/usr/bin/chmod 0600 /etc/hosts.allow /etc/hosts.deny

___ Modify the telnet service to use tcpwrappers. Edit the file **/etc/inetd.conf** using the following command:

/usr/bin/vi /etc/inetd.conf

The line in **/etc/inetd.conf** will look like the following:

telnet stream tcp nowait root /usr/sbin/telnetd -a

and will need to be modified to look like the following:

telnet stream tcp nowait root /usr/local/sbin/tcpwrapper /usr/sbin/telnetd -a

Configure ssh2

___ Generate the host key pair by issuing the following command:

/usr/local/bin/ssh-keygen2 –P /etc/ssh2/hostkey

___ Modify **/etc/sshd2_config** using the following command:

/usr/bin/vi /etc/ssh2/sshd2_config

/etc/sshd2_config should look like the following:

Port	**22**
ListenAddress	**0.0.0.0**
Ciphers	**AnyStd**
HostKeyFile	**hostkey**
PublicHostKeyFile	**hostkey.pub**
RandomSeedFile	**random_seed**
ForwardAgent	**yes**
ForwardX11	**yes**
PasswordAuthentication	**yes**
RhostsAuthentication	**no**
RHostsPubKeyAuthentication	**no**
PubKeyAuthentication	**yes**
VerboseMode	**no**

© SANS Institute 2000 - 2005 Author retains full rights.

QuietMode	**no**
KeepAlive	**yes**
IgnoreRhosts	**yes**
PermitRootLogin	**no**
PermitEmptyPasswords	**no**
StrictModes	**yes**
PrintMotd	**yes**
PasswordGuesses	**5**
Sshd1Path	**/usr/local/sbin/sshd1**
SyslogFacility	**AUTH**

Verify all files have an owner and group

___ Issue the following command to find files that belong to a user not listed in **/etc/passwd**:

/usr/bin/find / -nouser

___ If there are files that have no owner, issue the following command to save a listing of these files:

/usr/bin/find / -nouser > /tmp/files-without-owner.txt

___ After you have saved the listing of the files that have no owner, issue the following command to change the owner of these files to the userid **root**.

/usr/bin/find / -nouser –exec chown root \{\} \;

___ Issue the following command to find files that belong to a group not listed in **/etc/group:**

/usr/bin/find / -nogroup

___ If there are files that have no group, issue the following command to save a listing of these files:

/usr/bin/find / -nogroup > /tmp/files-without-group.txt

___ After you have saved the listing of the files that have no owner, issue the following command to change the owner of these files to the group **sys**.

/usr/bin/find / -nogroup –exec chgrp sys \{\} \;

© SANS Institute 2000 - 2005 Author retains full rights.

___ Transfer the two files to the main administrative system so that you can work with the development and installation teams to determine why these files do not have a valid owner or group associated with them and to determine the correct owner or group to associate with the file.

Setup log rotation

___ Create the script **/usr/local/bin/rotate-log.ksh** by typing the following:

```
cat > /usr/local/bin/rotate-log.ksh << EOF
#!/bin/ksh

if [[ \$1 = "" ]]; then
  echo "Usage: \$0 <log file to rotate>"
  exit -1
fi

DATE=\`date +"%Y%m%d-%T"\`
LOGFILE=\$1
ROLLED_LOG=\$LOGFILE.\$DATE

if [[ ! -f \$LOGFILE ]];  then
  echo "File \$LOGFILE: does not exist"
  exit 9999
else
  /usr/bin/mv \$LOGFILE \$fROLLED_LOG
  /usr/bin/chmod 0600 \$ROLLED_LOG
  /usr/bin/compress –f $ROLLED_LOG
fi
EOF
```

___ Create the script **/usr/local/bin/rotate-syslog.ksh** by typing the following:

```
cat > /usr/local/bin/rotate-syslog.ksh << EOF
#!/bin/ksh

if [[ \$1 = "" ]]; then
  echo "Usage: \$0 <syslog file to rotate>"
  exit -1
fi

DATE=\`date +"%Y%m%d-%T"\`
SYSLOGFILE=\$1
ROLLED_SYSLOG=\$SYSLOGFILE.\$DATE
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
if [[ ! -f \$SYSLOGFILE ]];  then
  echo "File \$SYSLOGFILE: does not exist"
  exit 9999
else
  /usr/bin/mv \$SYSLOGFILE \$ROLLED_SYSLOG
  /usr/bin/chmod 0600 \$ROLLED_SYSLOG
  /usr/bin/refresh -s syslogd
  /usr/bin/compress –f \$ROLLED_SYSLOG
fi
EOF
```

___ Set the owner, group and permission of these two scripts using the following commands:

```
/usr/bin/chown root.system /usr/local/bin/rotate-syslog.ksh
/usr/bin/chown root.system /usr/local/bin/rotate-log.ksh
/usr/bin/chmod 0700 /usr/local/bin/rotate-syslog.ksh
/usr/bin/chmod 0700 /usr/local/bin/rotate-log.ksh
```

___ Modify the root crontab to implement log rotation for the following files:

```
/var/adm/messages
/var/adm/authlog
/var/adm/wtmp
/var/adm/sulog
/etc/security/failedlogin
```

___ Modify the crontab file by issuing the following command:

```
/usr/bin/crontab -e
```

___ The following crontab entries must be added to the end of the root crontab:

```
# Rotate the following log files daily at midnight box time
0 0 * * * /usr/local/bin/rotate-syslog.ksh /var/adm/messages
0 0 * * * /usr/local/bin/rotate-syslog.ksh /var/adm/authlog
0 0 * * * /usr/local/bin/rotate-log.ksh /var/adm/wtmp
0 0 * * * /usr/local/bin/rotate-log.ksh /var/adm/sulog
0 0 * * * /usr/local/bin/rotate-log.ksh /etc/security/failedlogin
```

___ The following crontab entries for maintaining the archived logs must be added to the end of the root crontab:

© SANS Institute 2000 - 2005 Author retains full rights.

```
# keep only 14 days worth of these log files
0 0 * * * /usr/bin/find /var/adm –name “messages.*.Z” –mtime 14 –exec /bin/rm \{\} \;
0 0 * * * /usr/bin/find /var/adm –name “authlog.*.Z” –mtime 14 –exec /bin/rm \{\} \;
0 0 * * * /usr/bin/find /var/adm –name “wtmp.*.Z” –mtime 14 –exec /bin/rm \{\} \;
0 0 * * * /usr/bin/find /var/adm –name “sulog.*.Z” –mtime 14 –exec /bin/rm \{\} \;
0 0 * * * /usr/bin/find /etc/security –name “failedlogin.*.Z” –mtime 14 –exec /bin/rm \{\} \;
```

Backup the system before releasing it into production

Now that the system has been hardened, a backup image needs to be taken. Two backup tapes will be taken, one to be kept on-site and the other will be stored off-site.

___ Contact the server installation team to ensure that a tape drive is attached to the system and that a blank tape is inserted in the drive.

___ Create the offsite backup tape by issuing the following command:

/usr/bin/mksysb ‘-i’ ‘-X’ /dev/rmt0 > /tmp/offsite-tape.txt 2>&1

___ Once the **mksysb** command is completed, review the messages in the file **/tmp/offsite-tape.txt** and ensure that there were no errors. If no errors were logged, have the server installation team remove the tape and label it with the words “OFF SITE BACKUP, the server hostname, current date, and time. Verify that they place the tape in the bin for the tapes that are going off site.

___ Create the onsite backup tape by issuing the following command:

/usr/bin/mksysb ‘-i’ ‘-X’ /dev/rmt0 > /tmp/onsite-tape.txt 2>&1

___ Once the **mksysb** command is completed, review the messages in the file **/tmp/onsite-tape.txt** and ensure that there were no errors. If no errors were logged, have the server installation team remove the tape and label it with the words “ON SITE BACKUP, the server hostname, current date, and time. Verify that they log the tape into the tape library.

___ The server is now ready for production deployment. The /etc/hosts.allow file needs to be modified to remove the two lines which allow the secure server at IP address 192.168.1.100 access.

___ Contact the production support team to arrange moving the server to the production network. If you do not have a production support team, you will need to put this server onto the production network yourself.

© SANS Institute 2000 - 2005 Author retains full rights.

In either case:

- The server needs to be placed into a physically secure, locked room, with controlled access.
    - Ideally access to the room should be by electronic badge access that logs the accesses to the room. There should be a logbook for personnel who do not have regular access to the room to sign in and out.
- If the room has either drop ceilings or raised floors, verify that they do not allow access from adjoining rooms that are not part of this secure space.
- Ideally the room should be "hardened": redundant climate control systems, UPS systems for all computer systems, electric generator for providing power should the outage last longer than the capacity of the UPS batteries.
    - Minimally the room should be air-conditioned and each server is connected to a UPS.
- The system case should be locked to deter tampering with the internal components.
- The system should be physically secured with a cable or secured within a rack or locked cage.
- Follow your site's change control process, if applicable, to connect the server to the production network.

Steps to take once the system is in production to ensure security stays current

Once the system is in production, the attention paid to the security of the server cannot be reduced. As time goes by the system can become vulnerable due to security vulnerabilities being found in software packages that were once considered secure.

Here are several things that you must do to stay informed about system and security vulnerabilities for AIX

- Establish a regular schedule to review any new server or security fixes which have been released since the last system update. It is suggested that the review/update interval be no longer than once every three months.
- Use the Inventory Scout tool that was referenced in the section **Ensure system device microcode is at latest level** to keep the microcode on the system current.
- Use the URL http://techsupport.services.ibm.com/rs6k/ml.fixes.html that was referenced in the section **Ensure AIX maintenance level is up to date** to help keep the maintenance level of the system current.
- Subscribe to the following files from the AIX Service Mail Server
    - **Security_APARs** AIX security related updates
    - **Security** AIX related security alerts for current year
    - **New_AIXV4_Fixes** New AIX version 4 updates - updated weekly

© SANS Institute 2000 - 2005 Author retains full rights.

To subscribe to these files, send an email to **aixserv@austin.ibm.com** with a subject starting with the word **subscribe** followed by one or more file names separated by spaces.

To get a help file, leave the subject line blank. You will receive a return email that will contain a list of files that you can request or subscribe to along with instructions on how to request or subscribe/unsubscribe to the files.

- IBM's RS/6000 Support web site at URL http://techsupport.services.ibm.com/rs6000/support provides very good resources for keeping a server current on maintenance in addition to providing references for administering an AIX system.
- Subscribe to the CERT Advisory Mailing list by sending an email to majordomo@cert.org. In the body of the message type **subscribe cert-advisory**

  You can get very good security information from the CERT web site http://www.cert.org/
- Any vulnerabilities that you are alerted to which are considered a HIGH risk should be acted upon immediately. Take the appropriate cautions such as testing the fix on a test system, if one is available, prior to installing it on your production system.
- The SecurityFocus web site at URL http://www.securityfocus.com/ hosts a number of security related mailing lists. One suggested mailing list to subscribe to is **BugTraq**.

References

IBM RS/6000 Documentation Library, AIX 4.3 Installation Guide
http://www.rs6000.ibm.com/doc_link/en_US/a_doc_lib/aixgen/topnav/topnav.htm

Garfinkel, Simson and Spafford, Gene, Practical Unix Security, (O'Reilly and Associates, Inc., 1991)

Pomeranz, Hal, Solaris, Security Step by Step, Version 2.0, (The SANS Institute, 2001)

Bishop, Dr. Matt, UNIX Security Tools and Their Uses, (From SANS 2001, The SANS Institute, 2001)

MacFarlan, Allison, "Securing" an AIX (DNS) host, (http://www.sans.org/y2k/practical/Allison_MacFarlan_GCUX.doc)

F-Secure SSH Client & Server for Unix, (http://www.f-secure.com/download-purchase/manuals/docs/manual/12000006/enu/ssh.pdf)

© SANS Institute 2000 - 2005 Author retains full rights.