Global Information Assurance Certification Paper

AIX 4.3 Bastion Host Guidelines.

SANS Security Essentials GSEC Practical Assignment Version 1.2e

By : Nishchal Bhalla

Date : June 05, 2001

Table of Contents

The purpose of this document is to create a Bastion Host configuration for AIX version 4.3.

A Bastion Host is a server that is configured such that the Operating System (OS) is hardened for security. This type of configuration is used on Firewalls, Web Servers, FTP Servers, Mail Servers or any server that is put in direct connection with an outside network, such as the Internet.

Before implementing this document it is recommended that the changes be tested. Any changes must be made in compliance with the written corporate policy.

Installation

Insert CD in CD-ROM drive and power on the system after the POST (Power on Self Test) is completed, the machine searches for the bootable image and the menus (installation and maintenance menu) appear on the screen.

Trusted Computing Base Check

At the installation and maintenance menu, select the "Change/show installation settings and install option". At this option, select "Install Trusted Computing Base" and enable this option.

When TCB is installed, the trusted path, the trusted shell and system integrity checking are installed. Trusted path tries to ensure that the programs that you run are trusted programs.

The tcbck command audits the security state of the system by checking the installation of the files defined in the /etc/security/sysck.cfg file (the sysck database). Each file definition in the /etc/security/sysck.cfg file can include one or more attributes that describe proper installation.

Note:

- *During the POST (Power on Self Test), using the F5 key on the keyboard invokes the boot list. Modifications as to the list of devices once full install is completed should contain only the drive with the bootable image.*
- *The TCB check option can be enabled at install time only.*

Post Installation

After installing AIX, the operating system will run with default settings and brings up the Configuration Assistant. Configuration assistant helps configure basic settings (date & time, password, TCP/IP etc).

FixDist (tool for web download of fixes) and updates are available to download from IBM's site *http://service.software.ibm.com/aix.us/aixfixes*. Make sure all security patches have been applied. Obtain patch listing from *http://www.ers.ibm.com/tech-info/advisories/sva/index.html* to check if patches have been applied issue instfix -ik apar.

Reboot machine.

Note:

- *If the configuration assistant/installation assistant needs to be brought up again the install_assist (ASCII terminal) or configassist(CDE) can be used.*

Uninstalling Software

AIX, by default installs a few packages that are not required on a bastion host. Uninstall software like X11, http lite, all man pages etc. helps reduce the potential vulnerabilities on the system.

The following software and its dependent software should be de-installed (use smitty /software installation and maintenance/ Software Maintenance and Utilities/ Remove Installed Software).

PREVIEW only? (remove operation will NOT occur) no
REMOVE dependent software? yes
EXTEND file systems if space needed? no
DETAILED output? no

IMNSearch.rte.httpdlite
ifor_ls.base.cli
ifor_ls.client.base
ifor_ls.client.gui
ifor_ls.msg.en_US.base.cli
perl.rte
printers.rte
xlC.aix43.rte
xlC.cpp
xlC.msg.en_US.cpp
xlC.msg.en_US.rte
xlC.rte
IMNSearch.rte.httpdlite
ifor_ls.base.cli
ifor_ls.client.base
printers.rte
bos.docregister.com
bos.docsearch.client.com
bos.docsearch.rte
bos.help.msg.en_US.com
bos.help.msg.en_US.smit
bos.html.en_US.topnav.navigate
man
X11

Reboot machine.

File Permissions

The next step is to remove unnecessary permissions on files. The find command is used to search for setuid files, setgid files, world writeable files, world writeable directories, group writable files, group writable directories, files not owned by any user and files not belonging to any group.

```
find / -perm -4000 -type f -exec ls -l {} \; >setuid.list
find / -perm -2000 -type f -exec ls -l {} \; > setgid.list
find / -perm -0002 -type f -exec ls -l {} \; > worldwrite.file.list
find / -perm -0002 -exec ls -ld {} \; | grep drwxrwx > worldwrite.dir.list
find / -perm -0020 -type f -exec ls -l {} \; > groupwritefile.list
find / -perm -0020 -exec ls -ld {} \; | grep drwxrwx >groupwrite.dir.list
find / -nouser -type f -exec ls -l {} \; >nouser.list
find / -nogroup -type f -exec ls -l {} \;>nogroup.list
```

The result of each find is output in the "search type" dot list.

Setuid and Setgid files

- The files that need to be **setuid** are:
  /usr/bin/passwd
  /usr/bin/ps
  /usr/bin/su
  /usr/bin/uptime
  /usr/bin/w

- The only files that need to be **setgid** are :
  /usr/bin/mailx
  /usr/bin/mail

Using the setuid.list and setgid.list remove permissions on all the other remaining files.

Note :

- *Review to see if any other files that are used by any of your programs need to be setuid or setgid, if so, make sure you don't change permissions on them too.*

World writable files and directories

The only files that could be world writable are files inside the /proc and /tmp directories. Including the directories themselves. The /tmp and /var/tmp directories should both have the sticky bit set.

Group writable files and directories

Group writable files, the /etc /bin /sbin and /usr directories do not require group write permissions. Review to see if you need any additional files and directories to be group writable.

Nouser and Nogroup files

Hopefully the results of this should be empty, if not, it is imperative that you review each individual file and assign a user & group to it. If you are uncertain of which group and user it should belong to, change the permissions to nobody. Ensure you write down what permissions, user name and group you have assigned. If any of your programs break, you might have to tweak with these files.

Reboot machine.

Key File Modifications

Inittab Modification (/etc/inittab)

Modify /etc/initab file to remove daemons (rcnfs, piobe, qdaemon, writesrv and uprintfd) not required from inittab file.

```
#cp /etc/inittab /etc/inittab.orig
# chmod 000 /etc/inittab.orig
#for e in rcnfs piobe qdaemon writesrv uprintfd
>do rmitab $e
>done
```

Reboot machine.

TCP/IP Modification (/etc/rc.tcpip)

Modify rc.tcpip file to start only required daemons (syslogd & inetd).

```
# cp /etc/rc.tcpip /etc/rc.tcpip.orig
# chmod 000 /etc/rc.tcpip.orig
# sed -e 's/^start /#start/' rc.tcpip.orig >rc.tcpip
# cat >>rc.tcpip
start /usr/sbin/syslogd "$src_running"
start /usr/sbin/inetd "$src_running"
CTRL-D
```

Note

- *View /etc/rc.tcpip file and ensure that "start ()" (line #43) is not commented, if it is, uncomment it, the tcpip services will not start if the start() is commented out.*

Reboot machine.

Inetd.conf Modification (/etc/inetd.conf)

Modify inetd.conf file to start only required daemons (ftp & telnet).

```
#cp ientd.conf inetd.conf.orig
#chmod 000 /etc/inetd.conf.orig
# egrep "/ftp|/telnet" inetd.conf.orig >/etc/inetd.conf
```

Note :

It is always better to run Secure shell downloadable from ftp://ftp.ssh.com/pub/ssh.

Reboot machine.

netstat –an (displays ports the machine is listening on and active connections.)

User Modifications

Expire / Delete users

```
# for u in uucp guest lpd imnadm ; do rmuser -p $u; done
# for g in uucp printq; do rmgroup $g ; done
```

Checking integrity of Users / Group and Passwords

Ensure all IDs have a shell, if an ID doesn't assign /bin/false to it. Ensure only ROOT has a uid of 0.

```
# usrck -y ALL
3001-664 The account for user daemon has expired.
3001-664 The account for user bin has expired.
3001-664 The account for user sys has expired.
3001-664 The account for user nobody has expired.
3001-664 The account for user imnadm has expired.
# grpck -y ALL
# pwdck -y ALL
```

Network Tuning Parameters

Create and append rc.local.net records in the /etc/inittab file so that the changes are automatically made.

```
#cat >>/etc/rc.local.net
/usr/sbin/no -o clean_partial_conns=1
/usr/sbin/no -o ipsendredirects=0
/usr/sbin/no -o nonlocsrcroute=0
/usr/sbin/no -o bcastping=0
/usr/sbin/no -o tcp_mssdflt=1370
/usr/sbin/no -o icmpaddressmask=0
/usr/sbin/no -o udp_pmtu_discover=0
/usr/sbin/no -o tcp_pmtu_discover=0
/usr/sbin/no -o directed_broadcast=0
/usr/sbin/no -o ipignoreredirects=0
/usr/sbin/no -o ipsrcroutesend=0
/usr/sbin/no -o ipsrcrouterecv=0
/usr/sbin/no -o ipsrcrouteforward=0
/usr/sbin/no -o ip6srcrouteforward=0
CTRL-D

#chmod 700 /etc/rc.local.net
#mkitab "rclocalnet:2:once:/etc/rc.local.net >/dev/console 2>&1"
```

Reboot machine.

Login configuration

Modify /etc/security/login.cfg to display warning message.

add the following lines:
herald ="**********\n\t\t\t\B\bWARNING NOTICE\n\t\tYOU ARE CONNECTED TO A PRIVATE N
ETWORK.\n\t\tCONNECTION TO THIS NETWORK IMPLIES CONSENT\n\t\tTO BE MONITORED AND
RECORDED VIA THE NETWORK.\n\t\tUNAUTHORIZED USE OF THIS NETWORK OR THE DATA \n\
t\tSTORED HEREIN IS PROHIBITED AND PUNISHABLE BY LAW.\n\n**********
**********\n\n\n\nLogin:"

Enable Sak

Sak_enabled=true (enable secure attention key (Ctrl+X/Ctrl+R) on login ports to prevent Trojan Horse attack).

Modify /etc/security/user

Modify /etc/security/user file to display as shown below to change a few default settings like umask, dictionary list etc.

```
admin = false
login = true
su = true
daemon = true
rlogin = true
sugroups = ALL
admgroups =
ttys = ALL
auth1 = SYSTEM
auth2 = NONE
tpath = nosak
umask = 072
expires = 0
SYSTEM = "compat"
logintimes =
pwdwarntime = 5
account_locked = false
loginretries = 5
histexpire = 0
histsize = 3
minage = 0
maxage = 4
maxexpired = -1
minalpha = 2
minother = 1
minlen = 8
mindiff = 2
```

```
maxrepeats = 3
dictionlist =/usr/share/dict/words
pwdchecks =
```

Reboot machine.

Note:

- *Once every month a password cracker utility against the password file should be run. Ensure you have written permission to run a cracker program before doing so.*

Other Changes

Auto Restart

#Chdev –lsys0 –aautorestart=false
(Don't restart after crash). This should be changed as per the corporate policy.

Core File Size

#Chuser core=0 root (make core size that can be written to zero).

PATH

set | grep PATH
#vi /.profile and remove trailing periods
(Ensure there are no trailing periods in the path statement, if there are remove them. Ensure the path directory are not group and world writable.)

Reboot machine.

Crontab

#chmod 000 /var/spool/cron/crontabs/<ID> eg. lp sys adm
#rm /usr/lib/cron/cron.deny

#cat >>/usr/lib/cron/cron.allow
root
CTRL-D
Edit /var/spool/cron/crontabs/root and remove unnecessary entries. Review the crontab entries and remove unnecessary entries.

#cat >>/usr/lib/cron/cron.deny
lp
adm
daemon
bin
sys
nobody.

Imnadm

CTRL-D
Add any additional users that should not be allowed to have cron access except root.

Ensure all jobs run via ROOT's crontab are owned and only writable by ROOT Edit /etc/default/cron and add CRONLOG=yes

Disable login for root (/etc/security/user

Disable login for root, so administrators must su to root. Add to the root's stanza in /etc/security/user:
login=false #if you do not want root to login at the console
rlogin=false #if you do not want root to login remotely on the console.
ttys= tty0 #for root.

Root Logon

Ensure Root can login via the Console.

Smitty/Change / Show Characteristics of a User - select root ID To change
User can login remotely? --> false

Timeout

TheTMOUT andTIMEOUT environment variables should be set in the /etc/profile. Add the following

TMOUT=600 ; TIMEOUT=600 ; export readonly TMOUT TIMEOUT

Reboot machine.

Log Files

#/usr/lib/errdemon –s4194304 –B32768
(Increase error log buffers and log file size to provide a larger audit trail).

Regularly monitor the following logs for evidence of breaches or attempted breaches:

/var/adm/sulog

This file logs the use of the su command. It identifies the account that initiated the command, the account that was the target of the command, whether the command was successful or not, and the time and date when the command was run.

/var/adm/wtmp

This file stores information about current and previous system logins and logouts. You access this file with the last command.

/etc/security/failedlogin

This file captures all failed login attempts. You can access the information in this file by running: who /etc/security/failedlogin | more

/etc/utmp
This file stores information about the users who are currently logged in to the system. You can access the information in this file by running the who command.

Additional Software

Additional software like ssh (A client-server application that allows secure login or secure execution of commands on a remote computer. ftp://ftp.ssh.com/pub/ssh/.).

TCP Wrapper (It protects the inetd daemon. The TCP Wrapper program checks the incoming connection request against the access controls to ensure that it is a legal request. It also logs all connection requests to both successful and unsuccessful. ftp://ftp.porcupine.org/pub/security/index.html)

Port Sentry (It is designed to detect and respond to port scans. http://www.psionic.com/abacus/).

PGP (It is used in transmitting secure data via email or securely storing data should be used. It is used to communicate between two parties securely. http://www.pgpi.org/doc/faq/pgpi/en)

Details on installation of these can be found on the web on their respective sites.

Reference:

- IBM Red Books (Numbers GG24-4433-00, SG24-4558-00 SG24-5855-00, SG24-5971-00 & SG24-5962-00). http://www.redbooks.ibm.com/.
- Deroest, James and Ranade, Jay. AIX Version 4 System and Administration guide.
- Jose Pina Coelho, AIX FAQ November, 2000 http://www.emerson.emory.edu/services/aix-faq/.
- Man pages AIX 4.3.