**Solaris 11 Hardening Guide**

* **X displays must not be exported to the world**

Check status:

$ xhost

If access control is disabled set display and then run check again:

$ DISPLAY=MachineName:0.0; export DISPLAY

$ xhost

* **The audit system must alert the System Administrator (SA) if there is any type of audit failure.**

As root user issue command below (this check online applies to global zone):

# zonename

Verify the presence of an audit\_warn entry in /etc/mail/aliases:

# /usr/lib/sendmail -bv audit\_warn

If response is audit\_warn… User unknown, it should appear like this audit\_warn:user1,user2. Fix as below as root user:

# zonename

# pfedit /etc/mail/aliases

Add line at bottom:

audit\_warn:user1,user2

Update aliases file:

# newaliases

* **The operating system must configure auditing to reduce the likelihood of storage capacity being exceeded.**

Check that you are in the global zone:

# zonename

Check status of audit system (It must be auditing)

# pfexec auditconfig -getplugin

If the output of the above command does not contain ***p\_fsize=4M***, fix as follows:

Set size of a binary audit file to size specified in MB:

# pfexec auditconfig -setplugin audit\_binfile p\_fsize=4M

Restart the audit system:

# pfexec audit -s

* **The FTP daemon must not be installed unless required.**

Check to see if FTP is installed:

# pkg list service/network/ftp

If package installed and not required:

# pfexec pkg uninstall service/network/ftp

* **The operating system must be a supported release.**

Check OS version:

# uname -a

If not a supported release Upgrade:

# pkg publisher

# pkg set-publisher -G ‘\*’ <http://pkg.oracle.com/solaris/release> solaris

# pkg publisher

# pkg update –accept

# pkg list -af entire

* **The TFTP service daemon must not be installed unless required.**

Determine if TFTP package is installed:

# pkg list service/network/tftp

If installed and not needed:

# pfexec pkg uninstall install/installadm

# pfexec pkg uninstall service/network/tftp

* **The NIS package must not be installed.**

See if NIS package is installed  
 # pkg list service/network/nis

If installed remove:

# pfexec pkg uninstall service/network/nis

* **Login must not be permitted with empty/null passwords for SSH.**

Check if empty/null passwords are allowed for SSH:

# grep “^PermitEmptyPasswords” /etc/ssh/sshd\_config

If output is not:

# PermitEmptyPasswords no

Edit sshd\_config file at /etc/ssh/sshd\_config:

# pfedit /etc/ssh/sshd\_config

Find line PermitEmptyPasswords and change it to:

PermitEmptyPasswords no

Restart SSH service:

# svcadm restart svc:/network/ssh

* **SNMP communities, users, and passphrases must be changed from the default.**

As root, check SNMP configuration for default passwords:

# pkg search -l -Ho path snmpd.conf | awk '{ print "/"$1 }'

# more ***[filename]***

Identify community names or user password configurations, if anything is set to a default value, as root do this:

# pfedit ***[filename]***

Locate line system-group-read-community with default password of public and make password something more random. Make same changes for lines that read system-group-write-community, read-community, write-community, trap, and trap-community

* **The operating system must alert designated organizational officials in the event of an audit processing failure.**

First check zone (only applies to global zone):

# zonename

If global, verify presence of an audit\_warn entry in /etc/mail/aliases:

# /usr/lib/sendmail -bv audit\_warn

If response is audit\_warn… User unknown

# pfedit /etc/mail/aliases

Insert line where user1 and user2 are replaced by actual users:

audit\_warn:user1,user2

put updated file into service:

# newaliases

* **The telnet service daemon must not be installed unless required.**

Check to see if telnet daemon package is installed:

# pkg list service/network/telnet

If installed:

# pfexec pkg uninstall service/network/telnet

* **There must be no user .rhosts files.**

As root, check for .rhosts files:

# for dir in \

`logins -ox | awk -F: '($8 == "PS") { print $6 }'`; do  
find ${dir}/.rhosts -type f -ls 2>/dev/null  
done

If there is any output remove .rhosts files found:

# rm ***[filename]***

* **The operating system must not allow logins for users with blank passwords.**

See if system is enforcing a policy that passwords are required:

# grep ^PASSREQ /etc/default/login

If command does not return:

PASSREQ=YES

As root, edit /etc/default/login:

# pfedit /etc/default/login

And insert line below at bottom:

PASSREQ=YES

* **The system must not allow autologin capabilities from the GNOME desktop.**

Check if autologin is enabled for GNOME desktop:

# egrep "auth|account" /etc/pam.d/gdm-autologin | grep -vc ^#

If command returns anything other than “0”:

Edit /etc/pam.d/gdm-autologin:

# pfedit /etc/pam.d/gdm-autologin

Find lines below:

auth required pam\_unix\_cred.so.1

auth sufficient pam\_allow.so.1

account sufficient pam\_allow.so.1

And change them to:

#auth required pam\_unix\_cred.so.1  
#auth sufficient pam\_allow.so.1  
#account sufficient pam\_allow.so.1