i.t.solutions
uahuntsville

SECURITY RECOMMENDATIONS FOR SOLARIS SERVERS

AUDIENCE

This document is for Solaris server administrators. If you have questions about these procedures, please contact systems@uah.edu.

SECURITY REQUIRED TO CONNECT TO UAHUNTSVILLE NETWORK

I.t.solutions recommends several steps to secure your Solaris installation. For new Solaris installs, we require that the server not be connected to the UAHuntsville network until it is secured with at least the minimum protection. The minimal steps are as follows.

- Turning off unnecessary services.
- Enabling tcp wrappers.
- Configuring host access.

Note: Instead of tcp wrappers you can configure Solaris Firewall.

ADDITIONAL SECURITY MEASURES

Take these additional security measures to secure your Solaris server.

- Physical security of the machine is very important. The requirements for this will depend upon the use of the machine.
- Enable screen saver locking.
- Create warning banners.
- Install current Solaris patch sets that are appropriate for your operating system.
- Application security is also important and application software should be kept up-to-date.
- Remove un-needed applications.
- Passwords are very important. Use complex passwords. Protect the root password and share this with the minimum number of persons.
- Remove or lock unused accounts.
- Verify that there are no accounts with empty passwords.
- Install sudo and use this whenever possible to grant privileges for system tasks.
- File and directory permissions should be kept at the lowest level of privilege possible.
- Configure ssh security.
- Perform regular backups.
- Turn on extra logging.
- Root access should be logged.
- Perform operating system and service log monitoring and analysis routinely.
- Security logs should maintain one month of data if possible.

ADDITIONAL INSTRUCTIONS

TURNING OFF UNNECCESSARY SERVICES

IN SOLARIS 10

To disable inetd services in Solaris 10, use the svcadm command to disable services that are not needed.

Other services may be kept from starting by making modifications to the startup scripts in /etc/rc2.d or /etc/rc3.d such as renaming the startup script to cause the service not to be started on boot.

IN SOLARIS 9 AND UNDER

To disable services in Solaris versions below Solaris 10, first make a backup of inetd.conf, then edit inetd.conf and comment out those services that are not needed, then enter the following commands.

```
# pkill –HUP inetd
```

ENABLING TCP WRAPPERS

IN SOLARIS 10

To enable tcp wrappers in Solaris 10, enter the following commands.

```
#inetadm -M tcp_wrappers=true

#svcadm refresh inetd
```

IN SOLARIS 9 AND UNDER

To enable tcp wrappers in Solaris 9, you must edit the /etc/default/inetd file and set the ENABLE_TCPWRAPPERS parameter to YES. By default, TCP Wrappers was not enabled for inetd.

For Solaris 8 or below, tcp wrappers is not installed by default, but can be installed according to instructions:

http://www.sun.com/bigadmin/content/submitted/tcp_wrappers.html

Once the TCP Wrappers are in place, inetd services need to be configured to use tcpd.

Example: The following is a typical line in /etc/inetd.conf.

```
ftp    stream  tcp    nowait  root    /usr/sbin/tcpd  in.ftpd –l

# pkill –HUP inetd
```

CONFIGURING HOST ACCESS

In order for tcp wrappers to control The files /etc/hosts.allow and /etc/hosts.deny files must be created. Refer to Solaris's host_access for more information.

Example: The following /etc/hosts.allow and hosts.deny match the example above or a Solaris 10 server for which all tcp wrappers have been enabled.

/etc/hosts.allow

all:127.0.0.1

sshd: 172.16.12.1

/etc/hosts.deny

all:all

CREATE WARNING BANNERS

In order to successfully prosecute unauthorized activity on university-owned computers, each system needs to display a warning banner that conveys that unauthorized access is prohibited, access is logged, and there is no expectation of privacy.

This warning banner text can be placed in the file /etc/motd.

INSTALL CURRENT PATCH SETS

UAHuntsville has a support contract for the Solaris Operating System which covers updates, and patch sets are routinely downloaded from Sun and provided for campus access. You can obtain current patch sets in one of the following ways.

- If you have a support contract, register with Sun and use Sun's update manager application
- Download patch sets from on-campus via anonymous ftp and install those patches at the OS level.

Use the following steps to download and install patches from UAHuntsville.

Note: Be sure to select the **appropriate** patch set for your operating system.

1. FTP to the apollo18 server.

   ftp apollo18.uah.edu

2. Log in as anonymous. The password is your username on LDAP.
3. Change directory to the appropriate version number, enter binary mode, and get the correct file

   cd pub

   cd sun.patches

   cd OS-version-number (i.e: 10.0,9.0,8.0)

   bin

   get #_Recommended.zip where # will be 10, 9, or 8 depending on the OS version.

Note: There is a separate zip file for Solaris x86 installations

4. To install the patch set, read the CLUSTER_README. Follow instructions. Unzip the file.

    # unzip 9_Recommended.zip (for solaris 9)

5. Patch sets which contain kernel updates are generally recommended to be installed in single user mode. To enter single user mode you can use the command

    shutdown –i S at a system prompt

    or

    boot –s from a boot prompt

6. Change directory to the unzipped folder.

    # cd 9_Recommended (or 10_Recommended depending on the OS version)

7. Install the patch set. This may take about an hour or even more depending on the system, last patch date, etc.

    # ./install_cluster

8. Reboot the server.

    #reboot

CONFIGURE SSH SECURITY

Set the value for the variable “PermitRootLogin” to “no” in the sshd config file (/etc/ssh/sshd_config)

Set the value for the variable “Protocol” to 2 in the sshd_config file

After changes are made, restart sshd

Consider running sshd on a different port than port 22

TURN ON LOGGING

Enter the following commands to turn on general logging (if not enabled).

```
#touch /var/adm/loginlog
#chown root /var/adm/loginlog
#chgrp sys /var/adm/loginlog
```

Also turn on su logging if it is not enabled.

```
#touch /var/adm/sulog
#chown root /var/adm/sulog
#chgrp sys /var/adm/sulog
```