Global Information Assurance Certification Paper

GIAC Level Two Securing Unix
GCUX Practical Assignment
Version 1.6

Jeffrey S. Miles

Table of Contents

Solaris 7 Installation Checklist

Introduction

The intention of this document is not only to provide a checklist for a Solaris 2.7 operating system install, but to also provide explanations as to why certain procedures may or may not be implemented. The end result will be to have a Solaris 2.7 operating system install ready to use as a base for a Checkpoint Firewall-l version 4.1.

Preliminaries

In order to provide the maximum amount of security while building the box it should be connected to an isolated network. (i.e. no access to the internet) Additionally, the isolated network should be in a secured area that will only be accessible by a limited number of individuals. In our facility we have a lab area that is only accessible via a swipe card. A very small number of individuals have access to this area thus making it much more secure. Another precaution we will take is to use a separate box for downloading patches, utilities, & updates as well as any software compiling we may need to do. We can then utilize a tape drive, cd, or floppy depending on file size to move the compiled software from one unit to another. This will greatly reduce the possibility of the machine being compromised before it actually goes into production.

Operating System Install

Initial Preparation for Install

1. ___ Assemble the hardware.
2. ___ Turn on power to workstation.
   (Before the operating system can complete the boot cycle, hold down the Stop button and press A. This will halt the operating system and allow you to boot from the CD-ROM.)
3. ___ At the ok> prompt, type boot cdrom and hit return.
   (Please remember that Unix is case sensitive. Type all commands and text as seen in this procedure.)

   While the workstation is booting, this would be a good time to record the serial number of the workstation. This number will be important when registering the workstation for maintenance. The serial number is located on the CPU somewhere. The serial number can also be useful for tracking purposes if you have a lot of computers and they tend to recycled as new models are purchased and implemented.

   Workstation Serial Number: _____

Select Language and Locale

1. ___ The first window that is going to appear will be the "Select Language and Locale" window. This window is used to choose what character set you want to appear after the system is set up. If you are corresponding internationally,

and will need special characters to be recognized, then you may want to choose a particular set under the "Locales" box depending where you correspondence is coming from. However, in most cases the defaults of "English" in the "Languages" box and "USA(ASCII)" in the "Locales" is sufficient.

Network Identification

After clicking on the "Continue" button, a window will appear with a short explanation of what is going to take place during the install.

1. ___ After clicking on the "Continue" button, an ***"Identify This System"*** window will appear with a short explanation about setting up networking and time zones.
2. ___ After clicking on the "Continue" button, a ***"Host Name"*** window will appear. It is important to remember that when assigning a host name that it is not already in use somewhere else on the domain you will eventually attach the computer to. In other words it needs to be unique to that domain. If the hostname is not unique and the same as another host on the network, DNS will get confused and end up sending communication to the wrong computer or not sending any communication at all.
3. ___ After clicking on the "Continue" button, a ***"Networking Connectivity"*** window will appear. Since our computer is going to be used for firewall and will be checking communication between networks make sure "Yes" is chosen. And, since "Yes" is the default "Continue" can be clicked on and you can move on to the next window.
4. ___ The next window that will appear is the ***"IP Address"*** window. As in step 7 a unique hostname had to be chosen, so to must a unique ip address be assigned to the computer. It will be the only computer on the network with this address. This address will be assigned to the onboard Ethernet interface. This is commonly know as the external interface and will be the interface directing traffic to and from the internet. hme0 designation
5. ___ After clicking on the "Continue" button, a ***"Confirmation Information"*** window appears asking you to make sure the information you just put in is correct. If not click "Change" and re-enter the information. If everything looks correct then click on "Continue" to move on to the next widow.
6. ___ After clicking on the "Continue" button, a ***"Name Service"*** window will appear. Since most installations use DNS choose the "Other" option. You will have to manually enter DNS servers which we will address later in the document.
7. ___ After clicking on the "Continue" button, a ***"Confirmation Information"*** window appears asking you to make sure the information you just put in is correct. If not click "Change" and re-enter the information. If everything looks correct then click on "Continue" to move on to the next widow.
8. ___ After clicking on the "Continue" button, a ***"Subnets"*** window will appear. This window is simply asking if the computer is going to be part of a subnet. Since this computer is a firewall a range of addresses should have been assigned to the external network, which is where the communication takes place from step 4 of this section. This would be the subnet for this interface. Click "Yes" to

continue on.

9. ___ The next screen to appear is the ***"Netmask"*** screen. Enter the network mask for this computer.

Geographic Information

1. ___ After clicking on the "Continue" button, a ***"Time Zone"*** window will appear. I usually choose the *"Geographic region"* option which is the default. Then click the "Set..." button.
2. ___ The next window to appear is the ***"Geographic Region"*** window. Choose your region in left box and then choose the proper time zone in the right box.
3. ___ After clicking on the "Continue" button, a ***"Date and Time"*** window appears. Enter the correct time and date parameters and click "Continue".
4. ___ After clicking on the "Continue" button, a ***"Confirm Information"*** window appears asking you to make sure the information you just put in is correct. If not click "Change" and re-enter the information. If everything looks correct then click on "Continue" to move on to the next widow. In the "Solaris Install Console" window you will begin to see the installation taking place.

Interactive Installation

1. ___ After a short period of time a ***"Solaris Interactive Installation"*** window will appear. This window gives a description of next part of the installation. Items such as type of software install and filesystem layouts will be set up in this part of the installation.
2. ___ After clicking on the "Continue" button, an ***"Allocate Client Services"*** window appears asking you if you want to allocate space for diskless clients. Click "Continue".
3. ___ The next window to appear is the ***"Select Languages"*** window. This is language that will be used for the user interface. English is the default...So click on the "Continue" button.
4. ___ The next widow to appear is the ***"Select Software"*** window. In order to make the system the most secure, choose the **"Core System Support"**. As you will see further down in the document, there will be services that will still need to be removed as well as others needed to added in order for the system to functions properly as a firewall.
5. ___ After clicking on the "Continue" button, a ***"Select Disks"*** window will appear. Some things to take note of here. First, if you only have one disk drive in the computer, it is going appear in the right hand box and you can click "Continue" to move on. However, if you have more that 1 disk, the additional disk is going to show up in the left hand box. If you want to use the second disk, it must be moved to the right box by highlighting the disk and clicking on the top button between the boxes. This will allow the operating system to configure the disk as seen further down in the document.
6. ___ After clicking on the "Continue" button, a ***"Preserve Data"*** window appears. In order to get a clean install select "Continue". We do not want anything leftover from a previous install that could cause security breaches.

7. ___ After clicking on the "Continue" button, an ***"Automatically Layout File System?"*** window appears. This is asking if you want the system to automatically lay out the filesystems or do it manually? Choose "Manual Layout".
8. ___ The next window to appear is the ***"File System and Disk Layout"*** window. Since special filesystems will be needed for logging click on the "Customize" button. When configuring the internal disks in the firewall use the following charts as a guide.
One key thing to remember is that swap space (/swap on slice 1 of disk 0) should always be a minimum of twice the size of memory (RAM).

Suggested partitioning looks something like the following:

For one 9 GB drive

Filesystem	Size	Mounted on
/dev/dsk/c0t0d0s0	3679MB	/
/dev/dsk/c0t0d0s1	512MB	/swap #assuming 256 MB of RAM
/dev/dsk/c0t0d0s3	500MB	/var
/dev/dsk/c0t0d0s4	1000MB	/usr
/dev/dsk/c0t0d0s7	1000MB	/var/opt/

For two 4 GB drives:

Filesystem	Size	Mounted on
/dev/dsk/c0t0d0s0	800MB	/
/dev/dsk/c0t0d0s1	512MB	/swap
/dev/dsk/c0t0d0s3	1387MB	/var
/dev/dsk/c0t0d0s6	1000MB	/usr
/dev/dsk/c0t1d0s7	4.12GB	/var/opt/ - Disk two (2)

9. ___ Click ***"OK"*** to accept the filesystem layout.
10. ___ The ***"File System and Disk Layout"*** window will re-appear. Click "Continue" to go on to the next window.
11. ___ The next window to appear will be the ***"Mount Remote File Systems"*** window. Click "Continue" as we will not be mounting anything from a remote computer.
12. ___ The ***"Profile"*** window will appear next. This window is simply a confirmation of information you just put in. If all looks ok click the "Begin Installation". If you would like to make changes click the "Change" button.
13. ___ After clicking on the ***"Begin Installation"*** button, a window will appear asking if you want the system to reboot automatically or if you want to manually reboot. Click on ***"Auto Reboot".***
14. ___ At this point the operating system will be installed. Progress can be monitored in the "Solaris Install Console" window. You can also see the files being loaded in the progress window. At this point you can take a break. Depending on how fast your processor is this step usually take some time. Usually 10 to 15 minutes.

Assigning a Root Password

1. ___ When the installation has completed, the system will not have a root password. You can simply type "root" at the console login prompt and you will be at the root shell. So the next operation that needs performed is to assign a root password. This password is essential to the installer and administrator of the Unix system where the firewall will reside. Record the root password somewhere safe and entrust it only to those who will be responsible for maintaining the Unix system and the firewall software and security policy. Root password: _____ If you write the password in the blank line make sure this document is secure.
2. ___ To assign a root password, implement the following steps:
   At the "#" symbol on your screen type in "passwd root" and hit the enter key.
   The prompt "New password:" will appear. Enter a password.
   Next the prompt "Re-enter new password:" will appear. Re-enter the password.
   If the password is re-entered correctly, the following message will appear:
   "password (SYSTEM): password successfully changed for root"
3. ___ After assigning a root password a profile file needs also to be created for root. This file will house a basic set of variables and information needed to properly administer the system. To implement the profile file a file name ".profile" needs to created. Solaris has a .profile file in /etc/skel/ named "local.profile". Follow the procedure below to create a working .profile file for root.

   ```
   cp /etc/skel/local.profile /.profile
   ```

   Modify the file to look like the following:

   ```
   #
   # @(#)local.profile 1.4 93/09/15 SMI
   #
   stty istrip
   PATH=/bin:/usr/bin:/usr/sbin:/etc
   MANPATH= /usr/share/man
   export PATH MANPATH
   ```

4. ___ In order for root's profile to take affect, you will have to reboot the system. To reboot the system simply type "reboot"

Installing Sun Quad FastEthernet Card

Next the Ethernet drivers will need to be installed. The procedure below is for installing drivers for a Sun Quad FastEthernet Card. This card has four Ethernet ports that can be used for different networks attached to the firewall. Make sure these drivers are installed before patching the operating system.

Since a core installation was performed, if a cd is placed in the cdrom drive it will not load because the volume manager script (/etc/rc2.d/S92volmgmt) is not included in the installation. Therefore the cd will have to be mounted manually in order to add the files

necessary for the Ethernet card to operate correctly.

Mounting CDROM

1. ___ Create a directory on you system to mount the cd to
2. ___ mkdir -p /cdrom/sun_quadfast.
3. ___ mount -F hsfs -r /dev/dsk/c0t2d0s2 /cdrom/sun_quadfast_2_1

If a df -k command is issued, something similar to the following line should have been added to the filesystem listing:

/dev/dsk/c0t2d0s2 650 650 0 100% /cdrom/sun_quadfast_2_1

Installing Drivers

After the cd is mounted type in the following command to load the packages for the Ethernet card.

1. ___ pkgadd -d /cdrom/sun_quadfast_2_1/sol_2.7 SUMWqfed SUNWqfedu

Once the packages are added, unmount the cdrom

2. ___ umount /cdrom/sun_quadfast_2_1

Manually eject the cd.

System File Modifications and Additions

1. ___ Add "dns" after the "files" statement in the hosts line in the /etc/nsswitch.conf file.
2. ___ Add entries for all ethernet interfaces that will be used by the firewall in the /etc/hosts file. Please make sure you only enter values for the interfaces that will be used.

   Example: /etc/hosts file

IP address	Alias
_____	external
_____	internal
_____	dmz
_____	dmz1

3. ___ Create the following files:

   Hostname files for each of the Ethernet interfaces being used by the firewall.

   ___ touch /etc/hostname.hme0 external
   ___ touch /etc/hostname.qfe0 internal
   ___ touch /etc/hostname.qfe1 dmz
   ___ touch /etc/hostname.qfe2 _____
   ___ touch /etc/hostname.qfe3 _____
   ___ touch /etc/resolve.conf file. The following is just an example.

Example	Actual
mydomain.com	domain _____
nameserver 129.216.243.224	nameserver _____
nameserver 129.228.2.3	nameserver _____

4. ___ Prevent the firewall workstation from becoming a router by entering the file /etc/notrouter.

   touch /etc/notrouter

Packages & Patches

1. ___ Remove the following packages
Although the packages listed below are part of the core install they are not required for FW-1 v4.1 to operate correctly. Therefore they can be removed. To remove the packages, issue the "pkgrm" command followed by the package name.

Example: pgkrm SUNWsndmr

Name	Description
SUNWsndmr	Sendmail root
SUNWsndmu	Sendmail user
SUNWftpr	FTP Server, (Root)
SUNWftpu	FTP Server, (Usr)
SUNWpcelx	3COM EtherLink III PCMCIA Ethernet Driver
SUNWpcmci	PCMCIA Card Services, (Root)
SUNWpcmcu	PCMCIA Card Services, (Usr)
SUNWpcmem	PCMCIA memory card driver
SUNWpcser	PCMCIA serial card driver
SUNWpsdpr	PCMCIA ATA card driver
SUNWxwdv	X Windows System Window Drivers
SUNWxwmod	OpenWindows kernel modules
SUNWnisr	Network Information System, (Root)
SUNWnisu	Network Information System, (Usr)
SUNWcg6	GX (cg6) Device Driver
SUNWadmr	System & Network Administration Root
SUNWdtcor	Solaris Desktop /usr/dt filesystem anchor
SUNWsolnm	Solaris Naming Enabler
SUNWatfsr	AutoFS, (Root) system SUNWatfsu AutoFS, (Usr)

2. ___ Add the following packages
There are two lists below. The first list are packages that are required by Firewall 4.1 and must be installed. The second list are optional packages. However, if you are going to be doing any type of administration on the box the box, these packages will be helpful.

In order to add the following packages, the Solaris 7 Software disk will need to be mounted in the cdrom drive. Insert the cd into the drive and issue the following commands:

```
# mount -F hsfs -o ro /dev/dsk/c0t2d0s0 /cdrom
# cd cdrom/Solaris_2.7/Products/
```

Copy the directories listed below from the cd to the /var/spool/pkg directory. Example: cp -r SUNWlibC /var/spool/pkg The -r option is used to copy everything in the directory, including any directories that may be below the main directory.

Once all the directories have be copied over to the /var/spool/pkg directory, the "pkgadd" command will need to be issued.

```
# pkgadd -d /var/spool/pkg
```

When this command is issued, a list will appear with all the packages that were transferred from the cd. By hitting the "return" key at end of the list all the packages will be installed. The installation is an interactive installation. Basically, you will have to answer "yes" to a question for each package to be installed. When all packages are installed, the list will appear again. Hit the "q" key to exit out and you are finished.

Required packages by FW-1

Name	Description
SUNWlibC	Sun Workshop Compilers Bundled libC required by FWDIR/bin/cpconfig
SUNWter	Terminal Information required for FW-1 installation
SUNWscpu	Source Compatibility, (Usr) /usr/ucb/ln required for upgrades

Optional packages

Name	Description
SUNWadmc	Administration core libraries
SUNWadmfw	Network Administration Framework includes showrev(1M)
SUNWdoc	Documentation Tools
SUNWman	On-Line Manual Pages

3. ___ Install the operating system patches from Sun. Since the computer that is being prepared is on an isolated network, patches will need to be downloaded to another computer and placed on a cd or tape media to be transferred. They can also be placed on a laptop and transferred from the laptop via ftp. However, make sure to physically place the laptop on the isolated network before uploading to continue to maintain the highest level of security during the install.

Download the Solaris 2.7 recommended patch bundle from http://sunsolve.sun.com/pub-cgi/show.pl The name of the file is 7_Recommended. Place the bundle in /var/temp
This bundle is a zip file. Once the patches have been loaded onto the system, the "unzip" command will need to used to unzip the file.

```
# cd /var/temp
```

unzip 7_Recommended.zip

This will create a directory named "7_Recommended" To install the patches, change directories into this directory:

cd 7_Recmmended

Once in this directory, read over the CLUSTER_README file. The main thing to make sure of is that you have enough disk space to install the patches. With most modern systems this is not a problem. To actually install the patches issue the following command:

install_cluster

A warning will appear prompting you to make sure there is enough disk space. Notice the "4 MBytes of available space" qualifier about three quarters down in the paragraph.
Type "Y" to continue with the cluster install.
At this point the patches will begin to install.

Return Codes
You will see a number of failures with at return code of 8. Example:

Installation of 107038-01 failed. Return code 8

This means that the particular package that is to be patched with this patch is not installed. Again a core installation was done so a number of packages were not installed because they are not needed and therefore will not need patched.
You will see a number of failures with at return code of 2. Example:

Installation of 102980-07 failed. Return code 2

This means the patch was already installed from the cd.

4. ___ Date: _____
5. ___ Create a security patch install schedule. Security patches, if possible, should be installed 1 per week to keep current and assuming they have been issued.
6. ___ Reboot system for patches take effect.

Hardening the Box

Disabling Unnecessary Process During System Boot Up

Even though we installed a core set of files for our operating system, there are still other files in the boot directories that need to be secured. This is done by removing or renaming them.

1. ___ Disable NFS related files - Since this is a firewall there should be no mounting of other filesystems on the box. To stop this from happening follow the procedure below.

```
# cd /etc/rc2.d
# rm S73nfs.client K28nfs.server S74autofs S93 cacheos.finish
S73cachefs.daemon

# cd /etc/rc3.d
# rm S15nfs.server
```

```
# cd /etc
# rm auto_home    auto_master  autopush
# rm dfs/dfstab
```

2. ___ Disable auto configuration links - When these are disabled, it will prevent a user from issuing a sys-unconfig command by which they could change an ip address or subnet mask among other things and completely disable the system.

```
# cd /etc/rc2.d
# rm S30sysid.net S71.sysid S72autoinstall
```

3. ___ Disable Sendmail - Sendmail listens for incoming mail. Firewalls should not be mail servers.

```
# cd /etc/rc2.d
# rm S88sendmail
```

4. ___ Disable RPC related links - These services are very vulnerable to attack. Note: if you are using CDE (which you should not be) the S71rpc service is necessary.

```
# cd /etc/rc2.d
# rm S71rpc S76nscd
```

5. ___ Disable expreserve link - This script recovers vi buffers when the data was not saved and a machine was rebooted. Since there should not be a whole lot of editing going on this service is really not necessary.

```
# cd /rc2.d
# rm S80PRESERVE42.
```

Setting a More Secure umask for System Daemons

Because default umasks for system daemons are not setup at boot, the files the daemons create will be created world writable. Being so, they are susceptible to manipulation. By setting a more secure umask for these daemons, the files they in-turn create will be also more restrictive. By implementing the script below, the files that are created by the system daemons will have permissions of 700. This means that the owner is the only on who can read, write, or execute the file. Most of these are owned by root and should not be accessed by anyone other that those who are administering the box.

```
# cd /etc/init.d
# vi umask.sh
press the "i" key for insert
type in: umask 077
press the escape key (leaves edit mode)
while holding down the shift key, press the z key twice (this will save and exit
the file)
# chmod 744 umask.sh (this will make the file only executable by its owner
```

root. Root is the only one who can modify this file).
ln /etc/init.d/umask.sh /etc/rc0.d/S00umask.sh
ln /etc/init.d/umask.sh /etc/rc1.d/S00umask.sh
ln /etc/init.d/umask.sh /etc/rc2.d/S00umask.sh
ln /etc/init.d/umask.sh /etc/rc3.d/S00umask.sh
ln /etc/init.d/umask.sh /etc/rcS.d/S00umask.sh

Securing Network Interfaces

Place the following list of commands at the end of the /etc/init.d/inetinit file. These settings need to be placed at the end of the file because the inetinit file sets all kernal parameters to the interfaces to default settings. If they were at the beginning they would be over written with the defaults. These settings will help protect against, SYN flood attacks, ARP spoofing, Smurf attacks as well as DDoS attacks.

ndd -set /dev/tcp tcp_conn_req_max_q0 10240.
ndd -set /dev/ip ip_ignore_redirect 1.
ndd -set /dev/ip ip_send_redirects 0.
ndd -set /dev/ip ip_ire_flush_interval 60000.
ndd -set /dev/arp arp_cleanup_interval 60.
ndd -set /dev/ip ip_forward_directed_broadcasts 0.
ndd -set /dev/ip ip_forward_src_routed 0.
ndd -set /dev/ip ip_forwarding 0.
ndd -set /dev/ip ip_strict_dst_multihoming 1.

Secure the /etc/init.d/inetsvc File

Every line in the file should be commented out with the exception of the following:

/usr/sbin/ifconfig -auD4 netmask + broadcast +

This line is used to reset netmasks and broadcast addrsses

Clean Out Crontabs Directory

From the /var/spool/cron/crontabs file remove all users except root

Allow Only Root to Modify the cron and at Jobs List.

cd /var/spool/cron/crontabs
vi cron.allow
press the "i" key for insert
type in: root
press the escape key (leaves edit mode)
while holding down the shift key, press the z key twice (this will save and exit the file)
chown root cron.allow
chgrp root cron.allow
chmod 400 cron.allow

Repeat the process for the at.allow file.

Remove the cron.deny and at.deny file which are created with the system
rm -f /etc/cron.d/*.deny

Securing the passwd File

Because some scripts may want to see certain accounts we will not remove the them from the /etc/passwd file but will tighten the security on them. By doing so they will not be able to be used for logins or access the cron or at services.

1. ___ For each account in the /etc/passwd file with the exception of root make /dev/null the default shell. By doing this no one will be allowed to login using these accounts.
2. ___ For added insurance lock out all accounts by issuing a passwd -l <user> for every user in the passwd file with the exception of root. This will lock out those accounts by placing '*LK* in password field of the /etc/shadow file.

Locking Down root Logins

When attempting to login as root, depending on where the attempt is being made from, one of two things are going to happen. If your are attempting to login as root from the console, by default you will be allowed to do so, assuming you know the root password. However, if you attempt to log in as root from a remote location you will be denied unless you login as a legitimate user first and then su to root. This behavior can also be implemented at the console level also by editing the /etc/default/login file. By making this change anyone attempting to login is root will be logged because all su attempts are logged. Use the following procedure to make the change.

cd /etc/default
vi login
find the line that contains "CONSOLE=/dev/console" and place the cursor at the beginning of line.
cursor over to the first "/"
press the "x" key until "/dev/console" is erased
while holding down the shift key, press the z key twice (this will save and exit the file)

Now when you try to enter the computer via the console you will have to login as yourself before you can su to root.

Creating a Personal Account.

Up to this point if you have been working using the root shell, because of the previous step you are going to need to set up a personal login account before the machine is rebooted. Once the account is created a password will be assigned.

create home directory
touch /usr/users/<username>
useradd -m -d /usr/users/<username> -g 10 -s <default shell> -c <full name> <login id>
Create a password for yourself
passwd <login id>

You will be ask to verify the password and then you will get a message saying the password has be updated. Again, the next time you boot you will have to log in as yourself and then su to root.

Tightening Filesystems

Tightening the /usr filesystem

/usr is where system binaries are stored. One of the favorite tricks of hackers should they gain access to the box is to leave trojan horse programs that they can use when they are on your system. To prevent this we need to mount the /usr directory as read only. To accomplish this the /etc/vfstab file will need be edited. In the /etc/vfstab file there is a line that looks like the following:

```
#device          device          mount    FS     fsck   mount   mount
#to mount        to fsck         point    type   pass   at boot options
....
/dev/dsk/c0t0d0s3  /dev/rdsk/c0t0d0s3  /usr     ufs    1      no      -
```

The "-" at end of the line needs to be replaced with "ro" (read only). The system will need to be rebooted for the "ro" option take effect.

Tightening the /var filesystem

Next we want to make sure that if any setuid programs are executed from the /var directory that they are done so without full root priviledge.

```
#device          device          mount    FS     fsck   mount   mount
#to mount        to fsck         point    type   pass   at boot options
....
/dev/dsk/c0t0d0s4  /dev/rdsk/c0t0d0s4  /var     ufs    1      no      nosuid
```

The system will need to be rebooted for these options to take effect.

Additional Logging

In order to log events that are related to security, such as reboots, failed login attempts or attempts that a user invoked the su command, edit the /etc/syslog.conf file and then add the two files listed below.

1. ___ Editing the /etc/syslog.conf file

```
# cd /etc/
# vi syslog.conf
place cursor on the " # auth.notice" line
press the "o" key and new line will open below
add the following to that blank line
auth.info          /var/log/authlog    #Note the white space must
be tabs
when finished hit the escape key to exit edit mode
while holding down the shift key, press the z key twice (this will save
and exit the file)
```

2. ___ Creating the /var/log/authlog & /var/log/loginlog files

```
# cd /var/log
# touch authlog
# chown root authlog
# chgrp sys authlog
# chmod 600 authlog
# touch loginlog
# chown root loginlog
# chgrp sys loginlog
# chmod 600 loginlog
```

If you would like to rotate these logs take a look at /usr/lib/newsyslog. This will give an example of how this can be done.

Legal Notices

Modify the /etc/motd (message of the day) and /etc/issue files so they contain a notice that has been approved by your legal counsel. This message should contain notification that all who enter are being monitored and logged and if anything suspicious activity arises due to them being on the system, they will be confronted. Also if any criminal activity is found, the proper authorities will be contacted and prosecution could incur.

Open Boot Prom Settings

When the system is booted, we want it to boot only from the hard disk unless a special password is given. In order to do this Open Boot Prom (OBP) settings to must be secured. Specifically, the *security-mode* must be set to *command* and an obp password must be issued. DO NOT forget the obp password as it cannot be recovered. Without the password you will not be able to boot into single user mode, which will be needed to be done for backups, and you will not be able to boot from the CD-ROM should new software need added. The only fix for this is to order a new eeprom from Sun. To set the security-mode option:

1. __ Log on as root
2. __ Type eeprom security-mode=command
3. __ Enter and confirm the password

Set a More Restrictive UMASK for All Users on the System.

This is done by un-commenting the UMASK=022 line in /etc/default/login

Setting the TCP Initial Sequence Number Generation Parameters

By setting TCP_STRONG_ISS=2, will implement the RFC 1948 sequence number generation, which is unique-per-connection-ID. By doing this it will make hijacking session attempts much more difficult.

Password Aging

Since this machine is going to be protecting our network and be serving as a perimeter

protection device (firewall) we want to go to the extra step of implementing password aging. Even though this can be somewhat of a hassle there should not be that many administrators who will need access to the box therefore not to many complaints. If the administrators understand security there should be no complaints. To set up password ageing implement the following steps:

```
# cd /etc/default/
# vi passwd file
```

Once in the file place cursor over the "=" symbol on the "MAXWEEKS" line press the "a" for "append"
type in number to represent the number of weeks the password will last. (once per quarter or 13 weeks seems to be the compromising point).

Preventing Stack Overflows

Prevent stack based buffer overflows by adding the following two lines to the /etc/system file.

```
set noexec_usr_stack = 1
set noexec_user_stack_log=1
```

Activating NTP (Network Time Protocol)

Should something illegal happen, and prosecution need to take place proper evidence will need to be presented. Part of that evidence will include times the incident occurred as shown in logs. Because of this it is necessary to have accurate time on the machine. However, since we loaded a core install the ntp package will need to be added to our machine.
Downloading and installing ntp.
This program can be found at http://www.sunfreeware.com. I ftp'd into a mirror site, ftp://metalab.unc.edu/pub/solaris/freeware/sparc/7/ and downloaded the file ntp4.0.72j-sol7-sparc-local.

To install the gzip utility a pkgadd -d command must be issued.

```
# pkgadd -d ntp4.0.72j-sol7-sparc-local
```

Next we will have to find a source that keeps accurate time to retrieve the time from. There is a list of public NTP servers at http://www.eecis.udel.edu/~mills/ntp/clock2.htm. Out of the list pick a minimum of 2 to 3 sights and contact the administrator for each sight to get permission to connect. Once permission is granted, place the ip addresses of the servers in the /etc/ntp.conf directory.

Installing TCP wrappers

Prerequisites
For a successful installation of TCP wrappers, there are a three programs that will need to be installed on the computer that is connected to the network. These utilities are not part of the Solaris software and will need to be downloaded and installed. After this computer has generated the necessary files they can be transferred to the machine that is on the isolated network and put into place. Before downloading these files a created a working

directory, /var/utils/ to download the files to. The programs are:

gzip - used to decompress GNUgcc compiler and TCP Wrappers
GNUgcc compiler - needed to compile TCP Wrappers
TCP Wrappers

1. ___ Downloading and installing gzip.
This program can be found at http://www.sunfreeware.com. I ftp'd into a mirror site, ftp://metalab.unc.edu/pub/solaris/freeware/sparc/7/ and downloaded the file gzip-1.2.4-sol7-sparc-local.

To install the gzip utility a pkgadd -d command must be issued.

```
# pkgadd -d gzip-1.2.4-sol7-sparc-local
```

This will install gzip in /usr/local/bin. This path should be added to the login profile so that it can be invoked from the command line without typing the whole path.

2. ___ Downloading and installing GNUgcc compiler.
This program can also be found at http://www.sunfreeware.com. Again, I ftp'd into the mirror site, ftp://metalab.unc.edu/pub/solaris/freeware/sparc/7/ and downloaded the file gcc-2.95.1-sol7-sparc-local.gz. Then issue the following command:

```
# gunzip gcc-2.95.1-sol7-sparc-local.gz
```

This will create the file gcc-2.95.1-sol7-sparc-local. This file will be used by the pkgadd ulility to place the GNUgcc compiler onto the computer. Issue the following command to add the compiler to the computer:

```
# pkgadd -d gcc-2.95.1-sol7-sparc-local
```

This will install the gcc compiler in /usr/local/bin.

3. ___ Downloading and installng TCP Wrappers.
This program can be found at ftp://ftp.porcupine.com. Simply ftp to ftp.porcupine.org/pub/security/ and downloaded the file tcp_wrappers_7.6.tar.gz. To decompress the file issue the following command:

```
# gunzip tcp_wrappers_7.6.tar.gz
```

This will create the file tcp_wrappers_7.6.tar, to untar the file type in the following command:

```
# tar xvf tcp_wrappers_7.6.tar
```

Once the file is untarred, a directory will be created called: tcp_wrappers_7.6. Changed directories into this directory. There is a file named "Makefile" that needs to be modified. The first two lines that need to be edited are:

```
# SysV.4 Solaris 2.x OSF AIX
```

```
#REAL_DAEMON_DIR=/usr/sbin
```

Note: if vi is used as the editor, issue the ":set nu" command and line numbers will appear. The above two lines are lines 46 and 47.
Remove the comment (#) sign from the second of these two lines, (line 47) so that it looks like the following:

```
REAL_DAEMON_DIR=/usr/sbin
```

Then look for the lines: (lines 192 - 197)

```
# SunOS 5.x is another SYSV4 variant.
sunos5:
    @make REAL_DAEMON_DIR=$(REAL_DAEMON_DIR)
    STYLE=$(STYLE) \
    LIBS="-lsocket -lnsl" RANLIB=echo ARFLAGS=rv VSYSLOG= \
    NETGROUP=-DNETGROUP AUX_OBJ=setenv.o TLI=-DTLI \
    BUGS="$(BUGS) -DSOLARIS_24_GETHOSTBYNAME_BUG" all
```

Change the fourth of these lines to read: (line 195)

```
LIBS="-lsocket -lnsl" RANLIB=echo ARFLAGS=rv CC=gcc VSYSLOG= \
```

This tells the Makefile to use the GNUgcc compiler which we installed earlier.

Finally, compile the source code by issuing the following command:

```
# make sunos5
```

Note: in order for the "make" command to run from the command line, the path /usr/ccs/bin should be added to the login profile. You will have to logout and then log back in for the change to take effect.

After TCP Wrappers has compiled there are three files that will need to be moved from compiler host to the isolated host. The first is tcpd. This is the TCP Wrappers daemon and will need to be placed in the /usr/sbin/ directory. Once in the directory, issue the following commands on the file:

```
# chmod 555 tcpd
# chown root tcpd
# chgrp daemon tcpd
```

The second file, tcpd.h needs to be placed in the /usr/include/ directory. Once in the directory, issue the following commands on the file:

```
# chmod 444 tcpd.h
# chown root tcpd.h
# chgrp daemon tcpd.h
```

The third file, libwrap.a needs to be placed in the /usr/lib/ directory. Once in the directory, issue the following commands on the file:

```
# chmod 555 libwrap.a
# chown root libwrap.a
# chgrp daemon libwrap.a
```

Installing Open Secure Shell (OpenSSH)

Prerequisites

For a successful installation of OpenSSH, there are a four programs that will need to be installed on the computer that is connected to the network. These utilities are not part of the Solaris software and will need to be downloaded and installed. After this computer has generated the necessary files for SSH they can be transferred to the machine that is on the isolated network and put into place. Before downloading these files a create a working directory, /var/utils/ to download the files to. The programs are: zlib, perl, openssl, and openssh.

1. ___ Downloading and installing zlib.
   This program can be found at http://www.sunfreeware.com. Ftp into the mirror site, ftp://metalab.unc.edu/pub/solaris/freeware/sparc/7/ and download the file zlib-1.1.3-sol7-sparc-local.gz. Then issue the following command:

   ```
   # gunzip zlib-1.1.3-sol7-sparc-local.gz
   ```

   This will create the file zlib-1.1.3-sol7-sparc-local. This file will be used by the pkgadd utility to place the zlib package onto the computer. Issue the following command to add zlib to the computer:

   ```
   # pkgadd -d zlib-1.1.3-sol7-sparc-local
   ```

2. ___ Downloading and installing perl.
   Perl is needed to install OpenSSL. This program can be found at http://www.sunfreeware.com. Ftp into the mirror site, ftp://metalab.unc.edu/pub/solaris/freeware/sparc/7/ and download the file perl-5.005_02-sol7-sparc-local.gz. Then issue the following command:

   ```
   # gunzip perl-5.005_03-sol7-sparc-local.gz
   ```

   This will create the file perl-5.005_03-sol7-sparc-local. This file will be used by the pkgadd utility to place the perl package onto the computer. Issue the following command to add perl to the computer:

   ```
   # pkgadd -d perl-5.005_03-sol7-sparc-local
   ```

3. ___ Downloading and installing openssl.
   This program can be found at ftp://ftp.openssl.org/source/openssl-0.9.6.tar.gz. Once the file is downloaded decompress it by issuing the following command:

   ```
   # gunzip openssl-0.9.6.tar.gz
   ```

   This will create the file openssl-0.9.6.tar, to untar the file type in the following command:

```
# tar xvf openssl-0.9.6.tar
```

Once the file is untarred, a directory will be created called: openssl-0.9.6. Changed directories into this directory and issue the following commands.

```
#  ./config
# make
# make install
```

4. ___ Downloading and installing openssh.
This program can be found at ftp://ftp.openbsd.org/pub/OpenSSH/poratble/openssh-2.3.0p1.tar.gz. Once the file is downloaded decompress it by issuing the following command:

```
# gunzip openssh-2.3.0p1.tar.gz
```

This will create the file openssh-2.3.0p1.tar, to untar the file type in the following command:

```
# tar xvf openssh-2.3.0p1.tar
```

Once the file is untarred, a directory will be created called: openssh-2.3.0p1. Changed directories into this directory and issue the following commands.

```
#  ./config
# make
# make install
```

5. ___ Now that OpenSSL and OpenSSH are configured, there are a number of files that need to be transferred to the host on the isolated network. /usr/local/ssl/lib/libssl.a, /usr/local/ssl/lib/libcrypto.a, the entire /usr/local/ssl/include/openssl directory, all the ssh files from /usr/local/bin/: ssh ssh-add ssh-agent and ssh-keygen, and finally, /usr/local/sbin/ssh. These files will need to be placed in the same directories on the isolated machine as they were on the compiler machine.

Configuring Open Secure Shell (OpenSSH)

1. ___ Configure the /usr/local/etc/sshd_config.
See appendix for sshd_config file examples

2. ___ Secure the script by changing its owner, group and permissions by issuing the following commands on the script.

```
# chown root /usr/local/etc/sshd_config
# chgrp root /usr/local/etc/sshd_config
# chmod 600 /usr/local/etc/sshd_config
```

3. ___ Create a startup script /etc/init.d/sshd which will cause ssh to start when the system is booted. See appendix for examples.

4. ___ Make the following modifications to the file.

```
# chown root /etc/init.d/sshd
# chgrp sys   /etc/init.d/sshd
# ln -s /etc/init.d/sshd /etc/rc2.d/S75sshd
```

Bringing TCP Wrappers and SSH Together

In order for these two programs to work together, the /etc/hosts.allow and /etc/hosts.deny files need to be created. The /etc/services file needs to be modified along with the /etc/inetd.conf file.

1. ___ Creating /etc/hosts.allow

The /etc/hosts.allow file houses a list of allowed services and hosts, networks, and or domains allowed to access those services. For the purposes of this document, the service of ssh will be only be allowed from any host on the servicing domain (i.e. your local domain).

```
# cd /etc
# vi hosts.allow
press the "i" key for insert
type in: sshd: <servicing domain>
press the escape key (leaves edit mode)
while holding down the shift key, press the z key twice (this will save
and exit the file)
# chmod 644 hosts.allow (this will make the file only writable by its
owner root. Root is the only one who can modify this file).
```

2. ___ Creating /etc/hosts.deny

The /etc/hosts.deny file houses a list of non-allowed services and hosts, networks, and or domains not allowed to access those services. For the purposes of this document, all other services (other than ssh above) will be dis-allowed from any host.

```
# cd /etc
# vi hosts.deny
press the "i" key for insert
type in: ALL: ALL
press the escape key (leaves edit mode)
while holding down the shift key, press the z key twice (this will save
and exit the file)
# chmod 644 hosts.deny (this will make the file only writable by its
owner root. Root is the only one who can modify this file).
```

3. ___ Modifying /etc/services

```
# cd /etc
# vi services
find the line that begins with "ftp" and move cursor to that line
```

press the "o" key (a line will open up below the line the cursor was on)
insert the following text:
ssh 22/tcp
press the escape key (leaves edit mode)
while holding down the shift key, press the z key twice (this will save and exit the file)

4. ___ Modifying the /etc/inetd.conf file

cd /etc
vi inetd.conf
find the line that begins with "ftp" and move cursor to that line
press the "o" key (a line will open up below the line the cursor was on)
insert the following text:
ssh stream tcp nowait root /usr/sbin/tcpd sshd -i
While this file is in edit mode we want to comment out every other line in the file so that the only service that is allowed to this machine is ssh. In order to do so place a "#" before all lines except the one that begins with ssh.
Once finished.... press the escape key (leaves edit mode)
while holding down the shift key, press the z key twice (this will save and exit the file)

Modifying this file in this way will allow TCP Wrappers to catch the ssh request and log it to the /var/log/syslog file. Also note that the only way to access the box is through ssh. ftp and telnet are both disabled. You should get a ssh client installed on any computers that will need to access the box and would recommend using sftp from ssh.com for secure ftp transfers.

Not Going to Use SSH??

This is not recommended, but if ssh is not going to be used along with a secure ftp client, I would still use TCP Wrappers to limit who can access the system. In addition an /etc/ftpusers file should be created. This file works the opposite of most files in that who ever is in the file is denied access to the ftp service. All of the listings in /etc/passwd should be in this file with the exception of those users will have permission to ftp to the computer. To create and secure the /etc/ftpusers file:

cd /etc
vi ftpusers
press the "i" to enter edit mode
add the following list 1 entry per line: root daemon bin sys nobody noaccess nobody4 uucp nuucp adm lp smtp listen
press the escape key (leaves edit mode)
while holding down the shift key, press the z key twice (this will save and exit the file)

make the file readable and writable by root only

```
# chmod 600 ftpusers
# chown root ftpusers
# chgrp root ftpusers
```

Testing the Box

Now that the system has been hardened, test to make that everything is working as it should. Do you have connectivity? Are TCP Wrappers and SSH functioning properly? Is logging working properly? Are the legal messages place on machine showing up? Install and test the firewall software. Once everything is operating correctly and the box is ready for production, you may want to run a scan on the box to make sure services that are seen are the only ones expected to be seen. ISS, Nessus, nmap and Satan are recommended.

Making Backups

Two sets of backups should be made. The first should be made for security incident handling purposes and probably should be stored off-site. Should an incident occur the info could be compared to what was on the box to see what changes had been made. The second copy should be kept close by in case of a crash. Both copies should be stored in very safe and secure environment. Follow the procedure below to create backups using an 8 mm dat drive.

```
Boot the system in single-user mode
# reboot -- -s

Mount all filesystems
# fsck
# mount -a

Back up all ufs file systems to tape or other media TWICE
# mt /dev/rmt/0 rewind
for dir in / /usr /var /local
do
ufsdump 0f /dev/rmt/0n $dir
done
# mt /dev/rmt/0 eject
```

Repeat the above steps on new media. Be sure to back up any other filesystems that were created when building the system.

The "Making Backups" script was taken from Sans Institute "Solaris Security Step by Step"

Appendix

Example SSH sshd_config file

```
Port 22
ListenAddress 0.0.0.0
SyslogFacility AUTH
LogLevel INFO

HostKey /etc/ssh_host_key
ServerKeyBits 1024
KeyRegenerationInterval 900

CheckMail no
UseLogin no
PrintMotd no
KeepAlive no

PermitRootLogin no
IgnoreRhosts yes
RhostsAuthentication no
RhostsRSAAuthentication no
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords no
StrictModes yes
UseLogin no
LoginGraceTime 1801
```

Example SSH startup Scripts

```
#!/bin/sh

# Startup/shutdown script for sshd

SSHD=/usr/local/sbin/sshd

pid=`/usr/bin/ps -Af | /usr/bin/grep $SSHD | awk '{ if ( $3 == "1" ) print $2 }'`

case $1 in
'start')
        if [ "${pid}" = "" ]
        then
                if [ -x $SSHD ]
                then
```

```
                $SSHD
            fi
        fi
        ;;
'stop')
        if [ "${pid}" != "" ]
        then
            /usr/bin/kill ${pid}
        fi
        ;;
*)
        echo "usage: /etc/init.d/sshd {start|stop}"
        ;;
esac
```
[1]

Startup scrip for sshd, save it as /etc/rc3.d /S99sshd

```
#!/sbin/sh
#
case "$1" in
'start')
   if [ -x /usr/local/sbin/sshd ]; then
       echo 'Starting Secure Shell: sshd';
          /usr/local/sbin/sshd
       fi
       ;;
   'stop')
       /usr/bin/pkill -x -u 0 sshd
        ;;
    *)
       echo "Usage: $0 { start | stop }"
       exit 1
       ;;
    esac
    exit 0
```
[2]

```
#!/bin/sh -
#
#
PIDFILE="/etc/sshd.pid"
SSHD=/opt/slocal/sbin/sshd
case $1 in
start)
```

```
test -f $SSHD || exit 0
$SSHD
;;
stop)
test -f $PIDFILE || exit 0
PID=`cat $PIDFILE`
test "$PID" && kill "$PID"
> $PIDFILE
;;
*)
echo "Usage /etc/init.d/sshd {start | stop)";;
esac
exit 0
```
[3]

These scripts were found in various articles on the internet.

[1] www.scms.rgu.ac.uk/staff/jr/computing/uinix/ssh.html
[2] www.unixcircle.com/features/BuildingSolarisFW.php
[3] www.sans.org/y2k/practical/Jeff_Campione_GCUX.htm

References

Boran, Sean; *Hardening Solaris Securely installing a firewall bastion host*, http://securityportal.com/reaserch/solaris_hardening.htm

Campione, Jeff; *Solaris 8 Installation Checklist*, http://www.sans.org/y2k/practical/Jeff_Campione_GCUX.htm

Spitzner, Lance; *Armoring Solaris, Preparing Solaris for a firewall*, http://www.enteract.com/~lspitz/armoring.htm

Solaris Security Step by Step; The Sans Institute, Drafted and Edited by Hal Pomeranz: Deer Run Associates

Solaris Resources at Kempston; *Installing and Configuring TCP Wrappers on Solaris 7 and Solaris 8* http://www.kempston.net/solaris/tcpwrappers.html

Ibid; *Installing gzip, the gcc compiler and flex on Solaris 7 and Solaris 8* http://www.kempston.net/solaris/utilitysoftware.html

Gregory, Pete H., *Solaris Security* Sun Microsystems Press, A Prentice Hall Title, Prentice Hall PTR, Prentice-Hall, Inc Upper Saddle River, New Jersey 07458

Sobel, Mark G., *A Practical Guide to Solaris*, Addison-Wesley Publishing Company, One Jacob Way, Reading, Massachusetts 01867

Sun Freeware Software, http://www.sunfreeware.com

OpenSSH software, http://www.openssh.com
TCP Wrappers software, http://www.porcupine.org

Last Updated: July 22nd, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**