Global Information Assurance Certification Paper

SANS GIAC Certification
Level 2 GCUX
Certified UNIX Security Administrator
Securing UNIX Step by Step
Version 1.7

Practical Assignment
For
SANSFire in Washington

Submitted By:

Kurt Koenigsknecht
November 2001

Table of Contents

GCUX Practical Assignment

Select a single Unix or Linux operating system version and architecture. Develop a checklist of the steps that you would take to secure that specific system architecture and version (e.g., checklist for Red Hat Linux 7.0), from out-of-the-box to an "Internet ready" state. Make certain to list the commands or procedures you use and demonstrate what you have learned in class and through your own research. If a command or procedure is not fully obvious, you may add explanatory text in an Appendix or via a hyperlink.
Be sure to specify the hardware; the operating system and version; the type and version of any additional software installed; and the role/purpose of the machine (bastion DNS server; standard user workstation; public Apache web server; etc.).

We encourage you to review some of the existing GCUX practicals, particularly more recent papers or those marked "Honors", to get an idea of the type and level of work that is expected. Your work should meet or exceed this level of effort. If you reference earlier practicals, be certain to list the URLs of the ones that you reference.

In addition to listing your step by step procedures, you should also explain why certain actions are being taken. What is the risk involved? How does making a particular configuration change improve the security of the system? What risks can reasonably be left in place given the operational needs of the host? The test of a successful submission is that someone with less knowledge and experience than you should be able to follow the document and bring a Unix or Linux system to a safe state, and also understand the risk and countermeasures involved.

Your completed submission should be a minimum of 15 pages long, and should also meet all of the other requirements listed above under "Formatting and Minimum Length". It must include at least five references, and should contain appropriate diagrams and examples.

Introduction

Once the decision is made to expose a system to the Internet, securing that system from undesirables, while still fulfilling the business requirements, becomes priority number one. The best practices approach to securing a system is to utilize the principal of least privilege, while minimizing the amount of software on the exposed server. This becomes a delicate balancing act between securing the system while still meeting the business needs that the system was intended to fulfill. While Sun Microsystems had made steps by improving the "out of the box" security configuration (i.e. default ftp security configuration, and the /etc/default/init CMASK=022 entry to control processes started by init) of the Solaris 8 Operation System much still needs to be done.

Planning to provide only the services necessary to those whom require them is the best practice methodology that should be followed when a system is going to be exposed to the Internet. General experience confirms and a published document by Noordergraaf of Sun Microsystems http://www.sun.com/blueprints/1100/minimize-updt1.pdf states that the fewer software components on a server means fewer security holes to detect and patch. Statistics show the majority of system penetrations are accomplished through the exploitation of security holes in the operating system (OS) itself. Thus, minimizing the number of OS modules installed on a server can greatly improve overall system security by reducing the sheer number of vulnerabilities.

The addition of third party applications may require specific OS modules and services to be loaded and available respectively. The focus of this paper will be on the procedures for preparing a Sun Ultra1[1] system for use as an iPlanet IWS 4.1sp2 web server. Only installing the minimal OS modules necessary to install, configure and administrator the IWS 4.1sp2 application will accomplish this. Although most of the procedures used will be applicable to other environments, different application environments should be considered unique, thus requiring customized procedures for each of them.

[1] Due to limitations with laboratory equipment a more current system could not be utilized.

OpenBoot Prom (OBP)

Securing the OBP by enabling "security-mode"

The default setting for "security-mode" is "none", thus those with access to the systems keyboard will have unlimited access to the OBP commands via "Stop-A". Changes will be made to prevent un-unauthorized access to the OBP command prompt. Securing the OBP command interface will be done by performing the following tasks.
The Sun Microsystems Info Docs Article 14214 http://sunsolve.sun.com was used as a point of reference and can be reviewed should further details be necessary. The document is not available to those without SunSolve logins. The necessary information from the document is as follows:

_____ Secure the OBP with the following:

The valid "security-mode" levels are: none, command, and full. The implemented security policy mandates physical security of the systems and secure building access, thus it was determined the "command" level will be used to secure the OBP command prompt. This provides the OBP security desired while providing the entire IT staff the flexibility to be able to boot the system should it be required.

A brief description of the effects of the three security levels are:

none - Any command can be typed and no password is required (This is the system default).

command - The user can use the 'c' or 'b' (continue, boot) commands at the restricted monitor without a password.
A password is required if the user wishes to use the 'n' command to get to the fourth command mode or if a parameter is used with the 'b' command (e.g. to boot single user mode).

full - This is the most restrictive mode and the only command that can be executed without a password is the 'c' command.
All others (b,n) require a password.

CAUTION: The use of control characters such as ^L will cause the OBP to not recognize the password you have entered. It is recommended that the password be tested using the 'command' security level prior to selecting 'full'. If the password is not recognized, boot the system with no arguments and modify using the eeprom command.

CAUTION: Do not forget the password that you set for the OBP. If the password is forgotten, the system will not be

usable and the only fix is a hardware swap of the NVRAM chip.

Note: Do not set the security-password variable of the NVRAM directly. Let the system prompt you for the password.

At the "ok" prompt, enter the following commands which will change the OBP settings.

- **ok> password**
  - **Enter the new password, the system will ask for a second confirmation. (This will become the OBP password)**
- **ok> setenv security-mode command**
- **ok> reset**

_____ Document the OBP and POST levels

Current OBP Version_____ Current POST Version_____

Confirmation of auto-boot

Confirm "auto-boot?" is set to "true", this should be a default, yet verification will prevent any unexpected results. Setting the "auto-boot?" will be done with the following commands:

- **ok> setenv auto-boot? true**
- **ok> reset**

Document **auto-boot?** setting.

_____ Confirm Auto-boot? True or False _____(Select True)

Document the **boot-device** setting:

Boot Device _____

Installation of Core Operating System

The "Core" cluster contains only 79 packages and uses 100Mbytes; the "End User" cluster has 300+ packages and uses 500+ Mbytes. Choosing to install the fewer packages

found in the "Core" cluster will greatly reduce the vulnerabilities the system will be susceptible to. Loading additional packages should be considered as business needs dictate. Should additional packages be installed each (package) needs to be monitored for updated patch levels and/or published vulnerabilities. Don't take the easy way out and install the "Entire OS Plus OEM", it is not worth the increased risks possed to the organization.

Best practices mandate that the system stay disconnected from any network, other than the controlled setup network until, hardening and patches have been completed.

_____ Load the Core Operating System with the following instructions:

1. Insert Solaris 8 Software CD-ROM 1 of 2

Booting from the "Disk 1 of 2" instead of using the "Solaris 8 Installation CD-ROM" provides more control over the installation process.

2. From the "ok" prompt, Type "boot cdrom"

This starts the boot process used for system installation.

ok> boot cdrom

3. Select a Language.

Select "0" for the English Language.

4. Select a Locale

Select "0" for English (C- 7-bit ASCII)

5. The installation process will present:

   "The Solaris installation program is divided into a series of short sections where you'll be prompted to provide information for the installation. At the end of each section, you'll be able to change the selections you've made before continuing"

Select "Continue"

6. The installation process will present:

   "On the next screens, you must identify this system as networked or non-networked, and set the default time zone and date/time.

   If this system is networked, the software will try to find the information it needs to identify the system; you will be prompted to supply any information it cannot find.

To begin identifying the system, Choose Continue."

Select "Continue"

7. The installation process will present:

   "Specify Yes if the system is connected to the network by one of the Solaris or vendor network/communication Ethernet cards that are supported on the Solaris CD. See the hardware documentation for the current list of supported cards.

   Specify No if the system is connected to a network/communication card that is not supported on the Solaris CD, and follow the instructions listed under Help."

   Networked: _____

Specify "Yes" then select "Continue"

8. The installation process will present:

   "On this screen you must specify whether or not this system should use DHCP for network interface configuration. Choose Yes if DHCP is to be used, or No if the interfaces are to be configured manually."

   Use DHCP: _____

Specify "No" then select "Continue"

9. The installation process will present:

   "On this screen you must enter a host name, which identifies this system on the network. The name must be unique within the domain in which it resides; creating a duplicate host name will cause problems on the network after you install Solaris.

   A host name must be at least two characters; it should contain letters, digits and minus signs, (-)."

   Host name: _____

Specify a hostname _____ then Select "Continue"

10. The installation process will present:

"On this screen you must enter the Internet Protocol (IP) address for this system. It must be unique and follow your site's address conventions, or a system/network failure could result.

IP addresses contain four sets of numbers separated by periods (for example 129.200.9.1)

IP address: _____

Specify a IP address ____ . ____ . ____ . ____ then Select "Continue"

11. The installation process will present:

    "On this screen you should specify whether or not IPv6, the next generation Internet Protocol, would be enabled on this machine. Enabling IPv6 will have no effect if this machine is not on a network that provides IPv6 service. IPv4 service will not be affected If IPv6 is enabled."

    Enable IPv6: _____

Specify "No" then Select "Continue"

Note: The best practice is not to turn on those functions/features that will not be used to avoid vulnerabilities.

12. The installation process will present:

    "Confirm the following information. If it is correct, choose Continue, to change any information choose Change."

    Networked:
    Use DHCP:
    Host name:
    IP address:
    Enable IPv6:

Verify all this information presented, then Select "Continue"

13. The installation process will present:

    "Configure Kerberos Security:" _____

Specify "No" then Select "Continue"

14. The installation process will present:

"Confirm the following information. If it is correct, choose Continue; to change any information choose Change."

Configure Kerberos Security: No

Verify the information presented, then Select "Continue"

15. The installation process will present:

"On this screen you must provide name service information. Select the name service that will be used by this system, or None if your system will either not use a name service at all, or if it will use a name services not listed here."

Name Service: _____

Specify "None" then select "Continue"

Note: The naming service will be none, but it will be manually configured later on.

16. The installation process will present:

"Confirm the following information. If it is correct, choose Continue; to change any information choose Change.

Name Service: None

Verify the information presented, then Select "Continue"

17. The installation process will present:

"On this screen you must specify whether this system is part of a subnet. If you specify incorrectly, the system will have problems communicating on the network after you reboot."

System part of a subnet: _____

Specify "Yes", then Select "Continue"

18. The installation process will present:

"On this screen you must specify the netmask of your subnet. A default netmask is shown; do not accept the default unless you are sure it is correct for your subnet. A netmask must contain four sets of numbers separated by periods (for example 255.255.255.0).

Netmask: _____

Specify the netmask, _____._____._____._____then Select "Continue"

19. The installation process will present:

    "On the current screen you must select how to specify your default time zone.

    Select one of the methods and choose Set."

    Specify timezone by: _____

Specify "Geographic Region", then Select "Set"

20. The installation process will present:

    "On this screen you can specify your default time zone by geographic region.

    Select a region from the list on the left and a time zone from the list on the right."

    Region: _____ Time zone: _____

Specify the Region "United States", specify Time zones "Eastern", then select "Continue"

21. The installation process will present:

    "Accept the default date and time or enter new values"

    Date and Time: "**Presented as the current date and time**"

Verify the information presented, then Select "Continue"

22. The installation process will present:

    "Confirm the following information. If it is correct, choose Continue; to change any information choose Change.

    System part of subnet: Yes
    Netmask: 255.255.255.0
    Time Zone: US/Eastern
    Date and time: "Presented as current date and time"

Verify the information presented, then Select "Continue"

23. The installation process will present:

    "This system is upgradeable, so there are two ways to install the Solaris software.

    The Upgrade option updates the Solaris software to the new releases, saving as many modifications to the previous version of Solaris software as possible. Back up the system before using the Upgrade option.

    The Initial option overwrites the system disks with the new version of Solaris software. This option allows you to preserve any existing file systems. Back up any modifications made to the previous version of Solaris software before staring the Initial option.

    After you select an options and complete the tasks that follow, a summary of your actions will be displayed."

Select "Initial"

24. The installation process will present:

    "You'll be using the initial option for installing Solaris software on the system. This initial option overwrites the system disks when the new Solaris software is installed.

    On the following screens, you can accept the defaults or you can customize how Solaris software will be installed by:

    -Selecting the type of Solaris software to install
    -Selecting disks to hold software you've selected
    -Specifying how file systems are laid out on the disks

    After completing these tasks, a summary of your selections (called a profile) will be displayed.

Select "Continue"

25. The installation process will present:

    "Select the geographic regions for which support should be installed.

Select ONLY "North America –U.S.A (en_US.ISO8859-1)", then Select "Continue"

26. The installation process will present:

    "Select the Solaris software to install on the system.

NOTE: After selecting a software group, you can add or remove software by customizing it. However, this requires understanding of software dependencies and how Solaris software is packaged."

Specify "Core System Support", then Select "Continue"

27. The installation process will present:

    "Select the disks for installing Solaris software. Start by looking at the Required field; this value is the approximate space needed to install the software you've selected. Keep selecting disks until the Total Selected value exceeds the Required value.

    To move a disk from the Available to the Selected windows, click on the disk, then click on the button.

Specify the appropriate boot disk, cXtXdX then Select "Continue"

28. The installation process will present:

    "Do you want to preserve existing data? At least one of the disks you've selected for installing Solaris software has file systems or unnamed slices that you may want to save."

Select "Continue"

29. The installation process will present:

    "Do you want to use auto-layout to automatically layout file systems? Manually laying out file systems requires advanced system administration skills."

Select "Manual Layout"

30. The installation process will present:

    "The summary below is your current file system and disk layout, based on the information you've supplied.

    NOTE: If you choose to customize, you should understand file systems, their intended purpose on the disk, and how changing them may affect the operation of the system."

Select "Customize"

31. The installation process will present:

    "Customize Disks"

Slice	Name	Size
0	/	150
1	swap	256
2	overlap	1002
3		
4		
5	/var	200
6	/usr	244
7	/opt	150

Note: Due to lab environment limitations a 1GB internal disk was used.

Specify the desired disk layout, then Select "OK"

32. The installation process will present:

    "The summary below is your current file system and disk layout, based on the information you've supplied.

    NOTE: If you choose to customize, you should understand file systems, their intended purpose on the disk, and how changing them may affect the operation of the system."

Verify the information presented, then Select "Continue"

33. The installation process will present:

    "Do you want to mount software from a remote file server? This may be necessary if you had to remove software because of disk space problems."

Select "Continue"

34. The installation process will present:

    "The information shown below is your profile for installing Solaris software. It reflects the choices you've made on previous screens."

    The profile is displayed for review.

Verify the information presented, then Select "Begin Installation"

35. The installation process will present:

    "After Solaris software is installed, the system must be rebooted. You can choose to have the system automatically reboot, or you can choose to manually reboot the system if you want to run scripts or do other customization before the reboot. You can manually reboot a system using the reboot(1M) command."

Select "Auto Reboot"

Adding Packages Not Included In Core

The Core cluster does not include some of the software modules the system will require for performing administrative functions. The software modules can be found on the Solaris 8 Software 1 of 2 and 2 of 2 and should be installed as follows:

_____ **Install the following packages from the 1 of 2 CD-ROM**

1. Insert the **"Solaris 8 Software 1 of 2 CD-ROM"**
2. mount the CD-ROM to /mnt
    a. /usr/sbin/mount –F hsfs /dev/dsk/c0t6d0s0 /mnt

Note: The /mnt mount point is created by the core installation

3. Change directory to Solaris 8 Product
    a. /usr/bin/cd /mnt/Solaris_8/Product
4. Install the desired software modules from the CD-ROM
    a. /usr/sbin/pkgadd –d . **"Insert Package Name"**

- **SUNWntpr—Needed For NTP**
- **SUNWntpu—Needed For NTP**
- **SUNWdoc—Needed For Docs, required for SUNWman**
- **SUWWbzip—Needed to install some packages (i.e. SUNWgzip)**
- **SUNWlibC—Needed for iPlanet iWS**
- **SUNWadmc—Needed For showrev (command)**
- **SUNWadmfw—Needed For showrev (libraries)**
- **SUNWxcu4—Needed For OpenSSH X-Windows Tunneling**
- **SUNWxcu4x—Needed For OpenSSH X-Windows Tunneling**
- **SUNWxwplt—Needed For OpenSSH X-Windows Tunneling**
- **SUNWxwplx—Needed For OpenSSH X-Windows Tunneling**
- **SUNWxwrtl—Needed For OpenSSH X-Windows Tunneling**
- **SUNWxwrtx—Needed For OpenSSH X-Windows Tunneling**
- **SUNWxwice—Needed For OpenSSH X-Windows Tunneling**
- **SUNWxwicx—Needed For OpenSSH X-Windows Tunneling**

b. Answer **Yes** to all the questions.
c. /usr/bin/cd /
d. /usr/sbin/umount /mnt

_____ **Install the following packages from the 2 of 2 CD-ROM**

5. Insert the **"Solaris 8 Software 2 of 2 CD-ROM"**
6. mount the CD-ROM to /mnt
   a. /usr/sbin/mount –F hsfs /dev/dsk/c0t6d0s0 /mnt
7. Change directory to Solaris 8 Product
   a. /usr/bin/cd /mnt/Solaris_8/Product
8. Install the desired software modules from the CD-ROM
   a. /usr/sbin/pkgadd –d . **"Insert Package Name"**

      - **SUNWter—Needed for Terminal Access**
      - **SUNWaccr—Needed for Accounting**
      - **SUNWaccu—Needed for Accounting**
      - **SUNWman—Needed for Man Pages**
      - **SUNWbash—Needed for bash shell**
      - **SUNWzlib—Needed for OpenSSH**
      - **SUNWgzip---Needed to gzip of add on packages**
      - **SUNWast---Needed for tightening system security**

   b. Answer **Yes** to all the questions
   c. /usr/bin/cd /
   d. /usr/sbin/umount /mnt

Patching the System Current

Patching the system current is a best practice for reducing the vulnerabilities of the system. It is well known that many system compromises could have been prevented had the administrator just patched the system to current levels. For those reasons the system will be patched in two ways; with the Sun Recommended & Security Patch Cluster, and with those additional patches that are called out with the PatchCheck Tool.

Recommended and Security Patch Cluster

_____ **Install the Sun Recommended and Security Patch Cluster with the following procedure:**

1. On secure system download the Solaris 8 Recommended and Security Patch Cluster README
   a. FTP download the latest Recommended & Security Patch Cluster for Solaris

ftp://sunsolve.sun.com/pub/patches/8_Recommended.zip

b. Download the CHECKSUMS
ftp://sunsolve.sun.com/pub/patches/CHECKSUMS

c. Check the MD5 checksum to confirm validity of patch cluster

d. Review the README for special instructions.
ftp://sunsolve.sun.com/pub/patches/8_Recommended.README

Note: From this point forward it is assumed that the patch cluster, and all other downloads performed in this procedure, will be downloaded to a secure system. The secure system will have an open Ethernet port for the target system to be connected to via a cross over cable. Alternately, a CD-ROM can be burned for easier distribution to the system.

2. Move patch cluster to the /tmp folder on the machine to be patched
3. Unzip/uncompress the patch cluster
   a. /usr/bin/cd /tmp
   b. /usr/bin/unzip 8_Recommended.zip
4. Execute the cluster install script
   a. /usr/bin/cd /tmp/8_Recommended/install_cluster
   b. ./install_cluster

Note: The following subset of exit codes can be found in the "installpatch" script of any patch. To find the most current listing view the script located in the patch to be installed.

```
# Exit Codes:
#       0       No error
#       1       Usage error
#       2       Attempt to apply a patch that's already been applied
#       3       Effective UID is not root
#       4       Attempt to save original files failed
#       5       pkgadd failed
#       6       Patch is obsoleted
#       7       Invalid package directory
#       8       Attempting to patch a package that is not installed
#       9       Cannot access /usr/sbin/pkgadd (client problem)
#       10      Package validation errors
#       11      Error adding patch to root template
#       12      Patch script terminated due to signal
#       13      Symbolic link included in patch
#       14      NOT USED
#       15      The prepatch script had a return code other than 0.
#       16      The postpatch script had a return code other than 0.
```

```
#       17      Mismatch of the -d option between a previous patch
#               install and the current one.
#       18      Not enough space in the file systems that are targets
#               of the patch.
#       19      $SOFTINFO/INST_RELEASE file not found
#       20      A direct instance patch was required but not found
#       21      The required patches have not been installed on the manager
#       22      A progressive instance patch was required but not found
#       23      A restricted patch is already applied to the package
#       24      An incompatible patch is applied
#       25      A required patch is not applied
#       26      The user specified backout data can't be found
#       27      The relative directory supplied can't be found
#       28      A pkginfo file is corrupt or missing
#       29      Bad patch ID format
#       30      Dryrun failure(s)
#       31      Path given for -C option is invalid
#       32      Must be running Solaris 2.6 or greater
#       33      Bad formatted patch file or patch file not found
#       34      The appropriate kernel jumbo patch needs to be installed
#
```

Using "PatchCheck" to Complete Patching

_____ Install the PatchCheck Tool, if not already done so on the secure system, with the following procedure:

Although the Recommended & Security Patch Cluster provides a large number of the patches, many others still must be individually patched. The Sun Recommended & Security list is only a cluster of those patches the typical system might need, thus it can be assumed to be lacking for this environment. Sun created the "Patch Check" utility to assist in identifying and locating the patches for each unique system.

Patch Check determines the patch levels on your system against Sun's Recommended and Security patch list. Additionally, it operates from input files and lists all patches that pertain to packages installed on the system. This tool is similar to the PatchDiag Tool that may have been used in the past, with the added advantage of producing reports in HTML format that allow you to select and receive patches automatically.

Complete instructions are provided by Sun at the following URL:
http://sunsolve.sun.com/pub-cgi/show.pl?target=patchk

_____ Run the PatchCheck Tool and install the recommended patches with the following procedure:

Again, since the system is not yet networked, i.e. not yet patched and hardened, the PatchCheck tool will be utilized on the secure system. The following steps will be used:

1. On the target system generate the outputs necessary to later run PatchCheck on a remote system
    a. /usr/bin/showrev –p > /tmp/web-1.showrev.txt
    b. /usr/bin/pkginfo –l > /tmp/web-1.pkginfo.txt
2. Migrate the captured files to the secure system /tmp folder
3. Generate the Patch Check output
   The syntax is as follows: /usr/bin/perl patchk.pl –b –p <pfile> <sfile> <os_ver> <arch>

Where:
<pfile> is a file containing pkginfo –l output.
<sfile> is a file containing showrev –p output
<os_ver> is the OS version; this msut be a SUNOS number (i.e. 5.8)
<arch> is the architecture of the system where the data was obtained (i.e. sparc)

The command that will be used is as follows:

- **/usr/bin/perl patchk.pl -b –p web-1.pkginfo_l.txt web-1.showrev_p.txt 5.8 sparc**

The html output will be placed in /tmp.

4. Open the newly generated html file for review. The output will include five categories of patches:

    - Downreved Installed Patches
    - Uninstalled Recommended Patches
    - Uninstalled Security Patches
    - Uninstalled Y2K Patches
    - Other Related Uninstalled Patches

5. Generate Patch Suite
    a. Select **Create Patch Suite**

Note: In order to use the Patch Retrieval feature a registered SunSolve Online account is needed (i.e. requires a Sun Support contract)

5. Move patch cluster to the /tmp folder on the machine to be patched
6. Unzip/uncompress the patch cluster

   a. **/usr/bin/cd /tmp**
   b. **/usr/bin/unzip [patchid].zip**
7. Install each patch
   a. Review the README of each patch for special instructions
   b. **/usr/sbin/patchadd [patchdir]**

Update the system OBP and POST

_____ **Installation of OBP Patch 104881-07 or the then current OBP patch**

Update the system to the latest OBP version recommended by Sun Microsystems. For the Sun Ultra1, as of September 2001, the recommended level is OBP 3.25.0 POST 3.10.6. The instruction for updating can be found by searching with "Patch Finder" for Patch-ID# 104881-07 http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-access

Note: The patch number could change over time, always search for the current patch and revision.

Note: This patch is available even without Sunsolve login.

Keeping the OBP and POST versions current will reduce the likelihood of system malfunction and/or vulnerabilities due to known "bugs" in the older code sets.

While the OS is running the following command may be used to determine the current system firmware;

```
/usr/sbin/prtconf –V
or
/usr/platform/sun4/sbin/prtdiag –v | grep OBP
```

The firmware revisions may also be determined from the PROM monitor's "ok" prompt with the following command;

```
.version
```

Compare the outputs to the latest version documented in Patch-ID# 104881-07. If necessary, follow the upgrade instructions included to bring the OBP and POST versions current.

Confirming the umask 022

_____ **Confirm the default setting is 022**

Previous to Solaris 8 the default system file mode creation mask was 000. That meant that files created by system daemons where created with permission bits of 666. This was a vulnerability because it allowed normal users to overwrite the contents of system generated files.

Fortunately, Sun reduced this vulnerability by making a change with the release of the Operating Environment in Solaris 8. The default system umask was changed to 022 in the Solaris 8 Operating Environment to control processes started by init. Should the requirement to adjust this new default be necessary, it may be adjusted by altering the CMASK variable in the /etc/default/init file.

Since most administrators have become use to making this change, it has been included here for review and confirmation that it is configured correctly.

Suppressing unnecessary services

By default, Solaris is a powerful operating system that executes many useful services. However, most of these services are unneeded and pose a potential security risk thru the insecure default connectivity used (i.e. non-SSH). The /etc/inetd.conf file specifies which services the /usr/sbin/inetd daemon will listen for. By default, /etc/inetd.conf is configured for 39 services in Solaris 8. All the services, except telnet, will be commented out, thus disabling them.

_____ **Edit and comment out all the lines, except telnet, in the /etc/inetd.conf file.**

Confirm that all services, except telnet, are commented out with the following command, which should result in a null output.

- **/usr/bin/grep –v "^#" /etc/inetd.conf**

_____ **Confirm result NULL output except for telnet line**

Stopping Unnecessary Processes

Stopping unnecessary processes is an easy way to avoid vulnerabilities with processes that should have never have been available on the system anyway. Each process should be evaluated for its business and/or administrative needs and if none exist, terminate them. By renaming the startup scripts to something other than files that start with the capital "S" the services are not started at boot time. Using the "." dot and lower case "s"

makes the files hidden, as well as, providing a reminder of the original starting order. Make the following changes:

_____ **Stop Unnecessary Processes with the following Procedure**

1. Rename the "auto configuration" scripts to prevent "sys-unconfig" from being successfully run.

   - **/usr/bin/mv /etc/rc2.d/S30sysid.net /etc/rc2.d/.s30sysid.net**
   - **/usr/bin/mv /etc/rc2.d/S71sysid.sys /etc/rc2.d/.s71sysid.sys**
   - **/usr/bin/mv /etc/rc2.d/S72autoinstall /etc/rc2.d/.s72autoinstall**

2. Rename the NFS related links to prevent unwanted NFS serves and mounts.

   - **/usr/bin/mv /etc/rc2.d/S73nfs.client /etc/rc2.d/.s73nfs.client**
   - **/usr/bin/mv /etc/rc3.d/S15nfs.server /etc/rc3.d/.s15nfs.server**

   Also remove NFS related configuration files.

   - **/usr/bin/rm /etc/auto_* /etc/dfs/dfstab**

3. Rename the RPC related links to limit the many vulnerabilities from CDE, NIS and NIS+. Should the CDE environment be needed for administrative functions it can be manually activated.

   - **/usr/bin/mv /etc/rc2.d/S71rpc /etc/rc2.d/.s71rpc**

4. Rename sendmail related links to limit the many vulnerabilities of sendmail attacks. The system will no longer be able to receive mail or act as a mail server. The system will still be able send mail from the host.

   - **/usr/bin/mv /etc/rc2.d/S88sendmail /etc/rc2.d/.s88sendmail**

5. Rename the preserve related links. The system will no longer provide "vi" buffers when the system is rebooted, but the reduced risk of this vulnerable service is worth the sacrifice.

   - **/usr/bin/mv /etc/rc2.d/S80PRESEVE /etc/rc2.d/.s80PRESERVE**

6. Rename the nscd links, which provides a cache for the most common name service requests. The system will not be used as a user desktop so the service is not required.

   - **/usr/bin/mv /etc/S76nscd /etc/.s76nscd**

Clearing unnecessary crontabs

Removing unnecessary crontabs will reduce the likelihood of any vulnerability or unwanted actions arising from them. Remove the unwanted crontabs with the following procedure:

_____ **Remove the unnecessary contrabs with the following command:**

- **/usr/bin/rm /var/spool/cron/crontabs/adm**
- **/usr/bin/rm /var/spool/cron/crontabs/lp**

Securing System Accounts

Confirm ftpusers file

Preventing unwanted FTP access is very important because it is highly exploitable therefore; disabling it for unwanted users will be done. Fortunately, Sun reduced this vulnerability by making a change with the release of the Operating Environment in Solaris 8. The default for the Solaris 8 Operating Environment is to block FTP access from all installation generated system accounts.

Since most administrators have become use to making this change, it has been included here for review and confirmation that it is configured correctly.

_____ **Confirm /etc/ftpusers contains all the entries in the /etc/passwd file**

Note: This is now the default for the Solaris 8 Operating Environment.

Disable unnecessary accounts

Leaving unnecessary accounts active could provide an intruder with easy access to the system. By disabling the unnecessary accounts, including “sys", "uucp", "nuucp", and "listen" that vulnerability is significantly reduced.. Place the "NP" in the password field of the /etc/shadow file for each of the accounts. Also use the /dev/null to prevent login attempts to secured accounts. Use the following procedure to disable unwanted accounts.

_____ **Modify the /etc/passwd file to include “/dev/null” in the shell entry for each of the following accounts: daemon, bin, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4.**

Example:

- daemon:x:1:1::/:/dev/null

_____ **Modify the /etc/shadow file to include the "NP" in the password field of each of the following entries: daemon, bin, adm, lp, uucp, nuucp, listen, nobody, noaccess, nobody4.**

Example:

- daemon:NP:6445::::::

Using Strong Passwords

_____ **Use strong password policy**

This system will be used as an Internet Web server thus, the use of local user accounts will be kept to a minimum. Even so, the use of a strong password policy should not be overlooked as a defensive measure.

All passwords on the system must comply with the following:

- **All passwords must contain at least one number**
- **All passwords must contain at least one special character**
- **All passwords must be eight characters in length**
- **Passwords must be changed a minimum of every 30 days**

Hardening Networking Functions

Limit routing

To prevent undesirable routes, that may be inserted by an intruder, all routing will be done via the default route and/or static routes. This will ensure the machine will not dynamically route. Limit routing with the following steps:

_____ **Limit routing**

1. Create the /etc/defaultrouter file containing the IP address of the default router.

___.____.____.____ **Enter the default router here**

2. Create the /etc/notrouter file.

   Use the "touch /etc/notrouter" command to create the file. This will prevent the system from running in.rdiscd and in.routed at boot time.

Configure system DNS

Configuring the DNS might not necessarily be considered part of securing the system yet it still needs to be done correctly. Use the following steps to configure DNS:

_____ **Configure DNS**

1. Create the /etc/resolv.conf file with the appropriate DNS information

domain _____
nameserver_____
nameserver_____

2. Update the /etc/nsswitch.conf file to reflect DNS as the second method of naming service behind "files". Edit the /etc/nsswitch.conf file and modify the "hosts" entry to reflect the following:

- **hosts: file dns**

Note: If the system does not have a requirement to resolve more than a few entries populate the /etc/hosts file instead. This would eliminate the need for running DNS client services entirely. This would help protect against DNS spoofing, and DNS cache poisoning. The entries in the /etc/hosts file should contain fully qualified host names, as well as, the unqualified host names.

Modify /etc/init.d/inetsvc

Modify the /etc/init.d/inetsvc file to shutdown DHCP and named entries. The system will not be providing DHCP or be acting as DNS server so eliminating the services will reduce the likelihood of vulnerabilities.

Comment out all lines except the following:

- **/usr/sbin/ifconfig –auD4 netmask + broadcast +**
- **/usr/sbin/inetd –s &**

Additional Networking Lockdowns

Additional lockdowns should include making adjustments to the default /dev/ip ndd settings. This will be done to protect the system from SYN floods, ARP spoofs, smurf attacks, reduce the likelihood of the system being used for a DDOS, and preventing the system from responding to pings sent to the LAN broadcast address.

Create the /etc/init.d/netconfig script that will be run immediately following the inetinit (i.e. /etc/rc2.d/S69inet). Not placing the entries into the current /etc/init.d/inetinit file reduces the likelihood that patches and/or Operating System upgrades will remove the entries made. Many of the settings used are recommendations from the Sun BluePrints document Solaris Operating Environment, Network Settings for Security http://wwwwswest.sun.com/blueprints/1200/network-updt1.pdf

_____ Create the /etc/init.d/netconfig script (between the ----------):

Start----------Script
```
#!/sbin/sh
#Limit SYN Flood attacks
ndd -set /dev/tcp tcp_conn_req_max_q0 4096
ndd –set /dev/tcp tcp_ip_abort_cinterval 60000

#Disable timestamp and timestamp broadcast request, no need for them
ndd –set /dev/ip ip_respond_to_timestamp 0
ndd –set /dev/ip ip_respond_to_timestamp_broadcast 0

#Ignore IPv4 ICMP redirect errors, to prevent the install of bogus routes
ndd -set /dev/ip ip_ignore_redirect 1

#Only routers need to send redirect errors, disable sending them
ndd -set /dev/ip ip_send_redirects 0

#Disable Forwarded Source routed packets, just to be sure
ndd -set /dev/ip ip_forward_src_routed 0

#Disable Forwarding of Directed Broadcast, to prevent smurf attacks
ndd -set /dev/ip ip_forward_directed_broadcasts 0

#Enable Strict Destination Multihoming to prevent packet spoofing
ndd –set /dev/ip ip_strict_dst_multihoming 1

#Clear ARP entries after a reasonable period of time
ndd -set /dev/arp arp_cleanup_interval 60000
ndd -set /dev/ip ip_ire_arp_interval 60000

#Limit IP Spoofing by turning on TCP Strong
ndd –set /dev/ip tcp_strong_iss 2

#Disable response to echo request broadcasts
ndd –set /dev/ip ip_respond_to_echo_broadcast 0
```
End----------Script

- **/usr/bin/chown root:root /etc/init.d/netconfig**
- **/usr/bin/chmod 744 /etc/init.d/netconfig**
- **/usr/bin/ln –s /etc/init.d/netconfig /etc/rc2.d/S69netconfig**

Note: Solaris Operating System upgrades and patches may change the default behavior of the ndd settings. Confirm the default settings each time a system upgrade or applicable patch is completed.

Lock down remote access

To prevent remote hosts from gaining access to the system, lock down the files listed below with the method shown. This will prevent the entering of information into the files.

_____ **Lock down remote access**

- **/usr/bin/touch /.rhosts /.netrc /etc/hosts.equiv**
- **/usr/bin/chown root:root /.rhosts /.netrc /etc/hosts.equiv**
- **/usr/bin/chmod 000 /.rhosts /.netrc /etc/hosts.equiv**

Activate Logging

Not only should logging be activated to allow for review of system activity and maybe someday forensics, it should also provide obvious "keep out" warnings for those undesirables seeking access. The setup of notification and logging is a two-step process as follows:

_____ **Edit and/or replace the /etc/issue and /etc/motd files to include adequate "keep out" warnings with the following text:**

- **Warning: Authorized access only All violators are subject to prosecution**

_____ **Enable more logging with the following:**

- **Edit the /etc/syslog.conf file and uncomment the auth.notice entry**
- **/usr/bin/touch /var/adm/loginlog**
- **/usr/bin/touch /var/adm/sulog**
- **/usr/bin/chmod 600 /var/adm/loginlog /var/adm/sulog**
- **/usr/bin/chown root:sys /var/adm/loginlog /var/adm/sulog**

Rotate the logs on a regular basis. The script will only be kept the generated logs for four weeks. The script used was duplicated from "The SANS Institute Solaris Security Step by Step Version 2.0" guide, Appendix E. System backups will be used to retrieve logs of longer ages.

_____ Create the following script (between the ----------)

```
Start ----------Script
#!/bin/ksh
# rotate – A script to roll over log files
# Usage:   rotate /path/to/log/file [ mode [ #revs] ]

FILE=$1
MODE=${2:-644}
DEPTH=${3:-4}

DIR=`dirname $FILE`
LOG=`basename $FILE`
DEPTH=$(($DEPTH – 1))

if [ ! –d $DIR ]; then
        echo "$DIR: Path does not exist"
        exit 255
fi
cd $DIR

while [ $DEPTH –gt 0 ]
do
        OLD=$(($DEPTH – 1))
        if [ -f $LOG.$OLD ]; then
                mv $LOG.$OLD $LOG.$DEPTH
        fi
        DEPTH=$OLD
done

if [ $DEPTH –eq 0 –a –f $LOG ]; then
        Mv $LOG $LOG.0
fi

cp /dev/null $LOG
chmod $MODE $LOG

/etc/rc2.d/S74syslog stop
/etc/rc2.d/S74syslog start
End ----------Script
```

_____ **Create the following crontab entries for root.**

- 15 2 * * 0 /usr/local/bin/rotate /var/log/authlog 600 4
- 15 2 * * 0 /usr/local/bin/rotate /var/log/sulog 600 4
- 15 2 * * 0 /usr/local/bin/rotate /var/log/loginlog 600 4

Enable Accounting

Enabling accounting will provide additional methods for tracking changes to "normal" activity over time. This can sometimes provide that, ever so subtle, documented change that will lead to further investigation. Obviously a baseline needs to be available as to compare the outputs that accumulate over time. Start the baselines immediately when the system is put into production. It is likely the baseline will shift over time, thus updating the baseline on a monthly basis is recommended. "The SANS Institute Solaris Security Step by Step Version 2.0" guide was used as a guideline for the frequency and type of accounting to be enabled.

_____ Enable the "sa1" accounting scripts with the following changes to the "sys" user contrab.

- 20,40 8-17 * * 1-5 /usr/lib/sa/sa1
- 5 18 * * 1-5 /usr/lib/sa/sa2 –s 8:00 –e 18:01 –i 1200 -A

_____ **Edit the /etc/init.d/perf file and uncomment the two conditionals. (i.e. the two if/fi entries)**

Securing Remote Connections

TCPWrappers

Installing the TCP Wrappers provides the ability control access to services by IP address. Using the pre-compiled packages from the http://www.sunfreeware.com site provides a simple yet secure way to install the package. Always make sure to confirm the checksums of each package.

_____ **Install TCP Wrappers**

- **Download the "tcp_wrapper" from the sunfreeware site**
- **ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/tcp_wrappers-7.6-sol8-sparc-local-gz**
- **Confirm the CHECKSUM of the package.**

unzip the TCP_Wrapper gzip file

- **/usr/bin/gunzip tcp_wrappers-7.6-sol8-sparc-local-gz**

pkgadd the TCP_Wrapper package

- **/usr/sbin/pkgadd –d ./tcp_wrappers-7.6-sol8-sparc-local**

Copy tcp_wrappers "tcpd" to the /usr/sbin folder for use in the next step.

- **/usr/bin/cp /usr/local/sbin/tcpd /usr/sbin/tcpd**

Modify the /etc/inetd.conf file to reflect tcp_wrappers tcpd will be used to monitor access to telnet services. Change the telnet line to look like:

- **telnet stream tcp6 nowait root /usr/sbin/tcpd in.telnetd**

Configure TCP Wrappers

Configuring the TCP Wrappers to provide access to services by sshd ONLY. Notification, by e-mail, of failed attempts will also be configured.

_____ **Configure TCP Wrappers**

Create the hosts.allow file and set the appropriate ownership and permissions.

- **Create the /etc/hosts.allow file with the following contents:**

  sshd: ALL

- **/usr/bin/chown root:root /etc/hosts.allow**
- **/bin/chmod 600 /etc/hosts.allow**

Create the /etc/hosts.deny file and set the appropriate ownership and permissions:

- **Create the /etc/hosts.deny file with the following contents:**

  **ALL: ALL: **
  spawn (/usr/bin/mailx –s "[tcp/wrappers] DENY Access from %s connection attempt from %a" root@web1.localdomain.com**) : **
  DENY

- **/usr/bin/chown root:root /etc/hosts.deny**
- **/bin/chmod 600 /etc/hosts.deny**

OpenSSL and OpenSSH

Installing the OpenSSL and OpenSSH provides the ability for secure connections to the system. Using the pre-compiled packages from the http://www.sunfreeware.com site provides a simple yet secure way to install the package. Always make sure to confirm the checksums of each package.

_____ **Install OpenSSL and OpenSSH**

Download the "libgcc" package from sunfreeware.com

- **ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/libgcc-3.0-sol8-sparc-local.gz**

Download the "openssh" package from sunfreeware.com

- **ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/openssh-2.9p2-sol8-sparc-local.gz**

Download the "openssl" package from sunfreeware.com

- **ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/openssl-0.9.6b-sol8-sparc-local.gz**

- **Confirm the CHECKSUM of the packages**

unzip the three download files

- **/usr/bin/gunzip libgcc-3.0-sol8-sparc-local-gz**
- **/usr/bin/gunzip openssh-2.9p2-sol8-sparc-local-gz**
- **/usr/bin/gunzip openssl-0.9.6b-sol8-sparc-local-gz**

_____ **pkgadd the three packages**

- **/usr/sbin/pkgadd –d ./libgcc-3.0-sol8-sparc-local**
- **/usr/sbin/pkgadd –d ./openssl-0.9.6b-sol8-sparc-local**
- **/usr/sbin/pkgadd –d ./openssh-2.9p2-sol8-sparc-local**

Configure SSH

_____ **Configure SSH**

Modify the /usr/local/etc/sshd_config file to look like the following and complete the commands listed after the contents of the file:

```
#       $OpenBSD: sshd_config,v 1.38 2001/04/15 21:41:29 deraadt Exp $
```

```
# This sshd was compiled with
PATH=/usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin

# This is the sshd server system-wide configuration file.  See sshd(8)
# for more information.

Port 22
ListenAddress 0.0.0.0
HostDSAKey /usr/local/etc/ssh_host_dsa_key
HostKey /usr/local/etc/ssh_host_key
ServerKeyBits 1024
LoginGraceTime 180
KeyRegenerationInterval 900
PermitRootLogin no

IgnoreRhosts yes
RhostsRSAAuthentication no
IgnoreUserKnownHosts yes
StrictModes yes
X11Forwarding no
X11DisplayOffset 10
PrintMotd no
KeepAlive no

# Logging
SyslogFacility AUTH
LogLevel INFO
#obsoletes QuietMode and FascistLogging

RhostsAuthentication no
#
# For this to work you will also need host keys in
/usr/local/etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
#
RSAAuthentication yes

PasswordAuthentication yes
PermitEmptyPasswords no

CheckMail no
UseLogin no

Subsystem   sftp  /usr/local/libexec/sftp-server
```

Copy the /usr/local/etc/sshd_config to the /etc folder and set the appropriate ownership and permissions.

- **/usr/bin/mv /usr/local/etc/sshd_config /etc**
- **/usr/bin/chown root:root /etc/sshd_config**
- **/usr/bin/chmod 600 /etc/sshd_config**

Create Protocol 1 & 2 Keys

_____ Create the Server key files with the following command

- **/usr/local/bin/ssh-keygen –b 1024 –N '' –f /usr/local/etc/ssh_host_key**
- **/usr/local/bin/ssh-keygen –d –N '' –f /usr/local/etc/ssh_host_dsa_key**

Create SSH Startup

_____ Create the SSH startup file and set the appropriate ownership and permissions. The startup script will have the following contents (between the ------):

Start----------Script

```
#!/sbin/sh

case "$1" in
'start')

      if [ -x /usr/local/sbin/sshd -a -f /etc/sshd_config ]; then
            /usr/local/sbin/sshd-f /etc/sshd_config
      fi
      ;;
'stop')
      kill 'cat /etc/sshd.pid'
      ;;
*)
      echo "Usage: $0 { start | stop }"
      ;;
esac
exit 0
```

End----------Script

Set the appropriate permissions with the following command:

- **/usr/bin/chmod 744 /etc/init.d/s75sshd**

Create the link for the startup file with the following commands:

- **/usr/bin/cd /etc/rc2.d**
- **/usr/bin/ln –s /etc/init.d/s75sshd S75sshd**

Preventing Core file Creation

The "core" output contains the memory image of an executing process, which has unexpectedly terminated. Typically this makes the core file valuable when troubleshooting the system during times of instability. This same content may be used by undesirables for the purpose of gathering information, thus it will be disabled. Should the

system become unstable and the need for a core file become necessary it may be enabled by reversing the change listed below:

_____ **Modify the /etc/system file as to not generate a core file by inserting the following line:**

- **set sys:coredumpsize = 0**

NTP Setup

One of the most important parts of logging is to keep accurate time as to allow for accurate forensics. The NTP packages which have already been loaded need now to be configured. The system will be set up as a NTP client. Configure NTP with the following:

_____ **Configure NTP**

- Find three secondary NTP servers and the administrative contacts from the public NTP server list. **http://www.eecis.udel.edu/~mills/ntp/servers.htm**
- **Contact the administrative contacts to receive permission for connecting.**
- **Update the /etc/ntp.conf file to include the three TNP servers. The contents of the file should following the form listed below:**
    - **server IPADDRESS**
    - **server IPADDRESS**
    - **server IPADDRESS**

Run ASET to strengthen default system security levels

_____ **Strengthen default system security levels**

Default access to system files and directories is not a secure as desired for a system exposed to the Internet. Sun has provided the Automated Security Enhancement Tool (ASET) for enhancing the default system security levels. ASET will be used to set the system files automatically according to the security level desired. The ASET utility has three levels that can be used: low, medium, or high. Since the system will be exposed to the Internet the highest level of security will be used. Use the following command to enable the highest security level:

- **/usr/aset/aset –l high**

The aset utility will complete its task in the background once started. ASET provides a tool for monitor the progress of the utility. Use "taskstat" to check the current status of the aset run as follows:

- **/usr/aset/util/taskstat**

The ASET utility creates reports that can be found in: /usr/aset/reports/latest/*.rpt. Review them once the tasks are complete with the following command:

- **/usr/bin/more /usr/aset/reports/latest/*.rpt**

Loading iPlanet IWS 4.1sp2

_____ Work with IWS administrator to secure IWS 4.1sp2

An in-depth discussion on the installation/configuration and hardening of this application is beyond the scope of this document, yet the basics that are important for the installation and configuration can be highlighted. The system administrator, which will be assumed is not a IWS administrator, must work closely with the IWS administrator to insure the system is secure. Ultimately, the two together will be responsible for minimizing the security vulnerabilities present.

Some items to review/discuss with the IWS administrator:

- Make certain that the server runs with minimal privileges
- The web server should never be started with root or administrator ID's
- Remove unnecessary options from default HTML pages provided from the manufacturer; e.g. Web Publishing from a standard search
- Remove unnecessary accounts and groups from the web server's LDAP directory
- All web servers will have maximum logging enabled with output directed to a log server
- All old and sample scripts, web pages, and graphics files will be immediately removed from the server when they are not necessary to deliver the servers information.
- Validate that only content is indexed.
- All web pages, scripts and graphics will be set for ownership to the web server account that is used for initializing the server
    - After they have been placed in their directories permissions on these files will be set to read only
- The server will be set to disallow direct or indirect reading of directory structure or content
- All visual references to the server type, software type and version will be removed from web pages
- Disable the display of target IP addresses in web pages such that web browser status bars only display the targets name

File System Hardening

The Solaris Operating system provides several mount options that increase security when used effectively. The mounting of the /usr file system read-only will protect the OS binaries from being replaced with trojan horse programs or other unwanted modification. Since set-user-ID files can be used by attackers to create ways to gain higher privileges the "nosuid" option will be used to force all set-user-ID programs to execute with normal privileges on the non-root file systems. Make the following changes to the /etc/vfstab:

_____ Make the following modification to the /etc/vfstab file for the /usr file system.

- **/dev/dsk/cXtXdXsX /dev/rdsk/cXtXdXsX /usr ufs 1 no ro**

_____ Make the following modifications to the /etc/vfstab for the /var and /opt

- **/dev/dsk/cXtXdXsX /dev/rdsk/cXtXdXsX /var ufs 1 no nosuid**
- **/dev/dsk/cXtXdXsX /dev/rdsk/cXtXdXsX /opt ufs 1 no nosuid**

Note: The /usr file system may be remounted with the "mount –o remount, rw /usr" command when patches and/or packages need to be loaded. The only way to reset back to the "ro" is with a system reboot.

Verification

_____ **Verification of system security**

Verification of the configuration is as important as the hardening of the system. It provides the opportunity to uncover flaws and/or vulnerabilities that have been over looked or miss-configurations. The verification will be done as follows:

_____ **Confirm OBP can't be accessed with out password**

Confirmation can be done with the following:

- **Halt the system with:**
  - **/usr/sbin/init 0**
- **Confirm the system does NOT provide ok> prompt**
  - **If configured correctly the system will present:**

    Type boot, go (continue), or login (command mode)
    >

_____ **Confirm auto-boot is configured properly**

Confirmation can be done with the following:

- **Halt the system with:**
  - **/usr/sbin/init 0**
- **Power cycle the system, if configured correctly the system will complete the boot process**

_____ **Confirm patches are current with new run of PatchCheck**

Patches are being released on a daily basis so double-checking the patches one last time is important.

- **See the section titled "Using "PatchCheck" to Complete Patching" in the document**

_____ **Confirm automatic system reconfigure can't be executed**

Confirmation can be done with the following:

- **Create the file /etc/.UNCONFIGURED**
  - **/usr/bin/touch /etc/.UNCONFIGURED**
- **Reboot the system, if configured correctly the system will NOT ask for reconfiguration**
  - **/usr/sbin/init 6**
- **To avoid possible unexpected consequences down the road remove the /etc/.UNCONFIGURED file after a successful reboot.**
  - **/usr/bin/rm /etc/.UNCONFIGURED**

_____ **Confirm NFS mounts can't automatically be done**

Confirmation remote NFS mounts can't be done with the following:

From a remote host try to NFS mount the /, /usr, /var, and /opt folders with the following command:

- **/usr/bin/mount –F nfs web1:/ /mnt**
- **/usr/bin/mount –F nfs web1:/usr /mnt**
- **/usr/bin/mount –F nfs web1:/var /mnt**
- **/usr/bin/mount –F nfs web1:/opt /mnt**

Each of the mounts should FAIL with an error such as:

nfs mount: web1: : RPC: Rpcbind failure – RPC:

_____ **Confirm NFS exports can't automatically be done**

Confirmation exports of the /, /usr, /var and /opt can't be done automatically with the following:

- **Populate the /etc/dfs/dfstab file with the following lines**

  share –F nfs /
  share –F nfs /usr
  share –F nfs /var
  share –F nfs /opt

Reboot the system to confirm export of the filesystems does not occur:

- **Reboot the system**
  - **/usr/sbin/init 6**
- **Confirm NO sharing has been done, by confirming the output of the following command is NULL.**
  - **/usr/bin/share**

  The output MUST be NULL!

- **To avoid possible unexpected consequences down the road remove the /etc/dfs/dfstab file after a successful reboot.**
  - **/usr/bin/rm /etc/dfs/dfstab**

_____ **Confirm connectivity can only be established in with SSH**

Confirmation can be done with the following:

- **From a remote host run the following command:**
  - **telnet web-1**

  This should fail and send an e-mail to root verifying the DENY

- **From an OpenSSH client, which has port forwarding configured for telnet, open the browser and run the following command:**

  - **telnet://localhost:23**

Use "netstat –an" to verify the telnet connection establish over the "127.0.0.1.23" port on the Sun system, thus verifying the telnet has been established via SSH.

- **/usr/bin/netstat –an**

  Look for telnet over 127.0.0.1.23

_____ **Confirm that root can't login with SSH**

Confirmation can be done with the following:

Use OpenSSH client to attempt telnet connection as root.

- **telnet localhost:23**
- **Attempt login with "root" login and password**

  Login should fail with authentication failure.

_____ **Confirm that unwanted services are NOT running (i.e. RPC, routed etc…)**

Confirmation can be done with the following:

- **/usr/bin/ps –ef**

  Confirm NO "rpc" or "route" ANYTHING is running

_____ **Run Nmap against the system for confirmation of services available**

Using nmap to check system vulnerabilities is a great way to find unknown vulnerabilities. Download the nmap utility from the following web site.

- **Download the nmap utility from www.nmap.org**
- **Run nmap with the following flags to determine open ports**
  - Nmap –sT –p 1-65535 –O –I IP_ADDRESS_web-1

  Review discovered and listening ports for validity.

Disaster Recovery and/or Backup

Making a complete backup of the system is just as important as hardening the system. The system becoming inoperable and a timely restore not being possible is a Denial of Service is it not? Complete the backup and store the tapes in a safe off-site location and repeat at predetermined intervals.

_____ **Make a complete ufsdump of the system with the following commands:**

- **/usr/sbin/ufsdump 0ucf /dev/rmt/0un /dev/rdsk/cXtXdXsX**
- **/usr/sbin/ufsdump 0ucf /dev/rmt/0un /dev/rdsk/cXtXdXsX**
- **/usr/sbin/ufsdump 0ucf /dev/rmt/0un /dev/rdsk/cXtXdXsX**
- **/usr/sbin/ufsdump 0ucf /dev/rmt/0u /dev/rdsk/cXtXdXsX**

Note: The ufsdump above assumes the backup will be done in the following order /, /usr, /var, /opt with the last ufsdump rewinding the tape.

- **Store the backup in a secure off-site location and repeat at applicable intervals**

Physical Security

Physical security is one of those items that get taken for granted to often. Although physical security is getting more attention now than just a few years ago, far to many are naive to the risks that are exposed for those lacking a physical security policy. The use of a physical security policy to thwart Social Engineering and disgruntled employees is just as important as hardening the system.

_____ **Create a physical security policy that includes the following areas:**

- **Building access policies and procedures**
- **Computer area access policies and procedures**
- **Networking closet access policies and procedures**
- **Environmental controls**

Join Sun Security Bulletin mailing list

_____ **Complete Sun Security Bulletin Subscription**

Joining the Sun Security Bulletin mailing list will keep the administrator current on the latest security events pertaining to the Solaris Operating Environment. To receive security bulletins directly from the Sun Security Coordination Team, send an email to security-alert@sun.com and include subscribe cws *[your email address]* in the subject. For example: *subscribe cws alex.smith@sun.com*

References

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

Noordergraff, Alex, Solaris Operating Environment Minimization for Security: A Simple, Repoducible and Secure Application Installation Methodology; Sun BluePrints OnLine, November 2000. http://wwwswest.sun.com/blueprints/1100/minimize-updt1.pdf

Noordergraff, Alex, Watson, Keith, Solaris Operating Environment Security; Sun BluePrints Online, January 2000. http://www.sun.com/blueprints/0100/security.pdf

Reid, Jason, Watson, Keith, Building and Deploying OpenSSH for the Solaris Operating Environment; Sun BluePrints Online, July 2001. http://www.sun.com/blueprints/0701/openSSH.pdf

Watson, Keith, Noordergraff, Alex, Solaris Operating Environment, Network Settings for Security; Sun BluePrints Online, December 2000. http://wwwwswest.sun.com/blueprints/1200/network-updt1.pdf

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

Sun Microsystems, Advanced Installation Guide Solaris 8; Sun Microsystems, Inc. 2001

Sun Microsystems, ASET Man Pages; Sun Microsystems, Inc. 2001. http://docs.sun.com/ab2/coll.40.6/REFMAN1M/@Ab2PageView/16947?DwebQuery=aset&oqt=aset&Ab2Lang=C&Ab2Enc=iso-8859-1

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
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**