Global Information Assurance Certification Paper

Using Solaris 9 and Syslog-ng to Implement a Central Log Server

John T. Douglass
GCUX Practical Assignment Version 1.9

Abstract: This paper presents a step-by-step procedure for utilizing a Sun SPARCstation 5 running Solaris 9, with additional software packages such as Syslog-ng and IP Filter, as a centralized log server.

1. Introduction

GIAC Laboratory is a government research laboratory. During a routine internal cyber security audit, it was discovered that there was a deficiency in the logging of data from various networking equipment related to one of the research facilities. Although logging of the firewall access data was performed, it was not centralized. Furthermore, additional data was not logged for the network equipment located inside the facility.

GIAC Laboratory's Unix security administrator was asked to confer with the network administrator regarding the establishment of a secure centralized log server.

The facility network is an isolated network consisting of 6 network cabinets configured in a star. There are two bastion hosts, each with two network interfaces. Each bastion host is further protected by a Cisco PIX 515 firewall. A general network diagram is provided in Appendix A. The proposed central server will be an additional bastion host utilizing two network interfaces to log data both from the isolated network and the PIX firewall protecting the bastion hosts.

2. Description of System

The system hosting the centralized log server will be running Sun Solaris. The laboratory has an existing policy standardizing Unix services using the Solaris OE. All system administrators at GIAC Laboratory are familiar with the installation and maintenance of the OS and there exists internal procedures and policies governing the secure installation and maintenance of Solaris.

Due to limited resources, GIAC Laboratory decided to utilize existing hardware that was scheduled to be retired. A single centralized log server is currently configured, a redundant log server is highly recommended.

The hardware and software used consists of a Sun SPARCstation 5 running at 85Mhz with 64MB RAM installed. There are two Sun 2.1GB SCSI disks and a 4x CDROM installed internally. The system has a SunSwift card installed (combination SCSI and 10/100 Ethernet card) with an Exabyte 8505 XL 8mm tape drive attached. Although the system had a TGX graphics card, no keyboard/monitor/mouse were available, a laptop running Microsoft Windows 95 was attached to the serial port for use as a console during the install.

The following operating system and software will be configured:

- Solaris 9
- syslog-ng version 1.4.15

- IP Filter version 3.4.28
- Advanced Intrusion Detection Environment (AIDE) version 0.9
- Psionic LogSentry 1.1.1

Additional software is required for the compilation and installation of syslog-ng and AIDE. This software is covered further in the step-by-step procedure.

The centralized log server will serve as the loghost for eight or more Cisco network switches and two or more Cisco PIX 515R firewalls. The server will be the historical archive for the logs. Additional hosts and equipment may be configured at a later date to utilize the centralized log server.

The Unix security and system administrator will be responsible for the configuration and management of the system. The network administrator will have access to the system and the information stored in the logs. The log auditing performed by LogSentry will be emailed to the network and system administrators.

The syslog-ng package will replace the Solaris default syslogd. This package provides for greater flexibility and filtering of logs from multiple hosts. For more information regarding syslog-ng please see [1, 3, 14].

IP Filter will be installed on the server as a secondary level of protection. Although the log server will reside behind a Cisco PIX 515R firewall, IP Filter will allow protection from harmful traffic which may have evaded the firewall as well as network traffic from the interior network which sits behind the firewall, see Appendix A. For more information regarding IP Filter please see [5, 13].

Psionic LogSentry will be installed in order to perform the automatic auditing of the various logs that are being gathered. For more information regarding LogSentry please see [12].

Finally, AIDE will be used on the server to ensure the integrity of the host. Reports generated by AIDE will be sent to the system administrator. For more information regarding AIDE please see [8, 9].

3. Risk Analysis

The adequate logging and auditing of the data gathered from the network switches and the firewalls is a cyber security performance measurement for GIAC Laboratory. As a government laboratory contractor, there are contractual implications if GIAC Laboratory fails to satisfactorily meet the performance measurements.

GIAC Laboratory has traditionally existed in an environment that encouraged the free exchange of ideas. Computers and networks were simply tools in this

environment. However, in recent years events have occurred which have raised cyber security awareness and have led to the inclusion of contractual performance measures related to cyber security. Although contractual obligations have been added, in many instances no additional funding has been secured to meet these obligations, as is the case with the central log server.

By utilizing available hardware, personnel experience, and freely available software installation it is hoped that installation time and future maintenance of the central log server will be minimized.

The data that is being logged to the central log server may be used in forensic analysis of a cyber security related occurrences and in the solving of unexpected networking problems. From a security standpoint it is vitally important that the data be secure. For instance, an intruder who is able to access the logs may successfully hide his or her tracks. The network equipment logs include information regarding the status of an interface, and interface unexpectedly coming up or down may be an indication of an intruder at work.

Minimal services will be configured to run on this system. The IP Filter based firewall will be configured to allow incoming traffic only to the related syslog ports (udp/tcp 514) and to the secure shell server (tcp 22). Accounts on the machine will be limited to system administrators and the network administrator with no exceptions.

The key security concerns for this system are:

1. **Unauthorized Physical Access**: A primary concern for any piece of computer or network equipment is physical access to the system allowing for the disabling of the equipment. GIAC Laboratory is a secured installation with armed guards on the premise at all times. Unrestricted access to the laboratory facilities is limited to employees. All visitors are required to be escorted while on the premises.

   The location of the server room is in a secured facility requiring approved key card access to enter the facility. Additionally, the entrance to the server room is secured using a combination lock.

   Power and HVAC requirements also pose a risk to the system. Each facility is equipped with redundant HVAC systems and building wide uninterruptible power supplies backed by diesel generators. Additionally, each of the bastion hosts, including the central log server, and the networking equipment have individual uninterruptible power supplies attached.

2. **Hardware / Software Failures leading to data loss:** Failure of any piece of hardware is to be expected at some point in time. The central log

server configuration here provides multiple single points of failure. Nightly archival of the daily logs is performed to ensure minimal loss of historical data in the event of a hardware or software failure. However, the nightly backups will do nothing to ensure minimal loss of data during the downtime caused by the failure. Each piece of networking equipment being logged can be configured to log to multiple hosts, it is recommended that a redundant log host be configured in the future.

3. **Software configuration error:** Configuration errors either of the system itself or the syslog-ng program constitute a large concern or threat. Misconfiguration of the syslog-ng may lead to loss of log data. It must be ensured by both the system and network administrators that all logging operations are performing as expected prior to approval of the completion of the installation.

4. **Remote/Local compromise:** Misconfiguration of the underlying platform may lead to remote or local compromise of the server.

   Remote compromise of the server is minimized in a two-pronged approach. First, the box is secured using a "best practices" methodology – install minimal software and services, securely configure those services which are installed, regular maintenance. Second, an IP Filter based firewall is installed to limit the exposure of the server on the network. In particular, only ports tcp/22 (ssh), udp/514(syslog), and tcp/514(syslog) are allowed incoming to access the machine.

   Local compromise of the machine is of lesser concern. GIAC Laboratory is extremely careful in hiring only those job candidates who pass the security and background checks. Access to the machine will be limited to the system administrator(s) and the network administrator. These individuals, given their administrative capacity, have the ability to directly circumvent any security measure in place.

4. Step-by-Step Installation of Solaris 9

The following step-by-step procedure was utilized to install and secure the centralized syslog server. There were three basic phases: base OS installation, additional software installation, and hardening of the system.

4.1 Pre-installation

Prior to installation software packages listed in Table 1 and the latest Solaris 9 Recommended Patch Cluster should be downloaded and burned on to a CDR. This will allow the installation of the latest recommended and security patches, as well as the additional software, to be performed prior to placing

the system on the network. The latest stable versions are listed, however newer stable versions may now be available.

Table 1: Additional Software to be Installed

Software	Location
syslog-ng version 1.4.15	http://www.balabit.hu/en/downloads/syslog-ng/downloads/
libod 0.2.23	http://www.balabit.hu/en/downloads/syslog-ng/downloads/
IP Filter version 3.4.28	http://coombs.anu.edu.au/~avalon/
AIDE version 0.9	http://www.cs.tut.fi/~rammer/aide.html
mhash version 0.8.16	http://mhash.sourceforge.net/
Psionic LogSentry 1.1.1	http://www.psionic.com/products/logsentry.html
CIS Solaris Benchmark	http://www.cisecurity.org/
Solaris 9 patch cluster	http://sunsolve.sun.com/

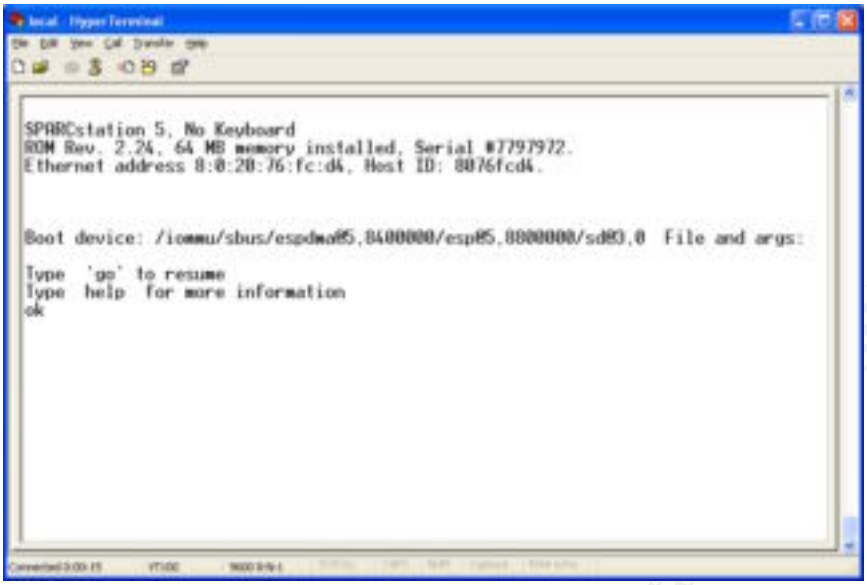
4.2 Installation of the base OS

Due to the limitation of the hardware being used for this server, the standard Solaris WebStart graphic installation could not be utilized. With the removal of the OpenLook environment in Solaris 9, the console based installation procedure using the command line interface (CLI) given below is nearly identical to the procedure when using the non-WebStart graphical installation. The difference between the two is discussed in step 2 below.

We will be performing an "initial" install of Solaris; if there is any existing data on the system that needs to be backed up please do so prior to beginning this procedure. Please ensure that the network cable is not plugged in and that the system is powered down. It is assumed that the system does not currently have a boot prom password.

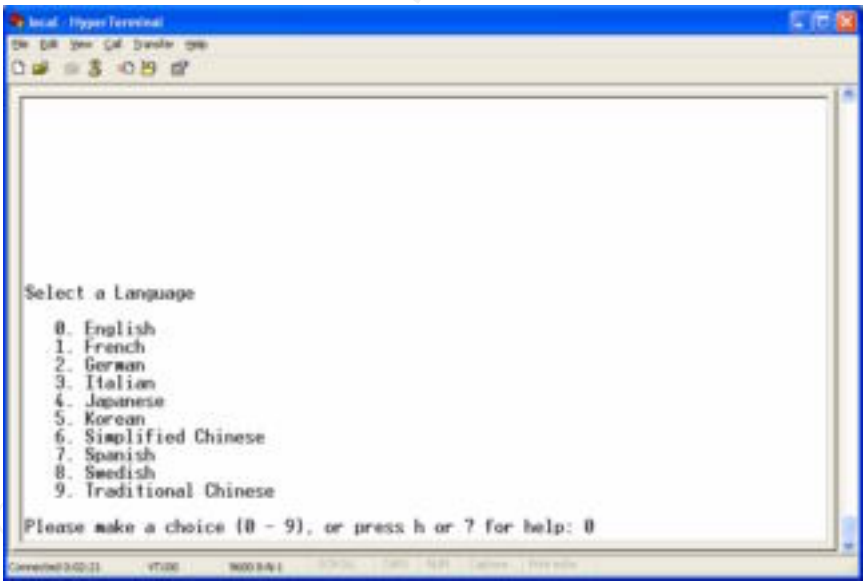
Prior to beginning the installation the administrator should know the following information for the system: machine name, ip address, netmask, primary Ethernet interface (hme0, le0, etc.), default router address, DNS server and search domains for the name service.

Following the instructions on the screen performs installation of the OS. In most instances, the "F2" key is used to proceed forward through the installation process. The "F6" key is used to provide additional help. The "Tab" or arrow keys may be used to move between selections, the "Return" or "x" can be used to make a selection.



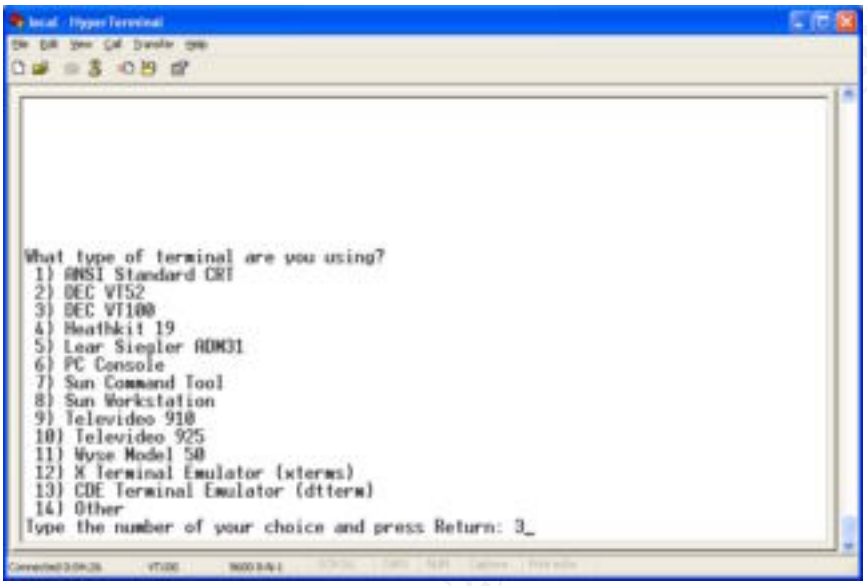
1. Power on the system. If you are using a serial console send a BREAK signal, if using a Sun keyboard press Stop-A (or L1-A on older keyboards) to attain the OpenBoot prompt. The console or screen should look similar to the above. Please insert the CD labeled “Solaris 9 Software 1 of 2” into the CDROM. At the OpenBoot prompt type:

   ```
   boot cdrom
   ```

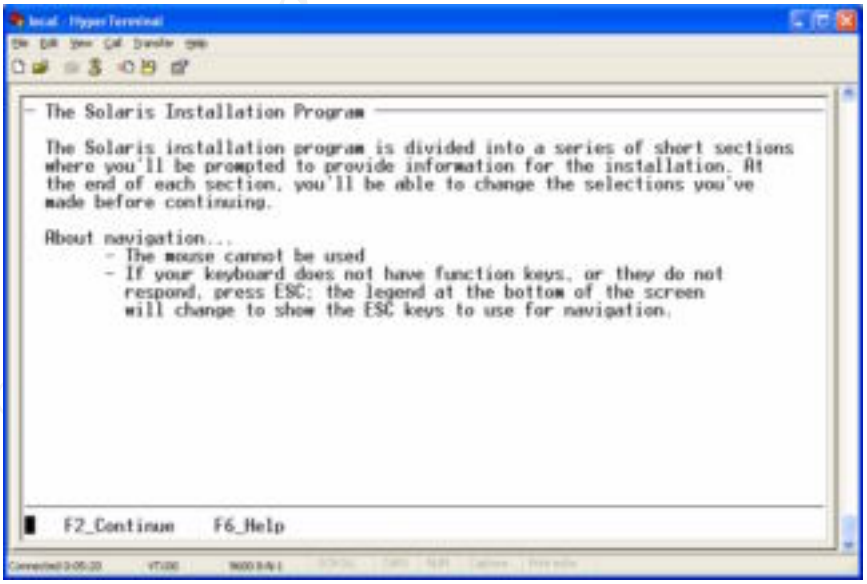


2. The Solaris install process will now automatically begin. Prior to entering the install environment, however, a choice of Language and Locale must be made. In my case, choosing option '0' when prompted for the Language (English) and Locale (7-bit ASCII) is appropriate. An example of the language choice screen is given above. After choosing

the language and locale, the graphic subsystem will start if available, and a console window will be placed in the middle of the screen with the installer ASCII based menu system. The following screen will be displayed if no graphics console is available:



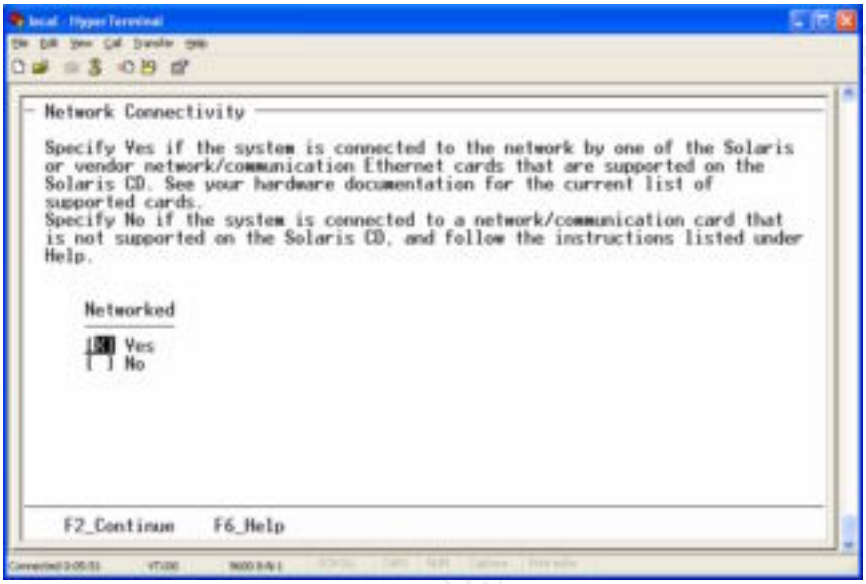
The only difference between installing from a serial console and a graphics based console is the screen above indicating what type of serial console is being used to perform the install. The appropriate



choice here was DEC VT100.

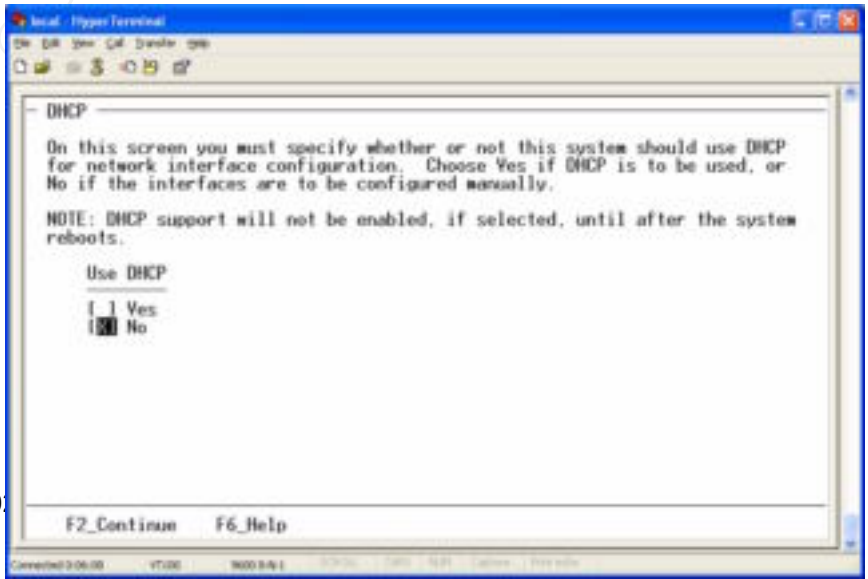
3. A general information screen is presented providing information regarding the navigation options in the Solaris Installation Program. In

this case, the HyperTerminal program has the ability to use the function keys as terminal keys. If the terminal does not have function keys or the terminal emulation program does not have this option, the user may follow the instructions on the screen regarding the use of

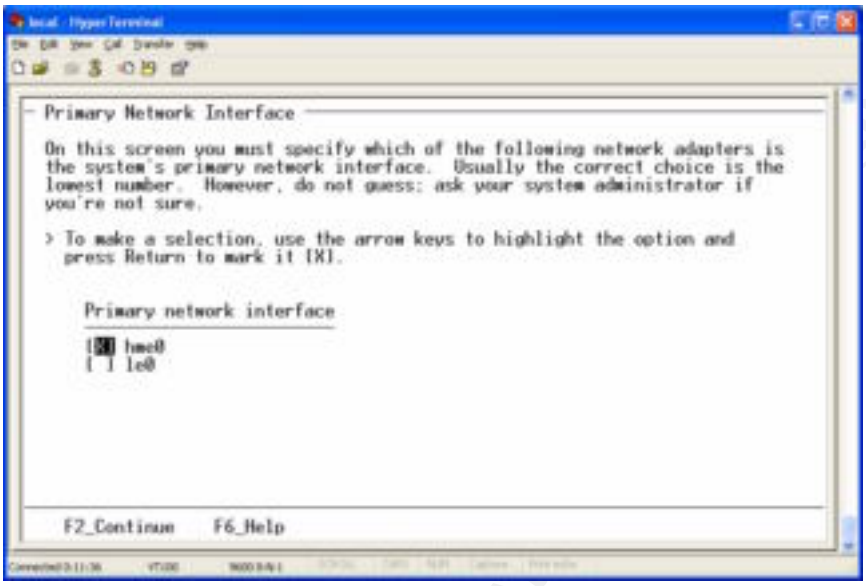


alternate key sequences to navigate the installation program.

4. After a second screen that confirms the desire to begin identifying the system, the above screen will appear. The correct answer in this case is “Yes” because although the system is not currently connected it shall be after installation is completed. Please select “Yes” and press “F2” to continue.

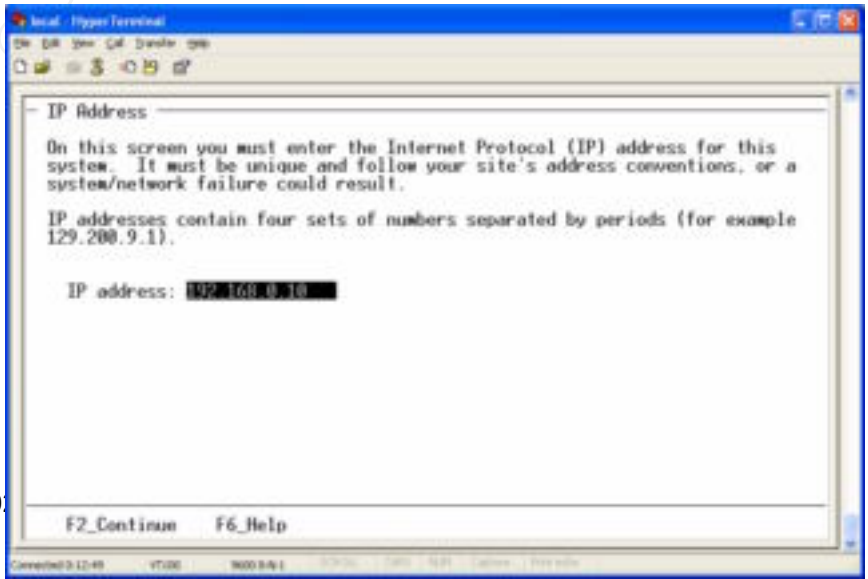


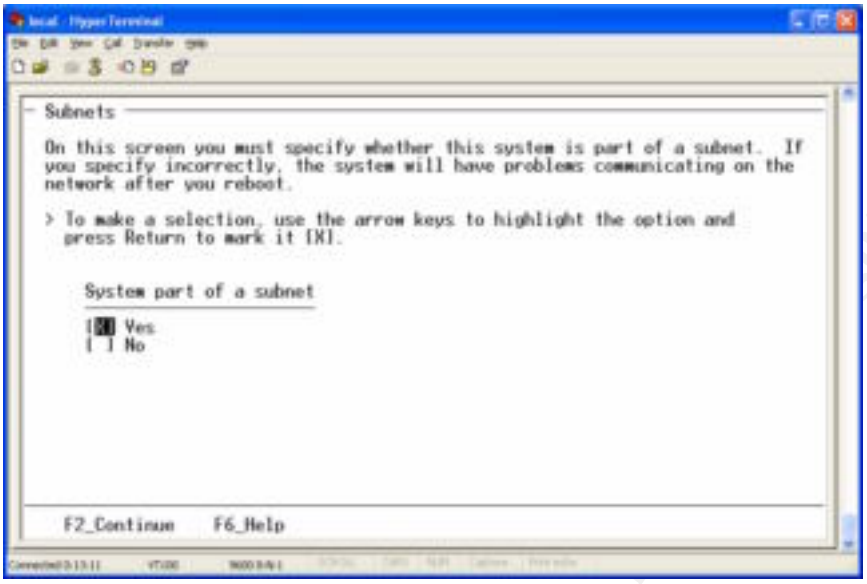
5. The next question the installation program asks regards whether the system uses Dynamic Host Configuration Protocol (DHCP) to



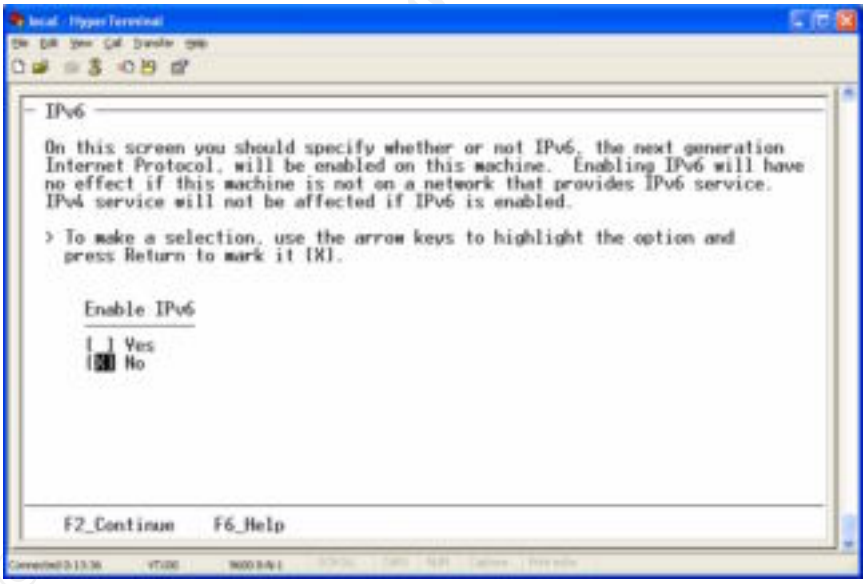
configure network interfaces. Please make sure “No” is selected and press “F2” to continue.

6. Next, the primary interface must be selected. In this instance, the “hme0” interface is chosen as the primary interface. This interface is a 10/100baseT interface, while the “le0” interface is a 10baseT only interface. Select the appropriate interface and press “F2” to continue.
7. After choosing the primary interface, the install program on successive screens will ask to enter the hostname and IP number. Enter the appropriate values for the host, hitting “F2” to continue to the next screen. The screen for entering the hostname is shown above.

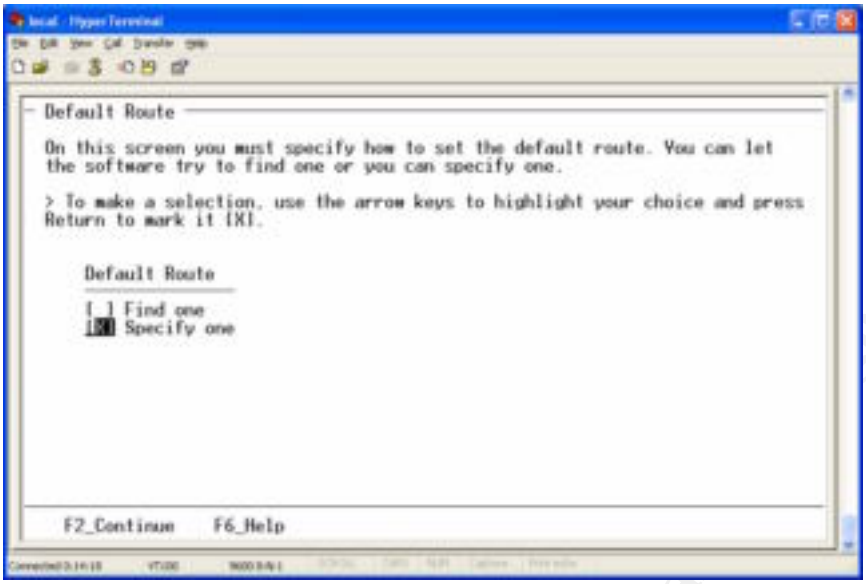




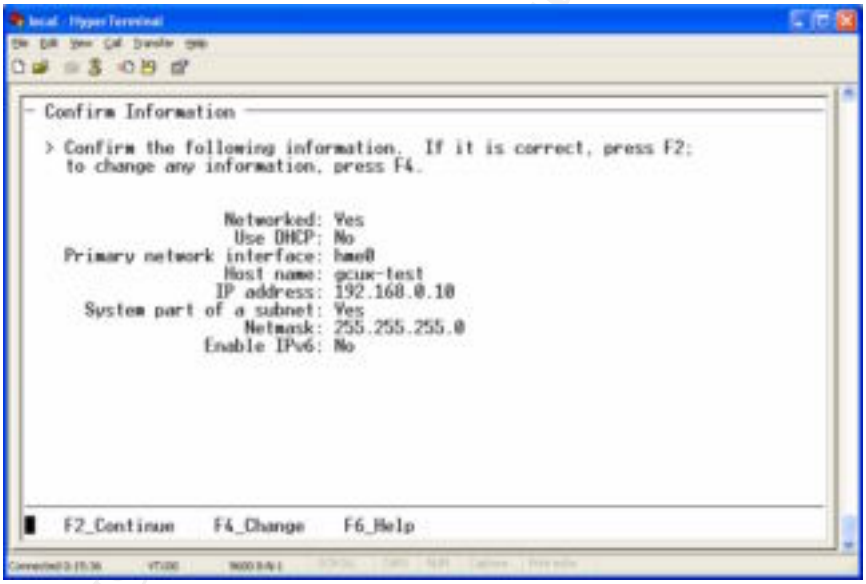
8. Next, the installer will ask if the system is part of a subnet. Answering "Yes" will be followed with a screen allowing for the input of a netmask for the system. For a typical installation, the appropriate answer is "Yes." Answering "No" will assume that no netmask is necessary and present the following screen.



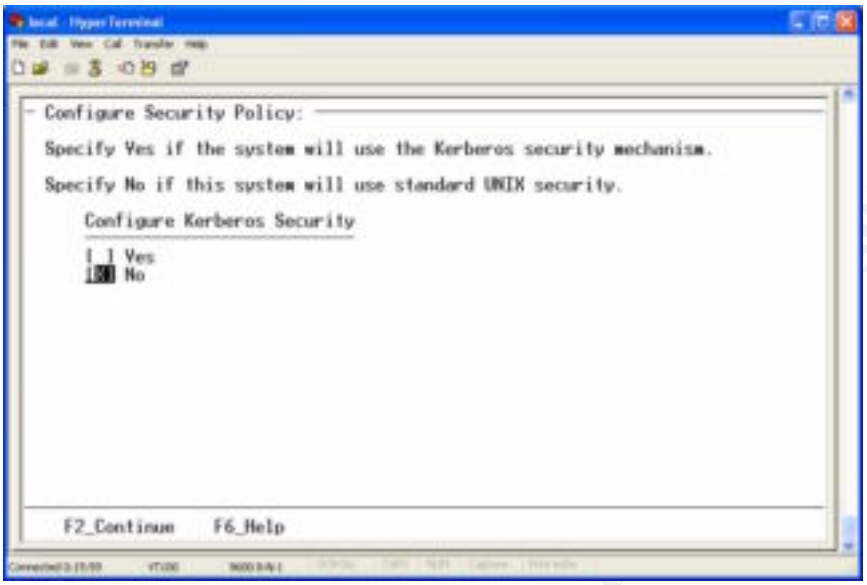
9. GIAC Laboratory has not migrated to IPv6 thus, the default answer of "No" is appropriate. Press "F2" to continue.



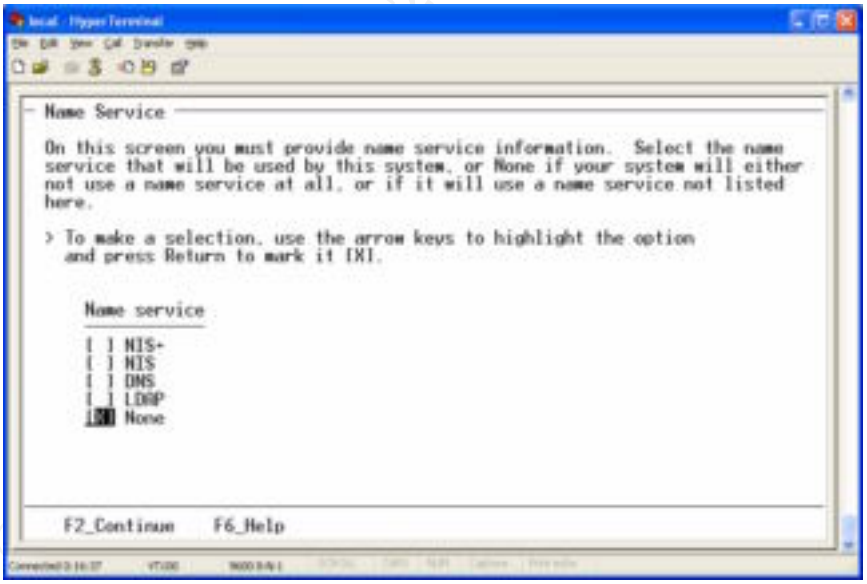
10. Next, the default router is specified. Please choose to “Specify one” and press “F2” to continue. On the ensuing screen, please enter the appropriate default route and press “F2” to continue.



11. After the setting of the default route, the installation program will ask the user to confirm the settings. If all information has been entered correctly the user may press “F2” to continue with the next phase of installation. If any information is incorrect, the user may press “F4” to return to the beginning of the network identification.

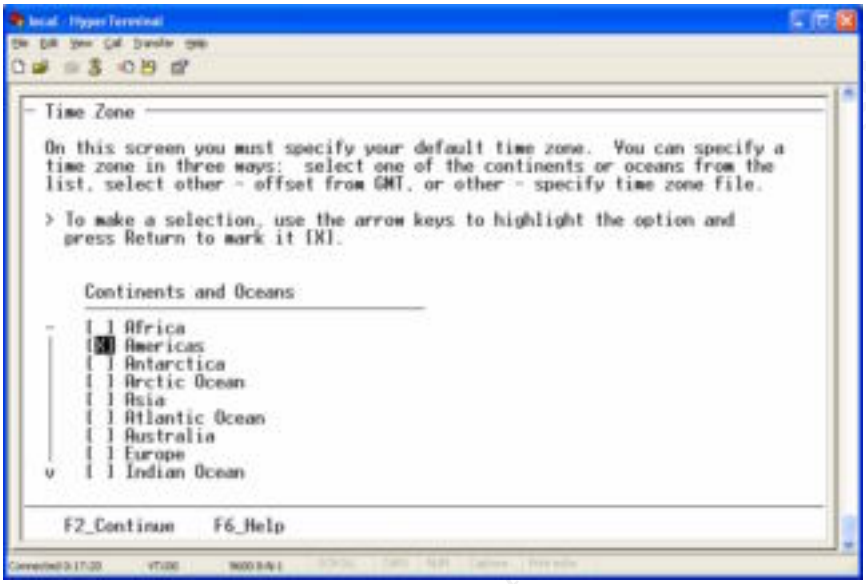


12. Next, the install program will configure the security policy. As Kerberos is not yet in use here at GIAC Laboratory we will not configure Kerberos at this time. The default for the screen is “No”, please hit “F2” to proceed. The following screen will ask for confirmation of this choice. Again, press “F2” to proceed.

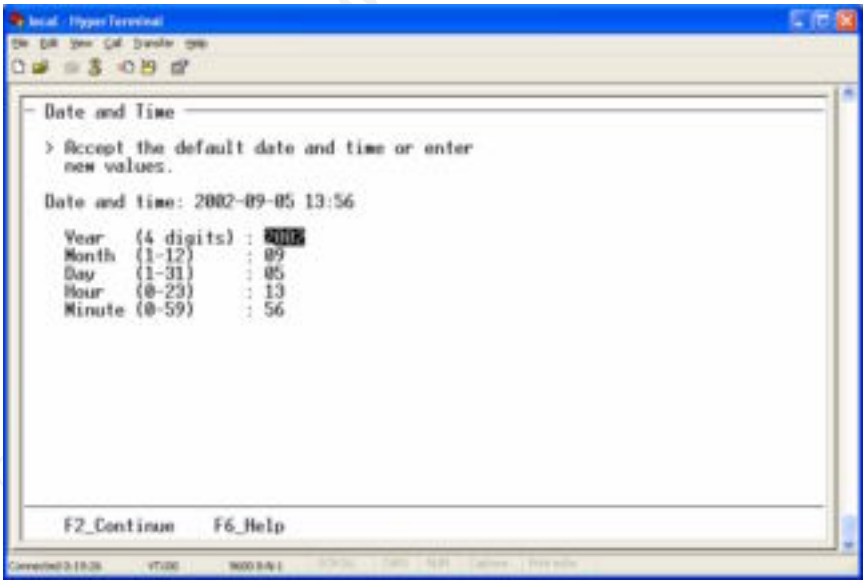


13. The next screen is used to configure the machine's primary name service. The default name service is “None.” For security and stealth only the local host file will be used for name resolution. This choice allows for this system to be completely independent. Since only a small number of machines will be configured to access this system, it will take minimal effort to maintain an up to date host file. Firewall log

rejections of unknown hosts can easily be resolved later. Hit “F2” to accept the choice of “None.” The subsequent screen asks for confirmation of this choice, hit “F2” to proceed.

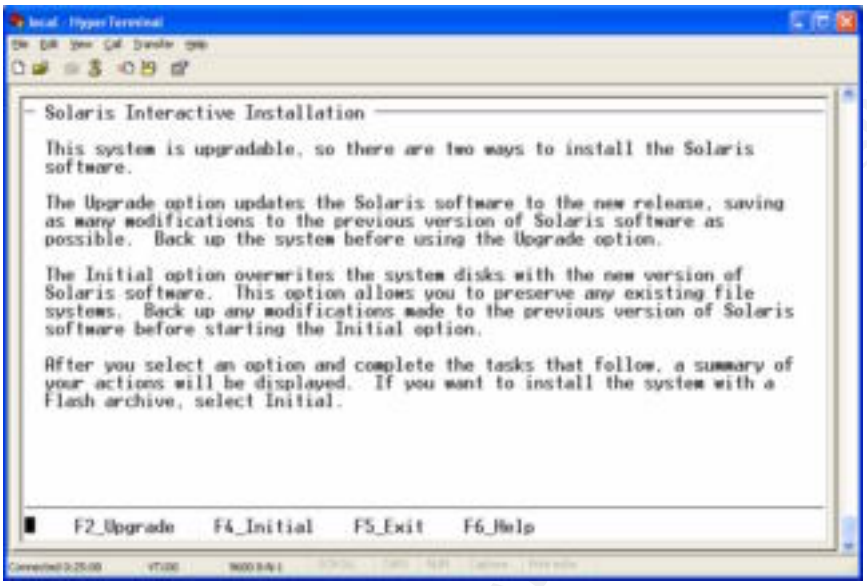


14. The next series of menus will configure the time zone. For installation at GIAC Laboratory we select “Americas,” “United States,” and “Mountain” on successive menus, pressing “F2” to continue.

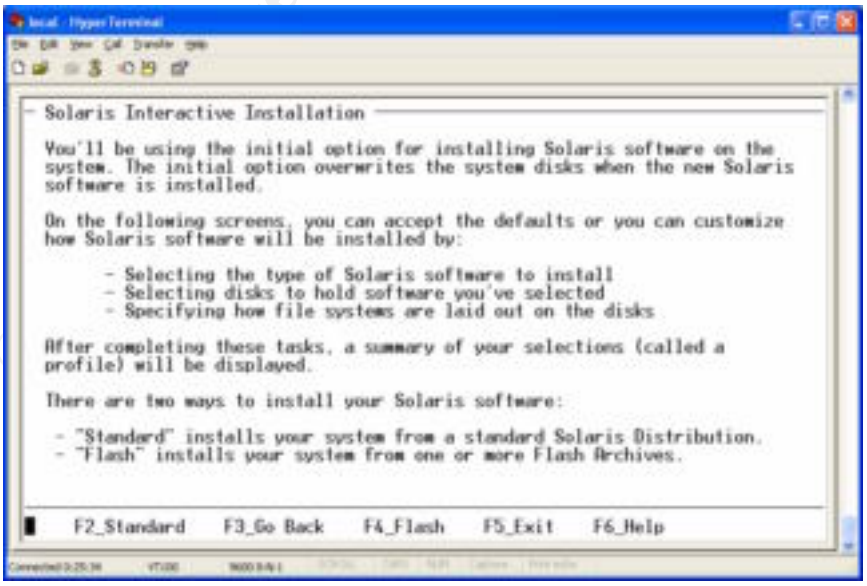


15. On the next screen, the current time and date are configured. Please adjust the time and date if necessary and press “F2” to continue. Following this menu, the user is asked to confirm the choice of time zone and the current date and time settings. Use “F2” to confirm the

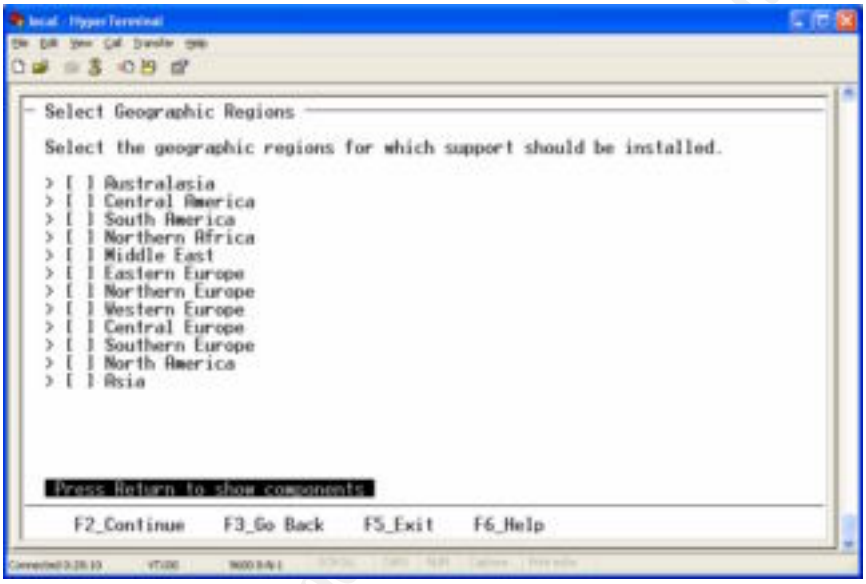
choices, use “F4” to return to the menu to change either value. This completes the system identification phase of the install program.



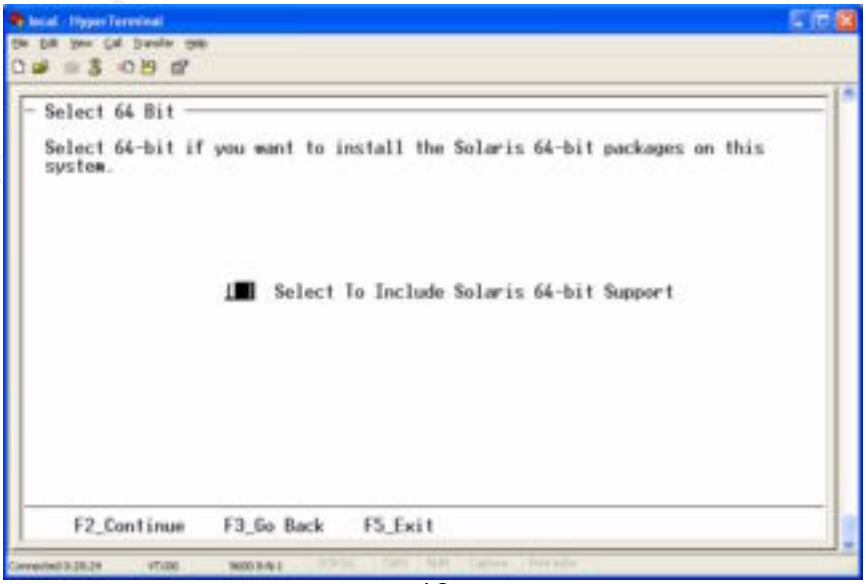
16. The next phase of the install program will allow for the selection of the software. The first menu presents a choice of two ways to install Solaris, either as an upgrade or as an initial install. It is highly recommended that the “Initial” install be chosen. The initial install method will ensure that there are no extra software packages and services installed, making for a more secure system. Press “F4” to choose the “Initial” install.



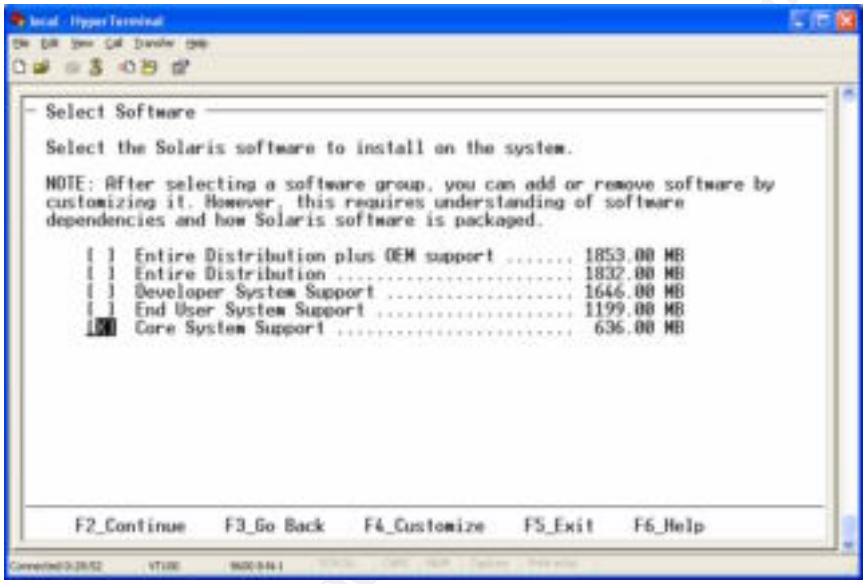
17. The next menu screen presents the options regarding the method of installing Solaris. Since Solaris 8 7/01, the “Flash” install method has been available. This allows the administrator to create a single reference image of a Solaris install on the network and then use that image to replicate to multiple hosts. This allows for rapid installation of machines that will be identically or similarly configured. However, GIAC Laboratory boxes are all custom installed and configured with wide ranges of hardware and software, for this reason the “Standard” method of installation is appropriate. Press “F2” to proceed.



18. The next menu presents a choice of geographic regions that should be configured. These are locales to be installed in addition to the local chosen at the very beginning of the install. There should be no reason to install further locales on the central log server. Press “F2” to proceed.



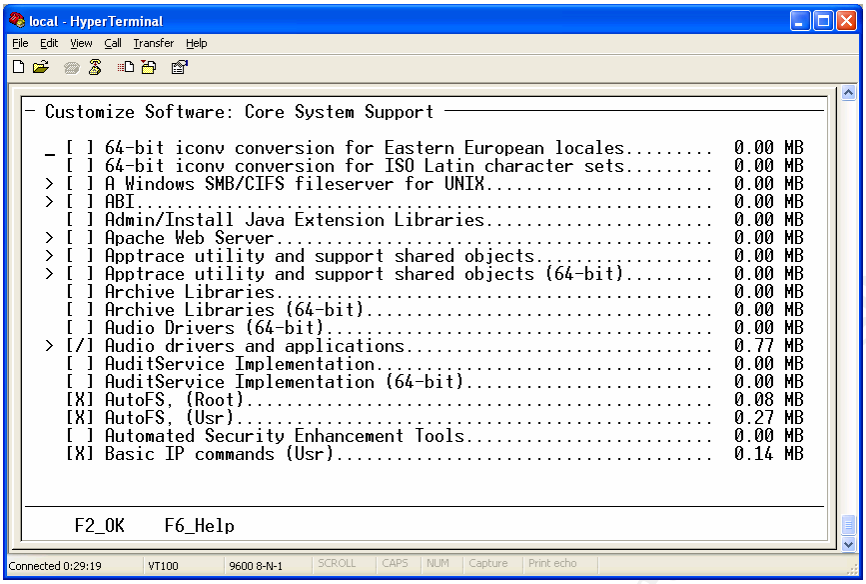
19. Solaris has fully supported the 64-bit architecture since Solaris 7. The sun4m architecture that the SPARCSstation 5 utilizes is a 32-bit architecture. The default of not installing 64-bit support should be chosen. The Solaris installer will automatically select inclusion of 64-bit support on those platforms that are capable of utilizing it. In that instance, the administrator may choose to override and install only the 32-bit version of Solaris. Press “F2” to continue.



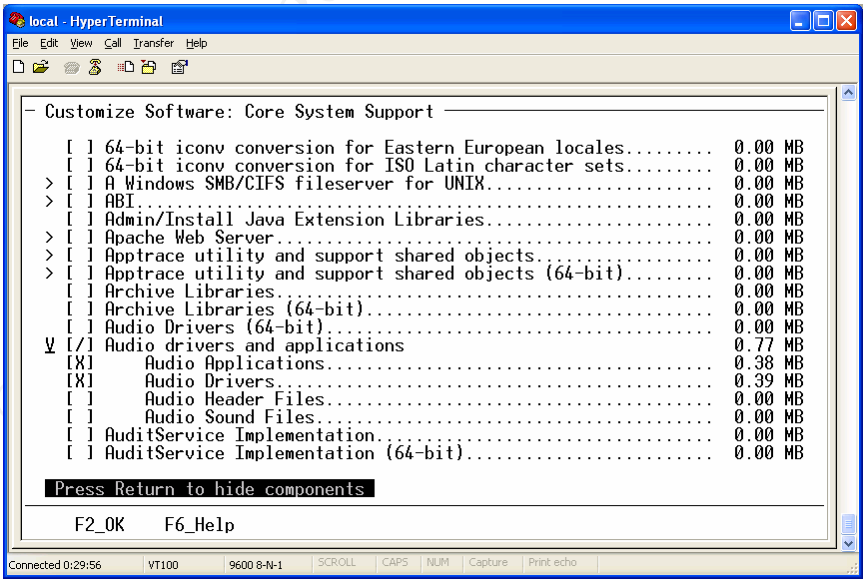
20. The next menu will allow for the choice of a software group. The Solaris install has several default software groups depending on what the system will be used for. In order to provide the most secure environment for our central log server choose the “Core System Support” and then press “F4” to further customize the system. During the customization of the core software unnecessary packages will be deselected. The “Core System Support” under Solaris includes such unnecessary software as the AutoFS file system, NFS and NIS client and server support, and many network daemons such as named and telnetd. By removing these packages prior to installing, we are ensuring a more secure system. The packages listed in Table 2 will not be needed on the log server and, thus, can safely be removed.

Table 2: Additional Solaris Software Packages to be Removed

Package	Description
SUNWauda	SunOS audio applications
SUNWaudd	SunOS audio device drivers
SUNWatfsr	Configuration and start-up of AutoFS file system
SUNWftpr	FTP Server Configuration Files
SUNWftpu	FTP Server and Utilities
SUNWkrbr	Kerberos version 5 support (Root)
SUNWkrbu	Kerberos version 5 support (Usr)
SUNWlldap	
SUNWnfscr	Network File System (NFS) client support (root)
SUNWnfscu	Network File System (NFS) client support (usr)
SUNWnfssr	Network File System (NFS) server support (root)
SUNWnfssu	Network File System (NFS) server support (usr)
SUNWnisr	Configuration files and directories for the Network Information System (NIS and NIS+)
SUNWnisu	utilities for the Network Information System (NIS and NIS+)
SUNWpiclr	PICL Framework init scripts
SUNWpiclu	PICL Daemon, Libraries, prtpicl client and plug-in modules
SUNWtnamd	Trivial Name Server (usr)
SUNWtnamr	Trivial Name Server (root)
SUNWssad	pln, soc, and ssd kernel device drivers
SUNWssaop	Administration utilities and firmware for SPARCstorage Array (SSA)
SUNWtnetd	Telnet Server Daemon (usr)
SUNWtnetr	Telnet Server Daemon (Root)

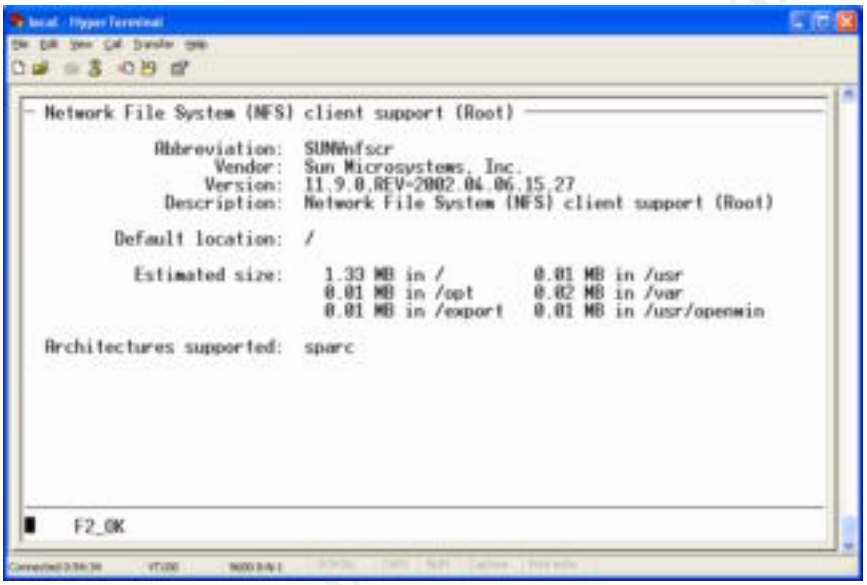


21. The software customization screen consists of four basic columns. The first column is used to indicate whether the listing is for a software cluster or an individual software package. An “>” in this column indicates that this is a cluster, in the screenshot above “ABI” is a software cluster. The second column indications whether the software is selected or not. An “X” in the column indicates the package is selected, a “/” indicates that a cluster is partially selected, and a “ “ in the column indicates nothing is selected. The third column gives a short package name or description. The fourth column indicates the amount of disk space each selected package or cluster will require.



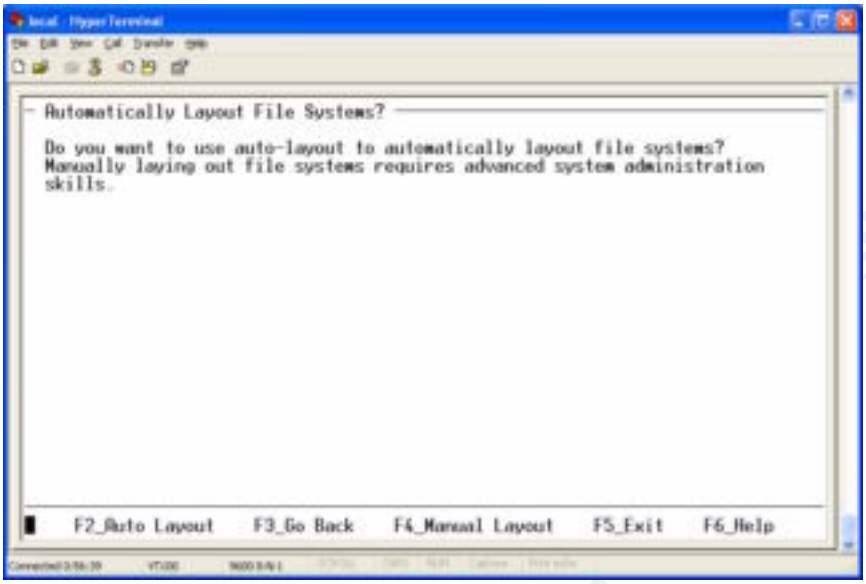
To navigate through the menu use the arrow keys. The left and right arrow keys allow you to choose which column. The up and down arrow keys allow for movement through the software list. As the user

navigates through the software and columns the menu at the bottom of the screen will change to indicate what allowable actions may be taken. For example, when the cursor is in the software cluster column and a cluster is indicated, a message will appear stating “Press return to show components.” Similarly, after showing the components a message will appear stating “Press return to hide components.” An example screen is shown above, the cursor is on the “Audio Driver and Applications” software cluster.

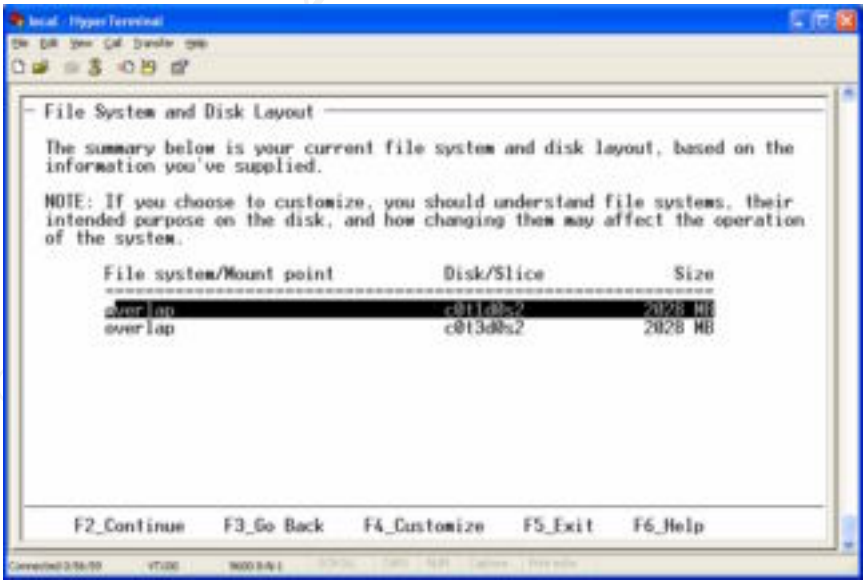


Similarly, when navigating through the selection column messages will appear indicating either “Press Return to select component” or “Press Return to deselect component.” If the navigation cursor is placed in the software column, the administrator may press return to receive information regarding the particular software module. An example information screen is shown above.

After deselecting the software listed in Table 2, press “F2” to continue.

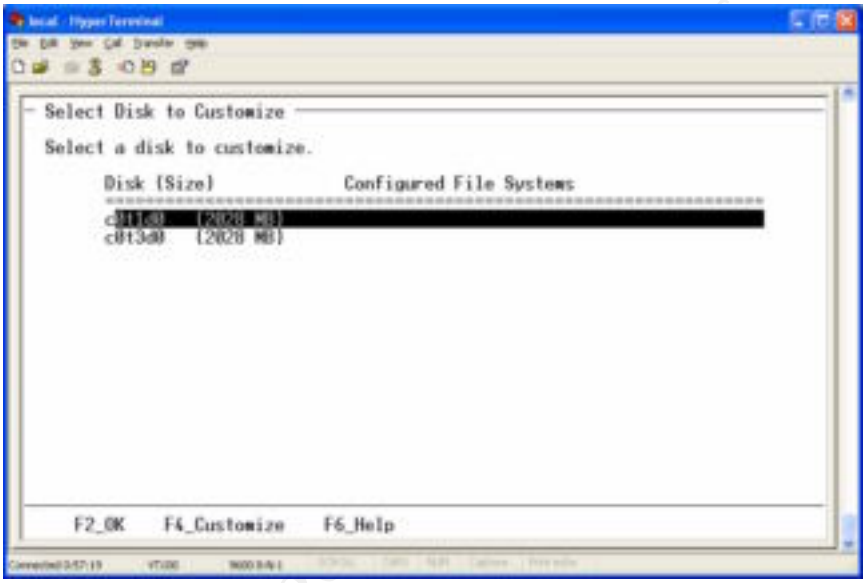


22. With the minimal software now selected, the final phase of the installation program is the selection and configuration of the hard disks in the system. On the test system, which has two 2GB drives, both drives will be selected to allow for maximum usage of disk space. By default only the boot drive will be selected, after selecting the secondary drive, press “F2” to proceed. The next screen will ask if existing data needs to be preserved, press “F2” to proceed.

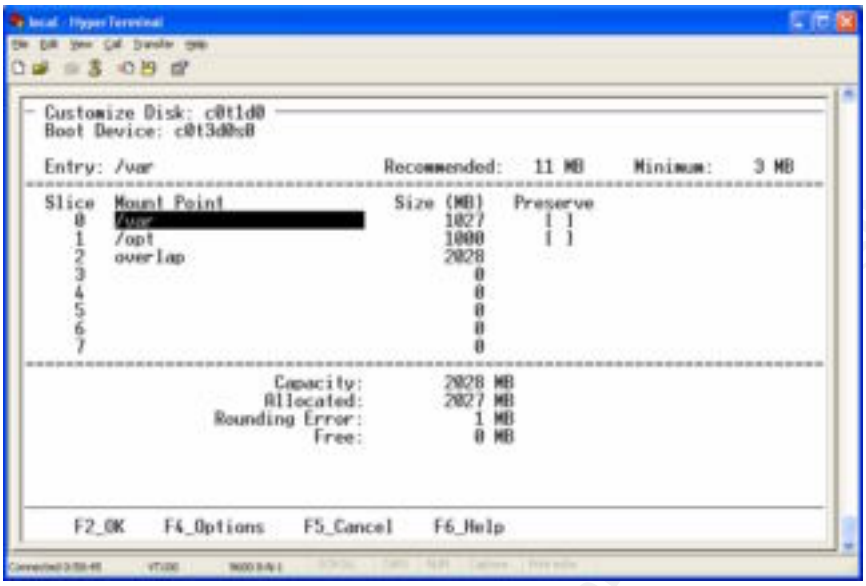


23. The next screen will determine what disk layout to use. There are two basic options, automatic layout and manual layout. From experience, I have found the best choice is manual layout. If the administrator is uncomfortable with this choice, auto layout may be chosen. After the Solaris installer lays out the file systems, the drive layout may be adjusted. Press “F4” to proceed with manual layout.

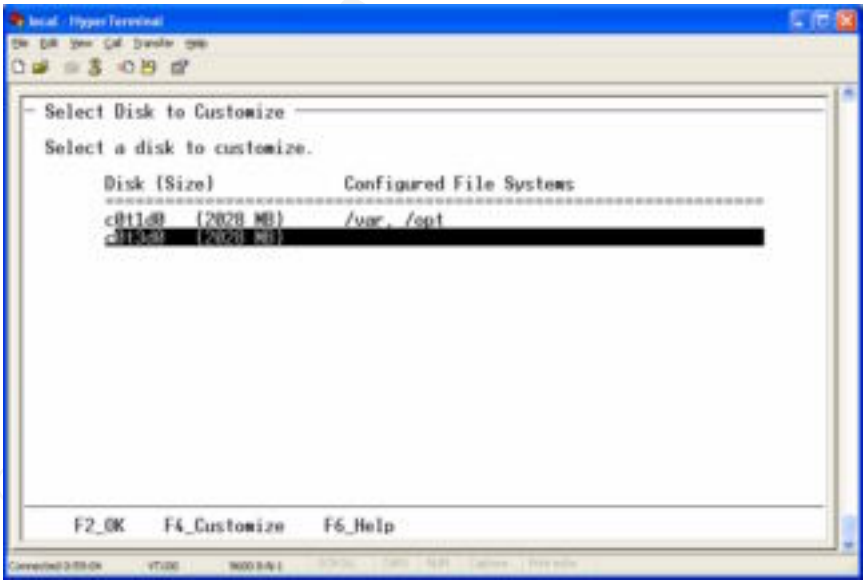
24. The above screen is a summary of the current disk layout. Please choose “F4” to proceed with customization of the file system layout.



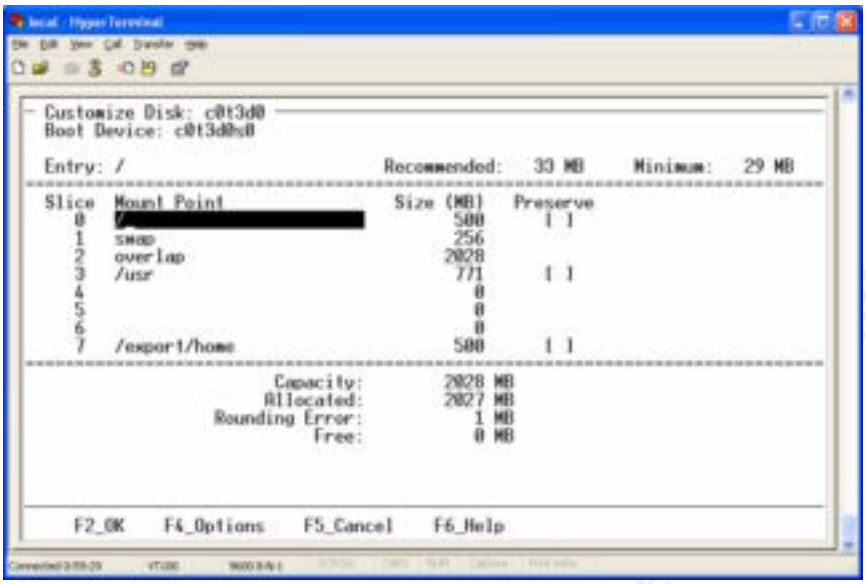
25. The next screen is used to select the disk we wish to customize. After customizing a disk, this same screen will appear with information regarding the file systems that have been configured. Select the first disk (c0t1d0) and choose “F4” to customize.



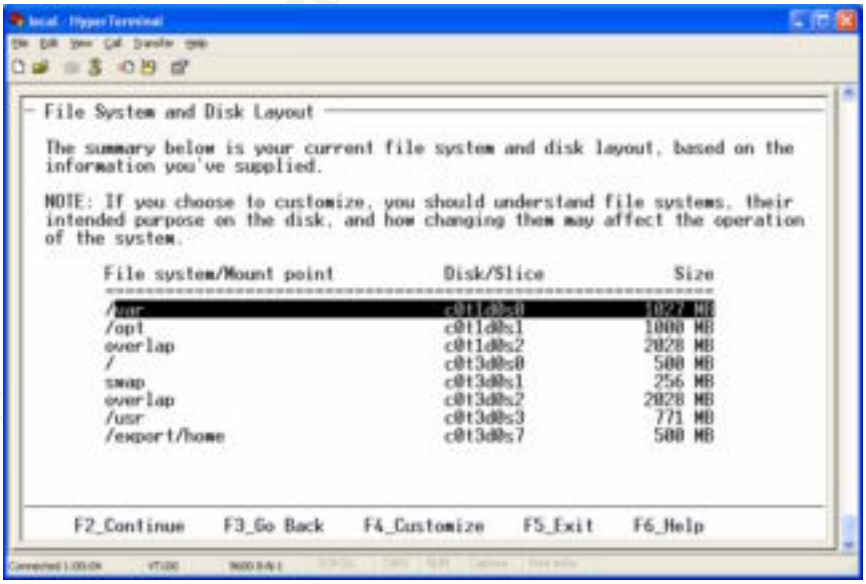
26. Using the arrow keys, navigate the mount point and size column entering appropriate values. In this instance, in order to maximize the disk space available for the current logs and to allow for easy installation of the additional software packages the disk was divided into two slices: /var and /opt. One gigabyte was allocated to the /opt file system, with the remainder of the disk space being allocated to /var. Press “F2” to accept the disk layout.



27. As previously mentioned, after successfully configuring one disk, the installer returns to the screen allowing for the selection of disks. Notice the configured file system information has been updated. Select the second disk (c0t3d0) and press “F4” to customize.



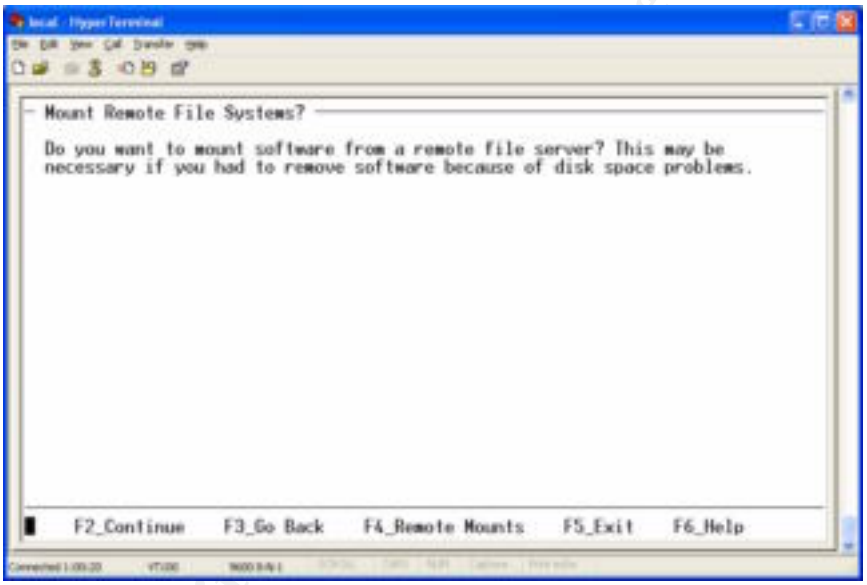
28. The above screen demonstrates the completion of the file system layout. In this instance, 500Mb is allocated to the root file system (/), 256Mb to swap, 500Mb to the home directory structure (/export/home) and the remainder (771Mb) to the /usr file system. By allocating adequate space to the root and /usr file systems, the machine will be easier to maintain and patch. By separating the /usr file system from the root file system, we will be able to further secure the box by mounting the /usr file system as read only. Press “F2” when customization of this disk layout is complete. On the next screen, press “F2” again to indicate that custom layout of the file systems is complete.



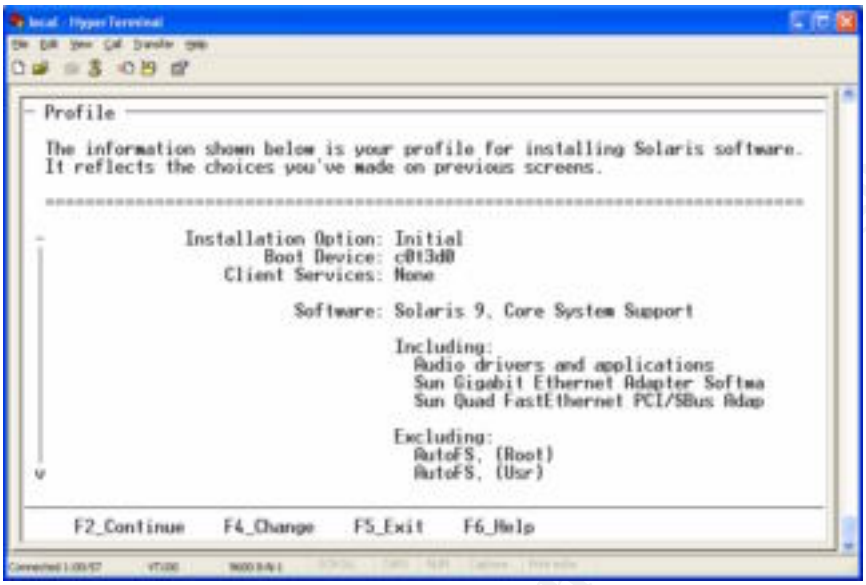
It is important to note that, on this system, c0t3d0 is the boot disk. Thus, we have lain out the /, /usr, swap, and /export/home file systems on the boot disk, while placing /var and /opt on the secondary disk.

One reason for doing this is that both / and /usr must be mounted in order for the system to boot, while /var and /opt are not required. A second reason is the desire to maximize the amount of space which may be allocated to the /var file system, where logs will be placed. Finally, if a larger disk can be procured in the future, this structure allows for easy replacement of the /var and /opt file system without the need to copy the entire operating system and simplifies the maneuver by not requiring copying of boot blocks on the boot drive.

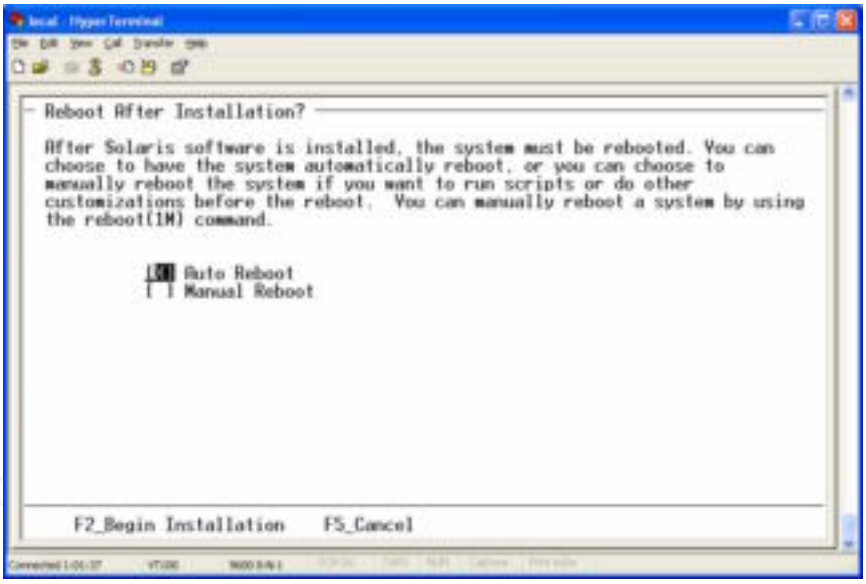
29. After completion of the customization, acceptance of the final disk layout is requested. Press “F2” at this juncture to accept the current layout and continue. If changes need to be made, “F4” may be pressed in order to return to the customization screens.



30. After acceptance of the disk layout, the Solaris install program moves to configuring the mounting of software from a remote file server. This system will not remotely mount file systems. Press “F2” to continue.



31. The Solaris installer is now ready to install the software. A profile listing the options selected during the software selection and reviewing the disk layout is given for the administrator to review. To accept the profile press “F2” to continue. “F4” may be pressed to return to the installer and make changes.



32. Finally, prior to installation the administrator must decide whether the system should automatically reboot or whether the installer should return to a shell prompt and the machine require a manual reboot. Press “F2” to begin the software installation.

Please note that the system does not have a configured root password yet. If the system is on the network and automatically rebooted then it will be live without a root password. By default Solaris does not allow root login from anywhere but console, even with Sun's ssh or with telnet installed. However, there still may be services, running on the network, which are unpatched and thus exposing the system to attack.

If performing a network based install ALWAYS choose to have a manual reboot so that at no time will a live unpatched system be on the network. In this instance, the machine is located in a secured environment and it is not currently connected to the network, thus allowing an automatic reboot is a safe choice.

33. Upon reboot, a console login prompt will be provided. Please login as user "root", no password is required. After successful login, use the `passwd` command to set a root password for this computer.

4.3 Installation of additional Solaris 9 OE and Companion CD packages

The "Core System Support" software group lacks certain software that will be either useful (e.g. GNU tar, GNU grep, top, etc.) or required (GCC compiler, ssh daemon) for completing the install and configuration of out central log server.

Table 3 lists additional packages that were installed on the server.

Table 3: Additional Solaris Packages to be Installed

Package Name	CD	Description
SUNWlibC	1 of 2	Sun Workshop Compilers Bundled libC
SUNWdoc	1 of 2	utilities and fonts for development, display, and production of documentation such as manual pages (nroff/troff)
SUNWzlib	1 of 2	The Zip compression library
SUNWlibCf	1 of 2	SunSoft WorkShop Bundled libC (cfront version)
SUNWscpr	1 of 2	utilities for user interface and source build compatibility with SunOS 4.x
SUNWscpu	1 of 2	utilities for user interface and source build compatibility with SunOS 4.x
SUNWbcp	1 of 2	utilities to provide a binary-compatible execution environment for SunOS 4.x applications
SUNWpsf	1 of 2	PostScript filters - (Usr)
SUNWpcr	1 of 2	client configuration files and utilities for the print service
SUNWpcu	1 of 2	client configuration files and utilities for the print

Package Name	CD	Description
		service
SUNWpsr	1 of 2	configuration and start-up files for the print service
SUNWpsu	1 of 2	client configuration files and utilities for the print service
SUNWscplp	1 of 2	print utilities for user interface and source build compatibility with SunOS 4.x
SUNWtoo	1 of 2	utilities for software development, including ld, ldd, od, and truss
SUNWscbcp	1 of 2	SPARCompilers Binary Compatibility Libraries
SUNWntpr	1 of 2	Network Time Protocol v3, NTP Daemon and Utilities (xntpd)
SUNWntpu	1 of 2	Network Time Protocol v3, NTP Daemon and Utilities (xntpd)
SUNWtcsh	2 of 2	Tenex C-shell (tcsh)
SUNWbash	2 of 2	GNU Bourne-Again shell (bash)
SUNWgcmn	2 of 2	Common GNU package
SUNWgtar	2 of 2	GNU tar
SUNWggrp	2 of 2	ggrep – GNU grep utilities
SUNWhea	2 of 2	SunOS C/C++ header files for general development of software
SUINWsutl	2 of 2	statically linked utilities for system disaster recovery
SUNWsra	2 of 2	libraries in archive (ar) format for source build compatibility with SunOS 4.x
SUNWsrh	2 of 2	SunOS C/C++ header files for source build compatibility with SunOS 4.x
SUNWsshr	2 of 2	Secure Shell protocol Client and associated utilities
SUNWsshu	2 of 2	Secure Shell protocol Client and associated utilities
SUNWsshdr	2 of 2	Secure Shell protocol Server
SUNWsshdu	2 of 2	Secure Shell protocol Server
SUNWsprot	2 of 2	Solaris Bundled Tools
SUNWcpp	2 of 2	Solaris cpp
SUNWlibm	2 of 2	Forte Developer Bundled libm
SUNWbtool	2 of 2	software development utilities, including ar, dis, dump elfdump, lex lorder, mcs, nm, prof, ranlib, rpcgen, size, strip, tsort, and yacc
SUNWman	2 of 2	System Reference Manual Pages
SUNWGlib	2 of 2	GLIB – Library of useful routines for C programming
SUNWgpch	2 of 2	The GNU Patch utility
SUNWless	2 of 2	The GNU pager (less)

Package Name	CD	Description
SUNWgzip	2 of 2	The GNU Zip (gzip) compression utility
SUNWzip	2 of 2	The Info-Zip (zip) compression utility
SUNWarc	2 of 2	system libraries in archive (ar) format for software development of statically linked executables
SFWgcmn	Companion	GNU common package
SFWgmake	Companion	The GNU make utility
SFWgcc	Companion	The GNU Compiler Collection
SFWtop	Companion	top - display information about processes
SFWsudo	Companion	Sudo - superuser do
SFWenscr	Companion	GNU enscript - convert text files to PostScript
SFWbison	Companion	GNU bison - a better yacc
SFWflex	Companion	GNU flex - a lex replacement

The following procedure is used to install the packages listed in Table 3, it should be repeated for each of the CDs (1 of 2, 2 of 2, and Companion):

1. Insert the appropriate CD in the CDROM drive and mount the CDROM using the following command:

   ```
   # mount -F hsfs -o ro /dev/dsk/c0t6d0s0 /mnt
   ```

   N.B. Typical older Sun workstation internal CDROM drives are attached as target 6 on controller 0 (c0t6d0s0), however this may not apply for all systems.

2. Change to the appropriate directory on the CD:
   a. 1 of 2: `/mnt/Solaris_9/Product`
   b. 2 of 2: `/mnt/Solaris_9/Product`
   c. Companion CD: `/mnt/components/sparc/Packages`

   ```
   # cd /mnt/[location]
   ```

3. Use the pkgadd command to install the package:

   ```
   # pkgadd -d . <pkgname> [<pkgname2> ...]
   ```

   N.B.: Multiple packages can be installed using one command line call to `pkgadd` as indicated in the command sample. Many packages will require the answering of questions to continue the install, please follow the instructions presented during the `pkgadd` command.

4. After installing the packages from a given CD, the administrator must unmount the CD using the following commands:

```
# cd /
# unmount /mnt
```

4.4 Patching the installation

After completion of the installation of the above packages, the latest patch cluster should be installed. The following procedure may be used to install the patch cluster that was burned on to a CDR during the pre-installation phase:

1. Place the CDR into the CDROM drive and mount the file system using the following command:

```
# mount -F hsfs -o ro /dev/dsk/c0t6d0s0 /mnt
```

2. Copy the patch cluster file to a local file system. In this example, an "adm" directory is created where the patches will be maintained:

```
# mkdir -p /opt/sfw/adm/patches
# cp /mnt/9_Recommended.zip /opt/sfw/adm/patches
```

3. Change to the location of the patch cluster and expand the zipped archive:

```
# cd /opt/sfw/adm/patches
# unzip 9_Recommended.zip
```

4. Change into the cluster directory and apply the patch cluster:

```
# cd 9_Recommended
# ./install_cluster
```

N.B.: It is important to read the "`CLUSTER_README`" and individual patch "`README-<patchid>`" files prior to installation. Many patches in the cluster may not apply, as the package to which they apply is not installed, the patch may already be installed, etc. Return codes are given for each patch installation in general; the following unsuccessful patch return codes may be safely ignored:

- ***2*** Attempt to apply a patch that's already been applied
- ***8*** Attempting to patch a package that is not installed

5. Some patches may require a reboot to complete installation. The general procedure for applying a patch cluster should include a reboot after completion of the "`install_cluster`" script:

```
# shutdown -i6 -g0 -y
```

5. Step by Step: Installation of syslog-ng

The system is now ready to have the additional software packages listed in Table 3 installed. The first package to install is the syslogd replacement syslog-ng. The syslog-ng installation requires the installation of libod; this package will be installed first. Each package was successfully compiled and installed using a default configuration using the following procedure:

1. Login as root using the password configured above. The following steps assume the use of the Bourne shell for the root environment; this is the default root shell under Solaris.

2. The following commands will prepare the system for installation of libod and syslog-ng. Additional paths are required to the default root environment so that the compiler and associated tool may be used. A symbolic link is used to make the default software location (`/usr/local`) be located where Sun adds their additional software packages (`/opt/sfw`). Further all source builds are done in an "adm" directory similar to the location of the patch cluster:

```
# PATH=$PATH:/usr/ccs/bin:/usr/sfw/bin:/opt/sfw/bin
# export PATH
# ln -s /opt/sfw /usr/local
# mkdir -p /opt/sfw/adm/src
# cd /opt/sfw/adm/src
# mount -F hsfs -o ro /dev/dsk/c0t6d0s0 /mnt
# cp /mnt/syslog-ng-1.4.15.tar.gz .
# cp /mnt/libol-0.2.23.tar.gz .
# gtar zxvf syslog-ng-1.4.15.tar.gz
# gtar zxvf libol-0.2.23.tar.gz
```

3. With the software archives now expanded, we will begin by installing the libol software. The following commands illustrate the compilation and installation of the libol software:

```
# cd libol-0.2.23
# ./configure
# make
# make install
```

This will compile and install the libol software. The software will be installed into a `/usr/local` hierarchy which was previously symbolically linked to the `/opt/sfw` hierarchy.

4. After the successful installation of libol, syslog-ng may now be compiled and installed. The following commands are used to compile and install syslog-ng:

```
# cd ../syslog-ng-1.4.15
# ./configure --with-libol=/usr/local/adm/src/libol-
0.2.23
# make
# make install
```

This will compile and install the syslog-ng software. The software will be installed into the `/usr/local` hierarchy. The main syslog-ng binary will be placed in `/usr/local/sbin`.

6. Step By Step: Installation of IP Filter

IP Filter is the next piece of software that needs to be compiled and installed. To compile and install IP Filter use the following procedure:

1. Prepare for installation by copying over the software from the mounted CDR.

```
# cd /opt/sfw/adm/src
# cp /mnt/ip_fil3.4.28.tar.gz .
# gtar zxvf ip_fil3.4.28.tar.gz
# cd ip_fil3.4.28
```

2. To compile and install the software the following commands are used:

```
# make solaris
# cd SunOS5
# make package
```

The above commands will first compile the IP Filter software for the Solaris environment. The make package command will create and install a Solaris software package for IP Filter. The default install location for this software package is `/opt/ipf`, although additional files are placed throughout the file systems.

7. Step By Step: Installation of AIDE

AIDE is a system integrity-checking tool that was developed as a free replacement to Tripwire. AIDE is dependent upon the installation of the mhash software. To compile and install the AIDE and related software use the following procedure:

1. Prepare for installation by copying over the software from the mounted CDR:

```
# cd /opt/sfw/adm/src
# cp /mnt/mhash-0.8.16.tar.gz .
# cp /mnt/aide-0.9.tar.gz .
# gtar zxvf mhash-0.8.16.tar.gz
# gtar zxvf aide-0.9.tar.gz
```

2. Since AIDE is dependent upon the mhash software, the mhash software is first compiled and installed using the following procedure:

```
# cd mhash-0.8.16
# ./configure
# make
# make install
```

   The above procedure will compile and install the mhash software into the `/usr/local` hierarchy.

3. With mhash successfully installed, the AIDE software may now be installed using the following procedure:

```
# cd ../aide_0.9/
# ./configure –without-zlib
# make
# make install
```

   The above procedure will compile and install the AIDE software into the `/usr/local` hierarchy.

8. Step By Step: Installation of LogSentry

The next piece of software, which needs to be installed, is Psionic LogSentry. This software is used to easily monitor the various log files that will be generated by our central log server. The following procedure is used to compile and install the LogSentry software:

1. Prepare for installation by copying over the software from the mounted CDR:

```
# cd /opt/sfw/adm/src
# cp /mnt/logsentry-1.1.1.tar.gz .
# gtar zxvf logsentry-1.1.1.tar.gz
# cd logcheck-1.1.1
```

   N.B.: LogSentry was previously known as logcheck and the current download while named logsentry-1.1.1.tar.gz will expand to the directory structure under logcheck-1.1.1, this however may change in later releases.

2. Since we do not have the Sun Forte compiler suite installed we must first edit the `Makefile` to use `gcc`. Using `vi` to edit the file `Makefile`, comment out the line:

```
CC=cc
```

   by placing a `#` at the beginning of the line and uncomment the line:

```
CC=gcc
```

   by removing the `#` from the beginning of the line. Save the changes and exit the editor. If unfamiliar with the use of the vi editor, please see the excellent tutorial provided by Purdue University [11] or the quick reference [7].

3. Now that the Makefile been modified, use the following command to compile and install the LogSentry software:

```
# make sun
```

9. Step By Step: Installation of the CIS software

The CIS Solaris Benchmark software comes in package format and can be added using the following procedure:

1. Prepare for installation by copying over the software from the mounted CDR:

```
# cd /opt/sfw/adm/src
# cp /mnt/cis-solaris.tar.Z .
# gtar zxvf cis-solaris.tar.Z
```

```
# cd cis
```

2. Add the CIS scoring software to the system using the following command:

   ```
   # pkgadd -d . CISscan
   ```

   This will install the CIS scoring tool in to the `/opt/cis` directory hierarchy.

This completes the installation of the secondary software packages. In the next section, configuration of the various pieces of software installed will be performed.

10. Configuration of syslog-ng, IP Filter, AIDE, and LogSentry

Proper configuration of each of the additional pieces of software is essential to the mission and security of the central log server. The subsequent sections will give the basic configuration used for each piece of software.

10.1 Configuration of syslog-ng

Configuration of the syslog-ng file consists of two main tasks. First, the syslog-ng binary must be configured to run a boot time. Second the `/etc/syslog-ng/syslog-ng.conf` file must be configured to log our data appropriately.

The configuration of our system is such that the syslog-ng software will be utilized for both local and network based logging. Appendix B lists a sample `syslog-ng.conf` file that provides extensive comments regarding the logging configuration.

There are four major directives in the configuration file for syslog-ng:

- *source*: The source directive is used to describe where logging information will be read from. The source may be a network connection, a pipe, an ipc door, etc.

- *destination*: The destination directive is used to describe where logging information should be logged to. Typically this is a file, however syslog-ng allows for destinations such as a pipe, network stream, or another program.

- *filter*: The filter directive is used to describe filters to be used on the incoming messages. For example filtering may be performed on the class or level of a message, the hostname of the machine from

which the message originated, or any regular expression match.

- *log*: The log directive ties together the source, filter, and destination directives to perform the actually action of logging a message.

For more information regarding the various configuration options for the configuration file, see the manual page included with the software distribution or visit the syslog-ng home page [1].

To configure the syslog-ng software to run at boot time we need to replace the init script, which starts the standard syslog daemon with one that will start syslog-ng. Appendix C lists an example init script for this purpose. This init script is a modified version of the standard Solaris syslog init script. To utilize this init script, replace the contents of `/etc/init.d/syslog`, with the information listed in Appendix C.

10.2 Configuration of the IP Filter Firewall

Appendix D gives an example IP Filter configuration file. This file severely restricts access and services to and from this machine. The file is well commented. For a good introduction to the use of IP Filter as a firewall please see *IP Filter Based Firewalls HOWTOW* [5]. The sample configuration file may be copied to `/etc/opt/ipf/ipf.conf` in order to configure the IP Filter firewall software.

There are two sets of rules that allow incoming traffic through. The first rule set regards incoming SSH connections. The second rule set allows the incoming udp and tcp connections to port 514, which is the syslog service. The Cisco PIX firewalls have been configured to use tcp connections versus the standard udp connection for syslog.

Additional rules may be added to the configuration file as needed. To reload the firewall with the new rules use the following command:

```
# /etc/init.d/ipfboot restart
```

Note, the comment lines at the top of the file indicate the addition of two static routes to the routing table. These routes are added at boot time through the use of the init script listed in Appendix E. This script can be placed in `/etc/rc2.d`.

10.3 Configuration of AIDE

A sample AIDE configuration file is given in Appendix F. The AIDE binary, configuration file, and the databases it generates should be stored

on read-only media such as a CDR for security purposes. However, prior to making a copy on a CDR we must first create our initial configuration file and databases. The creation of the initial configuration file and database is a refinement process. From the AIDE manual [7]:

" It is generally a good idea to ignore directories that frequently change, unless you want to read long reports. It is good practice to exclude tmp directories, mail spools, log directories, proc file systems, user's home directories, web content directories, anything that changes regularly. It is good practice to include all system binaries, libraries, include files, system source files. It will also be a good idea to include directories you don't often look in like /dev, /usr/man/.*, and /usr. Of course you'll want to include as many files as practical, but think about what you include."

Using the following procedure and the example configuration file the administrator may refine the AIDE configuration.

1. Using vi create the initial configuration file using the example in Appendix F.

   ```
   # vi /usr/local/etc/aide.conf
   ```

   Add the contents of the example configuration file.

2. Initialize the databases using the following command:

   ```
   # /usr/local/bin/aide \
   -config=/usr/local/etc/aide.conf --init
   ```

3. Make a copy of the AIDE binary, the config file and databases created by the initialization on to a CDR. Since this machine does not have a CDRW drive, the files will need to be copied to a secondary machine after this host is brought on to the network.

4. With the CDROM created above inserted and mounted, run a nightly cron job which will perform the command:

   ```
   /mnt/aide --config=/mnt/aide.conf --check
   ```

5. To add the nightly cron job to the system, use the following commands to enter the crontab editor:

   ```
   # EDITOR=vi; export EDITOR
   # crontab -e
   ```

Now add a line such as the following to run AIDE at 1:00am everyday:

```
0 1 * * * /mnt/aide --config=/mnt/aide.conf \
  --check
```

The output of the command is the report. As mentioned in the manual, directories that change frequently will produce long reports. The administrator should refine the `aide.conf` file if the report is includes too much information regarding files that change frequently. If the configuration file is modified, it is recommended that new databases be generated and copied to a CDR as in step 3 above.

If the configuration file is not changed but the databases need to be updated the administrator should copy the databases from the CD to a temporary location and run the following command:

```
# /mnt/aide --config=/mnt/aide.conf --update
```

10.4 Configuration of LogSentry

LogSentry is used to parse the log files on the system, sending new messages that it has not been configured to ignore to the administrator. As with the configuration of AIDE, the configuration of LogSentry is a refinement process by which the administrator configures LogSentry to ignore entries which he or she is not interested in.

The first step in the configuration of LogSentry is the addition of the various log file destinations listed in our syslog-ng.conf file to the list of logs that will be checked. To do this we edit the `/usr/local/etc/logcheck.sh` script using `vi` and add lines similar to the following for each destination in the list of Solaris log files:

```
$LOGTAIL /var/log/switch.log >> $TMPDIR/check.$$
```

After the addition of the appropriate log files to `logcheck.sh` we must add a line to the crontab to periodically run LogSentry. How frequently LogSentry is run is the preference of the administrator. LogSentry will generate email only if there are non-ignorable log entries discovered. The time between when LogSentry runs is the time delta between when a problem can occur and when the administrator will be notified. At GIAC Laboratory, on this system, LogSentry will be configured to run every 15 minutes. Using the same procedure to edit the crontab file as listed above, add the following entry to the crontab:

```
0,15,30,45 * * * * /usr/local/etc/logcheck.sh
```

LogSentry is configured to ignore messages in the log file through the use of the following files located in `/usr/local/etc`: `logcheck.ignore`, `logcheck.violations.ignore`. LogSentry uses a simple grep mechanism to report on the logs. By adding regular expressions to these files, LogSentry may be configured to ignore certain messages. Additionally, if there are violation signatures that the administrator desires to be looked for, or if there are hacking signatures that would appear in the logs, these signatures may be added to the `logcheck.violations` and `logcheck.hacking` files, respectively. Items in the `logcheck.hacking` file generate a separate report. Items in the `logcheck.violations` will appear in the "violations" section of the standard LogSentry report unless specifically ignored in the logcheck.violations.ignore file. See Appendix G for sample LogSentry reports.

11. Additional Configuration of System

The additional system software has now been configured. However, there are several local configuration tasks that must be completed before the system will be completely configured.

11.1 Configuration of the Secondary Ethernet Interface

This system is configured as a bastion host between two networks and, thus, has two network cards. The Solaris installation process configured only the single primary interface. In order to configure the secondary interface, we perform the following steps:

1. Add the hostname of the secondary interface to `/etc/hosts`.

   ```
   echo "192.168.1.2     gcux-test2" >>
   /etc/hosts
   ```

2. Create a new file named `/etc/hostname.le0` which contains the hostname to be used for the secondary interface:

   ```
   echo "gcux-test2" > /etc/hostname.le0
   ```

   Upon reboot, the secondary Ethernet interface will now be configured.

11.2 Configuration of Log File Rotation

Prior to Solaris 9, a secondary log rotation package would need to be

added to easily and effectively manage the rotation of system log files. Solaris 9 includes a new command `logadm` that provides this functionality. The following command example will configure the rotation of the `/var/log/pix.log` file:

```
# logadm pixlog -z 1 /var/log/pix.log \
    -a 'kill -HUP `cat /var/run/syslog-ng.pid`' \
    -t '/var/log/OLDLOGS/$basename.$
```

The log file is configured to rotate based upon the default size and time restrictions (>1 byte and older than 1 week), all but the last rotated log will be compressed using gzip, the old log files will rotate to the directory `/var/log/OLDLOGS` and the command "`kill -HUP `cat /var/run/syslog-ng.pid`` " will be run after log file has been rotated and the new log file created.

Similar `logadm` commands should be run for each destination log file listed in the syslog-ng.conf file.

11.3 Addition of Accounts for Administrative Users

Accounts need to be created for those people who will access this machine remotely. The following commands will configure the default home directory location to be used by the `useradd` command, create and account for a user, set the initial password for the user, and adjust the password expiration values to enforce the password policy of GIAC Laboratory.

```
# useradd -D -b /export/home
# useradd -c "Firstname Lastname" -m -u <uid> \
   -g sysadmin <loginname>
# passwd <loginname>
New Password:
Re-enter new Password:
password: password successfully changed for
<logginname>
# passwd -w5 -x180 <loginname>
```

The final command will force the user to change passwords every 180 days with a warning regarding the need to change passwords happening 5 days in advance.

11.4 Configuration of Network Time Protocol (NTP)

Solaris 9 ships with NTP software. Although not part of the "Core"

software group, NTP was added to the system in Section 4.3. To configure this software use following steps [4]:

```
# cat << END_CONFIG >> /etc/inet/ntp.conf
driftfile /etc/ntp.drift

server <srvr>
server <srvr>
server <srvr>

restrict default nomodify
END_CONFIG
# touch /etc/ntp.drift
```

Please replaces the `<srvr>` with the IP address of the appropriate local NTP servers. The NTP server will automatically start upon the reboot of the system.

11.5 Basic Hardening of the System

Now that basic system installation and configuration are complete it is time to perform a basic system hardening. At GIAC Laboratory we use the CIS benchmark [4] and related documentation as our "best practices" hardening tool.

There are many tools to assist in the securing Solaris such as JASS [17], Titan [18], and YASSP [20]. For a discussion of the relative merits of the SANS Step-by-Step Guide, Titan, and YASSP see *Solaris Security Recommendations from SANS Step by Step Guide, Titan, and YASSP* [2]. This document demonstrates how much the various methods of securing Solaris have in common. The administrator should evaluate each product based on the needs of his or her site.

The documentation included with the CIS benchmark (currently version 1.0.1b) provides a simple step-by-step mechanism for securing Solaris. Included with the package is a scoring tool that will produce detailed reports regarding the compliance of the system with the benchmark.

It is up to the individual administrator to decide if a procedure listed in the documentation is applicable to the system in question or not. In the case of this installation, the actions regarding the enabling of system accounting and kernel auditing were not taken. The action regarding mounting file systems 'nosuid' were modified to not include /opt because the sudo must run as suid and the command resides in /opt/sfw.

Several actions regarding ftp and telnet were taken to improve score. Since ftp and telnet are not installed on the system, these actions do not

have the effect of improving security.

A sample report from the CIS score program is given in Appendix H.

11.6 Backup of system

Now that the entire system is installed and configured, the system should be backed up to tape. There is an attached Exabyte 8505XL drive on this system, to back up the entire system we simply issued the following commands in sequence:

```
# ufsdump 0cuf /dev/rmt/0un /
# ufsdump 0cuf /dev/rmt/0un /usr
# ufsdump 0cuf /dev/rmt/0un /export/home
# ufsdump 0cuf /dev/rmt/0un /var
# ufsdump 0cuf /dev/rmt/0u /opt
```

It is recommended that two complete backups of the system be made and that these copies be kept separate from the machine and from each other.

11.7 Shutdown System and Bring on to the Network

Installation and configuration is now complete. It is time to shutdown the system. Plug in the network cables, and bring the system on line. It is not necessary to shutdown the system in order to simply bring the network interfaces on line, however with all the various configuration of software and security hardening a shutdown and reboot is recommended to ensure the system boots correctly.

Shutdown the system using the following:

```
# shutdown -i0 -g0 -y
```

Now ensure that the network cables are plugged in to the appropriate interfaces and boot the system using:

```
ok> b
```

Note, if security hardening included the addition of the eeprom security, the boot prompt may be different then shown above.

12. Ongoing Maintenance

Ongoing maintenance of the central log server is crucial to ensure the security of the host. Establishing a routine maintenance procedure for the host will ensure that the system will be as secure in the future as is it today. At GIAC Laboratory

there is an established best practice maintenance procedure for Solaris computers. The following sections highlight major maintenance tasks and considerations. While these highlights are in no way complete, a step-by-step document equaling this would be required to fully describe the ongoing maintenance procedure and falls outside the scope of this paper.

12.1 Routine Solaris Patches and Software Updates

12.1.1 Patch Maintenance

PatchPro is a relatively new software offering from Sun available for managing patches, and is included with the Solaris 9 distribution. The PatchPro software is a recent addition from Sun and works under the Solaris OE versions 2.6 to Solaris 9, although somewhat more limited in the earlier releases. The use of this for patching is still under investigation here at GIAC Laboratory, for more information regarding this product see [16].

The established procedure for maintaining patches under a Solaris system here at GIAC Laboratory involves the use of the PatchCheck software [15]. This software consists of a perl script that will utilize information about installed software and current installed patches combined with a list of the most recent available patches to produces an html based patch report. The PatchCheck software utilizes the output of the pkginfo and showrev commands to allow the generation of a patch report for any given machine to be generated on the machine where PatchCheck is installed. This patch report can then be used to select and download the necessary patches.

The list of updated patches is available nightly from Sun support website. At GIAC Laboratory, the information required to run the PatchCheck software is generated weekly on each machine, and sent via email to the system administrator. The system administrator will then run the PatchCheck software with the latest list of updated patches to produce the report. The report is then reviewed using a web browser and any patches deemed required could be downloaded and installed. Retrieval of patches through the PatchCheck software does require a Sun service contract and valid login to the SunSolve website.

12.1.2 Maintenance Updates

Beginning with Solaris 7, Sun has begun shipping quarterly maintenance updates. These maintenance updates can be used to summarily bring a system up to the current snapshot. The maintenance update will apply all patches up to the current snapshot.

The maintenance update may also include packages containing new features.

For a dedicated purpose system such as the central log server the use of the maintenance updates is not necessary. However, documentation on each maintenance upgrade should be reviewed in the event that the system may benefit from the additional functionality being provided in the maintenance update.

12.2 Mailing Lists

Information about recently discovered vulnerabilities is key to maintaining the system securely. Mailing lists can provide the administrator with appropriate information in a timely manner. Listed here are several mailing lists regarding Solaris, the additional software which has been installed, and general vulnerabilities:

Sun Security Alerts: security-alert@sun.com, for help on using the list send email to the aforementioned address with the subject line help.

AIDE Mailing List: for information and help on subscribing to the AIDE mailing list see the AIDE homepage (http://www.cs.tut.fi/~rammer/aide.html). This list is for general AIDE information, help, and announcements. The list is low traffic.

Syslog-ng Mailing List: for information and help on subscribing to the AIDE mailing list please see http://www.balabit.hu/en/downloads/syslog-ng/support/.

IP Filter Mailing List: Send mail to majordomo@coombs.anu.edu.au with "subscribe ipfilter" in the body of the mail. This is a moderate traffic list. Buqtraq and focus-sun Mailing Lists: Buqtraq is a high traffic list with general discussion and announcement of recent vulnerabilities, focus-sun is a low traffic list focusing on security concerns related to Solaris. For information and subscription see: http://online.securityfocus.com/cgi-bin/sfonline/subscribe.pl.

12.3 AIDE Integrity Checks and Reporting

The AIDE program has been installed and configured to perform nightly integrity checks of the file systems. Preferably, AIDE has been configured to run from a CDROM which would store the AIDE binary, the configuration file and the database which to check against.

If AIDE has been configured as such, we have removed the most fundamental problem -- which is that AIDE (and other integrity checking

programs such as Tripwire) is commonly configured to run under the same environment as the files being checked. An interloper who gains access will not be able to replace the AIDE binary, configuration file, or database with one that would hide their actions.

The second common problem with integrity checking programs is the configuration. The administrator will not likely have time to read long reports each day about every file that has changed on the system, thus AIDE needs to be carefully configured to report on those files and attributes which should not change. However, care must be taken to not ignore too much, as this will leave the system open to attack.

The third common problem with integrity checking programs is the complacency of the administrator with regards to the report. If the report generated shows a file has been changed and the administrator deems the change expected then the database file needs to be updated so that the file will no longer be reported as changed. Failure to do so will lead to a situation where the same file appears in the report each day, which may lead the administrator to miss an inappropriate change to the file since he or she has grown accustomed to the file being in the report.

12.4 Backup to Local Tape Drive

Routine backup of the system to tape is essential for recovery of the system in the event of a hardware or software failure. The entire system should be backed up whenever major modifications have been made to the system. These modifications would include the application of patches to the operating system, the upgrade of the additional software, etc. As with the initial backup, it is recommended that two copies be made with the copies being stored separate from the computer and each other.

The data that our log server is logging provides us with a historical record of events occurring on the network. This data is thus vital for use in such instances of forensic investigate of a cyber security breach or a network problem. In order to ensure availability of the historical data, the current log files and archived log files should be backed up nightly.

The current hardware configuration of the central log server may not allow for sufficient online historical archival of data, this will depend greatly on the quantity of data being logged to the system. In the case where insufficient data may be kept on line, the nightly archives of the log files may be used to supplement the online archives for historical purposes.

12.5 Log Monitoring Using LogSentry

LogSentry has been installed and is configured to run every 15 minutes

producing reports showing the recently logged activity. It is crucial that the administrator carefully configure the logcheck.violations, logcheck.violations.ignore, and logcheck.ignore files to report appropriately.

Failure to properly configure these files will lead to either extremely long reports or reports which have little or no information. In each case the administrator reviewing the report will likely miss important information.

As with any report, it is critical that the administrator carefully review the information presented. The LogSentry reports generated will have information regarding not only network related problems but also with problems that may be being experienced on the local machine making the reports integral to the ongoing maintenance of the central log server.

13. Checking of the Configuration

Now that the system is configured and on line, the configuration must be verified. The following sections highlight the verification of several of the major components of the system.

13.1 Verification of the System Hardening

One of the primary reasons that the CIS benchmark is used in the basic hardening of the system is that the software includes a scoring tool that will allow for verification and documentation of the hardening processes. To run the scoring tool use the following command:

```
# /opt/CIS/cis-scan
```

The result of the hardening of our system and the report generated are given in Appendix H. The overall score for our system is an 9.0 out of 10.

13.2 Verification of the syslog-ng Configuration and Operation

Prior to verification of the operation syslog-ng, each piece of networking equipment that will be logged to this central log server must be configured to use the server. Configuration of the Cisco equipment is to be performed by the network administrator and falls outside the scope of this document.

Assuming the network equipment is configured to properly use the central log server it is now possible to test the operation of syslog-ng. Using the following command:

```
# tail -f /var/log/pix.log
```

a log file may be actively monitored. The command will display on our console each line entered in to the log file as it appears. Similarly, the command may be used to monitor any other log file destination that has been configured.

While viewing the appropriate log file, have the network administrator generate events that should be logged to the log server from each piece of equipment. Verify that the log messages arrive and are logged appropriately.

13.3 Verification of the IP Filter Firewall Configuration

The IP Filter firewall configuration will be tested in two phases. First, tests are performed to ensure that expected services work correctly such as incoming syslog connections on udp 514 and incoming ssh connections from either interface. Successful verification of the syslog-ng software establishes that connections via udp/tcp port 514 are working appropriately. Next, the administrator should assure that he or she is able to log in to the log server using an ssh client.

The second phase of testing will ensure that their are no additional services exposed through the firewall. To verify, this the administrator should first log in to the central log server and run the following command:

```
# tail -f /var/log/ipf.log
```

Next, using a second box with the Nmap [10] tool installed a scanning attempt should be initiated using:

```
# nmap -P0 -p 1-65535 -sS <ip address>
```

The `ipf.log` file should show many unsuccessful connection attempts, while the Nmap output should show only udp port 514, tcp port 514, and tcp port 22 having services available.

Because the central log server has two interfaces the Nmap command should be tested on both interfaces. A laptop running Linux is utilized for this purpose at GIAC Laboratory. The laptop is used as a network scan, test, and debugging device and is easily moved from network to network. Tools such as Nmap, ethereal, and Nessus are installed.

For more information on the use of Nmap please see the *NMAP Guide* [6].

13.4 Verify LogSentry

LogSentry was configured to run from cron every 15 minutes. By this time the administrator should have received email reports from LogSentry. This is sufficient to ensure that LogSentry is configured to periodically check the logs. However, to ensure that LogSentry is checking each log file which needs to be checked the administrator should use the following command to log a test entry to the log file:

```
# logger -p local6.info "TEST OF LOGSENTRY"
```

This command will log an entry using the local6 facility and the info severity level. A message to each facility filtered should be given. For equipment here at GIAC laboratory messages should be sent for facilities `local0`, `local4`, `local6`, and `local7`.

The administrator may now run the LogSentry software:

```
# /usr/local/etc/logcheck.sh
```

Verify that each message sent using the logger command appears in the LogSentry report and that the appropriate people receive the report.

13.5 Verify AIDE

AIDE is installed as a file integrity-checking tool. It would be tedious to verify each rule in the configuration file. For the purposes of this paper the rule looking for changes in files in the `/etc` directory will be tested.

Using the passwd command, change either a user's or root's password:

```
# passwd user1
New Password:
Re-enter New Password:
password: password successfully changed for user1
```

This has the effect of modifying the /etc/shadow file. Now, as root, run the AIDE command with the check parameter:

```
# /mnt/aide --config=/mnt/aide.conf --check
```

This command should produce output which includes lines similar to the following:

```
AIDE found differences between database and
filesystem!!
Start timestamp: xxxx-xx-xx xx:xx:xx
Summary:
```

```
Total number of files=5672,added files=0,removed
files=0,changed files=1

Changed files:
changed:/etc/shadow
Detailed information about changes:

File: /etc/shadow
  Inode    : 96953                              , 96966

#
```

AIDE reports all information to standard output. Email of the AIDE report is automatically performed because cron will email the output of a command running under cron to the user that is running the cron job.

Verify that AIDE is configured to run from cron nightly by performing the following command:

```
# crontab -l | grep aide
```

A single line of output should be returned, similar to:

```
0 1 * * * /mnt/aide --config-file=/mnt/aide.conf \
  --check
```

We have now completed the verification of the various critical pieces of additional software installed on our central log server.

14. Conclusion

This document presents a step-by-step installation of Solaris 9 and additional software in order to configure a central log server. It is expected that the novice administrator could utilize this document for a basic installation and configuration. The guide strives to be as complete as possible; however, it cannot replace institutional policies and procedures for securing and maintaining a Solaris 9 box.

References

1. BalaBit IT Ltd. *Syslog-ng Homepage.* http://www.balabit.hu/en/downloads/syslog-ng/

2. David Brumley *Solaris Security Recommendations from SANS Step by Step Guide, Titan, and YASSP.* http://www.sans.org/newlook/resources/solaris_sec.htm

3. Campin dot Net. *Syslog-ng FAQ*. http://www.campin.net/syslog-ng/faq.html

4. Center for Internet Security *Level 1 Benchmark and Scoring tool for Solaris.* http://www.cisecurity.org/

5. Brendan Conoboy and Erik Fichtner *IP Filter Based Firewalls HOWTO.* http://www.obfuscation.org/ipf/ipf-howto.pdf

6. Lamont Granquist. *NMAP GUIDE.* http://www.insecure.org/nmap/lamont-nmap-guide.txt

7. James Hu, et. al. *VI reference*. http://www.cs.wustl.edu/~jxh/vi.html

8. Rami Lehti. *The Aide Manual.* http://www.cs.tut.fi/~rammer/aide/manual.html

9. Rami Lehti and Pablo Virolainen. *Aide Homepage.* http://www.cs.tut.fi/~rammer/aide.html

10. *Nmap Homepage.* http://www.insecure.org/nmap/

11. Purdue University. *VI Tutorial.* https://engineering.purdue.edu/ECN/Resources/KnowledgeBase/Docs/20020202121609

12. Psionic Technologies Inc. *Log Sentry Homepage.* http://www.psionic.com/products/logsentry.html

13. Darren Reed. *IP Filter Homepage.* http://coombs.anu.edu.au/~avalon/

14. Balázs Scheidler. *Syslog-ng Reference Manual.* http://www.balabit.hu/static/syslog-ng/reference/book1.html

15. Sun Microsystems. *PatchCheck version 1.1.* http://sunsolve.sun.com/pub-cgi/show.pl?target=patchk

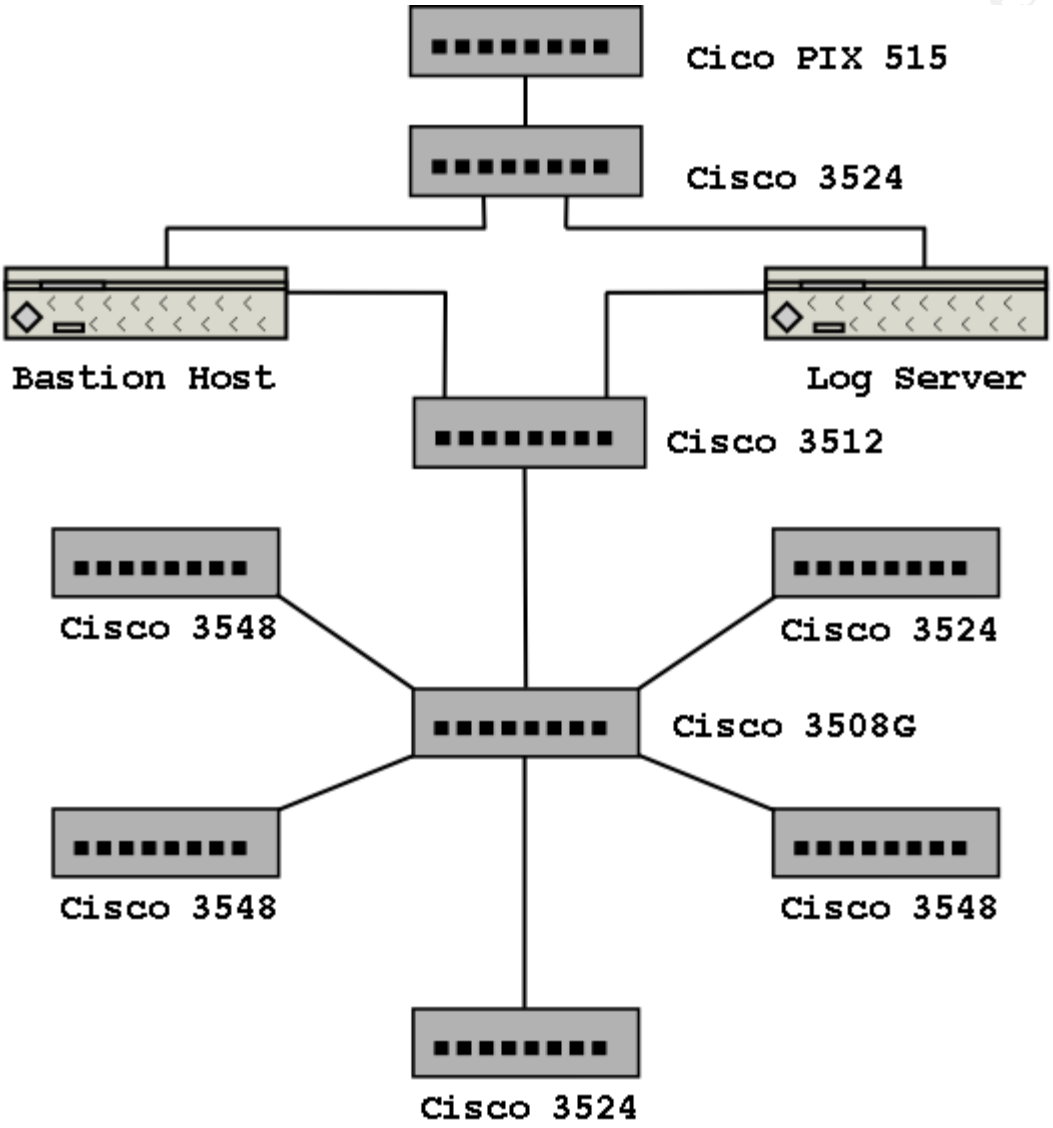
16. Sun Microsystems. *PatchPro Hub.* http://www.sun.com/patchpro/

17. Sun Microsystems. *Sun Security Toolkit (JASS).* http://wwws.sun.com/software/security/jass/

18. Titan Homepage http://www.fish.com/titan/

19. Yet Another Solaris Security Package (YASSP) http://www.yassp.org/

Appendix A – Network Diagram



Appendix B – syslog-ng.conf

```
#
# Syslog-ng example configuration file for Solaris
#
#use_fqdn()       add FQDN instead of short hostname
#use_dns()        use DNS (may cause DOS)
#sync()                number of lines buffered before written to file
#log_fifo_size()  number of lines fitting to the output queue
#
options { use_fqdn(yes);
          keep_hostname(yes);
          use_dns(no);
          long_hostnames(off);
          sync(0);
          log_fifo_size(1000); };

#
# local and network sources
#
# + will accept udp/tcp connections on port 514 from any host
# + keepalive option is for tcp only and will keep connection open
#     when the SIGHUP signal is seen
#
source local { sun-streams("/dev/log" door("/etc/.syslog_door"));
internal();};
source network { udp(); tcp(); };

#
# standard destinations for local standard system messages
#
destination authlog { file("/var/log/auth.log"); };
destination syslog { file("/var/log/syslog"); };
destination kern { file("/var/log/kern.log"); };
destination maillog { file("/var/log/maillog"); };

#
# special log destinations for our remote hosts
# (pixlog, switchlog) and for our IP Filter firewall (ipflog)
#
destination ipflog { file("/var/log/ipf.log"); };
destination pixlog { file("/var/log/pix.log"); };
destination switchlog { file("/var/log/switch.log"); };

#
# Some log files used to catch remaining messages
#
destination debug { file("/var/log/debug"); };
destination messages { file("/var/log/messages"); };

#
# console destination
#
destination console { file("/dev/sysmsg"); };

#
```

```
# filters for standard local system messages which come
# in on non-local facilities
#
filter f_authpriv { facility(auth) ; };
filter f_syslog { not facility(auth) and not facility(mail); };
filter f_kern { facility(kern); };
filter f_mail { facility(mail); };

#
# filters for IPFilter and the Cisco equipment
#
filter f_ipf { facility(local0); };
filter f_pix { facility(local4); };
filter f_switch { facility(local6, local7); };

#
# catch the rest
#
filter f_debug { not facility(kern, auth, mail, local6, local7, local4,
local0); };
filter f_messages { level(info .. warn) and not facility(auth, mail,
local0, local4, local6, local7); };

#
# filters for various emergency level messages
#
filter f_emergency { level(emerg); };

#
# log emergency level messages out to console
#
log { source(local); filter(f_emergency); destination(console); };

#
# log messages from local machine
#
log { source(local); filter(f_authpriv); destination(authlog); };
log { source(local); filter(f_syslog); destination(syslog); };
log { source(local); filter(f_kern); destination(kern); };
log { source(local); filter(f_mail); destination(maillog); };

#
# log IP Filter messages to the ipf.log
#
log { source(local); filter(f_ipf); destination(ipflog); };

#
# log switch and pix messages
#
log { source(network); filter(f_pix); destination(pixlog); };
log { source(network); filter(f_switch); destination(switchlog); };

#
# catch the rest of the messages
#
log { source(local); source(network); filter(f_debug);
destination(debug); };
```

```
log { source(local); source(network); filter(f_messages);
destination(messages); };

#
# Automatic sorting of host messages by $HOST and $YEAR$MONTH$DAY
#
# + will automatically create a directory structure for all messages
#   sorted first by host, then by date, then by facility.
# + with use_dns(no) we will have files based on ip address not
hostname
#
destination hosts {
file("/var/log/HOSTS/$HOST/$YEAR$MONTH$DAY/$FACILITY" owner(root)
group(root) perm(0600) dir_perm(0700) create_dirs(yes)); };

#
# logs all incoming messages from network source to the sorted
# destination
#
log { source(network); destination(hosts); };
```

Appendix C - /etc/init.d/syslog

```
#!/sbin/sh
#
# script to start syslog-ng on boot up for a Solaris machine.
# This script replaces /etc/init.d/syslog on a Solaris machine.
#
case "$1" in
'start')
        if [ -f /etc/syslog-ng/syslog-ng.conf -a -f
/usr/local/sbin/syslog-ng ];
then
                echo 'syslog-ng service starting.'
                #
                # Before syslogd starts, save any messages from
previous
                # crash dumps so that messages appear in chronological
order.
                #
                /usr/bin/savecore -m
                if [ -r /etc/dumpadm.conf ]; then
                        . /etc/dumpadm.conf
                        [ "x$DUMPADM_DEVICE" != xswap ] && \
                            /usr/bin/savecore -m -f $DUMPADM_DEVICE
                fi
                if [ ! -f /var/adm/messages ]; then
                        /usr/bin/cp /dev/null /var/adm/messages
                        /usr/bin/chmod 0644 /var/adm/messages
                fi
                /usr/local/sbin/syslog-ng >/dev/msglog 2>&1 &
        fi
        ;;

'stop')
        echo 'syslog-ng service stopping.'
        if [ -f /var/run/syslog-ng.pid ]; then
                syspid=`/usr/bin/cat /var/run/syslog-ng.pid`
                [ "$syspid" -gt 0 ] && kill -15 $syspid
        fi
        ;;

*)
        echo "Usage: $0 { start | stop }"
        exit 1
        ;;
esac
```

Appendix D - /etc/opt/ipf/ipf.conf

```
#
# The following routes should be configured, if not already:
#
# route add xxx.xxx.xxx.xx localhost 0
# route add xxx.xxx.xxx.xx localhost 0
#
# blocks various illegal packets
#
block in log quick from any to any with ipopts
block in log quick proto tcp from any to any with short
block in log all with frag
#
# block pin requests
#
block return-icmp in log proto icmp all

# block all incoming traffic except that explicitly allowed
# later.
#
block in log all

# Allow incoming/outgoing connections to ssh (tcp 22) on both
#interfaces
#
pass in quick on le0 proto tcp from xxx.xxx.0.0/16 to any port = 22
flags S keep state
pass in quick on hme0 proto tcp from xxx.xxx.0.0/16 to any port = 22
flags S keep state
pass out quick on le0 proto tcp from any to any port = 22 flags S keep
state
pass out quick on hme0 proto tcp from any to any port = 22 flags S keep
state

# allow udp/tcp port 514 in (syslog)
#
pass in quick on le0 proto udp from xxx.xxx.0.0/16 to any port = 514
pass in quick on le0 proto tcp from xxx.xxx.0.0/16 to any port = 514
pass in quick on hme0 proto udp from xxx.xxx.0.0/16 to any port = 514
pass in quick on hme0 proto tcp from xxx.xxx.0.0/16 to any port = 514

# allow email to go out
#
pass out quick on le0 proto tcp from any to any port = 25 flags S keep
state keep frags

# allow dns queries
#
pass out quick on le0 proto tcp from any to any port = 53 flags S keep
state keep frags
pass out quick on le0 proto udp from any to any port = 53 keep state
keep frags
```

Appendix E - /etc/rc2.d/S69inet2

```
#!/sbin/sh

#
# Add static route for ethernet interfaces to localhost
#
route add xxx.xxx.xxx.xx localhost 0
route add xxx.xxx.xxx.xx localhost 0
```

Appendix F – aide.conf

```
#
# aide.conf, based on sample configuraiton from "The Aide Manual" [8]
#
database=file:/mnt/aide.db
database_out=file:/tmp/aide.db.new
#
# Here are all the things we can check - these are the default rules
#
#p:      permissions
#i:      inode
#n:      number of links
#u:      user
#g:      group
#s:      size
#b:      block count
#m:      mtime
#a:      atime
#c:      ctime
#S:      check for growing size
#md5:    md5 checksum
#sha1:   sha1 checksum
#rmd160: rmd160 checksum
#tiger:  tiger checksum
#R:      p+i+n+u+g+s+m+c+md5
#L:      p+i+n+u+g
#E:      Empty group
#>:      Growing logfile p+u+g+i+n+S

#
# You can alse create custom rules - my home made rule definition
# goes like this
MyRule = p+i+n+u+g+s+b+m+c+md5

#
# Next decide what directories/files you want in the database
#
/$ MyRule         # check the files in the / directory, don't recurse
/etc p+i+u+g      # check only permissions, inode, user and group for
                  # etc
/bin MyRule       # check /bin, recurse
/sbin MyRule      # check /sbin, recurse
/var MyRule       # check /var, recurse
/kernel MyRule    # check /kernel, recurse
/platform MyRule  # check /platform, recurse
/opt MyRule       # check /opt, recurse
/usr MyRule       # check /usr, recurse

#
# Now we deselect some directories and files
#
!/var/log/.*            # ignore the log dir it changes too often
!/var/spool/.*          # ignore spool dirs as they change too often
!/dev/.*                # ignore the /dev directory
!/devices/pseudo/.*     # ignore the /devices directory
```

```
!/mnt             # ignore the /mnt area
!/proc            # ignore the /proc file system
!/var/run         # ignore the tmpfs file system /var/run
!/var/mail        # ignore the mailspool

!/var/adm/utmpx$        # ignore /var/adm/utmpx
!/var/adm/wtmpx$        # ignore /var/adm/utmpx
!/var/adm/lastlog$      # ignore /var/adm/lastlog
!/var/cron/log$         # ignore cronlog
!/var/saf/zsmon/log     # ignore the saf log
!/etc/mnttab$           # ignore mnttab
!/etc/ntp.drift$        # ignore the ntp driftfile
!/etc/utmppipe$         # ignore utmppipe
!/etc/.syslog_door$     # ignore .syslog_door
!/etc/saf/_sacpipe$     # ignore _sacpipe
!/etc/saf/zsmon/_pmpipe$ # ignore _pmpipe
!/etc/cron.d/FIFO$      # ignore the cron FIFO
```

Appendix G – sample LogSentry report

```
From: root@xxx.xxx.xxx.xxx
To: root@xxx.xxx.xxx.xxx
Subject: xxxx xx/xx/xx:xx.xx system check

Security Violations
=-=-=-=-=-=-=-=-=-=-
xxx xx 08:36:21 pix1 %PIX-2-106001: Inbound TCP connection denied from
xxx.xxx.xx.xx/42393 to xxx.xxx.xxx.xxx/80 flags SYN  on interface
outside
xxx xx 08:42:27 pix1 %PIX-2-106001: Inbound TCP connection denied from
xxx.xxx.xxx.xxx/42430 to xxx.xxx.xxx.xxx/80 flags SYN  on interface
outside
xxx xx 08:44:55 pix1 %PIX-2-106001: Inbound TCP connection denied from
xxx.xxx.xxx.xxx/42734 to xxx.xxx.xxx.xxx/80 flags SYN  on interface
outside

Unusual System Events
=-=-=-=-=-=-=-=-=-=-=-
xxx xx 08:36:21 pix1 %PIX-2-106001: Inbound TCP connection denied from
xxx.xxx.xxx.xxx/42393 to xxx.xxx.xxx.xxx/80 flags SYN  on interface
outside
xxx xx 08:42:27 pix1 %PIX-2-106001: Inbound TCP connection denied from
xxx.xxx.xxx.xxx/42430 to xxx.xxx.xxx.xxx/80 flags SYN  on interface
outside
xxx xx 08:44:55 pix1 %PIX-2-106001: Inbound TCP connection denied from
xxx.xxx.xxx.xxx/42734 to xxx.xxx.xxx.xxx/80 flags SYN  on interface
outside
xxx xx 08:30:01 switch2 7569: 2y2w: %LINK-3-UPDOWN: Interface
FastEthernet0/32, changed state to down
xxx xx 08:30:01 switch2 7570: 2y2w: %LINEPROTO-5-UPDOWN: Line protocol
on Interface FastEthernet0/32, changed state to down
xxx xx 08:30:06 switch2 7571: 2y2w: %LINK-3-UPDOWN: Interface
FastEthernet0/32, changed state to up
xxx xx 08:30:06 witch2 7572: 2y2w: %LINEPROTO-5-UPDOWN: Line protocol
on Interface FastEthernet0/32, changed state to up
xxx xx 08:40:57 switch4 7106: 2y0w: %LINK-4-ERROR: FastEthernet0/31 is
experiencing errors
```

Appendix H – CIS Ruler Output

```
*** CIS Ruler Run ***
Starting at time xxxxxxxx-xx:xx:xx

Couldn't open /opt/CIS/cis_ruler_suid_programs_sunos_5.9 -- list of
standard SUID programs for Solaris 5.9  .
Couldn't open /opt/CIS/cis_ruler_sgid_programs_sunos_5.9 -- list of
standard SGID programs for Solaris 5.9  .
Positive: 1.1 System appears to have been patched within the last
month.
Positive: 2.2 telnet is deactivated.
Positive: 2.3 ftp is deactivated.
Positive: 2.4 rsh, rcp and rlogin are deactivated.
Positive: 2.5 tftp is deactivated.
Positive: 2.6 network printing is deactivated.
Positive: 2.7 rquotad is deactivated.
Positive: 2.8 CDE-related daemons are deactivated.
Positive: 2.9 kerberos net daemons are deactivated.
Positive: 3.1 Miscellaneous scripts are all turned off.
Positive: 3.2 NFS Server script nfs.server is deactivated.
Positive: 3.3 This machine isn't being used as an NFS client.
Positive: 3.4 rpc rc-script is deactivated.
Positive: 3.5 ldap cache manager is deactivated.
Positive: 3.6 The printer init scripts are deactivated.
Positive: 3.7 volume manager is deactivated.
Positive: 3.8 Graphical login is deactivated.
Negative: 3.9 Mail daemon is on and collecting mail from the network.
Positive: 3.10 Web server is deactivated.
Positive: 3.11 snmp daemon is deactivated.
Positive: 3.13 Serial login prompt is disabled.
Positive: 3.12 inetd/xinetd not activated.
Positive: 3.14 Found a good daemon umask.
Positive: 4.1 Coredumps are deactivated.
Positive: 4.2 Stack is set non-executable
Positive: 4.3 NFS clients use privileged ports.
Positive: 4.4 Network parameters are set well.
Positive: 4.5 TCP sequence numbers strong enough.
Positive: 5.1 syslog captures auth messages.
Positive: 5.2 /var/adm/loginlog exists to track failed logins.
Positive: 5.3 cron usage is being logged.
Negative: 5.4 Couldn't read the /etc/rc2.d/S21perf file to check for
system acctg.
Negative: 5.4 Couldn't open /var/spool/cron/crontabs/sys to look for
sa1 and sa2 -- no system accounting.
Negative: 5.5 kernel-level auditing isn't enabled.
Negative: 6.1 /opt is not mounted nosuid.
Positive: 6.2 logging option is set on root file system
Positive: 6.3 /etc/rmmount.conf mounts all file systems nosuid.
Positive: 6.4 password and group files have right permissions and
owners.
Positive: 6.5 all temporary directories have sticky bits set.
Positive: 7.1 pam.conf appears to have rhost auth deactivated.
Positive: 7.2 /etc/hosts.equiv file not present or has size zero.
Positive: 7.3 All users necessary are present in /etc/ftpusers
Positive: 7.4 cron.allow and at.allow are configured correctly.
```

```
Positive: 7.5 crontabs all have good ownerships and modes
Positive: 7.7 Root is only allowed to login on console
Positive: 7.8 EEPROM is password-protected.
Positive: 8.1 All system accounts are locked/deleted
Positive: 8.2 There were no +: entries in passwd, shadow or group maps.
Positive: 8.3 All users have passwords
Positive: 8.4 Only one UID 0 account AND it is named root.
Positive: 8.5 root's PATH is clean of group/world writable directories
or the current-directory link.
Positive: 8.6 root account has no dangerous rhosts, shosts, or netrc
files.
Positive: 8.7 No user's home directory is world or group writable.
Positive: 8.8 No group or world-writable dotfiles!
Positive: 8.9 No user has a .netrc or .rhosts file.
Positive: 8.10 Umask appears to be good.
Positive: 9.1 inetd is not running, so tcpd isn't necessary.
Positive: 9.2 System is running sshd.
Positive: 9.3 This machine is synced with ntp.
Negative: 9.4 Fix-modes has not been run here.
Preliminary rating given at time: Wed Sep 11 15:59:42 2002

      Preliminary rating = 9.00 / 10.00

Ending run at time: Wed xxx xx xx:xx:xx 2002

      Final rating = 9.00 / 10.00
```