Global Information Assurance Certification Paper

A STEP-BY-STEP GUIDE TO INSTALLING AND SECURING THE TRU64 UNIX OPERATING SYSTEM VERSION 5.1A

GIAC Certified UNIX Security Administrator
Practical Assignment Version 1.9
December 2nd, 2002

1 Introduction / Description Of The System

The following guide was written as the practical assignment required to complete the Global Information Assurance Certification (GIAC) program. Specifically the Certified UNIX Security Administrator (GCUX) assignment 1.9, option a, securing UNIX step by step. This guide will describe in detail the steps involved to install and secure the Tru64 Unix operating system version 5.1A. The steps discussed below are based entirely on the experience of the author and the environment and institution that the OS is used in. This guide should be considered as a reference tool and not as an official or standard guide to the Tru64 operating system that other institutions or organizations should adhere to.

The system that the OS will be installed on is a HP AlphaServer DS20E, with dual 833Mhz Alpha 64-bit processors and 2GB of RAM. The two hard disks with 35GB and 72GB of space satisfy the requirements for the base operating system of 1629350.57 512-byte blocks (approx. 796MB) as well as for the associated products. It should also be noted that the graphics card is a PowerStorm 4D51T graphics module.

The system will be setup as a user workstation. The setup will be designed for a multi-user workstation with one primary user via the console and other users accessing the system via secure remote login using OpenSSH 3.4p1. This system will serve mail for the local users via Open Source Sendmail 8.12.6. Various production and administration software will be installed on this system as well. All distributed and third party software version information and the location where they can be obtained will be provided in the guide.

2 Risk Analysis

The primary security concerns of a user workstation as described above include access control, such as remote and console logins and data integrity. The main threats to the system are attackers gaining access via user accounts, exploiting software such as OpenSSH and Sendmail. The services that will be required include OpenSSH for remote connections and Sendmail for servicing mail to the users. OpenSSH will be secured to only allow SSH2 connections and denying direct remote logins to the root account. Sendmail will be configured to deny relay requests as well as disabling the expn and vrfy features that gather information about the accounts on the system. Other services that will be included are Syslog for remote logging and other basic services such as LPR printer service and the XNTPD time service. This system will be used as a single user system however other users accounts may be necessary. Remote account access will be restricted to non-root users using only the SSH2 protocol. Banners will be displayed before and after remote logins, as well as before console logins. This system will be a non-critical machine by acting as a

workstation for one primary user. Other accounts may be created but these will act as secondary accounts to those users. Sendmail will only serve mail to the primary user. In the event that the system goes down the risks will be minimal and only affect one user directly. Any other users will only be minimally affected by the loss of the machine, as this will be a secondary account for those users. The system will be exposed to the Internet and behind a network firewall.

3 OS Installation

The following sections describe the steps involved to install the Tru64 UNIX Version 5.1A operating system. The installation will only contain the base operating system with a few selected optional subsets. Select subsets from the *Associated Products* distribution will be installed later in the guide. Of the three types of installations, Mandatory, All Software or Customize select the custom installation. The Customize installation "…lets you choose which optional software subsets to install in addition to the mandatory software."[1] The mandatory software is the minimum needed to run the operating system.

At no time during the installation or modification of the operating system should the system be connected to the network. By having the system connected to the network before it has been secured could leave the system open to compromise. Once the installation is complete and the system is modified a decision will have to be made on when to put the machine on the network. Third party software will need to be installed to fully secure the system, however depending on the resources available the administer will have to decide how to get the software to the system, either offline by installing the software from a CD-ROM or online by downloading the software from the developer's website directly. This topic and the choices available will be discussed further in Section 5.

3.1 Pre-installation Tasks

Make sure that the following steps are completed before the full OS installation.

3.1.1 If the machine that the operating system is being installed on already has a previous version on it make a full backup of the current operating system.

3.1.2 Make sure that all the distribution media and documentation are present.

[1] Compaq. Compaq Tru64 UNIX Installation Guide. Houston, Texas: Compaq Computer Corporation, 2001. Product Version: Tru64 UNIX Version 5.1A.

3.1.3 Read the *Release Notes*, *Installation Guide* and *Installation Guide – Advanced Topics* before beginning the installation process.

3.1.4 Verify that all the necessary hardware and peripheral equipment is connected properly to the machine. This includes external CD-ROM drives, tape drives, extra disk drives, any other removable media etc.

3.1.5 Check the CERT Advisory boards at http://www.cert.org/advisories/ and the BugTraq mailing list provided by SecurityFocus at http://online.securityfocus.com/archive/1 for any security vulnerabilities for this version of the Tru64 OS. If so print out the advisory, or record in some way the vulnerability and any patches, fixes, or work arounds that will secure the vulnerability.

3.2 Upgrade The Firmware

To ensure that there are no compatibility issues with the OS and the hardware make sure that the firmware on the system is up to date with the requirements for this version of the OS. The steps below will describe how to do this.

3.2.1 If there was a previous version of the OS installed on the machine use the *shutdown* command to put the system into console mode.

- #shutdown –h now

3.2.2 If no previous OS was installed on the system then turning the machine on will cause the machine to boot to the console. This is indicated by the chevron prompt, also called the triple arrow prompt because it is represented by three “greater than” signs, “>>>”

3.2.3 From here determine the name of the device that corresponds to the CD-ROM. This done with the *show device* command. The line that contains the characters RRD or CD-ROM in the third column is the device name of the CD-ROM device.

- >>>show device

3.2.4 Insert The *Firmware Update* CD into the CD-ROM and boot from the system from it. Use the *boot* command.

- >>>boot *CD-ROM-Device-Name*

3.2.5 Follow the on screen instruction for upgrading the firmware. Once the upgrade is complete power off the system for at least 10 seconds to initialize the new firmware and then turn the system back on.

3.3 Processor Setup

There are a few steps that must be done to configure the system processor for this version of the OS.

3.3.1 Set the processor specific environment variables depending on the processor type in the system. Check Table 6.1 in the *Installation*

Guide for processor types and any specific environment variable that must be set.

3.3.2 Set the standard console environment variables.

- Reset the *boot_osflags* variable to ensure that the systems boot properly.
  - >>>set boot_osflags “”
- Set the automatic action to halt in case there is a problem during the installation. This will be changed back later in the guide to allow the system to reboot to multi-user mode automatically. If this is left at halt then when the machine is power cycled, either intentionally by the user, power outage, or a malicious person then the system will boot to the chevron prompt. At the chevron prompt severe damage can be done to the system, either intentionally or not.
  - >>>set auto_action halt

3.4 Begin OS Installation

The following steps are the main steps to installing the Tru64 UNIX operating system. The process is available with a text-based interface or with a graphical user interface. This guide will use the graphical user interface or GUI. The GUI is menu driven, meaning that there are buttons that allow for the administrator to proceed to the “next” step or go “back” to redo a step. No action is taken until the last step where all the choices and options are verified and the actual installation process begins. Also there are the standard “File”, “Edit” and “Help” pull down menus along the top of the window.

3.4.1 From the chevron, “>>>”, prompt, enter the *init* command.

- >>>init

3.4.2 Insert the *Operation System Volume 1* CD into the CD-ROM and boot off of it as before during the firmware upgrade.

- >>>boot *CD-ROM-Device-Name*

3.4.3 Once the system has booted off the CD-ROM select the language for the GUI.

3.4.4 The welcome screen. This screen is a general welcome and the basic instructions on using the GUI for the installation. In order to switch to the text-based version of the installation, select Quit from the pull down File menu. The text-based method is similar to the GUI in that no action is taken until the last step where all the information is verified, though the order in which the steps are done may differ from the GUI.

3.4.5 Enter in the host information. In this step various information is provided such as hostname and current date/time. If any information is not provided in this step, the administrator will be prompted again for this information in the configuration phase. In this step enter in the following information.

- Hostname. A few things to note about setting the hostname.

    - If the system had a previous OS installed then choose the hostname that the system had before. Changing the hostname in this case may affect how the network recognizes the system.
    - The hostname must be between 2 and 63 alphanumeric upper or lower case characters, i.e. a-z, A-Z, 0-9. Full hostnames, xxx.xxx.xxx.xxx, are allowed with each component having a max size of 63 characters, 254 total. Each component must be separated with a period
    - Hostnames must begin with a letter. Hyphens (-) and periods (.) are allowed.
    - The words "generic" and "binary" are reserved for use by the operating system so these do not qualify as hostnames.
- Current date and time.
- Geographic area or country.
- Location or time zone.

3.4.6 Set the root password. The super user or root account on UNIX is the account typically used for administration purposes and is usually only accessible to the systems administrator(s). During and after the installation process only one account is created and that is root. All other accounts must be created once the installation is complete. Good password practices are extremely advised when choosing the root password. The Tru64 OS has a minimum of 6 to a maximum of 16 characters for passwords. Passwords should contain a combination of letters and numbers. One of the first six characters must be a character other than a lower case letter, i.e. a number a special or upper case letter.

Good password practices are a must for the root password. If the root password is too simple it will be easy for an attacker to break in. While brute force attacks are still used, they are intrinsically slow. Most connections fail after a few failed login attempts. Such attacks are easily detected. If an attacker somehow gets hold on the encrypted password strings or even the /etc/passwd file, by password sniffing, social engineering etc, they can attempt to decrypt the encrypted password using any number of password cracking utilities that are out there. With the high speeds of today's computers this is becoming much easier to accomplish.

If no root password is specified now then the installation process will ask again for a root password. At this time a password must be chosen in order for the installation process to continue.

3.4.7 The next step is to pick the installation type. The default option is the Mandatory Only option. This type of installation will only install the minimum number of subsets required to run the OS. For the purposes

of this guide the installation type will be the Customize installation. This will install the base operating system as in the Mandatory Only Installation but will allow the administrator to choose additional subsets.

Clicking on the Customize installation option and then the Edit List button will bring up a window that lists all the optional subsets that can be selected. The first category of subsets is the required subsets. This is selected by default. These are the subsets that are installed when the installation type selected is Mandatory Only. Each category has a button that will expand the list to show all the available subsets under that category. For this guide the optional subsets that are to be installed are:

- General Applications: select DOS Tools and PERL Runtime.
    - DOS Tools will install the *mtools* commands that will allow the user to manipulate files on an MS-DOS file system such as a floppy disk.
    - The PERL Runtime will install the libraries necessary to install and run PERL programs.
- Kernel Build Environment: select the AdvFS Kernel Modules. This will install the Advanced File System.
- Printing Environment: select Local Printer Support. This subset will install the printer commands, utilities, configuration files etc.
- Reference Pages: select Ref Pages Admin/User and Ref Pages CDE Admin/User.
    - Ref Pages: Admin/User. This will provide for online reference pages for administrators and users.
    - Ref Pages: CDE Admin/User. This will install the online reference pages for the Common Desktop Environment (CDE) for general users and administrators.
- Software Development Software Subsets: select Standard Header Files, Standard Programmer Commands and Static libraries
    - Standard Header Files contain the header files needed for C programming.
    - Standard Programmer Commands contains libraries and utilities. Including the libraries in order to analyze programs with the lex and yacc parser packages.
    - Static Libraries will install static libraries for programs that cannot use the shared libraries.
- System Administration Software Subsets: select AdvFS, AdvFS Daemon, AdvFS GUI, Service Tools, System Accounting Utilities and System Exercisers.
    - AdvFS. This will install the AdvFS commands to create as well as maintain the Advanced File System.

- AdvFS Daemon will install the Advanced File System daemon.
- AdvFS GUI installs the GUI for the AdvFS administration utility.
- Service Tools will install the syscheck utility that helps report problems about system crashes.
- System Accounting Utilities provide files needed to do system accounting.
- System Exercisers installs programs that will aide in diagnosing problems with hardware and peripheral devices.

3.4.8 Select the customize kernel option. The default for the graphical user interface is the Mandatory Only option. By selecting Customize a menu of possible option is presented after the system is rebooted. (In Section 3.4.11 the system will reboot itself after installing the OS and will then prompt with a menu to select the kernel components to build the kernel.)

3.4.9 Pick Custom File System Layout installation. Selecting Customize File System Layout and then clicking on the Next button will bring up the dialog box to change the file system layout. Select Edit Partitions to change how each disk is partitioned. It has been the experience of the author that the user or users of the system will use all of the allotted space for the user's home directory no matter how much or how little space is allotted for them. So the /usr/users partition should be made as large as possible and preferably on a separate disk. The system in this guide has two disks, a 35GB and a 72GB disk. The 35GB disk will contain the root partition, the /usr and /var partition as well as one partition for swap space.

- Set the size of the 'a' partition to 1GB. This will be the root partition. The minimum space required for the root partition according to the *Release Notes for Version 5.1A* is 151787.57 512-Byte blocks, or approximately 74 MB. Allotting 1GB of space will leave plenty of room for expansion.
- The 'b' partition will be used for swap space. Set the size to 6GB. The swap partition is used to hold crash dumps of the system until the next time the system is rebooted. A full crash dump is equal to the size of physical memory, in this case 2GB. So it is good to have swap space with at least enough space to hold one crash dump, i.e. 4GB. Since the user data will go onto another disk more space can be allocated to this swap partition.
- The next partition is the 'g' partition. This will be the /usr partition. This partition is where the majority of the software subsets are installed. In order to accommodate the software subsets being installed and the possibility of more being installed in the future make this partition as large as possible. This partition will also include the /var file system. The /var file

system handles such directory as tmp and adm. Many programs use the tmp directory as a temporary place to store files. Also the /var partition holds volatile directories such as log files and the mail spool and cron information. Setting this partition too small might cause it to fill up more quickly and easily. Set the g partition to at least 12GB to 15GB to allow for the most space for logs and such as well as plenty of room for future subset installations. The rest of the disk could be used for this partition but it may be a good idea to leave some space in another partition for future expansion, extra swap space etc.

The 72GB disk will be reserved for the user's home directories as well as more swap space.

- The 'b' partition will be the second swap partition. Again 6GB is a good size for swap space.
- The g partition is the /usr/users partition and this will need to be as large as possible. A good size is about 30-45 GB this is a fair amount of space for the user as well as leaving some space still available for later additions, for example, more swap if need be, a back up of the root partition in the event of the first disk malfunctioning etc.

After the partitions are set, exit back to the Custom File System Layout dialog box. Here assign the Disk, Partition and Type fields to each of the file systems. Only the root, /usr, /var, swap1 and swap2 can be set during the full installation process. The /usr/users partition will have to be set up after the installation is complete.

3.4.10 Confirm and Install. Up to this point all choices made regarding the installation have not changed the system. No subsets have been installed and no changes have been made to the partitions on the hard disks. The Installation Summary window will list all the information so far collected and allow for any one of them to be changed. It is highly recommended that this window be checked to make sure that all the correct options are selected. Once all the options are confirmed select Finish from the menu at the bottom. When the Begin Installation dialog box comes up select OK. Again up until this point nothing has been installed or changed on the system. Selecting OK will begin the installation process.

3.4.11 The system reboot / configuration phase. Once the system has completed installing the OS a reboot of the system is required. When the installation is complete the commands necessary for booting off of the newly created system disk are displayed. It is a good idea to write these commands down for future reference. Enter the commands at the chevron prompt exactly as there are shown on the screen. See the *Compaq Tru64 UNIX Installation Guide* for an example of the boot command sequence.

In section 3.4.8 the option for customizing the kernel was selected. After the system reboots a menu will be displayed showing all the possible kernel options. The menu is text based and will list the possible options to build into the kernel. Select the options for NTP_TIME, CDFS and ADVFS and let the system build the kernel. See section 6.8 of the *Compaq Tru64 UNIX Installation Guide* for an example of the Kernel Option Selection menu.

The system should now boot to multi user mode once the kernel build process is complete.

3.4.12 The next step is to load the graphics software subsets. Note that this may not be necessary, depending on the requirements of the system's graphics card. The graphics card on this system will need to have these subsets installed to enhance the graphics capabilities. The software is on the *Associated Products Vol. 2* CD. This will enhance the graphics on the system. To install these subsets:

- Login as root and inset the *Associated Products Vol. 2* CD into the CD-ROM.
- Mount the CD-ROM with the *mount* command,
  - *#mount –o ro –o noversion –o rrip –t cdfs dev /cdrom*. Where *dev* is the device name of the CD-ROM. The typical device name is /devices/disk/cdrom0c for the Advanced File System. The target directory can be any directory. It may be a good idea to create an empty directory in the root directory specifically for mounting CD-ROM devices. Once mounted this is the directory that will contain the contents of the CD.
- Load the Digital PowerStorm 4D40T/4D50T/4D52T/4D60T Graphics Options with the *setld* command,
  - #setld –l /cdrom/PowerStorm_4D51T/kit.
- Once the subsets are loaded the system will have to be rebooted. The system will boot to the chevron prompt because the auto_action variable is still set to halt. At this point change the value to *restart* with then boot with the boot command. When the system comes back up the graphical display will be much more pleasing.
  - >>>set auto_action restart
  - >>>boot

3.4.13 The last step before modifying the newly created OS is to setup a partition for the users. While Customizing the file system in step 3.4.9 a partition on the second disk was created. However it could not be assigned as the root, /usr and /var file systems were. To do this log in as root and use the *diskconfig* command to verify the partition on the disk. Check that the 'g' partition is set to an AdvFS file type with appropriate size. Also check that the Domain Name and the Set name is assigned.

- Once the file partition is verified create the directory /usr/users if it does not already exist.
- Next edit the /etc/fstab so that the file system is mounted during boot time. Add a line like this:
  - *Domain-name#set-name* /usr/users adfvs rw 0 2
- In order to mount the new file system with out rebooting the machine use the mount command.
  - #mount –a, tries to mount all the entries in the /etc/fstab file.

4 Modify And Configure The OS

Now that the OS is installed and running it is time to modify several things that are defaults on the system. The OS as it stands is quite insecure. There are many processes and services that are installed and started by default that pose a threat to the system's security, SNMP for example. The steps outlined below will show how to setup banners and other notifications, disable services that are not needed but pose a threat, and provide ways to monitor the system.

4.1 System Setup Application

When logged in as root for the first time the System Setup Window is displayed. From here the administer can quickly configure the system's networking information, user services, time protocol, printers and other basic services. To launch the System Setup menu from the command line enter /usr/sbin/checklist from the root prompt. There are three options to select from, Quick Setup, Custom Setup and Cloning Information. The Quick Setup option will guide the administrator to setting up the basic services. Custom Setup will allow the administrator to do more advanced configuration. Cloning Information duplicates the configuration that is on another machine. This is convenient when setting up several identical machines. For this guide the Quick Setup option will be used. The Quick Setup option is a menu driven application that will move step-by-step through basic configuration tasks. The Quick Setup will go through the following tasks.

4.1.1 License Information. Here, enter the license information that came with the system, such as, authorization number, checksums, number of units etc.

4.1.2 The Network Interface Card. Here enter the hostname, IP address and network mask for the system. NOTE, make sure the system is not physically connected to the network, i.e. no network cables are connected to the machine. It is not yet time to put the machine on the network.

4.1.3 Routing. Select whether to use static routing or to use the gated or routed service.
4.1.4 DNS/BIND, enter here the information about the Domain Name Service server.
4.1.5 NTP will setup the system to use a Network Time Protocol server to keep time.
4.1.6 NIS and NFS. Skip this step. NIS allows multiple systems to share access to a single set of system files. NFS also allows multiple hosts to share files by mounting a remote file system. Both of these services can be useful in a closed network, but they have many vulnerabilities and should be disabled on a network exposed to the Internet.
4.1.7 Email and Printing. Enter the information for the email server and the names of the local printers.

4.2 Disable Useless Services

By default the OS sets up various services that are run at boot time. Most of these are necessary, for example the syslog daemon or cron. However there are some that are known to be very insecure. The two major insecure default services on the Tru64 OS are SNMP and Insight Manager. The Simple Network Management Protocol (SNMP) has many exploits and is inherently insecure. Disabling this service wherever possible is recommended. Similarly the Compaq Insight Manager should be disabled as well. Other services to disable include those run by the Internet Services Daemon or inetd. Note that disabling all the service run by inetd will disable some RPC services that may cause problems with certain CDE programs like dtmail.

4.2.1 Stop the SNMP daemon and change the startup script so that it is not started during reboot. In the /sbin/rc3.d directory there a several start up scripts for various services. Stop the service, and then use the move command to change the filename of the script so that it begins with a lower case “s”. This will cause the script to be ignored during the boot process.
- #./S*n*smpd stop. Where *n* is a number. The number indicates what order the scripts are started during boot time.
- #mv S*n*smpd s*n*smpd. This will rename the script so that it starts with a lower case “s”.

4.2.2 Stop the Insight Manager and change its script as in the previous step.
- #./S*n*insightd stop. Where again *n* is a number.
- #mv S*n*insightd s*n*insightd to disable the script.

4.2.3 The inetd.conf file is the configuration file for the inetd daemon. This file instructs the inetd daemon on how it is to handle Internet service requests, for example, ftp, telnet or finger. All of which are not necessary and are just another entryway for an attacker.

- Open up the /etc/inetd.conf file in a text editor. Comment out each and every line. A comment line begins with a pound "#" sign and is skipped over when the file is read.
- Once all the services are commented out the inetd daemon must be restarted. To do this use ps command to find the inetd process ID and then kill that process with the –HUP kill signal. This will cause the inetd daemon to stop and then re-read the configuration file.
    - #ps –ef | grep inetd. The second column is the process ID; use this with the kill command.
    - #kill –HUP *inetd-PID*

4.3 Disable Remote CDE logins

The operating system is designed to allow remote dtlogin session from the outside world. This poses a security risk to the system. Dtlogin, like telnet, is a very insecure way of remote login. The connection is not encrypted and the path from the host attempting the connection, typically an x-terminal, to the system cannot be trusted. If a third party is eavesdropping on the network then all accounts and passwords sent via remote dtlogin sessions can be captured in plain text. The only place the dtlogin screen is allowed is at the console itself. To disable remote CDE logins:

4.3.1 First, if it does not already exist, create this directory.
- #mkdir /etc/dt/config this is the configuration directory for the remote dtlogin service.

4.3.2 Second, copy the Xaccess and Xconfig files in the new directory.
- #cp /usr/var/.dt/config/Xaccess /etc/dt/config
- #cp /usr/var/.dt/config/Xconfig /etc/dt/config

4.3.3 Lastly edit the Xaccess file (in both directories to be safe) and comment out the line that contains "grants service to all remote displays." All lines can be commented out to be on the really safe side. A comment line begins with a pound "#" sign and is skipped when the file is read. Now when there is an XDMCP connection request the system will check the Xaccess file to see if it should allow access. Since the lines are commented out the service determines that the host making the request is not in the allow list, and therefore denies the request.

4.4 Setup Syslog

The system logging utility, syslog, is used to control the amount of logs that the system creates and where they are logged. The file that handles this is the /etc/syslog.conf file. There are three parts to the configuration file, the facility, severity and destination. The facility is the part of the system that is creating the log; these are the kernel (kern), user, mail, daemon, authorization (auth), syslog,

printing (lpr) and binary. The severity is a scale of the importance of the log entry, from the highest to lowest importance they are, emergency (emerg), alert, critical (crit), error (err), warning, notice, information (info), debug. The level of severity entered will allow all messages of that level and higher, for example a level of err will log err, crit, alert and emerg level logs. The destination is the log file that the logs are appended to which usually have the same name as the facility, i.e., kern.log, and user.log. Check the man pages of the syslog.conf file for the syntax of the syslog.conf file.

The syslog facility also allows for the administrators to utilize log hosting. For example putting in the domain name of another system for the destination will send that log to the other systems syslog facility and be logged there. This allows for multiple systems to send logs to one or two hosts where further analysis can be do done. To set up the syslog facility to log locally and remotely, complete the following steps.

4.4.1 Edit the /etc/syslog.conf file and add lines to log to the local system if they are not already there. Set the severity level to debug. This will log all messages to the log file. By setting the level to debug a large amount of information is going to be logged to the system, which can make monitoring these logs by hand very difficult. In Section 6, LogSentry will be installed and will automate the process of checking the log files on the system. The debug level will ensure that all possible log information is being recorded and checked with the LogSentry program. This is an example of a syslog.conf file:

```
#
# syslogd config file
#
# facilities:  kern user mail daemon auth syslog lpr binary
# priorities: emerg alert crit err warning notice info debug
kern.debug          /var/adm/syslog.dated/kern.log
user.debug          /var/adm/syslog.dated/user.log
mail.debug          /var/adm/syslog.dated/mail.log
daemon.debug        /var/adm/syslog.dated/daemon.log
auth.debug          /var/adm/syslog.dated/auth.log
syslog.debug        /var/adm/syslog.dated/syslog.log
lpr.debug           /var/adm/syslog.dated/lpr.log
binary.err          /var/adm/binary.errlog
msgbuf.err          /var/adm/crash/msgbuf.savecore
kern.debug          /var/adm/messages
kern.debug          /dev/console
*.emerg             *
```

4.4.2 To have the system log to another host add lines for each facility with the same severity of the local logs with a destination being the host name of the log host(s). Add the following lines to log to the log host where loghost.domain.com is the domain name of the loghost.

```
user.debug          @loghost.domain.com
```

```
mail.debug          @loghost.domain.com
daemon.debug        @loghost.domain.com
auth.debug          @loghost.domain.com
syslog.debug        @loghost.domain.com
lpr.debug           @loghost.domain.com
```

4.4.3 Next the syslog daemon must be restarted. Use the *kill –HUP* command to restart the daemon.

- #kill –HUP *syslogd-PID*

4.4.4 Finally, to allow the new system to log to the log host the host name must be in the /etc/syslog.auth file on the log host. On the loghost machine add a single line to the /etc/syslog.auth file with the domain name of the new machine. Once the new machine is on the network the logs will be sent to the log host.

4.5 Add Banners

Many institutions require some kind of disclaimer or warning be displayed before a person logs into a system. For example "The system that is being accessed is owned by XYZ Corporation and by doing so you consent to monitoring." The reasoning for this is that these banners may serve as a deterrent for some people, keeping unwanted persons out of a particular system. There are many other reasons, from using the banner to advertise the company institution to establishing liability, "…by accessing this system you agree to have your key strokes monitored…" for example, so that information gathered could be used for prosecuting. To create a banner simply add whatever text, warning, disclaimer is necessary to the /etc/issue file. The syntax of this file is plain ASCII text. Whatever text is in this file is displayed in a window at the multi-user console login screen.

4.6 Message Of The Day

Another method to display warnings or disclaimers is through the "message of the day" file. This file, /etc/motd, is designed so that the administrator can send a message to all users after the login. Whenever someone logs in remotely (the MOTD file is not displayed when a user logs in at the console) the contents of the MOTD file is displayed. Here the administrator can post information like maintenance schedules, new software, systems that may be down that the user might need to use. Also the administrator can put the same banner as in the /etc/issue file in the /etc/motd file so that the banner is displayed for those who login to the system remotely. However this time the banner is not displayed till after the user has successfully logged in.

Other information is stored in this file by default. Information like the version number and revision number of the operating system, the date the system was last updated, the location of the installation log files. Some of this information might be considered sensitive. If for example there is a known vulnerability in a specific OS version, an attacker may try to obtain that

information to then launch an attack on the system. If the attacker is able to successfully login to the system to see the MOTD then the information in that file is no longer a concern, the system is already compromised. With the availability of hacker tools, for example "root kits" made for probably all OS versions and designed to give non-privileged users privileged access, it is only a matter of time before an attacker has complete control over a system once access to obtained. However if there is an exploit against a certain OS version that will allow an attacker to gain access, the attacker could try social engineering tactics to get the information in that file.

Social engineering is where the attacker attempts to gain information (password, accounts etc) from a non-privileged user by posing as the administrator or some one else of high level. For example a common social engineering tactic is to pose as the admin and email the user for their username/password so that the "administrator" can access the account to fix a problem. On larger sites the users may not know the admin and/or not be savvy enough to know that the administrator will *never* need to know the password of a user to do any kind of maintenance, they have root access and with that complete control of the system. Root access gives the administrator access to all other user accounts. For the information in the /etc/motd file an attacker may try to use social engineering to get the user to give them the version information of the system which may allow the attacker to launch a specific attack. Therefore it is good practice to edit the /etc/motd file to remove all information referring to the OS and only leave in banners and announcements. Many patches and upgrades add information into the /etc/motd file so it will have to check and modified after any upgrades or patches to the OS.

4.7 Login Initialization Files

There are two files in the home directory of every account that contain settings for the shell that the account will run in. The first file is the *.login* file. This file is started only at the time of login and contains settings for the prompt, the mail account, type of terminal etc. The second is the *.cshrc* file and it is run every time a new shell is started. This file contains settings for things like the path and any aliases. The default *.login* file is sufficient, however it might be a good idea to check it to make sure that everything is in order. The *.cshrc* file should also be checked to make sure that the path is set properly. The path variable lists possible pathnames for a command. When a command is entered, for example *ls*, the path variable searches all the directories in its list for the directory with the *ls* command. Verify that the "set path" line contains the /usr/sbin, /usr/bin, /usr/bin/X11, /usr/dt/bin, /usr/local/bin, /usr/local/bin/X11 directories. This is mainly to make administration easier, with these directories in the path a user would only have to type *ls* instead or /usr/bin/ls every time the user wanted to list the contents of a directory.

4.8 The Root Forward File

The forward file is a comma-delimited list of email addresses that is in the home directory of each user, including root. The file is a 'dot' file meaning that the first character in the filename is a period. These files do not show up under a normal *ls* command but do with the –a option. The dot forward file (*.forward*) will forward any mail directed to that user to the email addresses listed in the file. Edit the *.forward* file and add in the email addresses of the administrator or log hosts so that any email directed to the root account on the system will get to the administrators. It is also a good idea to make sure that this file is not group or world writeable. Having a group or world writeable .forward file may pose a threat to security. Important and/or sensitive information may be sent to a possible attacker. Also the system may be setup to forward to an outside network thus allowing an attacker to send spam mail, perform a DOS on a mail server etc. while hiding the original sender. To check if the *.forward* file is group writeable use this command: *ls –al /.forward*. The permissions in the first column should read - rw - - - - - - - meaning readable and writeable by on the owner, root. If it reads other wise use the *chmod* command to change the permissions (mode) of the file *chmod u+rw,go-rwx /.forward*.

4.9 Set The Max-Proc-Per-User And The Max-Threads-Per-User

By setting the maximum processes per user and the maximum threads per user the administrator can regulate how much of the systems resources any given user can use. The maximum processes per user, or max-proc-per-user, will limit the number of processes a user can run thus prevent a possible DOS attack on the system, either intentionally or not. For example a user may be doing software development on the system. Now say that the user is testing his or her software and does not realize that the software has a bug in it where it will start an unending fork loop. Rather than use up all of the systems resources, resources that may be needed elsewhere, other users, ftp or web servers for example, the administrator can limit the number of processes and also threads that a user can use. To change the process and thread maximum do the following.

4.9.1 From the CDE, start the kernel tuner program.

- Click on Application Manager > System_Admin > Monitoring/Tuning > Kernel Tuner
- Or from the command line.
  - #dxkerneltuner
- From here select the proc subsystem from the list and change the value of max-proc-per-user to 128
- The max-thread-per-user should be somewhere around 4 times the max-proc value. Change max-threads-per-user to 512.

5 Install Patches And Third Party Software

This next section will discuss the installation of third party software onto the system. Since the system is not connected to any network a decision must be made on how to get the third party software onto the system. Most of the software described below are open source and are obtained via download from the developer's website. The version numbers of the software below will be provided, however please note that these versions are the latest as of the writing of this guide. In the future these may be replaced by newer versions.

There are several ways to get the software to the system. These include creating a hub network with a trusted machine that has all the software, burning the software to a CD and installing from there, or putting the system on the network now and downloading the software that is needed from the net. The decision depends on the particular site that the system will be put on.

Whichever method used it is important that the downloaded software be verified. Either by checksums, MD5 signatures or PGP encryption the integrity of the downloaded file must be verified. One efficient method is to have one host on a network that has the capability to verify the downloaded files, preferably by PGP, and download from there to the new system. There have been numerous attacks on these sites where an attacker puts a Trojan horse version of the software on the developer's site. In recent months, Sendmail, OpenSSL and OpenSSH have all had Trojans put on their sites. Once these versions are downloaded and installed they can install viruses, worms, backdoors etc. All of the sites that provide this software have signatures and checksums that will allow the user to verify their integrity. Checksums and MD5 signatures are useful however the file can be altered in such a way as to not change the signature, i.e. they can be spoofed and a Trojan horse program can have the same signature as the original. PGP however is much more reliable.

Also, as a precaution it may be a good idea to create a full backup of the system with the *vdump* command prior to installing any patches or software.

5.1 Install Patches

The first things to install are OS patches. Download and install any and all patches that are available for Tru64 v5.1a. Patches can be downloaded from the Compaq support site, http://ftp.support.compaq.com/patches/.new/unix.shtml. Once downloaded, install all the patches with the dupatch tool. Generally speaking make sure to install the patches in the order in which they were released, the newest patch being the one installed last. Often one patch will fix a security hole while creating another hole or bug, then a subsequent patch to fix those. Installing them in release order will ensure there are no conflicts with file applicability or compatibility. Also patches may undo some changes that the administrator has made to secure the system, for example creating a new startup script for a service or change a configuration file. After each patch give the system a quick look to see if anything has changed, use the *ps* command to see if any new services were started, check the /sbin/rc3.d directory for re-enabled

scripts and check configuration files like /etc/inetd.conf for any changes. Follow these steps for each patch kit.

5.1.1 Unzip and un-tar the patch in a directory outside the root partition. The documentation for the patches usually suggest install the patches from /tmp/CSPkit. Note that the root partition is generally small. Some patches can be upwards a hundred or so megabytes. Installing in a larger partition, for example /usr/local that has more available space, will lessen the chance of filling up a partition during installation.

- #gunzip /usr/local/*patch-name*.
- #tar –xof /usr/local/*patch-name*.

5.1.2 Once the file is un-tarred *cd* into the patch_kit directory that was just created. From there run the *dupatch* utility.

- #cd /usr/local/patch_kit
- #./dupatch.

5.1.3 After a few question on where the kit is located and the checksums are verified the main menu should appear. From here select the option to do a baseline analysis. This will check the file system for any incompatibilities with the patches and the system. Select no when asked if any of the patches with conflicts should be installed. Next select Patch Installation, then to check and install in multi-user mode. Follow the on screen instructions to select and install the patches. When asked to make the patches reversible or not select yes. This will allow the patches to be removed easily via the same dupatch utility.

5.1.4 Once all the patches are selected and installed the system will at least have to be rebooted. Some patches require the kernel to be rebuilt first and then a reboot of the system. When asked to rebuild the kernel a screen identical to the one from step 3.4.11. Select the kernel components and then reboot when prompted.

5.2 TCSH-6.12.00

The next piece of software to install is the TCSH shell. It is the preference of the author that this is included with the guide. The TCSH shell is one of many types of UNIX shell, csh, bsh, ksh, sh. All these shells are viable. The TCSH shell has many improvements over other shell, especially the csh shell. See the TCSH website for more information and to download the shell, www.tcsh.org/Home. Again this is the preferred shell of the author.

5.2.1 Download and install the TCSH shell. Download the shell from the Downloads section of the page above. Unzip and un-tar the distribution and enter the following commands (download the README file also and refer to it for more detailed instructions).

- #./configure
- #make
- #make install (installs the binary)

- #make install.man (installs the man pages)

5.2.2 The TCSH shell must be entered into the list of acceptable shells. Open the /etc/shells file in a text editor. Add one line containing the path to the TCSH binary with relation to the root directory, for example, /usr/bin/tcsh.

5.2.3 Next change the root account's shell either through the graphical dxaccounts command or the chsh / passwd –s commands. This will be the shell given to all users added to the system. It is important to note that changing the root shell may cause problems. Some systems do not always support every shell when in single user mode. To check boot to single user mode and then start the shell manually. If successful it is probably ok to change the root account's shell to the new shell.

5.3 TCP Wrappers 7.6

The next piece of software to install is TCP Wrappers. TCP Wrappers, written by Weitse Venema, was designed to track hacker activities. TCP Wrappers use the syslog facility to log activity from various services. As well as provide an additional level of security with the ability to block connections from specific address. Prior to TCP Wrappers the only authentication for services like ftp were passwords. As long as the password was correct the connection was assumed to come from the proper place. However "with TCP Wrappers you can narrow down the criteria so is has to be someone with the proper password from the correct place."[2] Information on TCP Wrappers as well as links to where it can be downloaded from can be found on the Stanford University TCP Wrappers site, www.stanford.edu/group/itss-ccs/security/unix/tcpwrappers.html.

5.3.1 Download the distribution from the link above. Unpack the software with gunzip and tar.
- #gunzip *filename*
- #tar –xof *filename*

5.3.2 Next edit the Makefile with any text editor. Edit the file so that uses the directory where the Internet daemons are kept. On Tru64 this is the /usr/sbin directory.

5.3.3 Use the make command to create the binary. The argument for the make command is the OS type that the software is being installed on. From Tru64 Unix use the "generic" OS type. Once the binary is made copy it to the daemon directory (/usr/sbin).
- #make generic
- #cp tcpd /usr/sbin/

[2] Stanford University. "TCP Wrappers Information and Configuration." Securing Your Host – Additional Info. 26 September 2000.
URL: http://www.stanford.edu/group/itss-ccs/security/unix/tcpwrappers.html

5.3.4 Edit the inetd.conf file in the /etc/ directory. For every tcp service, even if already commented out, change the "server path", the sixth column, to the pathname of the tcpd daemon, /usr/sbin/tcpd. Wrapping the service even though it is already commented out is just a precautionary measure. The comment is there so that the service is never started in the first place, but wrapping it as well will add protection if in the unlikely event that it is turned on again, either by accident or by design.

5.3.5 Kill and restart the inetd daemon with the –HUP signal

- #kill –HUP (inetd PID)

5.3.6 Lastly edit or create the /etc/hosts.allow and /etc/hosts.deny files. Add the line "ALL: ALL" to the hosts.deny file, this will deny anything that is not specifically allowed. In the hosts.allow file add in whatever services/hosts/domains that can access the system.

5.4 PERL 5.8.0

Next install the latest version of the PERL programming language. PERL is required because of the interdependency of the next three sections. Ultimately OpenSSH will need to be installed to allow SSH encrypted remote logins to and from the system. However the dependency is that OpenSSH requires OpenSSL, which requires ZLIB and the PERL programming language. So first install the PERL programming language. The default installation process given with the distribution is satisfactory. The software can be obtained from www.perl.com.

5.4.1 Unpack the software and switch to the new PERL directory.

- #gunzip *filename*
- #tar –xof *filename*
- #cd *newdir*

5.4.2 Run these commands to configure, make, test and install the PERL software.

- #sh Configure –de
- #make
- #make test
- #make install

5.5 ZLIB 1.1.4

ZLIB must be installed before OpenSSL. Download the ZLIB compression libraries from www.gzip.org/zlib. The default installation is again sufficient for the ZLIB libraries. Unzip and un-tar the distribution and from in the newly created directory and follow the instructions in the "Makefile" to install the ZLIB compression libraries.

5.5.1 Unpack the software and switch to the new ZLIB directory.

- #gunzip *filename*

- #tar –xof *filename*
- #cd *new*dir

5.5.2 Run the following commands to configure, make, test and install the ZLIB libraries.

- #./configure
- #make
- #make test
- #make install

5.6 OpenSSL 0.9.6g

There is one more piece of software that needs to be installed prior to OpenSSH. OpenSSL is a cryptography library that can be downloaded from www.openssl.org. Similar to the ZLIB installation, install the OpenSSL libraries.

5.6.1 Unpack the software as in step 5.5.1

5.6.2 Run these commands to install OpenSSL.

- #./configure
- #make
- #make install

5.7 OpenSSH 3.5p1

The next major piece of software to install is the free SSH protocol OpenSSH. Similar to the commercial versions of SSH, OpenSSH provides a system with secure versions of various connections tools. For example the ssh program replaces the insecure rlogin and telnet programs. Also included with OpenSSH are scp and sftp, for secure copying of files and secure ftp, which replaces ftp. A secure connection between machines is vital to maintaining system security. Insecure connections like rlogin and telnet transfer data unencrypted, this includes account and password information, which can be easily obtained by an attacker. OpenSSH (and the commercial SSH) encrypt the connection and any information before it is sent so that anyone listening on the network will only see encrypted data. OpenSSH can be downloaded from the www.openssh.com website.

5.7.1 The default installation for OpenSSH uses privilege separation. Privilege separation, or privsep, causes the daemon to run as root as it should, but all child processes are run as another user with lesser privileges. For example when the daemon is running that process is owned by root. Without privsep and someone uses ssh to connect to another machine the parent process starts a new or child sshd process with the same privileges as the parent, root in this case. With privsep the child process will have different (more limited) privileges than the parent process.

PLEASE NOTE however that as of the date that this guide was written, the privsep functionality of OpenSSH does NOT work with Tru64 UNIX. There has been work on a patch for this problem but to the knowledge of the author a definitive fix has not been released. Therefore to install OpenSSH on Tru64 the privsep option will have to be turned off after the installation is complete.

5.7.2 Once the software is downloaded and unpacked *cd* into the OpenSSH directory.

- #gunzip *filename*
- #tar –xof *filename*

5.7.3 From here compile and install the OpenSSH software.

- #./configure
- #make
- #make install

5.7.4 Once the installation is complete open the /usr/local/etc/sshd_config file in a text editor. There are a few changes that must be made to the configuration file.

- Change the option "UsePrivilegeSeparation" to no. This will disable the privsep feature and allow OpenSSH to run in the traditional (prior to the privsep implementation) manner.
- Uncomment the "Banner" option and put the pathname of the login in banner, /etc/issue. This option will have OpenSSH display the login banner before asking for the password.
- OpenSSH supports both SSH version 1 and 2. Version 1 is much less secure than version 2. By default OpenSSH will use SSH2 first but fall back to SSH1 if the more secure version is unavailable. SSH1 should be disabled. To do so edit the /usr/local/etc/ssh_config and /usr/local/etc/sshd_config files. In both files there is an option called "Protocol" with a value or 2,1. Change this value to 2 only. In the sshd_config file the 2,1 simply states that version 1 and 2 are supported. In the ssh_config file the 2,1 determines the preference of the two protocols. In this case the default is SSH2 but if that is unavailable then the connection will switch to SSH1. By changing these values to just 2 connections using version 1 will be denied.
- The option "PermitRootLogin" should be discussed. This option will either allow or deny direct remote root logins. This may make remote administration a little more difficult by not letting the administrators log in as root remotely. A work around is to create an unprivileged account for the system administrators. Once logged into this account use the *su* or the *sudo* commands to get root privileges. See the man pages for *su* and *sudo*. To disable remote root logins change the "PermitRootLogin" option to no.

5.7.5 Switch directories to the /sbin/rc3.d directory and stop and restart the sshd daemon with the sshd script. As before *n* is a number that signifies the order in which the scripts are started.

- #cd /sbin/rc3.d
- #./S*n*sshd stop
- #./S*n*sshd start.

5.8 Sendmail 8.12.6

The Sendmail utility will be installed next. Sendmail can be a security risk however most of the options or functionality of Sendmail need not be enabled. The default installation is all that is required for this system, with only a few options changed in the configuration files. Sendmail is a free mail utility from www.sendmail.org website. Sendmail is a Mail Transfer Agent (MTA) that will allow the system to send and receive mail.

5.8.1 As with OpenSSH the default installation is to use privilege separation. However with Sendmail the privsep feature will work with Tru64 UNIX. The first step to installing Sendmail is to create the user and group that are required by the privsep feature.

- Use the *dxaccounts* GUI to create a group named SMMSP with GID of 25 (if possible, the GID of 25 is simply to associate that account with Sendmail which binds to port 25). When *dxaccounts* is run it initially displays the users, to switch to a list of groups select "Local Groups" from the View pull down menu.
- Next create a user named SMMSP, again with UID 25 if possible. This new user SMMSP needs to be in the group SMMSP.
- Lastly lock the account by clicking on the "Lock Account" checkbox while creating the account, or set it's password to "*". Also do not give the user account a login shell, either leave the field empty or give it the /usr/bin/false dummy shell.

5.8.2 Once the software has been downloaded and unpacked *cd* into new directory.

- #gunzip sendmail.8.12.6.tar.gz
- #tar –xof sendmail.8.12.6.tar
- #cd sendmail-8.12.6

5.8.3 Compile and install Sendmail with the following steps

- Use *cd* to move into the sendmail directory and run the build script.
  - #cd sendmail/
  - #sh Build
- Move to the cf/cf directory and copy the appropriate .mc file to sendmail.mc. Then build the sendmail.cf file.
  - #cd ../cf/cf
  - #cp generic-osf1.mc sendmail.mc

    - #sh Build sendmail.cf
- Next edit the new sendmail.cf file with any text editor. Find the line beginning with “O PrivacyOptions=” and add to the current value the string “authwarnings, goaway”. This will disable the expand (expn) and verify (vrfy) commands that can be used when someone telnets to the sendmail port. Actually the goaway option will set all of the sendmail privacy options to their most private settings. The expn and vrfy options are important because they can provide information about the accounts on the system that might be considered sensitive. For example, vrfy verifies that a given address is valid and if so give the full address of that account. This is can be used by spammers to decide who to send spam mail to. Also this will give an attacker a valid account name on the system. Often the first step in launching an attack. The expn command will expand an alias into actual email address. This can be dangerous because a machine may have lists of address called staff, users, admin etc. This could give spammers valid email address of multiple users on the system.
- Backup the current versions of the sendmail binary and .cf file.
    - #cp /usr/sbin/sendmail /usr/sbin/sendmail.bak
    - #cp /etc/mail/sendmail.cf /etc/mail/sendmail.cf.bak
- Install the .cf files from the /cf/cf directory.
    - #sh Build install-cf
- Move back to the sendmail/ directory and install the binary.
    - #cd ../../sendmail
    - #sh Build install

5.8.4 Now that everything is installed check the file permissions and ownerships on all of the files involved. They should match the following.

- /etc/mail/sendmail.cf root system - r - - r - - r - -
- /etc/mail/submit.cf root system - r - - r - - r - -
- /var/spool/mqueue root system drwx - - - - - -
- /var/spool/clientmqueue smmsp smmsp drwxrwx - - -
- /usr/sbin/sendmail root smmsp - - -x - - r - - x
  (this file usually needs to be changed from - r - x r - s r - x with a chmod a-r /usr/sbin/sendmail command).

5.8.5 Test against relaying by using telnet to connect to the mail-abuse.org site. Relaying allows a person send mail to one system by relaying off of another system. The machine that is used to relay the message will appear as the sender to the recipient thus concealing the true sender. Spammers love open relays because it hides their email address and allows them to get their spam out to numerous address quickly. Also since the relaying machine is the sender of the spam mail as far as the recipients can tell, it will be the target of any complaints or other action if the spam is offensive.

The http://mail-abuse.org site provides a way to test if mail services will allow relaying or not. All that is required is that the administrator uses the telnet command below (the system must be connected to the network to do this. If the system is not yet live then do this step once the system is put on the network). This command will show the output of various relay attempts and return to the command prompt when completed. The last few lines will say whether or not the system rejected relaying attempts.

- #telnet relay-test.mail-abuse.org
  Trying ###.###.###.###
  Connected to *hostname*
  Escape character is '^]'
  Connecting to *localhost*
  …
  …
  …

  …
  …
  …

  System appeared to reject relay attempts.
  Connection closed by foreign host.

5.9 Miscellaneous Software

There are several programs that improve upon the system administrator's tasks that should be installed on the system as well. They do not pose a significant security risk but simply help with maintaining the system. The installations are straightforward enough that they will not be discussed; however a brief discussion of the programs will follow.

Top is a useful tool that displays real time information about the systems memory. It will show load averages, memory statistics, various process and how much memory they are using. This can be a useful program to deduce memory or load problems. Top is a freely available monitoring tool and can be downloaded from many sites including ftp.groupsys.com/pub/top. Also the List Open Files, or lsof, command can be useful in troubleshooting. Lsof will list all open files by process and all communications open by process. Lsof can be downloaded form such sites as www.tru64unix.compaq.com/demos/ossc-v51a/html/shwindex.htm. Acroread is a free pdf file reader and is available from Adobe Acrobat at www.adobe.com/products/acrobat/alternate.html. The ability to read PDF files can be of use since a lot of documentation online; manuals, guides, etc are in PDF format. Another useful tool is the Pine mailer program from www.washington.edu/pine. This email program is very versatile and is run through the command line. The GUI mail utility that comes with Tru64 is fully

functional however a command line mail utility can be much more useful when logged in remotely.

6 System Stabilization

Now that this OS is installed and modified the next step is to stabilize the system. This will include creating a full backup of the system, installing backup software and setting up system monitoring software. The importance of these steps cannot be stressed enough. The previous sections dealt with ensuring that there are limited entry points for an attacker to gain access to the system. However that is only one part to securing a system. It is just as important to make sure that there are backup measures and system monitoring in place. Therefore in the unfortunate event that an attacker does gain access to the system the damage that is done is as well documented as possible and there is minimal downtime in getting the system back into production.

6.1 Install LogSentry 1.1.1

The next system-monitoring tool to install is LogSentry. LogSentry, formerly logcheck, can be downloaded from the Psionic Technologies website, www.psionic.com/products/logsentry.html. LogSentry checks the system's logs for suspicious activity. The program is setup to report based on three levels of severity, active system attacks, security violations and unusual activity. The logs are checked against several configuration files that contain strings that commonly signify attacks or suspicious activity. Monitoring the log files is important as it is often the first sign that there may be an attack on the system. Since the system uses syslog to send log entries to the central log hosts where a similar analysis is done, why install a log-checking program on this system locally? Having the logs checked locally as well as remotely will add an extra level of security. Also on a large network the logs on the log hosts may have further filtering and log entries may not be detected on the log host.

6.1.1 Download the software from the website given above. Once unpacked compile and install according to the documentation provided.

6.1.2 Edit the LogSentry script, *logcheck.sh*, so that all the desired log files are included.

6.1.3 Create a cron entry that will run the script. How often the logs are checked depends the network environment. A highly active network may want to have LogSentry run several times a day to make it as close to real time as possible. Less busy networks could do with running the script only a few times a day. Note that LogSentry keeps track of where is last stopped in the logs so that it doesn't keep reporting the same logs over and over again. The more time there is between checks will make the report email that much larger.

- To create a cron entry copy the /var/spool/cron/crontabs/root file to another directory, for example /usr/local/etc. Edit this file and add a line for the *logcheck.sh* script. Again how often the script is run will depend on the network the system is in. For example,

  00 6,12,18,0 * * 0,6 */pathname/logcheck.sh*
  00 1,3,5,7,19,21,23 * * 1-5 */pathname/logcheck.sh*
  00,30 9-17 * * 1-5 */pathname/logcheck.sh*

  will run the script every six hours on Saturday and Sunday, every other hour before and after the normal workday (Monday through Friday), and every half an hour during normal business hours (9am-5pm Monday through Friday), respectively. When finished submit the cron file with the *crontab* command, #*crontab root*. See the man pages for cron or section 6.3.4 for more information about setting up a cron entry.

6.2 Install And Setup Legato Networker 6.0.1

Legato Networker is a program that is included with the Tru64 OS, found on the *Associated Products Vol. 2* CD that creates backups of the system. A good backup and recovery system is a must on any system. Whether a user deletes their presentation by accident, the administrator changes important system files, an attacker finds their way into the system or a hardware failure occurs, being able to quickly an easily recover lost files and getting the system back into production is vital. Networker lets the administrator create a backup schedule with full and incremental backups.

6.2.1 To install the Networker software subsets first mount the CD-ROM as in step 3.4.13
- *#mount –o ro –o noversion –o rrip –t cdfs dev /cdrom*. Where *dev* is the device name of the CD-ROM as before.

6.2.2 Next use the setld command to install the subsets.
- #setld –l /cdrom/Networker/kit

6.2.3 Once the subsets are install launch the Networker administration program, *nwadmin*. Under the Server menu select registration. If the enabler code has not already been set then do so (See the help menu for information on setting the enabler code). Once that is set then send an email to service@legato.com to request an authorization code. Once the authorization code is received enter it in the appropriate field in this window. Without an authorization code the program will expire after the trial period.
- #/usr/opt/networker/bin/nwadmin

6.2.4 To select a backup schedule open the Client Setup window under the Clients pull down menu. The type of backup schedule depends on the network environment. A simple user workstation may only need to have a full backup be done say once a month with incremental backups done every day. Backups should be done during off hours as

they may slow the system down depending on how much data is being backed up. The default time for backups is at 3:33am this will be sufficient.

6.2.5 Networker sends notifications about the backups for example summaries on successful backups, notices that the backup media is full. By default these are sent to the root account on the local machine. This is sufficient since the system will forward all email to the root account to the administrators.

6.2.6 Finally select the Group Control button and select the Start button. This will start the backup schedule. A backup will immediately begin. Since the software was just installed there is no record of backups so the first backup will be a full backup by default.

6.3 Setup Tripwire ASR 1.3.1

Tripwire is a program that checks the integrity of the file systems on the machine. Once installed Tripwire works by checking all the files on the system against a database that it creates and verifies that the characteristics, i.e. size, timestamps, checksums etc, are consistent with the database. Any changes, additions or deletions to the file systems are then reported to the administrators. Tripwire will allow an administrator to see what files or directories were altered or added by an intruder. Because of this it is important to keep the integrity of the database secure. A very skilled attacker may replace the database with an altered one to hide their tracks if the database is not kept secure. Preferably the database will be kept on some sort of removable and write protected media, a CD for example.

6.3.1 First download Tripwire ASR 1.3.1 from this website www.tripwire.com/products/triwpire_asr. This is the Academic Source Release of the tripwire program. The program was first created as a free utility but has since become a commercial product. There are great improvements to the core program available commercially, however the ASR version will be discussed in this guide.

6.3.2 Once downloaded compile and install the program according to the documentation. Once installed the *tripwire* and *siggen* binary files must be moved to either a disk that can be set as read only by a hardware setting or some type of removable media such as a CD-ROM. The *tripwire* binary is the main tripwire program; *siggen* allows the user to get a tripwire signature of a file with out having to run the entire program. This is useful for a quick check on one or two files.

6.3.3 To create the database run tripwire from the command line with the initialize, *-init*, argument. This may take several minutes to compete. Once the database file is created copy it to the database

directory and remove the original, also make a copy of the database to keep on floppy or CD-ROM. In the event that the system is compromised, having a clean copy on floppy will help to determine the integrity of the database on the compromised machine.

- #*pathname*/tripwire –init

  Tripwire(tm) ASR (Academic Source Release) 1.3.1
  File Integrity Assessment Software
  (c) 1992, Purdue Research Foundation, (c) 1997, 1999 Tripwire Security Systems, Inc. All Rights Reserved. Use Restricted to Authorized Licensees.
  ### Phase 1: Reading configuration file
  ### Phase 2: Generating file list
  ### Phase 3: Creating file information database
  ###
  ### Warning: Database file placed in ./databases/*filename*
  ###
  ### Make sure to move this file and the configuration
  ### to secure media!
  ###
  ### (Tripwire expects to find it in '*config_pathname*'.)

- #scp ./databases/*filename config_pathname*
- #rm ./databases/*filename*

6.3.4 Now that the database is created and secured, create a cron entry that will run tripwire at the desired time. While tripwire is running it will use much of the system's resources. It may be necessary to run tripwire during off hours when there is minimal activity of the system.

- Do not directly edit the root cron file. New cron files should be resubmitted with the *crontab* command. As root copy the /var/spool/cron/crontabs/root file to another location, /usr/local/etc/ for example. Edit this new file and resubmit it with the *crontab* command.
- #xedit /usr/local/etc/root.
- add this line; 0 0 * * * *pathname/tripwire*. This will run tripwire at midnight everyday of the week. The fields in a cron entry are the minute (0-59), hour (0-23), day (1-31), month (1-12), day of the week (0-6 for Sunday to Saturday) and the command to be run. Asterisks will count for all possible values.
- #crontab /usr/local/etc/root. This will copy the /usr/local/etc/root file to the crontabs directory, *crontab* will only affect the crontab file of the authority that the command was invoked. For example if running *crontab* as root the

/var/spool/cron/crontabs/root file would be affected, if running *crontab* as adm then the /var/spool/cron/crontabs/adm file would be changed.

6.4 Create A Full Dump

The next step in stabilizing the machine is to manually create a full backup of the system with the (v)dump command. There is one caveat about the Networker backup software installed in step 6.2. The system uses Networker to create a backup but in order to restore from that backup the Networker programs and index databases need to be on the system. If the file system that contains those programs is lost due to a hardware failure for example the administrator will not be able to use the backups created with Networker. For this reason it is also a good idea to manually create a full backup using the UNIX command vdump. This way if the Networker programs are unavailable the file system can be rebuilt enough so that the Networker backups can be used. The manual backups do not need to be done often, once every few months will be sufficient.

6.5 Physical Security

Finally the Physical security of the system must be maintained. This includes restricting access to the system and protecting the system from environmental damage.

6.5.1 Make sure the system is behind closed and locked doors during off hours. Physical access to a machine means root access to an attacker. By continually power cycling the system it will often cause one or more file system to become "dirty" and cause the system to boot to single user mode where it can be "cleaned" with the *fsck* command. Once in single user mode the attacker will have complete control of the system.

6.5.2 Some systems have doors on them that allow easy access to the CD-ROM or tape drives or the inside of the system itself. Some system may have a door that allows access to the hard disks that are not screwed to the chassis but are connected to slots that allow for easy removal of the disks. It is important to keep all doors such as these locked to prevent tampering.

6.5.3 Make sure that all accounts, including root, on the system allow for screen locking. While the system is not in use, the user may have gone to lunch for example, the system should lock after a certain amount of time. It is important that all users, especially root, lock the screen whenever they are going to be away from the system, even if it is to just go into the next room of a few minutes. Tru64 has a screen-locking button on the CDE Front Panel. The button that resembles a pad-lock will lock the screen and require the

account's password to unlock it. All users are urged to use this button when they leave the system unattended.

6.5.4 Connect the system to a UPS or uninterruptible power source. These devices allow the system to remain on even when the power from the wall outlet is cut off, possibly from a power outage. Most will only support the system for a few minutes if the power is out, long enough to shutdown the system properly. The more useful part of a UPS is during brown outs, short losses of power that would cause the system to reboot if it were not connected to a UPS.

6.5.5 Keep the system safe from environmental hazards such as water and fire. Make sure the room that the system is in has a sprinkler system installed to control fires. Cover the systems with plastic covers in case the sprinklers do go off, the sprinklers may cause more damage to a system than a small fire on the opposite side of the room or another floor. Put the system on a raised surface to prevent damage if there is a flood.

6.5.6 Keep the system up to date with the patches for the operating system and new versions of the third party software. It may be a good idea to join a mailing list so that information about patches and updates are received as soon as possible. Most of the websites given above will have such lists that the administrator can join. Also perform audits on a regular basis. Look over the entire system, from top to bottom, and verify that all parts of the hardening process are still intact and that all services are running properly.

6.5.7 Finally keep a set up full backups off site. If the unfortunate happens and the facility the system is housed in is destroyed, either by fire, flood etc having an offsite copy of the system backups will allow for a quicker recovery and minimize data loss.

7 Final System Check

This final section will be a quick check of some of the major steps discussed in this guide.

7.1 Test The Sendmail Configuration

For Sendmail check that the proper version is running, that the expn and vrfy commands are disabled and that relaying is denied.

7.1.1 Telnet to port 25 on the local host and verify that the proper version is running, version 8.12.6.

- #telnet *hostname* 25
  Trying ###.###.###.###
  Connected to *hostname*
  Escape character is '^]'
  ### *Hostname Version info date time*

quit

7.1.2 Check that the expn and vrfy telnet commands are not functioning.

- #telnet *hostname* 25
  Trying ###.###.###.###
  Connected to *hostname*
  Escape character is '^]'
  ### *Hostname Version info date time*
  expn
  ### ##### Sorry, we do not allow this operation
  vrfy
  ### ##### Cannot VRFY user; …
  quit

7.1.3 If not already done so, check that relaying is being denied by using telnet to connect to relay-test.mail-abuse.org.

- #telnet relay-test.mail-abuse.org
  Trying ###.###.###.###
  Connected to *hostname*
  Escape character is '^]'
  Connecting to *localhost*
  …
  …
  …

  …
  …
  …

  System appeared to reject relay attempts.
  Connection closed by foreign host.

7.2 Test OpenSSH

Test OpenSSH to see if the correct version is running. Connect to and from the log hosts or administration system to exchange RSA keys. These keys are part of the verification process from SSH.

7.2.1 Test that the correct version of OpenSSH is running with the –V option. This option will have OpenSSH simply return the version information.

- #slogin -V

7.2.2 Use slogin or ssh to connect to and from the log hosts or administrators machine in order to exchange RSA keys. Use the –v (lowercase v for verbose) option to check that the protocol 2.0 is used. SSH1 is older and is less secure that SSH2.

- #slogin –v *hostname*

- Look for the line that says “Enabling compatibility mode for protocol 2.0”.

7.3 Confirm That Syslog And LogSentry Are Working

To verify that syslog is logging properly check the log host for entries from the new machine. By now several logs should have already been sent via syslog. For quick check use any mail utility, pine, dtmail or the mail command line command on the new system and send a message to the root account from the root account. Check the /var/adm/syslog.dated/current/mail.log file on the log host, the email just sent should have been logged. LogSentry keeps a marker of where it last stopped checking the logs. To check to see if LogSentry is working properly first run the script manually by starting the logcheck.sh script, *./pathname/logcheck.sh*. Next create a log entry that LogSentry will report, for example try and use the *su* command to change to the root user. Then run LogSentry again.

7.4 Check The Running Processes

With the *ps* command check the current running processes and make sure that the services that were disabled are not running. Look at the /etc/inetd.conf file to make sure that all the useless services are commented out. It may also be a good idea to reboot the system to see if the startup scripts in the /sbin/rc3.d directory that were moved are not started during reboot. Restart the machine and check that they are in fact not running. As an example the output of the ‘*ps –ef* ‘ command may look similar to the following.

- #ps -ef

root	0	0	0.0	Dec 23	39:51.10	[kernel idle]
root	1	0	0.0	Dec 23	1:14.58	/sbin/init –a
root	3	1	0.0	Dec 23	0:01.68	/sbin/kloadserv
root	23	1	0.0	Dec 23	0:00.02	/sbin/update
root	140	1	0.0	Dec 23	13:53.41	/usr/sbin/syslogd
root	144	1	0.0	Dec 23	0:01.69	/usr/sbin/binlogd
root	560	1	0.0	Dec 23	0:05.43	/usr/sbin/xntpd
root	587	1	0.0	Dec 23	0:00.00	/usr/sbin/inetd
root	620	1	0.0	Dec 23	0:17.56	/usr/sbin/cron

  …
  …
  …

- Make sure processes such as */usr/sbin/portmap*, */usr/sbin/snmpd, /usr/share/sysman/bin/insightd* are not running. If they are, stop the process with the *kill* command, *kill –9 PID*. Also check the /sbin/rc3.d directory and verify that the start up scripts have been disabled as in step 4.2.

7.5 Run Tripwire Manually

Lastly run the tripwire program manually to test the system. Update the database with any changes to the system by using the –update or –init option. Once the new database is created and copied over to the database directory/media create a new file or directory in a place that Tripwire checks. Run the Tripwire program again and verify that the newly created file/directory was caught by Tripwire. Delete that test file/directory and update the database.

- #*pathname*/tripwire

  Tripwire(tm) ASR (Academic Source Release) 1.3.1
  File Integrity Assessment Software
  (c) 1992, Purdue Research Foundation, (c) 1997, 1999 Tripwire Security Systems, Inc. All Rights Reserved. Use Restricted to Authorized Licensees.
  ### Phase 1: Reading configuration file
  ### Phase 2: Generating file list
  ### Phase 3: Creating file information database
  ### Phase 4: Searching for inconsistencies
  ###
  ### Total files scanned: 51562
  ### Files added: 437
  ### Files deleted: 0
  ### Files changed: 84
  ###
  ### Total file violations: 521
  …
  … *(list of files.)*
  …
  ### Phase 5: Generating observed/expected pair for changed files
  ###
  ### Attr Observed (what it is) Expected (what it should be)
  ### ==== ==================== ======================
  …
  … *(list of files with the altered attribute.)*
  …
- # *pathname*/tripwire –init (output as in step 6.3.3.)
- #scp ./databases/*file_name config_pathname*
- #rm ./databases/*file_name*
- #touch /*testfile*. This will create a file of size 0 in the root partition. When tripwire is run again it should report only this file.
- #*pathname*/tripwire
  …
  …
  …
  …
  ### Total files scanned: 51563

```
###                    Files added:              1
###                    Files deleted:            0
###                    Files changed:            0
###
###                Total file violations:         1
###
added –rw-r- -r- -     root        0     date    /testfile
…
…
…
```

- #rm /testfile
- #*pathname*/tripwire –update /*testfile* (output as in step 6.3.3.)
- #scp ./databases/*file_name config_pathname*
- #rm ./databases/*file_name*

8 Summary.

To recap there are two major parts to securing an operating system. First the OS must be installed with as little functionality as possible. What this means is that no unnecessary software or processes should be on the system. This only complicates the administration of the machine by adding more features, services, program and possible entry points that have to be monitored. If it is not necessary do not install it. The second part to securing a system is to monitor the integrity of the system at all times. It would be nice to be able to say that a system cannot be compromised, that no attacker can get in. However an administrator must assume that the system could be compromised at any time. If the system is not closely monitored an intruder may not be detected until it is too late. And with no system monitoring, finding out what the attacker did and devising a plan to restore the system may be impossible. That is why it is important that the administrator have monitoring and backup tools in place. Checking the integrity of the file system, examining the log files for signs of an attack, maintaining backups for quick recoveries etc are essential in administering a system.

References:

Compaq. Compaq Tru64 UNIX Installation Guide. Houston, Texas: Compaq Computer Corporation, 2001. Product Version: Tru64 UNIX Version 5.1A.

Compaq. Compaq Tru64 UNIX Installation Guide – Advanced Topics. Houston, Texas: Compaq Computer Corporation, 2001. Product Version: Tru64 UNIX Version 5.1A.

Compaq. Compaq Tru64 UNIX Release Notes for Version 5.1A. Houston, Texas: Compaq Computer Corporation, 2001. Product Version: Tru64 UNIX Version 5.1A.

Frisch, Æleen. Essential System Administration, Second Edition. O'Reilly & Associates, Inc, 1991, 1995.

Stanford University. "TCP Wrappers Information and Configuration." Securing Your Host – Additional Info. 26 September 2000.
URL: http://www.stanford.edu/group/itss-ccs/security/unix/tcpwrappers.html

Carnegie Mellon Software Engineering Institute, "CERT/CC Advisories" November 25, 2002
URL: http://www.cert.org/advisories.

Sendmail Consortium, "Welcome to sendmail.org." Sendmail Home Page. URL: http://www.sendmail.org

Psionic Technologies Inc. "Psionic LogSentry."
URL: http://www.psionic.com/products/logsentry.html

Tripwire Inc, "Intrusion Detection & More – The Original Data & Network Integrity Solution." URL http://www.tripwire.com/products/tripwire_asr/

Pomeranz, Hal. Common Issues and Vulnerabilities in UNIX Security. Hal Pomeranz and Deer Run Associates, 2000-2001.

Pomeranz, Hal. UNIX Security Tools. Hal Pomeranz and Deer Run Associates, 2002.

Acheson, Steve, and John Green, and Hal Pomeranz. Topics in UNIX Security. Acheson, Green and Pomeranz 2002.

Brotzman, Lee E., and Hal Pomeranz. Running Unix Applications Securely. Brotzman and Pomeranz, 2002

Brotzman, Lee E. Linux/Solaris Praticum. Lee E. Brotzman 2000-2002