Global Information Assurance Certification Paper

GIAC Certified UNIX Security Administrator (GCUX)

Practical Assignment Version 2.0, Option 1:
Securing Unix Step-by-Step

Setting Up a Secure Mail Server with HP-UX 11i v1, Qmail and Qpopper

Submitted August 3, 2004

Patrick Wallek
Securing Unix
SANS 2004 Conference

TABLE OF CONTENTS

TABLE OF FIGURES

ABSTRACT

This paper will explain how to install and secure the HP-UX 11iv1 (also known as HP-UX 11.11) operating system on an HP9000 server. The default HP-UX installation is fine if the machine it is installed on has no network access and no users accessing it. If it is attached to a network, and especially if it is Internet accessible, you must take some significant additional steps to secure the system. Detailed instructions show the steps that must be taken to secure HP-UX once it has been installed.

Once the operating system has been installed, we will install, configure and secure SMTP and POP3 server software. This will allow this machine to act as a secure mail server for internal corporate use.

PROJECT SUMMARY

An Information Services manager requested that I build a system that will reside in our DMZ and act as an SMTP / POP3 server. The server will be used for receiving specific types of mail from some of our external customers. This request was made because of some perceived instability with our main corporate Internet e-mail server.

This machine will act somewhat as a “back door” for critical e-mail messages. These e-mail messages are used by some internal applications. These applications will initiate a POP3 connection to the mail server to retrieve the messages. The server will not store any email long-term.

This server will run Qmail for its MTA and Qpopper as its POP3 server.

This server will allow very little direct access, other than POP3. No users other than the system administrator will have any capability to log in and reach an HP-UX shell prompt.

The server for this project, for the time being, is an older HP9000 Model E55 running HP-UX 11.11 (a.k.a. HP-UX 11i Version 1). If the project is successful, there is a possibility of acquiring a newer server with more built-in redundancy and capacity. The E55 will serve nicely as a proof-of-concept machine.

RISK ANALYSIS

This server will reside in our DMZ. Even though the DMZ firewall should stop most attacks on the system there is no reason to leave a system wide open. The data on this server is not super-critical. The e-mail that this server receives does make some tasks a whole lot easier, but if anything happens to this machine there are workarounds that are possible. However, we will try to mitigate any possibility of problems by securing the system as best we can.

When this server is setup, we will use the HP-UX 11iv1 (HP-UX 11.11) base OS. We want to install as few HP-UX components as is feasible. Once the OS has been installed it will be patched as completely as possible to immediately eliminate as many known problems as possible. It will also be analyzed regularly to see if any additional patches are required.

Almost all access to this machine via the network will be denied. The only exceptions are the POP3 traffic and the system administrator logging in via Secure Shell. No users, other than the system administrator, will have shell access to this system and only specifically configured users will have POP3 access. This server will not be available to corporate users.

The mail server daemon of choice for this project is Q-mail because of its small size, security and fairly simple implementation and maintenance. The native HP-UX sendmail daemon was not considered for this due to concerns from our IS security department. Only SMTP traffic from outside will be allowed into this server and all outside email relaying will be denied.

The POP3 daemon of choice for this project is Qpopper. Other POP3 daemons were tried, but none of the other open source products worked well with HP's Trusted Computing Base to secure the system. Qpopper integrates seamlessly via PAM to allow easy authentication.

HARDWARE SUMMARY

The machine being used for this project is an older HP9000 Model E55 with the following specs:

- 96 MHz Processor
- 320 MB RAM
- 2 x 4 GB Disk Drives
- Add-on HP-PB 10/100 Mb NIC

There is no built-in redundancy, like dual power supplies or hot swappable disk drives for the OS, but if this works and performs well, we may be able to upgrade the server at a later date.

SOFTWARE SUMMARY

HP Software

- HP-UX Foundation Operating Environment* - Ver. 11.11 (11i Ver. 1) - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B9089AC
- Compressed Dump – Ver. A.01.01 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=CDUMP11i
- Glance Plus Pak* – Ver. C.03.71.00 - http://www.openview.hp.com/products/gppak2k/index.html
- Ignite/UX – Ver. B.5.3.35 – http://software.hp.com/products/IUX/
- Mirror Disk/UX* - Ver. B.11.11 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B2491BA
- Online JFS* - Ver. B.11.11 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B3929CA
- Bastille – Ver. b.02.01.01 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6849AA
- HP Perl Bundle – Ver. 5.8.0 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=PERL
- Security Patch Check – Ver. b.01.05 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA
- Kernel Random Number Generator – Ver. b.11.11.07 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=KRNG11I
- HP Secure Shell (SSH) – Ver. a.03.71 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA
- HP TCP Wrappers – Ver. B.11.11.01.001 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=TCPWRAP
- HP IP Filter – Ver. a.03.05.09 - http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B9901AA
- HP GCC – Ver. 3.3.3 - http://h21007.www2.hp.com/dspp/tech/tech_TechSoftwareDetailPage_IDX/1,1703,547,00.html
- HP Binutils – Ver. 2.14 - http://h21007.www2.hp.com/dspp/tech/tech_TechSoftwareDetailPage_IDX/1,1703,547,00.html

(The HP GCC and Binutils bundles are also available as part of the Linux Porting Kit for HP-UX 11.0 and 11i. This is apparently available only via CD / DVD media and must be ordered from HP, still for free, from http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B9891AA)

- December 2003 Support Plus Patch Bundle for HP-UX 11.11 - http://www.software.hp.com/SUPPORT_PLUS/qpk.html

All software listed above, with the exception of those with an asterisk (*) beside their name, is available for free from the HP Software Depot links provided. The products denoted by the * are products you must purchase. More information on those products is available from the links provided. You get HP-UX, and the license to use HP-UX, when you purchase a server, although you can purchase it separately from HP. The Mirror Disk/UX and Online JFS software can be purchased as stand-alone products, as we have done. If you upgrade to the HP-UX Enterprise Operating Environment, when you purchase HP-UX (with or without a server), then Mirror Disk/UX and Online JFS are included.

Some of the products listed above (Perl, SSH, TCP Wrappers, IP Filter, GCC, Binutils) are available on the Internet from various sites as open source products. I have chosen to use products that HP has tested, compiled and released since HP will support them if I have problems.

Non-HP Software

The following software is freely available for download from the web sites mentioned. I know that all of the versions listed work together. If you happen to find a newer version of any of the products, it will probably work, but I don't make any guarantees.

- CFG2HTML – Ver. B.1.87 - http://come.to/cfg2html
- Lsof – Ver. 4.71 – source code http://hpux.connect.org.uk/hppd/hpux/Sysadmin/lsof-4.71/
- Gnu make – Ver. 3.80 - http://hpux.connect.org.uk/hppd/hpux/Gnu/make-3.80/
- CIS HP-UX Tool Archive - http://www.cisecurity.org/bench_hpux.html
- Patch – Ver 2.5.4 - http://hpux.connect.org.uk/hppd/hpux/Sysadmin/patch-2.5.4
- Netqmail - Ver. 1.05 source code - http://www.qmail.org/
- Daemontools – Ver. 0.76 source code - http://cr.yp.to/
- Ucspi-tcp – Ver. 0.88 source code - http://cr.yp.to
- Qpopper – Ver. 4.0.5 source code - http://www.eudora.com/qpopper/

STEP-BY-STEP GUIDE FOR INSTALLING AND SECURING THE OPERATING SYSTEM AND APPLICATIONS

Conventions

Any commands or other user input that is required will be *italicized*.
Any prompts that the user will see will be **bold**.

For example, the following means to enter 'sea' at the "MAIN MENU: Enter command or menu>" prompt.

Keys on the keyboard will be denoted in all capital letters and surrounded by <>.

For example, Please press the <ENTER> key.

MAIN MENU: Enter command or menu> *sea*

Screen Navigation

All of the screens referenced during the installation process and during the software install and uninstall processes can be navigated very easily with the keyboard.

During installation, the <TAB> key will move you from field to field on the screens and the <SPACE BAR> will 1) Select or deselect a choice in a list and 2) Activate a menu item or button.

When using the swinstall and swremove programs later in the process, the <TAB> key will activate the menu at the top of the program windows. The <LEFT ARROW> and <RIGHT ARROW> keys will move you from item to item in the menu and the <UP ARROW> and <DOWN ARROW> keys will move you up and down to the various menu selections. You can press <ENTER> or the <SPACE BAR> to select a menu choice.

You can also use the arrow keys to navigate through the software selection portion of the window. The <UP ARROW> and <DOWN ARROW> keys will scroll up and down and the <LEFT ARROW> and <RIGHT ARROW> keys will scroll you left and right which will allow you to see more of the description of some of the products. The <SPACE BAR> will select or deselect an item in the list for you.

Installing HP-UX 11.11

The easiest way to install the operating system is via a terminal directly attached to the console port of the machine. An HP 700/92 or 700/96 terminal works very well.

However, I am using Hyperterminal on my Windows XP Pro PC to do this. I have an HP cable (part # 24542, I think) with one end plugged into the console port of the E55

via a 9-pin to 25-pin null modem adapter and the other end plugged into the serial port of my PC. I set Hyperterminal to 9600-baud, 8 parity bits, no flow control, 1 stop bit, VT100 terminal emulation and pointed it to the appropriate serial port on the PC. Some of the screens do not behave exactly as they should, but it is a fairly functional set up.

We will now begin installing the HP-UX operating system. Follow these steps and you should not have any problems.

1. If the machine is turned off, turn it on. If the machine is turned on, reboot it with the command:

   # *shutdown –ry 0*

   In either case, watch the machine as it proceeds through its self-tests. You will eventually be prompted "To discontinue, Press any key within 10 seconds". At this point, press the <SPACE BAR>, or any other key, to interrupt the boot process. You should now be at the following prompt:

   MAIN MENU: Enter command or menu>

2. Insert the first of the 3 CDs labeled "core os install and recovery version B.11.11" into the CD-ROM drive and boot from it. On this machine I issue the command:

   MAIN MENU: Enter command or menu> *bo 56/52.2*

   Next I will be asked if I want to interact with IPL. I don't.

   Interact with IPL (Y or N)? *N*

   The machine will now begin booting from the CD.

   If you do not know what device your CD-ROM drive is, you can do a

   MAIN MENU: Enter command or menu> *sea ipl*

   This will look for all devices on the system that you can boot from and list them. From this list you should be able to determine which device is your CD-ROM. You can then boot from that device.

3. When you have booted from the installation CD, you will get the "Welcome to the HP-UX Installation/recovery process!" menu. At this menu "Install HP-UX" should already by selected. Press <ENTER> to proceed to the next screen.

4. The next screen you get will be the "User Interface and Media Options" menu. In the "Source Location Options:" section select "Media Only Installation", which

should be the default. Next select “Advanced Installation” from the “User Interface Options:” section. Now select OK to proceed.

5. You should now have the “Media Installation Selection” screen up. The default selection should be “CD/DVD Installation”. If it is not then select “CD/DVD Installation” and then select OK to continue.

6. After a few seconds you should get a window with the title “/opt/ignite/bin/itool()”. We are now getting to the nitty-gritty of HP-UX installation process. I will cover each section of this screen (Basic, Software, System, File System and Advanced) and then changes that need to be made on each screen.

BASIC

The following are the menu selections on this screen that I have changed from the default:

ENVIRONMENT – HP-UX 11i Base OS – 32 bit

The default for the Environment selection is “HP-UX 11i OE – 32bit”. Since we want to start with as stripped down an OS as possible, we select the “HP-UX 11i Base OS” instead (See Figure 1).

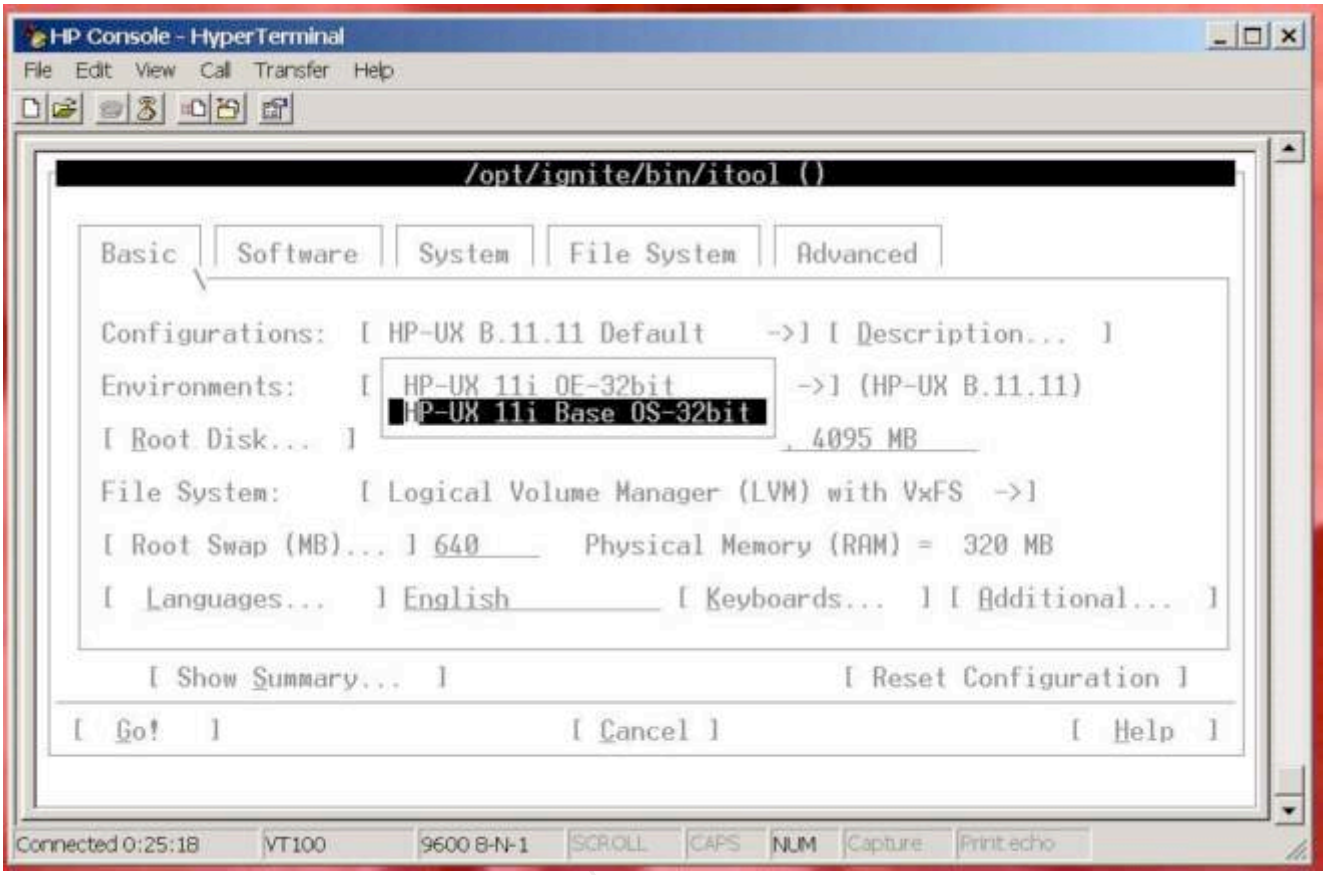

Figure 1 – HP-UX 11i Base OS

Depending on your machine, you may have to change the ROOT DISK selection. Since I only have two disks in this machine, which will be mirrored later anyway, it does not matter which disk is selected. You should make sure that the disk that is listed is the disk you intend to install the operating system on.

SOFTWARE

We want to NOT install as much of the software as possible. We will unmark as much as the tool will allow us. Unfortunately, we cannot unmark all the software we don't want, even though it is impossible for some of it to work on this machine. We will uninstall the rest of the unnecessary software later.

The software we want to deselect (change the "Marked?" column from YES to NO) is:

- XIMIAN GNOME
- Java2 RTE for HP-UX
- Java2 Plugin for HP-UX
- Java2 1.3 RTE
- Mozilla 1.2 for HP-UX
- Mozilla 1.2 Source Distribution

- Java2 1.3 Netscape Plugin
- HP-UX Apache based Webserver
- HP-UX Tomcat based Servlet Engine
- HP-UX Webmin based Admin tool
- HP-UX XML Web Server Tools
- Perl Programming Language (Note – We will install a newer version of Perl later)

SYSTEM

The selection for the "Final System Parameters" item should be set to "Set Parameters Now". If it is not, <TAB> to that menu item and set it to "Set Parameters Now".

We will set almost all of the parameters now so we don't have to worry about them later.

We will first set the hostname, ip address, subnet mask, date and time as shown in Figure 2.

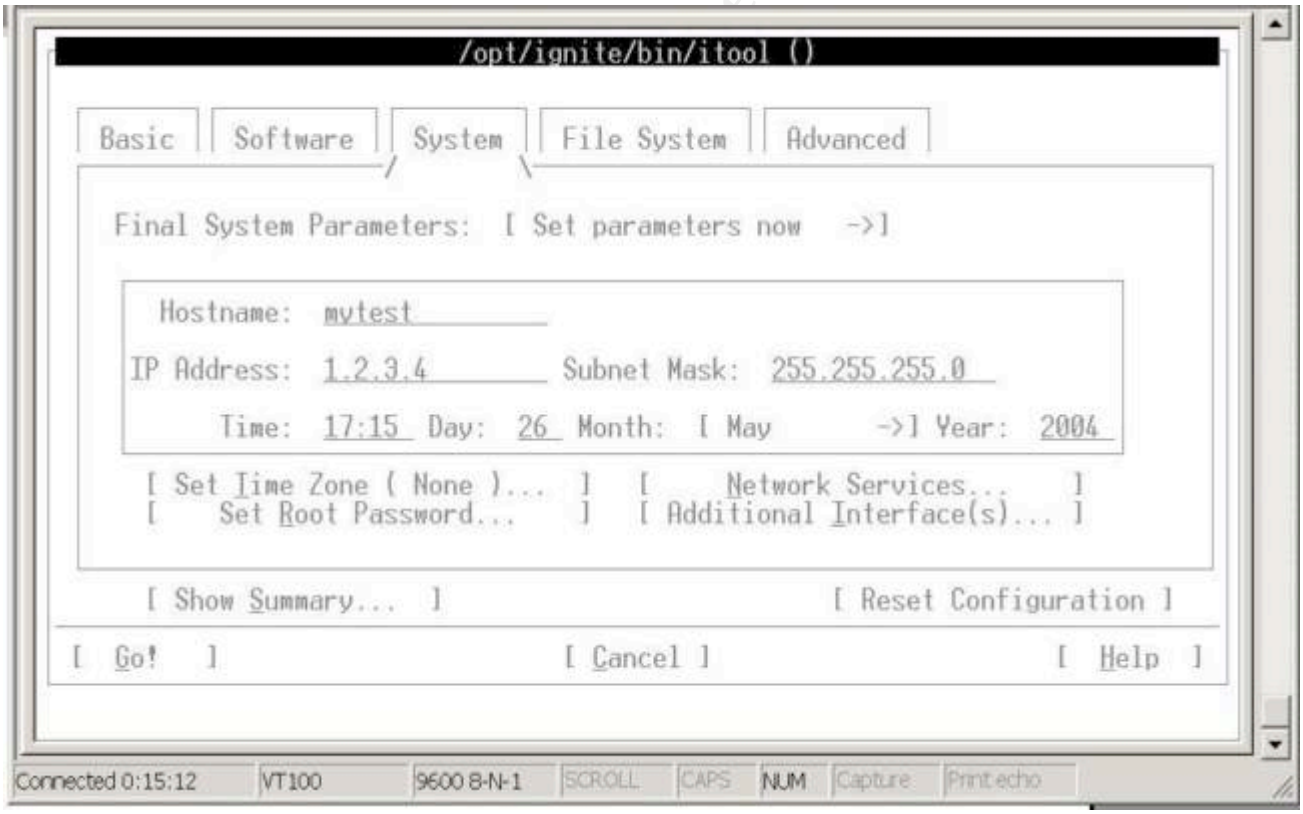

Figure 2 – Network Properties

Next, <TAB> down so you have the "Set Time Zone (None)…" highlighted and then press <ENTER>. The window that comes up will allow you to select whatever time

zone is appropriate for your area. We will select "Central Standard/Daylight CST6CDT".

Next, <TAB> down to "Set Root Password…". You will need to enter the password twice and the system will verify that you entered the same thing twice.

Next we will go to the "Network Services…" selection and press <ENTER>. This will bring up another window with several selections as in Figure 3.

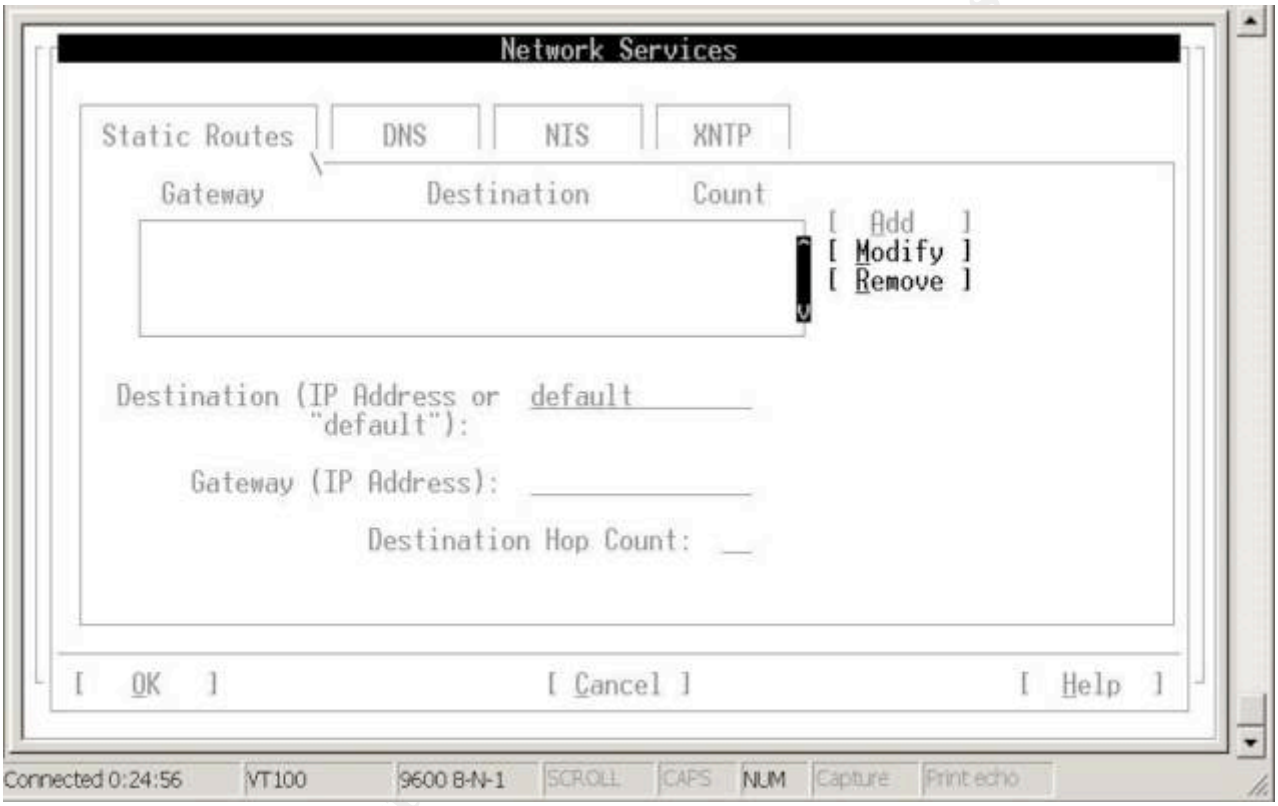

Figure 3 – Network Services

We will be setting up the "Static Routes," "DNS," and "XNTP" services.

To set up your default router, <TAB> down to the "Gateway (IP Address:)" field and enter the IP address of the appropriate router. In our case it is 1.2.3.1. Now, <TAB> down to the "Destination Hop Count:" field and enter 1. Next, <TAB> back to the "[Add]" selection and press the <SPACE BAR> to add the default route. You should now see an entry added in the windows to the left of the Add, Modify and Remove selections. If this looks correct, we can proceed to DNS.

Now, <TAB> up to the "DNS" <TAB> at the top of the screen and press <ENTER>. This will bring up the DNS screen. The cursor should already be in the "Domain Name:" field. Enter the appropriate domain for your environment. Next <TAB> down to the "DNS Server IP Address:" field and enter the IP address for your DNS server. Finally,

<TAB> up to the “[Add]” selection and press <ENTER> to add the DNS server to the list. You can enter up to 3 servers, if necessary, by just using the <TAB> key to navigate back to the “DNS Server IP Address:” field and entering the next IP address and then go to “[Add]” again. Repeat the process until you are done.

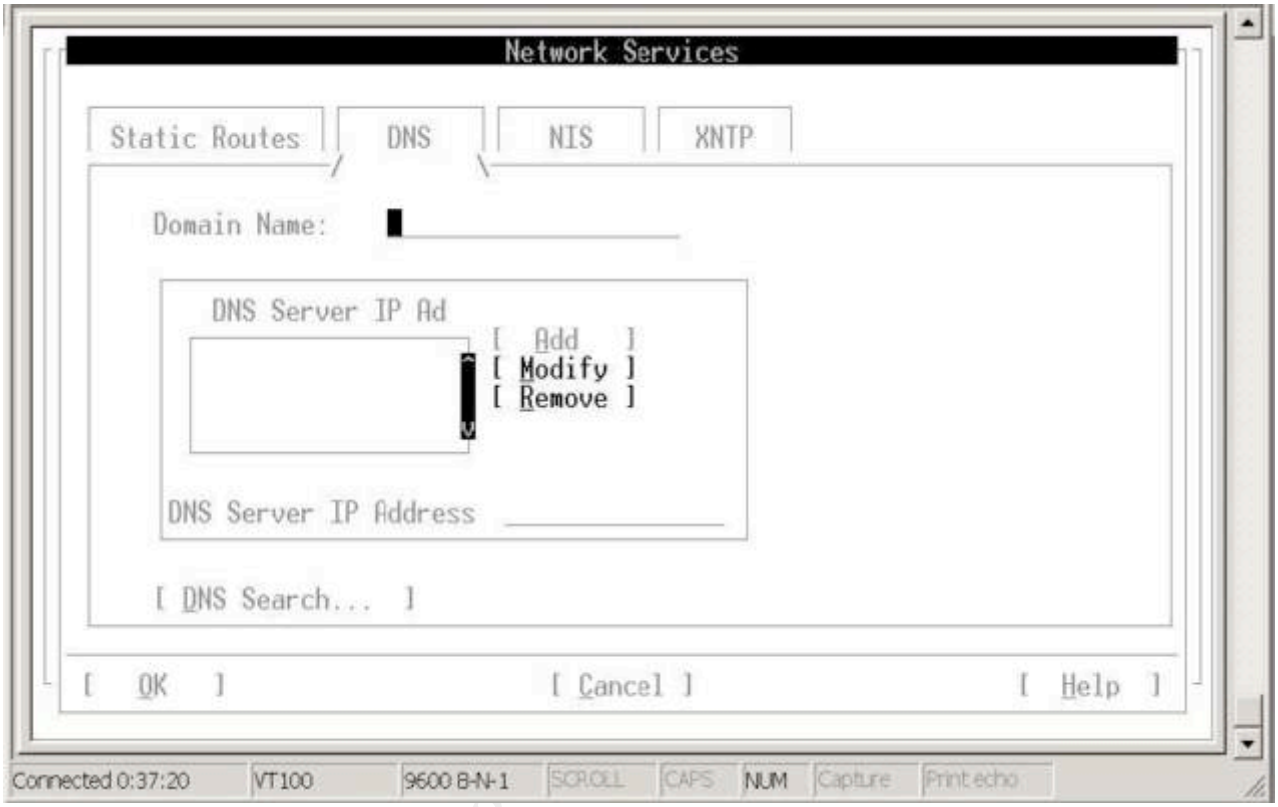

Figure 4 – DNS Configuration

We will skip over the NIS section and go straight to the XNTP configuration section since we are not using NIS in our environment.

Press the <TAB> key until XNTP is highlighted at the top of the screen and the press the <ENTER> key. This section is very straightforward. All you need to do is enter the IP address of the NTP server you wish to use in the “XNTP Server Address:” field. That is all there is to it.

Now, <TAB> down to OK and press <ENTER>. This will take us back to the “System” <TAB> of the “/opt/ignite/bin/itool” screen.

If you have an additional LAN interface on your machine that you wish to configure you can go to the “Additional Interfaces” selection and press <ENTER>. This will bring up a “Network Interface(s)” window, which will allow you to configure an IP address and subnet mask for any additional network interfaces on your system. We do not have any additional network interfaces to configure so we will just skip over this portion of the configuration.

FILESYSTEM

If you are not already in this window, press the <TAB> key until “FILE SYSTEM” is highlighted at the top of the screen and then press <ENTER>.

This screen will allow us to set up our root volume group (VG00) and all of the logical volumes that it requires. The default allocation of disk space is not appropriate for what we wish to do so we will change the amount of space allocated to ALL logical volumes (from now on LV) except the primary swap LV. The goal is to size each LV appropriately so we have enough space to install the operating system, but also fit it all on a single 4 GB disk drive since we plan on mirroring the drives for redundancy later.

To modify an LV you must highlight it in the list of LVs (use the <UP ARROW> and <DOWN ARROW> keys to scroll through the list), <TAB> to the item(s) you want to change, change them, <TAB> back to the “[Modify]” selection, and press <ENTER>. You must then <TAB> back into the window with the list of LVs, scroll to the next LV you want to change and repeat the process.

I will only note the values that I am changing for each LV below.

- /stand – Size: Fixed MB – 120
- /tmp – Size: Fixed MB – 128
- /home – Size: Fixed MB – 25
- /opt – Size: Fixed MB – 700
- /usr – Size: Fixed MB – 1300
- /var – Size: Fixed MB – 1024

You want to make ABSOLUTELY sure that the selection area next to “SIZE” is set to “FIXED MB” for ALL logical volumes, as in Figure 5. You do NOT want to use “FREEMB”, “FREE %” or any of the other selections.

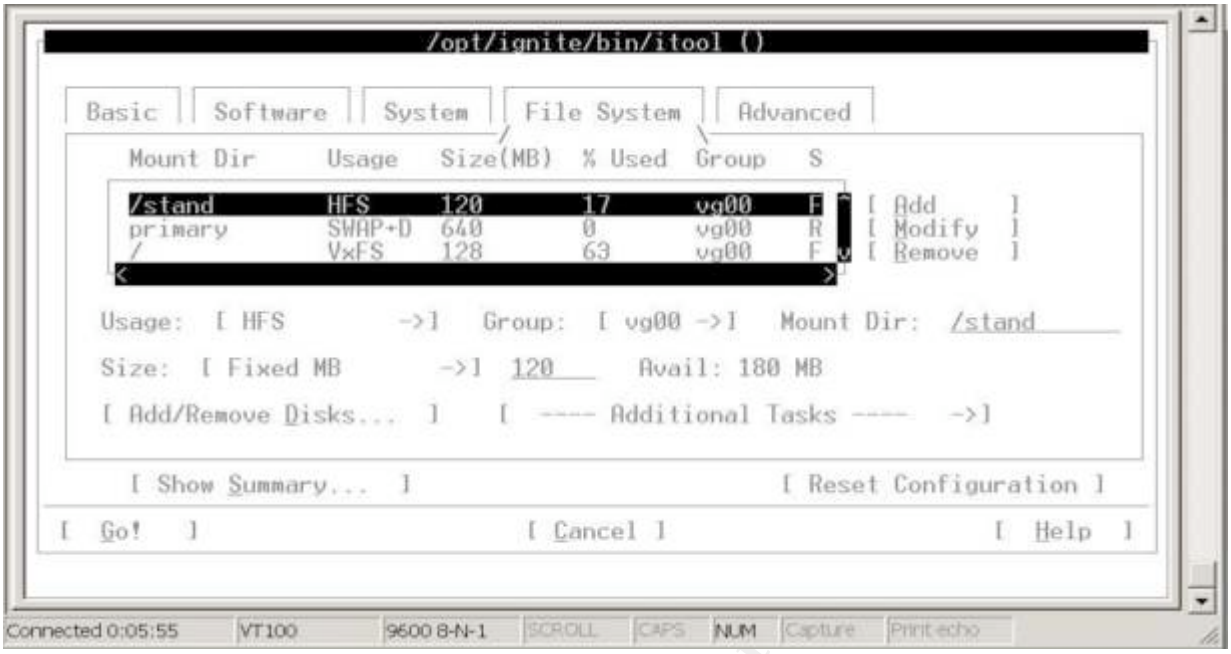

Figure 5 – File System Configuration

On the File System screen you will see two additional selections; "[Add/Remove Disks…]" and "[---- Additional Tasks ---- ->]". We are not going to worry about the "Add/Remove Disks" area, as there is nothing we need to do there during this installation.

We do need to go into the "Additional Tasks" menu though. Press the <TAB> key until you get to "Additional Tasks" then press <ENTER> then scroll down to "File System Parameters" and press <ENTER> again. This will bring up a window titled "Advanced File System Parameters". When this window opens, you will get a warning about VxFS file systems and which parameters can be changed. You may just press <ENTER> to acknowledge this warning.

Once the window is up, we want to check each file system and make sure the "Largefiles" option is set to NO, as in Figure 6. We have no file systems that are larger than 2GB, so there is no point in having large files enabled on any of them. Scroll through the list of file systems and check the value of the "Largefiles" option. If it is set to YES, press the <TAB> key until YES is highlighted and press <ENTER> to bring up the YES or NO list. Select NO and press <ENTER> again. Press <TAB> until "Modify" is highlighted and press <ENTER>. Then press the <TAB> key until you are back in the list of file systems. You will most likely have to make this change for the /home, /opt, /tmp, /usr and /var files systems.

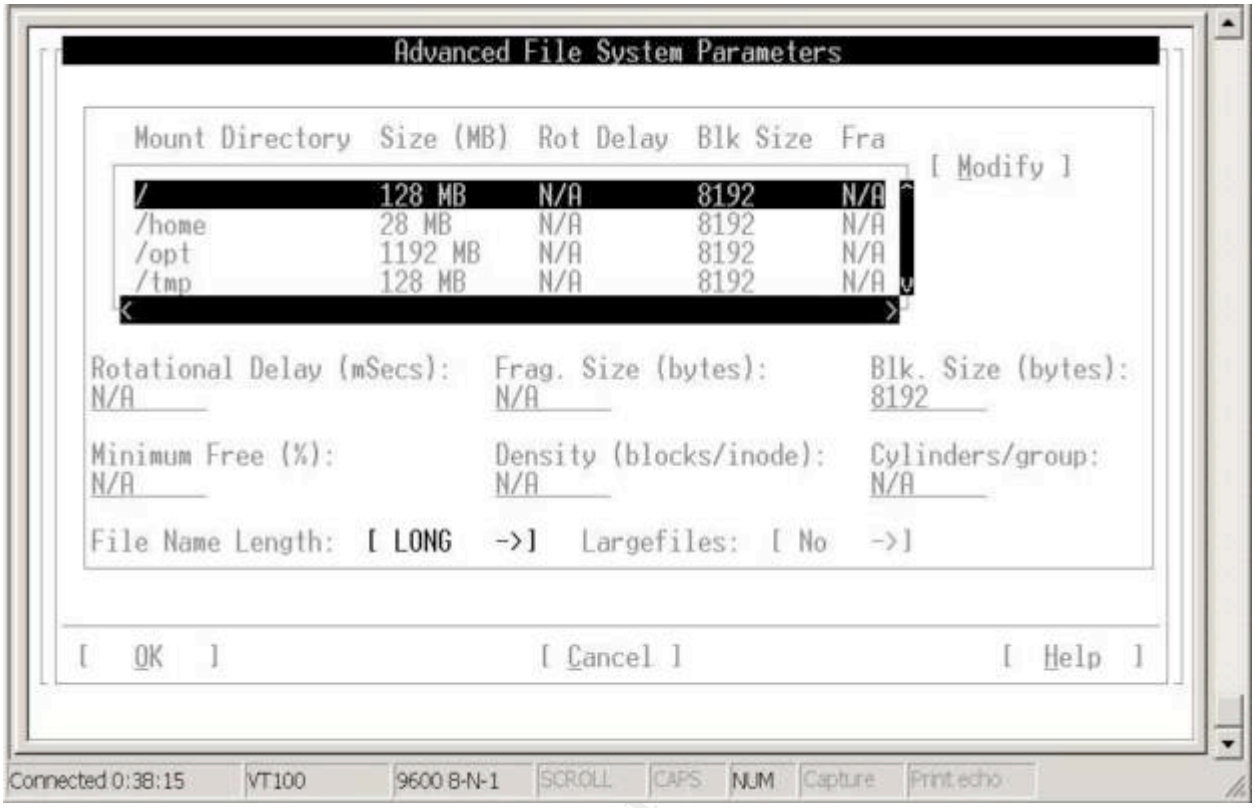

Figure 6 – Advance File System Configuration

Once you are done, <TAB> down to OK and press <ENTER> to get back to the "/opt/ignite/bin/itool ()" screen. We are not going to worry about any other additional tasks for this installation, as the defaults will work fine.

NOTE: If you are installing the operating system on a drive that is 18GB or larger, then you will need to go to "Additional Tasks" and select "Group Parameters". This will bring up the "Advanced Group Parameters" screen. For larger boot drives you should change the "Phys Ext Size (MB)" parameter to be at least 8. You can also change some of the other VG parameters, if you deem it necessary.

ADVANCED

This screen allows you to execute specific scripts as part of the OS installation. We don't need to worry about anything here for this installation.

GO!

At this point we are essentially done with preparing to install the HP-UX operating system. If you are interested, you can <TAB> down to the "Show Summary" selection and see what will be done when the OS is installed on this system.

The “General Summary” will show the products that are going to be installed, the volume group, logical volume and file system configuration and the approximate percentage of each file system that will be used when the installation is done.

The “Hardware Inventory” shows a summary of the machine you are installing the operating system on. If you think that the information is incorrect, now is the time to investigate and attempt to resolve the problem.

If you are satisfied with the output, <TAB> down to OK and press <ENTER> to return to the main screen. You are now ready to install the operating system. As a final sanity check I usually <TAB> through each of the main screens (Basic, Software, System, and File System) just to make sure that the information is correct. When you are satisfied that all is OK, <TAB> down to “GO!” and press <ENTER>.

You will then get a confirmation screen similar to Figure 7.

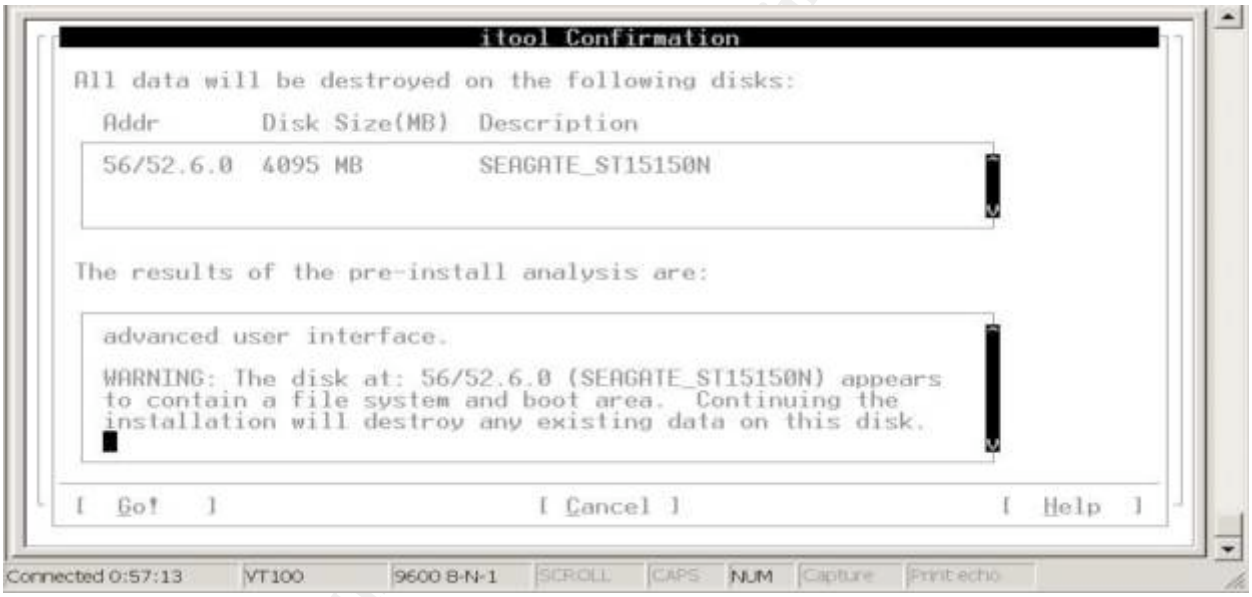

Figure 7 – Warning before Installation Proceeds

If you are absolutely sure about the warnings that are presented on this screen, then <TAB> down to “GO!” and press <ENTER>.

The installation should now start. You will need to keep an eye on the progress of the installation process and switch CDs when prompted. You will have to use all 3 HP-UX installation CDs. The speed of the installation depends entirely on the machine you are installing on. It could take anywhere from a few minutes per CD to an hour or more.

When the installation is finished the machine will reboot automatically at least once and quite possibly twice. This is normal. Once the machine is up and at a login prompt, you should be able to log in as the root user with the password you set earlier in the installation process.

Installing Additional Software

Now that we have finished the initial installation of the operating system we are going to install some additional software, both HP and non-HP, onto the system. All the software we are going to install can be downloaded from the links provided earlier. Once all of the software has been downloaded to your PC, it will need to be copied to the system you are installing. Since we have not turned off network services yet, you can transfer it via FTP.

Once all of the software has been copied to the HP-UX machine, some of the packages may need to be gunzip'ed. So you need to do:

*gunzip *.gz*

Once that is done, we are going to give all of the files the same extension. We are doing this so we can easily create a software depot and install lots of software at once and with a single reboot of the machine rather than 3 or 4 or 6 reboots. To get all files to have the same extension you need to:

- Rename any files ending with .sd so that they end with .depot
- Rename any files ending with .tar so that they end with .depot

Once you have done that we can create a software depot file with ALL the software in it. When I created the depot, I was working out of the /var/tmp/products directory. You should substitute the appropriate path for whatever directory the files are in on your machine. I am also creating the depot in /var/tmp/products and I am calling it utility.depot.

*for SW in *.depot*
CONTINUE>> *do*
CONTINUE>> *swcopy –x enforce_dependencies=false –s /var/tmp/products/${SW} * @ /var/tmp/products/utility.depot*
CONTINUE>> *done*

This will run for a while, but once it is completed you should have a directory called utility.depot in /var/tmp/products or where ever you created it.

We will now install the products we initially require from this software depot via the swinstall utility.

We will install everything EXCEPT TCP Wrappers and IP Filter. We will install those later in the process.

To install the software:

1. Invoke the swinstall program.

*swinstall*

2. When prompted, press <ENTER> to continue.

3. In the "Specify Source" window that comes up, you may need to specify the "Source Depot Path" if it isn't already there. In our case it should be /var/tmp/products/utility.depot. If you need to change it, simply press the <TAB> key until you are in the "Source Depot Path" field and then type in the path to the depot we created above. Once that is done <TAB> down to OK and press <ENTER>.

4. The main swinstall window will now come up. The lower part of the window consists of the list of software in the depot that we specified in step 3 above. We will now need to select the software we want to install. We do this by scrolling through the list and pressing the <SPACE BAR> to highlight the software we want to select.

   We need to select the following software in the list:

   - B2491BA – Mirror Disk/UX
   - B3701AA – Glance Plus Pak
   - B6834AA – HP-UX Security Patch Checker
   - B6849AA – Bastille
   - CFG2HTML – Config to HTML
   - FSDOC – Veritas File System Docs
   - Ignite-UX-11-11 – HP-UX Installation Utilities
   - KRNG11i – HP-UX 11.11 Strong Random Number Generator
   - OnlineJFS – Online Features of the VxFS File System
   - T1471AA – HP-UX Secure Shell
   - VRTSvlic – VERITAS License Utilities (for OnlineJFS)
   - Perl – PERL
   - ANY and ALL Patches that are listed. ALL of PHCO_*, PHKL_*, PHNE_* and PHSS_*

   Once all the software we need has been selected press the <TAB> key to activate the menu at the top of the window. Scroll to the ACTIONS menu and press <ENTER> to activate the menu. Finally, scroll down to "Mark for Install" and press <ENTER> again.

   You may get a warning that some of the software has dependencies. You can ignore this error, as all dependencies should be met when the software is actually installed. You may just press the <SPACE BAR> or <ENTER> to acknowledge the message.

5. Once the software has been marked, reactivate the menu and go back to the ACTIONS menu and scroll down to "Install…" and press <ENTER>.

This will start an analysis to make sure all software can be safely installed. It will verify that all dependencies are met and that there is sufficient disk space to hold all of the software that we selected.

6. When the analysis completes, it may say that not all products will be installed. It may say something like "Products scheduled: 29 of 31". That is OK. It is most likely just some patches that were installed when we installed the operating system. If you want to verify this, press the <TAB> key until the "Products…" selection is highlighted and press <ENTER>. You will then get a list of all products and what their status is. Look for anything marked as SKIP. If it is a patch then you are OK. If it is one of the other products you should check the log file to try and determine why it is going to be skipped and correct the problem.

   If you are satisfied that all is OK with the products listed, <TAB> to OK and press <ENTER> to close the Products list. You can then <TAB> to OK and press <ENTER> to start the patch installation.

   You will get a warning that the system will be rebooted after the install finished because kernel filesets will be installed. Since we are still in the process of installing the system, <TAB> to YES and press <ENTER>.

   The installation will now start. This could take a while. Take a break!

7. When the installation completes, the DONE button will be activated and the "STATUS: " line will say READY. <TAB> down to DONE and press <ENTER>. You will get a warning message that the system will be rebooted when you press OK. When you are ready for the system to reboot, press <ENTER> and wait for the system to come back up.

   Be aware that there could be a significant delay at the "Configuring All Unconfigured Filesets" step of the bootup process. Do not be alarmed.

   When the system boots up completely again, go ahead and log on as root.

Mirroring VG00

We will now mirror VG00 (the boot/root volume group) to the 2nd disk drive in our system. This will provide us with some redundancy so that the system can stay up should one of the 2 disk drives ever fail.

The disk drive we installed the operating system on is /dev/dsk/c0t6d0. If yours is different, make a note of it.
The disk drive we are going to mirror to is /dev/dsk/c0t5d0 (you will also need to use /dev/rdsk/c0t5d0 in some steps). If yours is different, make a note of it.

The steps to mirror the VG00 volume group are:

 # pvcreate –f –B /dev/rdsk/c0t5d0
 # mkboot /dev/dsk/c0t5d0
 # mkboot –a "hpux –lq" /dev/dsk/c0t5d0
 # mkboot –a "hpux –lq" /dev/dsk/c0t6d0
These commands will allow you to boot from either drive even if one of them fails.

 # vgextend vg00 /dev/dsk/c0t5d0
 # for LV in 1 2 3 4 5 6 7 8
> do
> echo "Extending mirror on /dev/vg00/lvol${LV}"
> lvextend –m 1 /dev/vg00/lvol${LV} /dev/dsk/c0t5d0
> done

This may take a while. It's a good time for another break.

 # lvlnboot –v
Verify that all information is correct.

 # setboot –a 56/52.5.0
This will set the alternate boot path that is to be used if the primary path is not available. It uses the SCSI hardware path, which can be found via the ioscan command.

 # setboot
Just to verify that the settings are correct.

 # lifcp /dev/rdsk/c0t5d0:AUTO –
 # lifcp /dev/rdsk/c0t6d0:AUTO –
This verifies that the boot strings, which should be "hpux –lq" (without the quotes), are correct for each disk.

You will also need to update the LIF area on the disk so that you have offline diagnostics available to you should you ever need them.

We will use the /usr/sbin/diag/lif/updatediaglif command on our machine since it is a 32-bit machine. If you happen to have a 64-bit machine, you will need to use the /usr/sbin/diag/lif/updatediaglif2 command.

 # mkboot –b /usr/sbin/diag/lif/updatediaglif –p ISL –p AUTO –p HPUX –p PAD –p LABEL /dev/rdsk/c0t5d0

To verify that the update was successful, compare both drives.

 # lifls /dev/rdsk/c0t5d0
 # lifls /dev/rdsk/c0t6d0

The output should be almost exact. If you notice that the items are in a slightly different order on one drive as compared to the other, that is normal and nothing to worry about.

Mirroring is now complete. If you want to verify that you can boot from the mirrored boot disk we just created, reboot the system. When prompted to "Press any key within 10 seconds….." do so to interrupt the boot process. Then at the prompt type '*bo alt*' and answer *N* to the "**Interact with IPL?**" question. Your system will now try to boot from the mirrored disk. If all works well, the system should come up without any problems and you will be able to log in.

Create /etc/nsswitch.conf

In order for name resolution to work correctly, we need to create the /etc/nsswitch.conf file. We will use the /etc/nsswitch.files file as a template.

*cp /etc/nsswitch.files /etc/nsswitch.conf*

*vi /etc/nsswitch.conf*
Modify the hosts line in the file so that it reads:

hosts: files [NOTFOUND=continue] dns

*chmod 444 /etc/nsswitch.conf*

Create the /cdrom directory

I always prefer mounting a CD to the /cdrom directory. Since I never know when I will need a CD, I will go ahead and create the /cdrom directory so it is available.

*mkdir /cdrom*

*chmod 555 /cdrom*

Patching the HP-UX operating system

Now, we will start the process of patching the operating system. This will be done in 3 steps. First, we will install the latest general release patch bundle. I used the December 2003 version during this process. Second, we will run the security_patch_check utility to get a list of security patches that we still need. Third we will go to HP's IT Resource Center web site to run a custom patch analysis and get anything else that we need.

Patching Step 1 – Install the December 2003 Quality Pack for HP-UX 11iv1

The link to download this patch bundle was given previously in this paper. If you have not downloaded it yet, please go to http://software.hp.com/SUPPORT_PLUS/qpk.html and download it now.

1. Transfer the file you downloaded, from the above link, to the HP-UX machine. In our case, I have renamed the file to DEC2003QP.depot and I have stored the file in the /var/tmp directory.

2. Invoke swinstall and point the "Source Depot Path" to /var/tmp/DEC2003QP.depot and <TAB> down to OK and hit RETURN.

3. Once the main swinstall window is up, press the <TAB> key to activate the menu and go to the ACTIONS menu. In the ACTIONS menu select "MANAGE PATCH SELECTION" and press RETURN.

4. In the "MANAGE PATCH SELECTION" Window that comes up, <TAB> down to "AUTOMATICALLY SELECT PATCHES FOR EXISTING SOFTWARE ON THE TARGET" and press RETURN. You will get a confirmation window telling you "Only patches that pass the filter will be marked." That is what we want, so <TAB> to YES and press RETURN.

5. All appropriate patches will now be selected by swinstall. Once the main swinstall window returns, go back up to the ACTIONS menu and select "INSTALL…" to start the install analysis.

6. When the analysis finishes, assuming it has run successfully and the "STATUS:" line reads "READY", <TAB> down to "OK" and press <ENTER> to start the patch installation. If the analysis failed then you will need to figure out where and why it failed, fix the problem and re-run the patch analysis.

   You will be warned that the kernel will be rebuilt and the system will be rebooted after the installation finishes. <TAB> to YES and press <ENTER>. Now you can sit back and wait as the patch installation could take a while.

7. When the patch installation finishes, the "STATUS:" line should say READY. <TAB> down to DONE and press <ENTER>. You will again be warned that the system will reboot when you select "YES". That is what we want, so <TAB> to YES and press <ENTER> to let the system reboot. When the system is coming back up, it may seem like it is stuck on the "Configuring all unconfigured filesets" step. This is normal. Once the system is back up, it is time for the next step in the process.

Patching Step 2 – Running the security_patch_check tool

There are 2 different ways to run the security_patch_check tool:

1. If you have Internet access from the HP-UX machine you can just run:

   # */opt/sec_mgmt/spc/bin/security_patch_check –r*

   This will go to the HP download site and retrieve the latest security catalogs for the tool to use.

2. If you do not have Internet access from the HP-UX machine, but do have it elsewhere, you can download the security catalog files yourself and transfer them to the HP-UX machine. To download the files go to: ftp.itrc.hp.com and log in as anonymous with your e-mail address as the password and then navigate to the /export/patches directory. The 2 files you want are security_catalog.sync and security_catalog.gz.

   Once you have downloaded them, you must transfer them to your HP-UX machine and place them in the /opt/sec_mgmt/spc/bin directory.

   You can now run:

   # */opt/sec_mgmt/spc/bin/security_patch_check*

   NOTE: The first time you run the security_patch_check tool, a license agreement will be displayed. Once you have read it you must type in the word 'accept' at the prompt.

When this tool runs, you may get warnings about world writeable directories. You should make a note of these directories and change the permissions on those directories so that they do not have world writeable permissions.

You will also get warning messages about patches with critical and/or non-critical warnings that are installed on your system. You should review these patches to determine whether or not they could be problematic for you and appropriate steps should be taken.

The output we are most concerned with is the "List of recommended patches for most secure system:" (see figure 8 – This was the output from my system. Yours will almost certainly be different.).

```
List of recommended patches for most secure system:

#  Recommended  Bull(s) Spec? Reboot? PDep? Description
-------------------------------------------------------------------------------
1  PHCO_28481   215 252 Yes   No     Yes   cumulative 10.20 libc compatibility
support
2  PHCO_28848   293     No    No     No    Software Distributor Cumulative
3  PHCO_29010   304     No    No     No    shar(1)
4  PHCO_29209   312     Yes   No     No    lpspool subsystem cumulative
5  PHCO_29382   262     No    No     No    uucp(1) cumulative
6  PHCO_29622   1006    No    No     No    Directory
7  PHCO_29955   294     Yes   No     Yes   libc cumulative
8  PHNE_27796   209     Yes   No     Yes   libnss_dns DNS backend
9  PHNE_29774   281     Yes   No     No    sendmail(1m) 8.9.3
10 PHNE_29783   1002    Yes   Yes    Yes   ONC/NFS General Release/Performance
11 PHNE_29887   192 205 No    Yes    Yes   cumulative ARPA Transport
12 PHNE_30068   303     No    No     No    Bind 8.1.2
13 PHSS_29371   289     No    No     No    X/Motif Runtime Periodic
14 PHSS_29740   263     Yes   No     Yes   CDE Applications Periodic
15 PHSS_29964   276 299 Yes   No     Yes   HP DCE/9000 1.8 DCE Client IPv6
16 PHSS_30011   297     Yes   No     No    CDE Base
17 PHSS_30189   1018    No    Yes    No    Xserver cumulative
18 PHSS_30478   1018    No    No     No    X11 Font Library
-------------------------------------------------------------------------------
```

Figure 8 - List of recommended patches for most secure system

You will need to download the recommended patches from the HP ITRC Patch Database. The Patch Database determines if there are any prerequisites for the patch specified and automatically adds them to your patch list so that all appropriate patches may be downloaded at once.

I will not go into details here about how to use the ITRC Patch Database. For more information, visit the ITRC at http://itrc.hp.com.

When I download patch bundles using this method, I always select the gzip'ed bundle. The bundle I downloaded based on the patch list in Figure 8 was about 95 MB. The files will be named with a date and time stamp in the name. The file I used was named hpux_800_11.11_05041030.tgz. If you accessed the ITRC Patch Database from your PC, you will need to transfer the file that was downloaded to your HP-UX machine. I transferred mine to the /var/tmp directory. Once the file is there do the following:

*cd /var/tmp*

*gzcat hpux_800_11.11_05041030.tar | tar –xvf –*
(Use whatever filename is appropriate for your patch file)

*./create_depot_hp-ux_11*

This will create the patch depot from which we will install the patches. The depot is created as a sub-directory in the directory you are running this from. In my case it created the directory /var/tmp/depot. This depot allows us to install all the patches at one time and only reboot the machine once.

This script will also create a .text file for each patch in the bundle. You should review the text file for each patch and see if there are any "SPECIAL INSTALLATION INSTRUCTIONS" that must be done before installing the patch or if there is anything in the patch that may cause you problems.

Install the patches in the depot using swinstall as we have done previously. The "SOURCE DEPOT PATH" that I used is /var/tmp/depot since that is what the create_depot_hp-ux_11 script created. Your "SOURCE DEPOT PATH" will depend on where your depot was created in the steps above.

Once the patch installation has finished, the machine will more than likely reboot. Again.

Patching Step 3 – Patch Assessment from the ITRC Patch Database

HP's ITRC Patch Database allows you to run a "Patch Assessment" on your system. This assessment will recommend any additional patches needed on your system to get it as up to date as possible.

To get to the patch assessment area you need to go to http://itrc.hp.com and select the "patch database" link. Once the "patch database home" page has loaded, you need to select the "run a patch assessment" link.

There is good documentation on how to do this on the "run a patch assessment" page so I will not go into that here. Just follow the directions to run the patch assessment and download the recommended patch bundle.

When I ran the assessment, I ran it with the "HP Recommended Target Configuration (hpRecommended)" assessment profile. That will get you the most current stable patches.

Once you have run the analysis and downloaded the file containing the patches, you can proceed just like Patching Step 2 above. Transfer the downloaded file to your HP-UX machine, run the gzcat and the create_depot steps, review the patch text files and install with swinstall.

When the installation has finished, the machine will reboot yet again.

Once the reboot has completed, you have finished patching your system. For now.

SECURING THE HP-UX OPERATING SYSTEM

We will now begin the process of securing the HP-UX operating system that we have just finished installing and patching. Some of the steps I take here are based on personal experience, training classes, and reading, while others are based on recommendations made by Kevin Steves in his "Building a Bastion Host Using HP-UX 11" document (http://www2.itrc.hp.com/service/cki/docDisplay.do?docLocale=en_US&docId=200000066258828). That document is a very good read. In many cases he goes into much more detail about his reasons for doing certain things.

Removing Unnecessary OS Products bundles

We will remove some of the automatically installed HP-UX software that is absolutely not needed. We will do this by using the swremove utility. Swremove behaves almost exactly like swinstall, except that it removes software.

To do this, invoke swremove from the command line. Once the main swremove screen comes up, you will need to go through the list of products and select each product that you want to remove by using the arrow keys to scroll up and down in the list, press the <SPACE BAR> to highlight a product and then press the 'm' key to mark the product for removal.

I removed the following products from my system:

Software Name	Revision	Description
Base-VxVM	B.03.50.5	Base VxVM
FDDI-00	B.11.11.02	PCI FDDI and drivers
FibrChanl-00	B.11.11.09	PCI/HSC FC drivers
GigEther-00	B.11.11.14	PCI/HSC Gig Ether drivers

Next, scroll down to the row labeled "HPUXBase32" and press return. This will drill down into the sub-products that comprise the HPUXBase32 product. From here, mark the following software for removal:

Software Name	Revision	Description
Asian-Core	A.03.00	Asian Core
Asian-PRINTER	A.03.00	Asian Printer
Asian-TERM	A.03.00	Asian TERM
Asian-UTILITY	A.03.00	Asian Utility
DCE-Core	B.11.11	HP DCE/9000 Core Client Software
DistributedPrint	B.11.11	Distributed Print
FCMassStorage	B.11.11	Fibre Channel MassStorage

GSS-API	B.11.11	GSS API Version 1.0
Spelling	B.11.11	Spelling
LSSERV	B.11.11	LicensePower/iFOR ARK
UUCP	B.11.11	Unix to Unix Copy
SystemComm	B.11.11	System Communication Utilities
TerminalMngr	B.11.11	Terminal Mngr

Now use the <UP ARROW> key to scroll back to the top of the list to the "..(go up)" and press <ENTER>. When the main list comes back up, scroll down to "HPUXBaseAux" and press <ENTER> to drill down into those sub-products. I selected the following products for removal:

Software Name	**Revision**	**Description**
Judy-lib	B.11.11.04.13	Judy Library & related files
Partition Manager	B.11.11.01.06	Partition Manager for HP-UX
SCR	B.11.11.38	System Config. Repos.

Now that all products have been selected, go up to the ACTIONS menu and select "Remove…". This will do the removal analysis. If it succeeds, you can <TAB> to OK and proceed with the removal of the unwanted products. The machine will reboot when this is done.

Prevent Unnecessary software from starting

Now that we have removed some unnecessary software, and the machine has come back up after its reboot, we are going to edit a bunch of files in the /etc/rc.config.d directory so that HP-UX will NOT start a lot of daemons, services and software by default.

To accomplish, this I did the following:

*cd /etc/rc.config.d*

*vi **

When I finish editing the file, I do a *:w!* to save the file and then a *:n* to go to the next file to be edited.

I reviewed ALL files in the directory. The following table is a list of the files I modified and the variable names I changed. In all cases mentioned, I changed their value from 1 (one) to 0 (zero).

FILE MODIFIED	VARIABLE MODIFIED
Dmiconfig	START_DMI
Rpcd	START_RPCD
SnmpHpunix	SNMP_HPUNIX_START
SnmpMaster	SNMP_MASTER_START
SnmpMib2	SNMP_MIB2_START
SnmpTrpDst	SNMP_TRAPDEST_START
comsec	TTSYNCD
emsagtconf	AUTOSTART_EMSAGT
envd	ENVD
fc_td_conf	FC_TD_START
hparamgr	HPARAMGR_START_STOP
hparray	HPARRAY_START_STOP
hpfcmsconf	FCMS_START
Lp	LP
mailservs	SENDMAIL_SERVER
nfsconf	NFS_CLIENT NFS_SERVER AUTOMOUNT START_MOUNTD
Ptydaemon	PTYDAEMON_START
pwgr	PWGR
scrdaemon	SCR_DAEMON
vt	VTDAEMON_START
xf86	XF86_DLKM_LD[1] XF86_DLKM_UNLD[1]

If you do not have all of the files mentioned here, do not fret. It is probably because we have removed some of the products in the previous step.

Remove Unnecessary Services from /etc/inetd.conf

Now, we are going to remove almost all of the services from the /etc/inetd.conf file. If the inetd daemon is not listening for something, then that makes it that much harder to exploit a potential security hole.

We will edit the file by doing:

*cp /etc/inetd.conf /etc/inetd.bak*
Make a backup copy of the file just in case

*vi /etc/inetd.conf*

Now, delete ALL lines in the file EXCEPT the telnet, ftp and registrar lines. We will delete telnet and ftp after we get SSH installed and configured. The registrar daemon

will stay, as the EMS software uses it and we want to know when something goes wrong.

Once you have deleted everything, do a *:wq!* to save the file and exit vi.

Now do an

*inetd –c*
This will force inetd to reread the /etc/inetd.conf and all services except for telnet, ftp and registrar are now effectively disabled.

Installing lsof

We will now install the lsof utility. The web site for this utility was mentioned at the beginning of this paper. If you have not downloaded the source code yet, please do so now. Once you have downloaded the source code, transfer it to your HP-UX machine then do the following:

*cd /var/tmp*
(or where ever you put the file on the HP-UX machine)

*gzcat lsof-4.67.tar.gz* | *tar –xvf –*
(lsof-4.67.tar.gz is what the file I used was called. Yours may be different. Use the appropriate name)

Before we go any further, we must install the gcc compiler and binutils software from HP. The download site for these was also given previously in this paper. If you have not downloaded the software and transferred it to the HP-UX machine, please do so now.

Once you have the software on the HP-UX machine, use swinstall to install the software, just as we have done numerous times previously.

We will also need to compile and install the gmake software since it is not included in HP's binutils and gcc bundles. Download the software from the link given previously, transfer it to the HP-UX machine and do the following:

*cd /var/tmp*
(I almost always use /var/tmp to work from – Use whatever directory you transferred the file to)

*gzcat make-3.80.tar.gz* | *tar –xvf –*
(or whatever filename is appropriate)

*cd make-3.80*
(if you have a newer version, switch to the appropriate directory)

*./configure*

*make*

*make check*

*make install*
If all of the above steps were successful, gmake should now be installed.

Once all of the software is installed successfully, you may proceed with compiling and installing lsof.

To compile and install lsof:

*cd /var/tmp/lsof-4.67*
(If your lsof extracted to a different directory please use the appropriate directory name)

*./configure hpuxgcc*

When the configure script asks a question about the HASSECURITY option, answer YES.

*gmake*

*gmake install*

No one but root should be using this utility so:

*chown root:sys /usr/local/bin/lsof*
*chmod 500 /usr/local/bin/lsof*

Configuring SSH

SSH should have been installed when we installed the utility.depot bundle of software earlier. We now need to configure SSH.

1. Add the user that you will use to log in to this machine. You can use sam, useradd, modify the /etc/passwd file directly, whatever makes you happy.

2. Login as the user you just created and generate your SSH keys by executing the following command:

   $ ssh-keygen –b 1024 –t dsa

   I accepted the defaults at all prompts EXCEPT for the passphrase.

3. Exchange keys as appropriate with the machine(s) that you will SSH from.

4. Now test and make sure that SSH works as you expect.

If you need more information on how to use SSH, you can go here http://www.docs.hp.com/hpux/internet/index.html#HP-UX%20Secure%20Shell and browse through the Secure Shell release notes. There are several references to outside documentation there.

Prevent root login except from the system console

*echo console > /etc/securetty*

This will prevent root from logging in from anywhere EXCEPT the system console. This will force you to log in as a regular user and then do an '*su* –' to switch to root.

Disable telnet and ftp in /etc/inetd.conf

*vi /etc/inetd.conf*

Delete the telnet and ftp lines now that SSH is configured and working. The only thing left in this file is registrar and we will secure that more later.

*inetd –c*

Force inetd to re-read its configuration file and disable telnet and ftp.

Remove Extraneous User IDs

There are several users defined by default in HP-UX that typically aren't used for much. We are going to remove several of these.

First, I am going to run a global 'find' command to verify that the users I am going to remove do not own any files. I will also do a 'ps –ef | grep user' for each user to make sure that they do not have any running processes.

I will automate this with the following script:
(Note – I am not specifying the users root, bin, sshd or my personal user account since I know that they are needed.)

```
#  for USER in daemon sys adm uucp nuucp lp hpdb nobody www webadmin
> do
> echo "Working on ${USER}"
> find / -user ${USER} –exec ll –d {} \;
> ps –ef | grep "${USER} "
> echo ""
```

> *done*

(Note the space between the closing } and the " in the 'ps –ef' line above. That is intentional.)

Based on the results of the above script, we are going to remove the users sys, uucp, nuucp, hpdb, nobody, www and webadmin. Be sure to remove the logfiles that are owned by the webadmin user.

We are going to leave the users adm, daemon and lp alone since they own files and we may need the lp spooler at some point in time.

To remove the users, we will use the userdel command.

*for USER in sys uucp nuucp hpdb nobody www webadmin*
> *do*
> *echo "Deleting user ${USER}"*
> *userdel ${USER}*
> *done*

If you now take a look at the /etc/passwd file, it should be much smaller.

Remove Extraneous Groups

We are now going to do the same thing for groups that we did for users above for the same reasons.

We will search for files with the following groups: adm, daemon, mail, lp, tty, nuucp, nogroup. We are skipping the groups root, users, bin, sshd, other and sys since I know those need to be kept.

*for GROUP in adm daemon mail lp tty nuucp nogroup*
> *do*
> *echo "Working on ${GROUP"*
> *find / -group ${GROUP} –exec ll –d {} \;*
> *done > /tmp/group.out 2>&1*

After reviewing the /tmp/group.out file, we will leave the groups adm, mail, lp and tty alone and only delete the daemon, nuucp and nogroup groups.

To delete the groups, edit the /etc/group file with the vi editor and delete the appropriate lines. Once you are done, save the file and exit.

Convert the System to Trusted

We will now convert the system to a trusted system. Doing this conversion will remove the encrypted passwords from the /etc/passwd file and store them in files in the /tcb directory structure which only the root user can access.

This conversion is very simple. Do the following:

*/usr/lbin/tsconvert*
Creating secure password database...
Directories created.
Making default files.
System default file created...
Terminal default file created...
Device assignment file created...
Moving passwords...
secure password database installed.
Converting at and crontab jobs...
At and crontab files converted.

This process expires ALL passwords on the system. We will now unexpire the passwords for all users.

*/usr/lbin/modprpw –V*

Change chown privileges

We will now change the chown privileges on the system. This will prevent anyone except root from changing the ownership of a file.

Before disabling chown:

*getprivgrp*
global privileges: CHOWN

*echo -n > /etc/privgroup*

*chmod 400 /etc/privgroup*

Now let's test it:

*/sbin/init.d/set_prvgrp start*

*getprivgrp*
global privileges:

Fix PAM

Since we will not be using CDE, there is no reason to have the dtlogin and dtaction entries in the /etc/pam.conf file. We will simply remove the entries we don't want.

*vi /etc/pam.conf*
Remove all lines that begin with 'dtaction' or 'dtlogin'. When you are finished save the file and exit from vi.

Change the default umask value

On this server, just as an added layer of protection, we are going to modify the default umask for all users in the /etc/profile. Since this is a mail server, the only user that should be logging in to a shell is the administrator. Even so, we will set the umask so any files or directories that we create are as restrictive as possible. If needed, we will modify the files or directories after we create them.

*vi /etc/profile*

Go to the end of the file and insert the line:

umask 077

Save the file and exit vi.

This will take effect next time anyone logs in. To be sure that this file is used, any user that needs to get to a shell prompt will be created so that /usr/bin/sh (the POSIX shell) is their default shell.

Enable inetd logging

We are going to enable the logging facility for the inetd daemon. We want to know whenever the inetd daemon spawns a process. This is just another facility to check and make sure that everything that happens on this server is supposed to.

To enable inetd logging do:

*vi /etc/rc.config.d/netdaemons*

Find the line that reads 'export INETD_ARGS=' and modify it so that it is:

export INETD_ARGS="-l"

Note that the option in quotes after the hyphen (or dash) is a lower-case L (l as in log) and NOT the number 1.

This will take effect next time you reboot the system. If you want it to take effect now, you can stop and restart the inetd process with the following commands:

*vi /sbin/init.d/inetd stop*

*/sbin/init.d/inetd start*

Modify home directories

As both a safety and security precaution, we are going to move the home directory for root. By default root's home directory is /. We are going to move it to /home/root. This will prevent us from filling up the / filesystem if we do something stupid, as root, in our home directory, which could potentially cause many system problems.

*vi /etc/passwd*

Modify the root entry so that it now looks like:

root::0:3::/home/root:/sbin/sh*

Now, we need to copy all of the dot files and directories to /home/root. This can be done in a couple of easy steps.

*cp –Rp .[a-z]* /home/root*

*cp –Rp .[A-Z]* /home/root*

Once you have copied the files, you should log out and log back in as the root user. This will just verify that everything still works. Once you do that, you can remove the dot files and directories from the / directory.

We also want to make sure that the permissions are appropriate for root's home directory and files. We want to restrict them as much as possible so we will set everything to 600 permissions (r-x------).

*cd /home*

*chmod –R 600 root*

You will also want to do the same thing for any other users home directory as well. No user should be able to write to any other user's home directory.

Disable the samd daemon

The samd daemon is another daemon that we really do not need to run so we will disable it. Samd is run via the /etc/inittab file, so to disable it we must edit /etc/inittab and remove the samd line.

*vi /etc/inittab*

Remove the line containing samd and also go ahead and remove any lines that are commented out. Save the file and exit when you are done.

This will take effect next time you reboot the system. If you need the /etc/inittab file to be re-read now you can do:

*init q*

Prevent the syslog daemon from listening on the network

We don't want the syslog daemon (syslogd) to listen for messages from other machines on the network. This is just one more potentially exploitable hole. To prevent this, we are going to modify the syslog daemon startup arguments.

*vi /etc/rc.config.d/syslogd*

Find the line that starts with "SYSLOGD_OPTS" and make it look like:

SYSLOGD_OPTS="-DN"

Note that everything on the above line is in UPPER CASE letters.

In order for this change to take effect, we must stop and restart syslog.

*/sbin/init.d/syslogd stop*

*/sbin/init.d/syslogd start*

Disable the swagent daemon

The swagent daemon (swagentd) is yet another daemon that we don't need to have running all the time. Swagentd, however, is used when the machine boots up. We are going to create a script that will stop swagentd once the machine has booted completely.

The steps I took to do this are the same steps as in the "Building a Bastion Host Using HP-UX 11" document by Kevin Steves (http://www2.itrc.hp.com/service/cki/docDisplay.do?docLocale=en_US&docId=2000000

66258828). Rather than going into a lot of detail here, I will leave you to retrieve this document yourself.

Remove extraneous startup/shutdown scripts

There are MANY startup and shutdown scripts in /sbin/init.d that we do not need. Quite a few of the items were turned off when we modified their configuration files in the /etc/rc.config.d directory. Just to make sure that they don't start, we are going to remove them.

We must remember to remove the startup / shutdown script itself from /sbin/init.d and we must also remember to remove the S and K links from /sbin/rc?.d for each script.

You should review the list of rm commands that I run below to make sure that you are not going to remove the startup / shutdown scripts for something that you need. For example, if you have a fairly new machine which supports OLAR, then you would not want to remove the pci_olar script.

Based on this, I am going to execute the following rm commands:

```
# rm /sbin/init.d/nis* /sbin/rc?.d/*nis*
# rm /sbin/init.d/Snmp* /sbin/rc?.d/*Snmp*
# rm /sbin/init.d/OspfMib* /sbin/rc?.d/*OspfMib*
# rm /sbin/init.d/Dmisp* /sbin/rc?.d/*Dmisp*
# rm /sbin/init.d/Rpcd* /sbin/rc?.d/*Rpcd*
# rm /sbin/init.d/audio* /sbin/rc?.d/*audio*
# rm /sbin/init.d/comsec* /sbin/rc?.d/*comsec*
# rm /sbin/init.d/dce* /sbin/rc?.d/*dce*
# rm /sbin/init.d/ddfa* /sbin/rc?.d/*ddfa*
# rm /sbin/init.d/dtlogin.rc* /sbin/rc?.d/*dtlogin.rc*
# rm /sbin/init.d/gated* /sbin/rc?.d/*gated*
# rm /sbin/init.d/hparamgr* /sbin/rc?.d/*hparamgr*
# rm /sbin/init.d/hparray* /sbin/rc?.d/*hparray*
# rm /sbin/init.d/hub* /sbin/rc?.d/*hub*
# rm /sbin/init.d/lp* /sbin/rc?.d/*lp*
# rm /sbin/init.d/mrouted* /sbin/rc?.d/*mrouted*
# rm /sbin/init.d/named* /sbin/rc?.d/*named*
# rm /sbin/init.d/pci_olar* /sbin/rc?.d/*pci_olar*
# rm /sbin/init.d/ppp* /sbin/rc?.d/*ppp*
# rm /sbin/init.d/ptydaemon* /sbin/rc?.d/*ptydaemon*
# rm /sbin/init.d/pwgr* /sbin/rc?.d/*pwgr*
# rm /sbin/init.d/rarpd* /sbin/rc?.d/*rarpd*
# rm /sbin/init.d/rbootd* /sbin/rc?.d/*rbootd*
# rm /sbin/init.d/rdpd* /sbin/rc?.d/*rdpd*
# rm /sbin/init.d/rwhod* /sbin/rc?.d/*rwhod*
# rm /sbin/init.d/sendmail* /sbin/rc?.d/*sendmail*
```

*rm /sbin/init.d/slsd* /sbin/rc?.d/*slsd**
*rm /sbin/init.d/spa* /sbin/rc?.d/*spa**
*rm /sbin/init.d/tps.rc* /sbin/rc?.d/*tps.rc**
*rm /sbin/init.d/vlan* /sbin/rc?.d/*vlan**
*rm /sbin/init.d/webadmin* /sbin/rc?.d/*webadmin**
*rm /sbin/init.d/xf86* /sbin/rc?.d/*xf86**
*rm /sbin/init.d/xfs* /sbin/rc?.d/*xfs**

Turn off nettl console logging

Since the majority of servers in data centers do not have a console attached to them all the time, there is not much reason to send log messages to the console. So we are going to turn off nettl's feature that sends log messages to the console.

*nettlconf –L –console 0*
This turns the feature off permanently and it will persist through a reboot.

Now stop and restart nettl so that the change is effective.

*nettl –stop*
*nettl –start*

Clean up after the pwgr daemon

The pwgr daemon is started by default. This daemon is really only useful on large systems that have many users logging in. Since we have turned off pwgr on our system, we are going to clean up files that it left behind.

First, let us make sure that pwgr is not running:

*ps –ef* | *grep pwgr*

If it is still running, kill it.

Now, we will remove its leftover files:

*rm /var/spool/pwgr/**
*rm /var/spool/sockets/pwgr/**

Check for open network ports

We will now check and see what network ports are still open and listening for connections. We will do this with a combination of the netstat and lsof commands.

If you have not rebooted the server recently, go ahead and reboot now. We want to make sure that as few services as possible are started.

To check and see what is running, execute the following commands:

*netstat –an*

*lsof –i*

You will probably see lots of ports related to the EMS and diagnostics utilities. If you like, shut both of those down so you can see what is left.

*/etc/opt/resmon/lbin/monconfig*

At the EMS prompt, choose <K> to kill EMS. That may take a couple of minutes. Once it has finished, choose <Q> to quit.

*/sbin/init.d/diagnostics stop*

Now, execute the above netstat and lsof commands again. You should see far fewer processes running now. Ideally, you should only see ports for the sshd and xntpd daemons. If there is anything else running, investigate it and see if it can be disabled.

I prefer to leave diagnostics and EMS up and running so I can be notified if/when there is a problem with the server.

Resetting File and Directory Permissions

Now we will reset the default permissions on a few of the HP-UX command files. There are a number of files that have the set-uid and set-gid bits set by default. There are a few of those that are needed, but on a secure system as many files as possible should have the set-uid and set-gid bits removed.

With the basic OS commands, set-uid and set-gid are generally employed to allow a regular user to run commands as root (like the passwd command so a user can change his/her own password). Since the administrators should be the only people logging on to this system, they should have admin/root access and, as such, much of the need for set-uid and set-gid goes away.

We will first look at the files on the system. We will use the following find command to list all set-uid and set-gid files on the system.

*find / \(-perm –4000 –o –perm –2000 \) –type f –exec ls –ld {} \; > suid_sgid_file_list*

Now review the list. When I ran this on my system, it returned 231 files as having the set-uid or set-gid bit set.

Next, we will remove the set-uid and set-gid bits from all files and then manually set it back for two files that will definitely need it.

*find / -perm –4000 –type f –exec chmod u-s {} \;*
Remove set-uid from all files

*find / -perm –2000 –type f –exec chmod g-s {} \;*
Remove set-gid from all files

Now, we will add the set-uid bit back to the /usr/bin/passwd and /usr/bin/su programs so that I can, as a normal user, change my own passwd and use su to log in as root.

*chmod u+s /usr/bin/passwd /usr/bin/su*

We will now search for any files and directories on the system that are world writeable. There are really only 4 instances where the world write permission bit should be set. Anything else will be changed so that we have one less hole for a hacker to exploit.

*find / -perm –002 ! –type l –exec ll –d {} \; > world_write_files_dirs*

The previous command will search through the entire system and find all files and directories that have the world write permission bit set. We will now remove that permission from all files and add it back to the few that need it.

*find / -perm –002 ! –type l –exec chmod o-w {} \;*

*chmod 1777 /tmp /var/tmp /var/preserve*

We set the sticky bit (the 1 preceding the 777) so that non-privileged users (ie. non-root users) can only remove their own files.

*chmod 666 /dev/null*

The /dev/null file must be writeable by everyone. If it is not, strange system behavior can result.

Network Security

The next step in the process is to set some network parameters via the ndd command. We will add entries to the /etc/rc.config.d/nddconf file. The entries in this file will be processed and the values set when the system reboots.

Edit the /etc/rc.config.d/nddconf file and insert the following lines:

```
TRANSPORT_NAME[0]=ip
NDD_NAME[0]=ip_forward_directed_broadcasts
NDD_VALUE[0]=0

TRANSPORT_NAME[1]=ip
NDD_NAME[1]=ip_forward_src_routed
NDD_VALUE[1]=0

TRANSPORT_NAME[2]=ip
NDD_NAME[2]=ip_forwarding
NDD_VALUE[2]=0

TRANSPORT_NAME[3]=ip
NDD_NAME[3]=ip_ire_gw_probe
NDD_VALUE[3]=0

TRANSPORT_NAME[4]=ip
NDD_NAME[4]=ip_pmtu_strategy
NDD_VALUE[4]=1

TRANSPORT_NAME[5]=ip
NDD_NAME[5]=ip_send_redirects
NDD_VALUE[5]=0

TRANSPORT_NAME[6]=ip
NDD_NAME[6]=ip_send_source_quench
NDD_VALUE[6]=0

TRANSPORT_NAME[7]=tcp
NDD_NAME[7]=tcp_conn_request_max
NDD_VALUE[7]=4096

TRANSPORT_NAME[8]=tcp
NDD_NAME[8]=tcp_syn_rcvd_max
NDD_VALUE[8]=1000

TRANSPORT_NAME[9]=ip
NDD_NAME[9]=ip_check_subnet_addr
```

NDD_VALUE[9]=0

TRANSPORT_NAME[10]=ip
NDD_NAME[10]=ip_respond_to_address_mask_broadcast
NDD_VALUE[10]=0

TRANSPORT_NAME[11]=ip
NDD_NAME[11]=ip_respond_to_echo_broadcast
NDD_VALUE[11]=0

TRANSPORT_NAME[12]=ip
NDD_NAME[12]=ip_respond_to_timestamp_broadcast
NDD_VALUE[12]=0

TRANSPORT_NAME[13]=ip
NDD_NAME[13]=ip_respond_to_timestamp
NDD_VALUE[13]=0

TRANSPORT_NAME[14]=tcp
NDD_NAME[14]=tcp_text_in_resets
NDD_VALUE[14]=0

Once you have done that, you can force the parameters to take effect immediately by executing:

*ndd –c*

Run Bastille

If you have X-windows access to this machine, you can run HP's Bastille tool to help you further secure your machine. If you do not have X-windows access, you can manually apply the changes that Bastille made to my system. I would highly recommend though, if you don't have X-windows access that you get at least a demo of some software that will allow you to run X-windows on your PC. The Bastille tool is a very good one.

To run Bastille, make sure your DISPLAY environment variable is set appropriately and execute:

*/opt/sec_mgmt/bastille/bin/bastille*

The first time you run Bastille, you must accept the license agreement. Bastille will now start asking you a series of questions. If answered YES to everything EXCEPT:

Run Security_patch_check daily/weekly? *NO*
Proxy required for FTP? *NO* → Not needed since we answered NO above

Single-user mode password? *NO* → If you want to have to type a password to get to single-user mode you can answer YES.

I also changed the following so that they were different from their default values:

Umask – *077*
Password Expiration – *30*
Password Warning – *5*
Responsible for granting authorization – *Your Company Name Here*

Once we have finished answering Bastille's questions, it will ask if we want it to apply the configuration. I answered YES. Once the configuration is applied, a TODO list will be generated in /var/opt/sec_mgmt/bastille/TODO.txt, which will have some additional steps that you will have to do. You should review this file and follow its recommendations.

What Bastille did on my system:

- Created the /etc/issue file so it shows when users login. A copy of the /etc/issue file is available in Appendix A.
- Modified the kernel so that the parameter executable_stack is now 0. This provided stack execution protection.
- Suggested additional ndd parameter changes. The Bastille recommendations were incorporated in the ndd section above.
- I had to manually create the /.secure/etc directories so that auditing would start next time the system boots.
- I then rebooted the system so that the new kernel with stack execution protection would be active.

Install and Configure the IPFilter Software

We will now install and configure the IPFilter software that you can download from HP. This software should have been included in the bundle of software we created earlier in this exercise. To install IPFilter, invoke swinstall, set the "Source Depot Path…" to '/var/tmp/utility.depot' (or whatever you set yours to). Once the main swinstall window is up, select the IPFilter software from the list, mark it for installation, and then install it.

Installing this software WILL reboot the system.

When the system comes back up after the reboot, we will use the Bastille tool to help us configure IPFilter. Remember that Bastille requires X-windows access to this machine. If you don't have X-windows, you can use the ipf.conf file supplied at the end of this paper.

To use Bastille:

*/opt/sec_mgmt/bastille/bin/bastille*

- When the GUI starts, select IPFilter and click Next.
- Answer YES to the question “Should Bastille set up basic firewall rules with these properties?”
- Answer NO to “Block incoming Secure Shell?”
- Answer YES to “Are you done?”
- Click “Save Config”.
- Click “Apply Config”.
- Check the TODO.txt file, in /var/opt/sec_mgmt/bastille, for any additional actions that are required.

When complete, you should have a pretty good firewall set up on your HP-UX machine.

Install and Configure the TCP Wrappers Software

One of the last things to do to secure this system is to install and configure the TCP Wrappers software. This software allows us to secure processes that are run via inetd.

To install TCP Wrappers, invoke swinstall, use the utility.depot that we created earlier (and used in install IPFilter above) and select and install the TCP Wrappers software.

Once the software has been installed, there are several files that you have to configure. Those files are /etc/tcpd.conf, /etc/hosts.allow and/or /etc/hosts.deny. You will also have to modify your /etc/inetd.conf so that it calls the TCP Wrappers software to run any daemons configured there.

I configured my TCP Wrappers with the following files:

/etc/tcpd.conf:

```
##
#
# @(#)tcpd.conf $Revision: 1.001 $ $Date: 01/08/08 14:50:49 $
#
# tcpd(1M)  reads its configuration information from this file upon
# execution through inetd(1M).
#
# See the tcpd.conf(4) manual page for more information.
##
##
#  Timeout value for client's user name lookup
##
#rfc931_timeout              0
```

```
##
#  Action to be taken on reverse lookup failure
##
#on_reverselookup_fail      deny
##
#  Logging information level
##
log_level                  normal
```

/etc/hosts.allow (You will need to modify this file with your server name on the registrar line):

```
##
# @(#)hosts.allow $Revision: 1.001 $ $Date: 01/08/08 14:50:49 $
#
# The lines in the file contain the service daemon list and
# the Internet addresses or names of the hosts and/or networks
# allowed to use those services.
# The form for each entry in this file is:
#
# <daemon list> : <client list> [: <option> [: <option> ...] ]
#
# See the hosts_access(5) and hosts_options(5) manual pages for
# more information.
##
registrar: mytest.example.com, mytest, localhost
```

/etc/hosts.deny (This denies anything that is not explicitly allowed):

```
##
# @(#)hosts.deny $Revision: 1.001 $ $Date: 01/08/08 14:50:49 $
#
# The lines in the file contain the service daemon list and
# the Internet addresses or names of the hosts and/or networks
# denied to use those services.
# The form for each entry in this file is:
#
# <daemon list> : <client list> [: <option> [: <option> ...] ]
#
# See the hosts_access(5) and hosts_options(5) manual pages for
# more information.
##
ALL: ALL
```

/etc/inetd.conf (modified so that TCP Wrappers is used):

registrar stream tcp nowait root /usr/lbin/tcpd /etc/opt/resmon/lbin/registrar

You are now done. You should see entries in /var/adm/syslog/syslog.log whenever the registrar daemon runs. This is normal.

Tools from the Center for Internet Security

If you want to see how your system scores with the Center for Internet Security Benchmark tool for HP-UX, visit http://www.cisecurity.org/bench_hpux.html and download the HP-UX tool archive.

Once you have downloaded and transferred it to your HP-UX system, you must extract the tar archive. I worked from /var/tmp.

*cd /var/tmp*
*uncompress cis-hpux.tar.Z*

*tar –xvf cis-hpux.tar*

There is an hp_checkperms script that is included with this package. I ran it, looked at its recommendations and decided not to do anything, because the recommendations make no sense whatsoever to me. You can run the script and judge for yourself.

We will use swinstall, from the command line, to install the CISscan.pkg file. This is what scans your system and gives you your score. Don't forget to start the swagentd process (/sbin/init.d/swagentd start) or else swinstall will not work.

*swinstall –s $(pwd)/CISscan.pkg CISscan*

swinstall will now run and install the CISscan software. When the install has finished we can run it:

*/opt/CIS/cis-scan*

Once it has finished and given you your score, review the log file to determine if there are any actions you can take to better secure your system. The log file is located in /var/opt/CIS/tester.logs and the file you want to look at is cis-most-recent-log.

Focus on the Negative lines in the file and take care of those as best you can. There will be some things that are not possible or just not worth the effort.

Following this paragraph is a list of some items that were found during my first run of the cis-scan utility. The items that the cis-scan utility noted as negatives are shown in red. My notes and observations, if any, immediately follow each item.

Negative 5.1 - /opt not mounted read only; /var, /home, /tmp, and /stand not mounted nosuid.

Be aware that mounting /opt read-only can lead to some frustrations if/when you need to install patches or other software. You may want to wait until the system has been completely installed to do this. A copy of my /etc/fstab is included in Appendix A.

Negative 5.2 - /etc/group not owned by root:sys

Run the chown command on the file so that the ownership is appropriate.

Negative 5.2 - /tcb/files/auth/?/* should not be world readable, writeable or executable.

The files it is talking about are the files for each user, like /tcb/files/auth/r/root. You can do a chmod on the files to remove the rwx permission for world, but any time someone logs in as that user the world read permission will be automatically reinstated by HP-UX.

Negative 5.7 - /var/dt/Xerrors and /var/sam/log/samagent.log should not be group writeable.

Easy change. Just chmod the files to remove group write.

Negative 5.9 - checkperms not run.

It has been run, but I don't agree with its recommendations, so I did not apply the proposed modifications.

Negative 6.4 - /etc/shells doesn't exist

Created the /etc/shells file and added /usr/bin/sh and /sbin/sh to it. Did a 'chmod 444 /etc/shells' so that it is readable by anyone.

Negative 6.7 – Non-root accounts in cron.allow and at.allow.

Edit the /var/adm/cron.allow and /var/adm/at.allow files and remove all entries EXCEPT root.

Negative 8.1 – Users adm, daemon, bin and lp have valid shells in /etc/passwd.

Edit /etc/passwd and modify each user mentioned above and change their shell to /usr/bin/false.

Negative 8.6 - /usr/local/bin in roots PATH and is group writeable

Did a chmod on the directory to remove the group write permission bit.

Negative 8.7 – The sshd user has a world readable and executable home directory.

Removed world read and execute permissions even though the home directory is /var/empty.

Negative 8.11 - /etc/profile, /etc/csh.login, /etc/d.profile and /etc/d.login need 'mesg n' set.

Edited each file and put 'mesg n' (without the quotes, of course) as the last line in each file.

Once you finish reviewing and making changes based on the negatives in the log file, you can re-run cis-scan and see how much your score improves.

The final score for my system is 7.97 out of 10. I can live with that!

At this point, we have finished the hardest part of this exercise. Installing and securing the operating system itself is very definitely a time consuming and tedious process, as you have no doubt seen.

Cleanup

Before we actually start compiling and installing, Qmail and Qpopper, we should do a bit of cleanup.

Go through the /tmp and /var/tmp directories and remove anything that you no longer need. As long as you have a copy of the patches and various software packages on your PC or somewhere else, there is no need to keep them here.

Once you have done that, go ahead and create an Ignite/UX make_tape_recovery tape. This will come in VERY handy if something happens and you have to restore the entire system. The Ignite recovery will definitely be faster than going through everything we just did.

The command I like to use to create the make_tape_recovery tape is:

*`/opt/ignite/bin/make_tape_recovery –I –a /dev/rmt/0mn –v –x inc_entire=vg00`*

Note that you MUST use a no-rewind tape device. Also, be sure to use whatever tape device file is appropriate for your system.

Once the make_tape_recovery process finishes you can proceed with Installing Qmail.

COMPILING, INSTALLING AND SETTING UP QMAIL

We will now embark on the journey of installing and configuring Qmail. We are using Qmail instead of Sendmail because Qmail is not as complex, fairly easy to set up and configure and pretty easy to administer. It has also been said that Qmail is more secure than Sendmail.

Before we start this process, you should now download, if you haven't already, the following software:

- Patch – Ver 2.5.4 (http://hpux.connect.org.uk/hppd/hpux/Sysadmin/patch-2.5.4)
- Netqmail - Ver. 1.05 source code (http://www.qmail.org/)
- Daemontools – Ver. 0.76 source code (http://cr.yp.to/)
- Ucspi-tcp – Ver. 0.88 source code (http://cr.yp.to)
- Qpopper – Ver. 4.0.5 source code (http://www.eudora.com/qpopper/)

Once the software has been downloaded, transfer it to a directory on the HP-UX machine. I prefer to work out of /var/tmp. In this case, I created a directory in /var/tmp called qm and transferred all of my files there so that they are not in the base /var/tmp directory.

There are several good references for Qmail on the http://www.qmail.org web site. Two very good ones are:

Life with Qmail by Dave Sill – http://www.lifewithqmail.org/

Qmail HOWTO – http://www.flounder.net/qmail/qmail-howto.html

Installing the GNU Patch utility

The first thing we need to do is install the Patch utility. This utility allows you to patch source code files. It is a fairly simple install.

*cd /var/tmp/qm*

*gzcat patch-2.5.4-ss-11.00.tar.gz | tar –xvf –*

*cd patch-2.5.4*

At this point, you should review the HPUX.Install file for installation information. I used the basic installation process with no problems. Execute the recommended steps and watch for any errors that may occur. If you run across any, they need to be fixed before you proceed. I had no problems doing the following:

*./configure*

*gmake*

*gmake test*

*gmake install*

If everything was error free, then the Patch utility should now be installed.

Setting up the environment

Most of the installation of Qmail will be done based on Chapter 2 of *Life with Qmail*.

*umask 022*

You absolutely MUST set your umask as above before you start the Qmail installation. Most problems I have seen have been a direct result of incorrect permissions on files. Having the umask set correctly from the start eliminates most of the problems.

*mkdir –p /usr/local/src*

*mv netqmail-1.05.tar.gz ucspi-tcp-0.88.tar.gz /usr/local/src*

*mkdir –p /package*

*mv daemontools-0.76 /package*

*chmod 1755 /package*

*cd/ usr/local/src*

*gzcat netqmail-1.05.tar.gz | tar –xvf –*

*cd netqmail-1.05*

*./collate.sh*
Watch for any errors on this step. If there are any, take care of them before proceeding. I have done this a couple of times and I haven't seen any errors yet.

*cd ..*

*gzcat ucspi-tcp-0.88.tar.gz | tar –xvf –*

*rm *.tar.gz*

*cd /package*

*gzcat daemontools-0.76.tar.gz | tar –xvf –*

*rm *.tar.gz*

 # mkdir /var/qmail

Create Qmail Users and Groups

When you create the user IDs you must modify the file so that it appears as below. You can start with the Linux section of the IDS file (remove all lines from the file except that section) and then modify it appropriately.

*cd /usr/local/src/netqmail-1.05/netqmail-1.05*

*cp INSTALL.ids IDS*

*cat IDS*

```
groupadd nofiles
chgrp nofiles /var/qmail
chmod 770 /var/qmail
useradd -m -g nofiles -r yes -d /var/qmail/alias -s /usr/bin/false alias
useradd -m -g nofiles -r yes -d /var/qmail -s /usr/bin/false qmaild
useradd -m -g nofiles -r yes -d /var/qmail -s /usr/bin/false qmaill
useradd -m -g nofiles -r yes -d /var/qmail -s /usr/bin/false qmailp
groupadd qmail
chgrp qmail /var/qmail
useradd -m -g qmail -r yes -d /var/qmail -s /usr/bin/false qmailq
useradd -m -g qmail -r yes -d /var/qmail -s /usr/bin/false qmailr
useradd -m -g qmail -r yes -d /var/qmail -s /usr/bin/false qmails
```

To run the file and add the groups and users do:

*sh ./IDS*

Once it has finished, your /etc/passwd file should have the following entries at the end of the file:

```
alias:*:103:102::/var/qmail/alias:/usr/bin/false
qmaild:*:104:102::/var/qmail:/usr/bin/false
qmaill:*:105:102::/var/qmail:/usr/bin/false
qmailp:*:106:102::/var/qmail:/usr/bin/false
qmailq:*:107:103::/var/qmail:/usr/bin/false
qmailr:*:108:103::/var/qmail:/usr/bin/false
qmails:*:109:103::/var/qmail:/usr/bin/false
```

And your /etc/group file should have the following entries at the end:

nofiles::102:
qmail::103:

Build Qmail from source

We can now build Qmail from its source code. Before we start, we will need to edit the files conf-ld and conf-cc located in the current directory, which should be /usr/local/src/netqmail-1.05/netqmail-1.05. In each file, we will need to look for any occurrences of "cc" and replace them with "gcc" (all without the quotes, of course) since we are using the gcc compiler.

Once that is done, we can do the following:

*gmake setup check*

During this step, keep an eye open for any error messages. Most warning messages can be ignored.

When that finishes run:

*./config*

Qmail itself is now built. Now, we have to build and configure the other products we will use to run Qmail.

Build ucspi-tcp from source

We are now ready to build and install the ucspi-tcp product.

*cd /usr/local/src/ucspi-tcp-0.88*

Before we start, we will need to edit the conf-ld and conf-cc files for this product, just as we did with Qmail. In each file, we will need to look for any occurrences of "cc" and replace them with "gcc" (all without the quotes, of course) since we are using the gcc compiler.

First, we need to patch the product.

*patch < /usr/local/src/netqmail-1.05/other-patches/ucspi-tcp-0.88.errno.patch*

Now, we can build the product.

*gmake*

*gmake setup check*

If you didn't see any errors anywhere, you have finished building ucspi-tcp.

Build daemontools from source

We now have to build and install the daemontools package.

*cd /package/admin/daemontool-0.76/src*

Again, we will need to edit the conf-ld and conf-cc files for this product, just as we did with Qmail. In each file, we will need to look for any occurrences of "cc" and replace them with "gcc" (all without the quotes, of course) since we are using the gcc compiler.

Next, we need to patch daemontools before we do the actual installation.

*patch < /usr/local/src/netqmail-1.05/other-patches/daemontools-0.76.errno.patch*

Now, we can do the build and install:

*cd ..*

*package/install*

When the installation completes, there should be a new entry in the /etc/inittab file.

SV:123456:respawn:/command/svscanboot

There should also be a couple of svscan processes running as well.

*ps –ef | grep svscan*
```
root   945     1  0 13:36:11 ?        0:00 /bin/sh /command/svscanboot
root   949   945  0 13:36:12 ?        0:01 svscan /service
```

We have now finished building, installing and configuring the daemontools package.

Configuring Qmail

Now we get to have fun. It's now time to start configuring Qmail so that it does what we want it to do. As we configure Qmail, keep in mind that the end result, when the WHOLE server is finished, will be that this will be a POP3 server. The mail delivery options we choose must reflect that.

The first thing we need to do is create the /var/qmail/rc file. There are several templates to choose from in the /var/qmail/boot directory. We are going to use the home template.

This will take any incoming mail for a user and store that mail in a Maildir file in that user's home directory.

*cd /var/qmail*

*cp /var/qmail/boot/home rc*

*chmod 755 rc*

Next, we need to create the /var/qmail/bin/qmailctl script. This script has numerous functions. It can start and stop qmail, display qmail statistics and a host of other things. The easiest way to create this script is to go to http://www.lifewithqmail.com/qmailctl-script-dt70 and copy to your PC and then transfer it to the HP-UX machine. I have also included the script in Appendix A if you want to attempt to type it in yourself.

Once the script exists in /var/qmail/bin you need to do the following:

*chmod 555 /var/qmail/bin/qmailctl*

*ln –s /var/qmail/bin/qmailctl /usr/bin*

Next, we need to create the scripts that will control all of the Qmail services. To do this, we need to do the following:

mkdir –p /var/qmail/supervise/qmail-send/log

mkdir –p /var/qmail/supervise/qmail-smtpd/log

Now we need to create several files. These are all fairly short and not too bad to create with vi.

The files you need to create and their contents are:

File: /var/qmail/supervise/qmail-send/run
Contents:

```
#!/bin/sh
exec /var/qmail/rc
```

File: /var/qmail/supervise/qmail-send/log/run
Contents:

```
#!/bin/sh
exec /usr/local/bin/setuidgid qmaill /usr/local/bin/multilog t /var/log/qmail
```

File: /var/qmail/supervise/qmail-smtpd/run
Contents:

```
#!/bin/sh

QMAILDUID=$(id -u qmaild)
NOFILESGID=$(id -g qmaild)
MAXSMTPD=$(cat /var/qmail/control/concurrencyincoming)
LOCAL=$(head -1 /var/qmail/control/me)

if [ -z "$QMAILDUID" -o -z "$NOFILESGID" -o -z "$MAXSMTPD" -o -z "$LOCAL" ]; then
        echo QMAILDUID, NOFILESGID, MAXSMTPD, or LOCAL is unset in
        echo /var/qmail/supervise/qmail-smtpd/run
        exit 1
fi

if [ ! -f /var/qmail/control/rcpthosts ]; then
        echo "No /var/qmail/control/rcpthosts!"
        echo "Refusing to start SMTP listener because it'll create an open relay"
        exit 1
fi

exec /usr/local/bin/softlimit -m 2000000 \
/usr/local/bin/tcpserver -v -R -l "$LOCAL" -x /etc/tcp.smtp.cdb -c "$MAXSMTPD" \
-u "$QMAILDUID" -g "$NOFILESGID" 0 smtp /var/qmail/bin/qmail-smtpd 2>&1
```

File: /var/qmail/supervise/qmail-smtpd/log/run
Contents:

```
#!/bin/sh
exec /usr/local/bin/setuidgid qmaill /usr/local/bin/multilog t /var/log/qmail/smtpd
```

Now, change the permissions on all of the files that we just created.

 # chmod 755 /var/qmail/supervise/qmail-send/run
 # chmod 755 /var/qmail/supervise/qmail-send/log/run
 # chmod 755 /var/qmail/supervise/qmail-smtpd/run
 # chmod 755 /var/qmail/supervise/qmail-smtpd/log/run

We now need to create a file in the /var/qmail/control directory called concurrencyincoming. To do this:

 # echo 20 > /var/qmail/control/concurrencyincoming
 # chmod 644 /var/qmail/control/concurrencyincoming

We now need to set up the logging directory.

 # mkdir –p /var/log/qmail/smtpd
 # chown qmail /var/log/qmail /var/log/qmail/smtpd

Last, we need to create symbolic links in the /service directory for the /var/qmail/supervise/qmail-send and /var/qmail/supervise/qmail-smtpd directories we created above.

*ln –s /var/qmail/supervise/qmail-send /service*

*ln –s /var/qmail/supervise/qmail-smtpd /service*

Once you create the links to the /service directory, which was created as part of the daemontools installation, qmail will start. If you do not want qmail running right now, just do a:

*qmailctl stop*

Configure SMTP Relay Controls

In order to be able to actually send e-mail from this machine, we need to tell Qmail to allow the localhost and anyone on our internal network to send mail via SMTP from this machine. This assumes an internal Class B network of 1.2.*.*.

To set this up we do the following:

*echo '127.:allow,RELAYCLIENT=" " ' >> /etc/tcp.smtp*
*echo '1.2.:allow,RELAYCLIENT=" " ' >> /etc/tcp.smtp*

To get these changes to take effect, we do:

*qmailctl cdb*

If you have an internal Class A network, you could substitute '1.:allow,REALAYCLIENT=" " ' or if you have an internal Class C network you can substitute '1.2.3.:allow,RELAYCLIENT=" " ' in the 2nd statement above. Just be sure to use whatever your internal IP addressing scheme is. This allows you to prevent outsiders from using your e-mail server as an open relay.

You can make changes to the /etc/tcp.smtp file at any time. If you do, be sure to rerun the 'qmailctl cdb' command so that Qmail will re-read the file and activate the changes.

Verify that Sendmail is not Running

Since we are using Qmail as our MTA on this machine, we definitely do NOT want, nor do we need, sendmail running. With the security steps we did earlier, it should not be running, but let's verify that it is not anyway.

*ps –ef | grep sendmail | grep –v grep*

You should not get any results back from this. If you do, then sendmail is still running and needs to be deactivated. To stop sendmail do:

*`/sbin/init.d/sendmail stop`*

And once you do that, you need to modify the /etc/rc.config.d/mailservs file such that the line that contains SENDMAIL_SERVER looks like:

export SENDMAIL_SERVER=0

To be absolutely sure that the sendmail daemon will not start, we will remove the link in /usr/lib to the sendmail binary and also rename the sendmail binary.

*`rm /usr/lib/sendmail`*

*`mv /usr/sbin/sendmail /usr/sbin/sendmail.donotuse`*

*`chmod 0 /usr/sbin/sendmail.donotuse`*

Substitute Qmail for Sendmail

In order for everything to work correctly, we must fool some things to get them to work. We are going to create symbolic links so that anything that still calls sendmail will actually use Qmail.

*`ln –s /var/qmail/bin/sendmail /usr/sbin/sendmail`*

*`ln –s /var/qmail/bin/sendmail /usr/lib/sendmail`*

Create E-mail Aliases

The last thing we need to do before we actually try to send a message with Qmail is create some aliases that Qmail uses for different functions. The aliases we will create are for root, postmaster and mailer-daemon. The root and postmaster aliases are pretty standard aliases. The mailer-daemon alias is used for e-mail that may bounce for one reason or another.

To create the aliases:

*`echo user@example.com > /var/qmail/alias/.qmail-root`*

*`echo user@example.com > /var/qmail/alias/.qmail-postmaster`*

*`ln –s /var/qmail/alias/.qmail-postmaster /var/qmail/alias/.qmail-mailer-daemon`*

*`chmod 644 /var/qmail/alias/.qmail*`*

Use whatever e-mail address is appropriate for your environment in place of the user@example.com in the above commands.

Starting and Testing Qmail

Now comes the fun part. We will try to start Qmail and see if we can actually send a message with it.

To start Qmail:

*qmailctl start*

Wait a few seconds and check the status of Qmail by doing:

*qmailctl stat*

All four services should be up and the time should be greater than one second. If they are not all up, or the time is only one second, then you have problems and need to figure out what they are.

The biggest problem I have seen is permissions. You absolutely must make sure your umask is 022 before you start this process.

To check for problems, you can use the inst_check script from Life with Qmail. This script is available online from http://www.lifewithqmail.org/inst_check . This script does a very good job of checking for problems. Just download the script, transfer it to the HP-UX machine (I would put it in /var/qmail/bin), change the permissions on it to 500 (no one but root should run it) and run it. It will analyze your Qmail environment and report on any problems it finds. If you fix the problems that inst_check finds, Qmail should work.

Once you fix anything that inst_check reports as a problem, you may have to stop and restart Qmail. To do so:

*qmailctl stop*

*qmailctl start*

Wait a few seconds and check the status again:

*qmailctl stat*

Once all four services show as being up for more than one second, you can try sending a message via Qmail.

*mailx –s "Test from Qmail" user@example.com < /etc/hosts*

The e-mail address you use should be one you can easily check, like your regular corporate address. If you receive the message with the contents of the /etc/hosts file from the system, then Qmail is working.

You can also check the /var/adm/syslog/mail.log file to verify that the message was sent without any errors. The mail.log file is a very good troubleshooting tool.

NOTE: Qmail requires that the filesystem be mounted with suid capability. When securing the system earlier, one of the recommendations was to mount /var with the nosuid option. That will not work in this case. If you have mounted /var as nosuid, then you need to remove that option from the /var entry in the /etc/fstab file and reboot the machine.

Allow E-mail into the Server

In order for us to be able to send e-mail TO this machine, we must modify the /etc/opt/ipf/ipf.conf file. While we are modifying the file, we will go ahead and add a line to allow pop3 access to this machine as well. We need to add the lines:

pass in quick proto tcp from any to any port = smtp
pass in quick proto tcp from any to any port = pop3

I added the above lines to my ipf.conf file immediately after the comment lines:

These rules specifically do not log netbios udp or portmapper
packets because these protocols tend to be very noisy on networks

A complete copy of my /etc/opt/ipf/ipf.conf file is included in Appendix A.

Once that is done you need to stop and restart IPFilter by doing:

*`/sbin/init.d/ipfboot stop`*

*`/sbin/init.d/ipfboot start`*

Send a Test Message TO the Server

Once IPFilter is configured appropriately, you can try sending a test message TO the Qmail server. Just be aware that ANY user you send an e-mail to MUST exist on the server. We will talk about adding users to the server a little later, after we have configured the POP3 server functionality.

You could send the test message to 'root@mytest.example.com' (or whatever you named the server). Be aware though, that you configured an alias for the root user earlier, so that message will probably be relayed right back to you. If it is, that indicates that Qmail is functioning appropriately, for both sending and receiving messages.

To send the message to the server, just use your normal corporate e-mail program and address it directly to the server, as in my root example above.

Again, you can check the /var/adm/syslog/mail.log to see if the message was received. This should work without any problems.

INSTALLING AND CONFIGURING QPOPPER

Now we are going to compile and install the Qpopper software on the HP-UX machine so that it can act as a POP3 server. Qpopper was chosen because: 1) It worked. It has the flexibility to use PAM for authentication where others didn't. 2) It is FREE! I like FREE!

The first thing you need to do is download the software from the address given earlier in this paper. When you have the file downloaded, transfer it to your HP-UX machine.

Compiling and Installing Qpopper

This file that we download is a gzip'ed tar file of the Qpopper source code. As such, we have to compile it like we have everything else.

The first thing we need to do is extract the source code from the gzip'ed file.

Switch to the directory you transferred the software to on your HP-UX system. As usual, I prefer to work out of the /var/tmp directory.

*cd /var/tmp*

*gzcat qpopper4.0.5.tar.gz | tar –xvf –*

*cd qpopper4.0.5*

NOTE: The following command should be typed on a SINGLE COMMAND LINE. I am splitting into multiple lines for readability.

*./configure --enable-home-dir-mail=Maildir --enable-log-login --enable-auth-file-/opt/qpopper/qpopper.allow --enable-specialauth --enable-server-mode --with-pam=pop3*

The configure script should run without any problems. Once it has completed, we can compile and install the software.

*make*

Keep an eye open for errors during the make process. There should not be any, but if there are they will need to be resolved before you go to the next step.

*make install*

The installation creates an executable file called popper and copies that file to /usr/local/bin. I do not want it there. I want to run popper out of the /opt directory since

we are going to mount it as read only when we finish setting this up. So we are now going to move /usr/local/bin/popper to /opt/qpopper.

*mkdir /opt/qpopper*

*chmod 755 /opt/qpopper*

*mv /usr/local/bin/popper /opt/qpopper/popper*

Verify that the permissions of the qpopper executable are appropriate. They should be 755.

*ll /opt/qpopper/qpopper*

If the permissions are not correct:
*chmod 755 /opt/qpopper/qpopper*

Create the qpopper.allow file

We now need to create the qpopper.allow file. We specified in the configuration script the location of the qpopper.allow file. This file provides an extra level of authentication. If the user that tries to invoke qpopper, via their POP3 mail client, is not in this file, then they will be denied access.

This file should contain the user id of people that will need to retrieve their e-mail from this machine. The file should be readable and writeable by the root user ONLY.

```
# cat /opt/qpopper/qpopper.allow
user
resu
user1

# ll /opt/qpopper/qpopper.allow
-rw-------   1 root       sys            16 Jun 17 15:28 /opt/qpopper/qpopper.allow
```

Modify files to allow qpopper to run

In order for Qpopper to work, we must modify the /etc/inetd.conf file, the /etc/services file and the /etc/hosts.allow file. Qpopper will only run when a request is received via the normal POP3 network port and, since we are using TCP Wrapper, only if it is received from an authorized network address.

Edit the /etc/inetd.conf file and insert the following line:

pop3 stream tcp nowait root /usr/lbin/tcpd /opt/qpopper/popper –s

Verify that the following line exists in your /etc/services file:

pop3 110/tcp pop-3 # Post Office Protocol - Version 3

The above line should be there by default. If it is not you will need to add it.

The last file to edit is the /etc/hosts.allow file. This will tell TCP Wrapper which IP addresses are allowed to use the POP3 server. Your file should be similar to:

```
##
# @(#)hosts.allow $Revision: 1.001 $ $Date: 01/08/08 14:50:49 $
#
# The lines in the file contain the service daemon list and
# the Internet addresses or names of the hosts and/or networks
# allowed to use those services.
# The form for each entry in this file is:
#
# <daemon list> : <client list> [: <option> [: <option> ...] ]
#
# See the hosts_access(5) and hosts_options(5) manual pages for
# more information.
##
registrar: mytest.example.com, mytest, localhost
sshd: .example.com
popper: .example.com
```

The above TCP Wrapper configuration file allows anyone in the example.com domain access to popper and sshd. This can be customized as you see fit.

Modify /etc/pam.conf for authentication

We now need to modify the /etc/pam.conf file so that we can authenticate users via the PAM functionality of HP-UX. This allows us to have the system set up in Trusted mode making the system much more secure.

The /etc/pam.conf file should be similar to the following file:

```
#
# PAM configuration
#
# Authentication management
#
login    auth required        /usr/lib/security/libpam_unix.1
su       auth required        /usr/lib/security/libpam_unix.1
ftp      auth required  /usr/lib/security/libpam_unix.1
pop3   auth required  /usr/lib/security/libpam_unix.1
OTHER        auth required        /usr/lib/security/libpam_unix.1
#
```

```
# Account management
#
login    account required     /usr/lib/security/libpam_unix.1
su       account required     /usr/lib/security/libpam_unix.1
ftp      account required     /usr/lib/security/libpam_unix.1
pop3     auth required  /usr/lib/security/libpam_unix.1
#
OTHER        account required     /usr/lib/security/libpam_unix.1
# Session management
#
login    session required     /usr/lib/security/libpam_unix.1
pop3     auth required  /usr/lib/security/libpam_unix.1
OTHER        session required     /usr/lib/security/libpam_unix.1
#
# Password management
#
login    password required  /usr/lib/security/libpam_unix.1
passwd       password required  /usr/lib/security/libpam_unix.1
pop3     auth required  /usr/lib/security/libpam_unix.1
OTHER        password required  /usr/lib/security/libpam_unix.1
```

Note the four separate occurrences of the pop3 line. That same entry must be added in each of the sections.

Setting up users

The last thing we need to do before we actually test, is set up a couple of user IDs on this system. When that is done, we can try sending e-mail to them and try connecting to the machine with a POP3 client to retrieve their messages.

The easiest way to do this is to use the following command line:

```
# useradd –s /usr/bin/false –d /home/resu –m resu

# chmod go-rx /home/resu
```

I am using the username resu as an example. Substitute whatever username and home directory are appropriate for the user you are adding. I am specifying a shell of /usr/bin/false because the user should NOT be logging in directly to this machine. They should only retrieve their e-mail with a POP3 client. You should also check the permissions of the home directory. In this case, it was created with group and world read and execute permissions. I don't want those permissions so I removed them.

You will now need to set the password for the user you just created.

```
# passwd resu
```

Testing Qmail and Qpopper

You can now send a test message to resu@example.com. To see if the message was received, change to the /home/resu directory and do an 'ls –l'. Look for the Maildir file. That file does not exist by default. If the file now exists, and the size is greater than zero, then your message most likely made it through.

To verify that the message is actually there you can do a 'cat Maildir' and see what is there. You should see the test message you just sent. If that is the case, then Qmail is properly receiving the messages and storing them in the appropriate Maildir files.

To test the POP3 functionality you will need to set up a POP3 compliant e-mail client. If you don't have one, you can download Eudora for free. Eudora is available at http://www.eudora.com .

When setting the client up you can set both the POP3 Server Name and the SMTP Server Name to be the name of the server we have just built. In my case, it is mytest.example.com. You will need to use the user id you set up above, resu in this example, and whatever password you assigned.

Once the client is set up, you should be able to login to the server via POP3 and download whatever e-mail is available for that user.

It should work fine. I had very little trouble getting Qpopper to work. It is a fairly simple, but seemingly fairly robust, program.

If everything worked, you can give yourself a pat on the back as you should now have a working Qmail / Qpopper e-mail server.

LAST STEPS

There are a couple of last points to consider; 1) Mount the filesystems on the machine as recommended by the CIS tool. 2) Install and use something like Tripwire so you know when important files change.

Change /etc/fstab Mount Options

If you are going to mount your filesystems as recommended by the CIS security scan tool, then you should do that now. The one exception that has to be made from their recommendations is that the /var filesystem can NOT be mounted as nosuid. That will break Qmail.

If you want to follow their recommendations as closely as possible, take a look at my /etc/fstab located in Appendix A. Modify your /etc/fstab to match, and your filesystems will be mounted with the new options next time you reboot the machine.

Install Tripwire

It would be a very good idea to install and use a tool like Tripwire (http://www.tripwire.com) to help you keep track of changes to important system files. The problem is that Tripwire for HP-UX is not free. You must buy the product. Considering that I had a budget of $0 for this project, that was not an option.

I am hoping to be able to buy Tripwire and install it in the future.

GENERAL TESTING

Most of our testing has been done as we have been installing the various products on the system. Qmail and Qpopper should be functioning normally if you have followed the steps I have outlined.

If you wish to test the network security of the system, you can employ scanning tools like Nmap (http://www.insecure.org/nmap/), Nessus (http://www.nessus.org/) or Tara (http://www-arc.com/tara/). We are not going to utilize any of these tools at this time. My two main reasons are 1) I don't want to freak out our security people, and 2) I don't know that this system would be able to handle the scan. The last thing I want to do is crash the system.

Since the machine will be in the DMZ, with a firewall between it and the Internet, the risk of not running a port scan on this machine is acceptable.

If you wish to verify that services like telnet and ftp are not running, try connecting to the machine with those commands. You should get a "Connection Refused" message. If you do not, you need to go back and look at your /etc/inetd.conf file again.

ONGOING MAINTENANCE

There is a certain amount of ongoing maintenance and monitoring that will be required with this server. These tasks include, but are not limited to, backing the system up, keeping the system current on patches, reviewing the various system log files, monitoring disk space, and user administration.

Backups

Backing the system up is, in my opinion, the single most important maintenance task that must be done. If the system crashes, you absolutely MUST be able to restore it in a timely fashion.

To back this system up, I am going to use HP's Ignite/UX product. Since this is an e-mail server, nothing should be changing on this system on a regular basis except for the e-mail that is passing through the machine. User modifications, additions, and deletions should be few and far between as well, at least in my case.

I will set up a cron job to run the backup every Saturday morning at 10:30 AM. The cron job will execute a script called /usr/local/bin/sys_recovery.sh. This script will in turn run the actual Ignite/UX make_tape_recovery command, which will back the system up and notify me of the success or failure of the backup. The sys_recovery.sh script can be found in Appendix A.

Here is the excerpt from cron that schedules this job:

30 10 * * 6 /usr/local/bin/sys_recovery.sh

Keep Current On patches

The second most important task facing system administrators is keeping their system(s) current on patches, especially security patches. With a machine such as this mail server, that is even more important. HP's security_patch_check tool should be run on a regular basis, at least weekly. This tool will inform you when there are additional security related patches that need to be installed.

If this machine has Internet FTP access, you can just schedule a cron job to run the security_patch_check tool and e-mail you the results.

00 8 * * 6 /opt/sec_mgmt/spc/bin/security_patch_check –r 2>&1 | mailx –s "Security Patch Check results" user@example.com

If you do not have Internet FTP access from this machine, you will need to manually download the security catalog files and transfer them to the /opt/sec_mgmt/spc/bin directory on this machine. The files you need to download are security_catalog.sync and security_catalog.gz. These files are available from ftp.itrc.hp.com and are located in the /export/patches directory.

Once you have the list of patches from the security_patch_check tool, you can download them from the HP ITRC Patch Database and install them just like earlier in this process.

Remember that you will probably have to modify your /etc/fstab file to remove the ro (read-only) mount option from the /opt filesystem and reboot the machine before you install any patches. You will also have to make sure that the swagentd process is running since we stop that process as part of the system boot process.

Don't forget to change /etc/fstab back to mounting /opt as read-only once you have finished installing the patches.

Monitor / Review System Log Files

A system administrator should have some sort of process that will automatically monitor the critical log files on a system. Occasionally the system administrator should go to the

machine and review the log files to make sure that the monitoring process is not missing something important.

HP's OpenView Vantage Point Operations product is our standard for system monitoring. This product allows you to create templates that will monitor anything you want on a system. We have installed the VPO client on this system and the system administrator is paged if something abnormal is detected.

The problem with VPO is that it is an enterprise level product and is very expensive. There are other tools that can help you to monitor your log files.

Logcheck, http://sourceforge.net/projects/sentrytools/ , is one of those products. As far as I know, logcheck will run on HP-UX. I am not 100% certain of that though.

Monitoring Disk Space

Disk space monitoring is also a pretty important task. You do not want the server to run out of disk space in a critical file system, like /home where all users' mail is stored, and start refusing e-mail messages.

Ideally you should have a script that runs every few minutes and monitors the available space left for each filesystem and if it reaches a preset level, say 98%, then you get paged.

This is another thing that I use VPO for. There are options within VPO to monitor disk space on a system so if anything gets above 96% I get paged so I can take care of the problem.

User Administration

You also need to be sure you take care of any user administration needs on this machine. You will likely always be informed when someone needs an account set up. That is the easy part. The more difficult part is making sure you are informed when someone's account needs to be removed.

You should periodically check the Maildir files in each users home directory to see when they last received e-mail. If it has been a while, you may want to check and see if that person is still an active employee.

Ideally, you should have an employee termination process, and you should be part of that process so that an employee's access can be removed.

One thing to keep in mind is that you may be required by law, or company policy, or both, to keep that employee's e-mail for a certain amount of time. You should check with your legal department on this issue.

TROUBLESHOOTING

Qmail

Once everything has been installed and is functioning normally, there really isn't a whole lot that can go wrong. I have had a Qmail server running for several months and I have had no trouble whatsoever with Qmail.

The few times I have had complaints of mail not being received, it has generally been due to problems on the Internet or the address was incorrect or something similar.

If you do have problems with Qmail, then your first step should be to run the inst_check script that I reference earlier in this document. That is the single best tool for troubleshooting Qmail problems.

If you are having trouble sending e-mail from this server, your first stop should be the /var/adm/syslog/mail.log file. You should be able to see any problems with outgoing messages in that file. Concentrate on the errors there and you should be able to solve your problems.

Qpopper

I do not yet have this server in production, so I have not had any complaints from users about not being able to get their e-mail. However, the Qpopper product seems to be very robust and trouble-free so far.

The only issue I have had was in setting up a new user and forgetting to add the user id into the /opt/qpopper/qpopper.allow file. Once I did that, I had no more problems.

There is a troubleshooting section in the "Qpopper Administrators Guide". In the event of a problem, that would be a very good place to start.

Passwords

The other thing I can see being problems are passwords. If this is going to be a high volume e-mail server, I would look seriously at trying to implement some sort of mechanism so users can reset their own passwords. In this case, this will be a very low volume and low user count server, so I can manage that password issue.

APPENDIX A

/etc/issue

```
**************************************************************************
                    NOTICE TO USERS

This computer system is the private property of Your Company, Inc.,
whether individual, corporate or government.  It is for authorized use only.
Users (authorized or unauthorized) have no explicit or implicit
expectation of privacy.

Any or all uses of this system and all files on this system may be
intercepted, monitored, recorded, copied, audited, inspected, and
disclosed to your employer, to authorized site, government, and law
enforcement personnel, as well as authorized officials of government
agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring,
recording, copying, auditing, inspection, and disclosure at the
discretion of such personnel or officials.  Unauthorized or improper use
of this system may result in civil and criminal penalties and
administrative or disciplinary action, as appropriate. By continuing to
use this system you indicate your awareness of and consent to these terms
and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the
conditions stated in this warning.

**************************************************************************
```

/etc/fstab

```
# System /etc/fstab file.  Static information about the file systems
# See fstab(4) and sam(1M) for further details on configuring devices.
/dev/vg00/lvol3 / vxfs delaylog 0 1
/dev/vg00/lvol1 /stand hfs nosuid,defaults 0 1
/dev/vg00/lvol4 /home vxfs nosuid,delaylog 0 2
/dev/vg00/lvol5 /opt vxfs ro 0 2
/dev/vg00/lvol6 /tmp vxfs nosuid,delaylog 0 2
/dev/vg00/lvol7 /usr vxfs delaylog 0 2
/dev/vg00/lvol8 /var vxfs delaylog 0 2
```

/var/qmail/bin/qmailctl

```
#!/bin/sh

# description: the qmail MTA

PATH=/var/qmail/bin:/bin:/usr/bin:/usr/local/bin:/usr/local/sbin
export PATH

QMAILDUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`

case "$1" in
  start)
    echo "Starting qmail"
    if svok /service/qmail-send ; then
      svc -u /service/qmail-send /service/qmail-send/log
    else
      echo "qmail-send supervise not running"
    fi
    if svok /service/qmail-smtpd ; then
      svc -u /service/qmail-smtpd /service/qmail-smtpd/log
    else
      echo "qmail-smtpd supervise not running"
    fi
    if [ -d /var/lock/subsys ]; then
      touch /var/lock/subsys/qmail
    fi
    ;;
  stop)
    echo "Stopping qmail..."
    echo "  qmail-smtpd"
    svc -d /service/qmail-smtpd /service/qmail-smtpd/log
    echo "  qmail-send"
    svc -d /service/qmail-send /service/qmail-send/log
    if [ -f /var/lock/subsys/qmail ]; then
      rm /var/lock/subsys/qmail
    fi
    ;;
  stat)
    svstat /service/qmail-send
    svstat /service/qmail-send/log
    svstat /service/qmail-smtpd
    svstat /service/qmail-smtpd/log
    qmail-qstat
    ;;
```

```
  doqueue|alrm|flush)
    echo "Flushing timeout table and sending ALRM signal to qmail-send."
    /var/qmail/bin/qmail-tcpok
    svc -a /service/qmail-send
    ;;
  queue)
    qmail-qstat
    qmail-qread
    ;;
  reload|hup)
    echo "Sending HUP signal to qmail-send."
    svc -h /service/qmail-send
    ;;
  pause)
    echo "Pausing qmail-send"
    svc -p /service/qmail-send
    echo "Pausing qmail-smtpd"
    svc -p /service/qmail-smtpd
    ;;
  cont)
    echo "Continuing qmail-send"
    svc -c /service/qmail-send
    echo "Continuing qmail-smtpd"
    svc -c /service/qmail-smtpd
    ;;
  restart)
    echo "Restarting qmail:"
    echo "* Stopping qmail-smtpd."
    svc -d /service/qmail-smtpd /service/qmail-smtpd/log
    echo "* Sending qmail-send SIGTERM and restarting."
    svc -t /service/qmail-send /service/qmail-send/log
    echo "* Restarting qmail-smtpd."
    svc -u /service/qmail-smtpd /service/qmail-smtpd/log
    ;;
  cdb)
    tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp
    chmod 644 /etc/tcp.smtp.cdb
    echo "Reloaded /etc/tcp.smtp."
    ;;
  help)
    cat <<HELP
stop -- stops mail service (smtp connections refused, nothing goes out)
start -- starts mail service (smtp connection accepted, mail can go out)
pause -- temporarily stops mail service (connections accepted, nothing leaves)
cont -- continues paused mail service
stat -- displays status of mail service
```

```
cdb -- rebuild the tcpserver cdb file for smtp
restart -- stops and restarts smtp, sends qmail-send a TERM & restarts it
doqueue -- schedules queued messages for immediate delivery
reload -- sends qmail-send HUP, rereading locals and virtualdomains
queue -- shows status of queue
alrm -- same as doqueue
flush -- same as doqueue
hup -- same as reload
HELP
    ;;
  *)
    echo "Usage: $0
{start|stop|restart|doqueue|flush|reload|stat|pause|cont|cdb|queue|help}"
    exit 1
    ;;
esac

exit 0
```

/etc/opt/ipf/ipf.conf

```
# Copyright 2002, Hewlett Packard Company
#
# WARNING: This file was generated automatically and will be replaced
# the next time you run bastille.  DO NOT EDIT IT DIRECTLY!!!
#
#IPFilter configuration file

# block incoming packets with ip options set
block in log quick all with ipopts


################################################################################
# The following rules were inserted from the file
# /etc/opt/sec_mgmt/bastille/ipf.customrules
# and should be edited there rather than here.  Re-running bastille
# will create a new ipf.conf file including any custom rules from
# that file.
#
#   DO NOT EDIT THIS FILE DIRECTLY!!!
#
#   RULES INSERTED FROM /etc/opt/sec_mgmt/bastille/ipf.customrules
#   ARE BELOW.  THESE MAY BE OVERWRITTEN IF YOU RERUN BASTILLE!!!
#
#   #    #    #    #    #    #    #    #    #    #
#   #    #    #    #    #    #    #    #    #    #
```

```
#  #   #   #   #   #   #   #   #   #
#  #   #   #   #   #   #   #   #   #
# ### ### ### ### ### ### ### ### ###
#  ###  ###  ###  ###  ###  ###  ###  ###
#  #   #   #   #   #   #   #   #   #

#######################################################
 # These rules will allow connections initiated from
 # this host along with the return connection

 pass out quick proto icmp all keep state
 pass out quick proto tcp all keep state
 pass out quick proto udp all keep state

 # End allow outgoing rules
 #######################################################

 # These rules specifically do not log netbios udp or portmapper
 # packets because these protocols tends to be very noisy on networks
 pass in quick proto tcp from any to any port = smtp
 block in quick proto udp from any to any port = netbios_ns
 block in quick proto udp from any to any port = netbios_dgm
 block in quick proto udp from any to any port = portmap



#  #   #   #   #   #   #   #   #   #   #
#  ###  ###  ###  ###  ###  ###  ###  ###  ###
# ### ### ### ### ### ### ### ### ### ###
#  #   #   #   #   #   #   #   #   #   #
#  #   #   #   #   #   #   #   #   #   #
#  #   #   #   #   #   #   #   #   #   #
#  #   #   #   #   #   #   #   #   #   #
#
#  RULES INSERTED FROM /etc/opt/sec_mgmt/bastille/ipf.customrules ABOVE
#
#########################################################################

#########################################################################
#  The following rules explicitly allow certain types of connections
#

# do NOT allow isee incoming connections
# pass in quick proto tcp from any       to any port = 2367  flags S keep state keep frags

# do NOT allow tftp incoming connections
```

```
# pass in quick proto udp from any           to any port = tftp

# Allow SecureShell incoming connections
pass in quick proto tcp from any           to any port = 22     flags S keep state keep frags

# do NOT allow bootp incoming connections
# pass in quick proto udp from any port = bootpc to any port = bootps     keep state

# do NOT allow snmpTraps incoming connections
# pass in quick proto udp from any           to any port = snmp-trap  keep state

# do NOT allow webadmin incoming connections
# pass in quick proto tcp from any           to any port = 1188    flags S keep state keep
frags

# do NOT allow webadminautostart incoming connections
# pass in quick proto tcp from any         to any port = 1110    flags S keep state keep
frags

# do NOT allow wbem incoming connections
# pass in quick proto tcp from any           to any port = wbem-https flags S keep state
keep frags

# do NOT allow snmpGetSet incoming connections
# pass in quick proto udp from any           to any port = snmp       keep state

# do NOT allow DNSquery incoming connections
# pass in quick proto udp from any           to any port = domain     keep state

# do NOT allow hpidsagent incoming connections
# pass in quick proto tcp from any       to any port = hpidsagent flags S keep state keep
frags

# do NOT allow hpidsadmin incoming connections
# pass in quick proto tcp from any       to any port = hpidsdmin  flags S keep state keep
frags

# do NOT allow DNSzonetransfer incoming connections
# pass in quick proto tcp from any to any port = domain flags S keep state keep frags

#Block any incoming connections which were not explicitly allowed
block in log all
```

/usr/local/bin/sys_recovery.sh

```
#!/bin/sh

DATE=$(/usr/bin/date '+%m%d%y')

HOSTNAME=$(/usr/bin/hostname)

LOG_DIR=/var/adm/logs/sysrecover

LOG_FILE=${LOG_DIR}/${HOSTNAME}.${DATE}

LVMCONF_DIR=/etc/lvmconf

TAPE=/dev/rmt/0m

NTAPE=${TAPE}n

/usr/bin/mt -f ${TAPE} rewind

/usr/bin/date > ${LOG_FILE}
/usr/bin/echo "" >> ${LOG_FILE}

/opt/ignite/bin/make_tape_recovery -a ${NTAPE} -I -m tar \
    -t "$(uname -n) system recovery tape created on ${DATE}" \
    -v -x inc_entire=vg00 1>> ${LOG_FILE} 2>> ${LOG_FILE}

sleep 120
/usr/bin/mt -f ${NTAPE} offl

/usr/bin/echo "" >> ${LOG_FILE}
/usr/bin/date >> ${LOG_FILE}

STATUS=$(grep -i completed ${LOG_FILE} | awk '{print $5,$6,$7,$8,$9,$3,$2}')

                echo "For more information check the ${LOG_FILE}" | mailx \
              -s "$(uname -n) $STATUS" wallekp@hqnas06,ankoleu@hqnas06
```

REFERENCES

Wong, Chris. HP-UX 11i Security. Upper Saddle River: Prentice Hall PTR, 2002

Garfinkel, Simson and Spafford, Gene and Schwarts, Alan. Practical Unix & Internet Security. Sebastopol: O'Reilly & Associates, Inc, 2003

Poniatowski, Marty. HP-UX 11i System Administration. Upper Saddle River: Prentice Hall Ptr, 2001

Steves, Kevin. "Building a Bastion Host Using HP-UX 11." August 29, 2002 http://www2.itrc.hp.com/service/cki/docDisplay.do?docLocale=en_US&docId=200000066258828 (April 20, 2004)

Sill, Dave. "Life with qmail." June 30, 2004 http://www.lifewithqmail.com/lwq.html (May 12, 2004)

Gellens, Randall and Miller, Gigi and Anthony, Scott and Rouleau, Armand. "Qpopper Administrator's Guide" March 2001 http://www.eudora.com/download/eudora/qpopper/4.0/free/final/Qpopper.pdf (May 17, 2004)

Last Updated: April 23rd, 2018

Upcoming Training

SANSFIRE 2018	**Washington, DC**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANS Network Security 2018	**Las Vegas, NV**	**Sep 23, 2018 - Sep 30, 2018**	**Live Event**
SANS London October 2018	**London, United Kingdom**	**Oct 15, 2018 - Oct 20, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**