

APPENDIX P

Procedures to Upgrade Security on the SCO UNIXWARE 7.1.1 Server

There are several files that need to be modified on your SCO Unixware 7.1.1 Server. I'll list and walk-through each one below. Also, there are various operating system patches that will have to be applied to the system, these will be discussed in greater detail below as well. You must be logged in as the root user for ALL tasks in this document.

- (1) Open a terminal window and change directory to `“/etc/default”`.
- (2) Edit the `“login”` file and add a line to the end of the file to read, `“CONSOLE=/dev/console”`. Next locate & change a line to read, `“MAXTRYS=3”`. Next locate & change a line to read, `“LOGFAILURES=3”`. Next locate & change a line to read, `“DISABLETIME=99999”`. Save the file.
- (3) These changes will ensure that the root user can ONLY login at the console and will hopefully make it more difficult for a hacker to continuously attempt to log into your system.
- (4) Edit the `“passwd”` file and locate & change a line to read `“PASSLENGTH=8”`. Save the file. This change will ensure that passwords are at least 8 alphanumeric characters in length.
- (5) Edit the `“useradd”` file and locate & change a line to read `“INACT=90”`. Save the file. This change will inactivate any accounts that have been idle for 90 days.
- (6) Please ensure none of your users have blank passwords and make sure passwords are aged properly according to the policy in the SA manual.
- (7) Another security ‘risk’ to our system is the C-compiler that is loaded with the Unixware 7.1.1 operating system. We will remove that now. Change directory to `“/usr/ccs/bin”`. At the root prompt, type `“rm cc”` and press enter.

Note: This next section is to be completed only if **Update 7.1.1** is **NOT** on your system. To determine if it is, open a terminal window and type `“pkginfo update711”` and press enter. If you see `“update update711 Unixware 7 Update 7.1.1”`, then skip to (2) below. Otherwise, the next part of the security upgrade is to apply the Update 7.1.1 package that is located on the **Unixware 7 Updates CD-ROM (Disk 2 of 3)** that came with your system. It will be applied using the SCO ADMIN tool.

- 1) Insert the Unixware 7 Updates CD-ROM (Disk 2 of 3) into the cd-rom drive. Ensure that you are logged in as the root user. Enter **Sco Admin** and select **“Software Management”**. Then select **“Application Installer”**. Click on **“Update View”**. Scroll down and highlight **“Update 7.1.1”**, then click on **“Install”**. Accept defaults for any question asked. When the update has completed, exit the SCO Admin tool. Open a terminal window and reboot the system by typing the command, `“shutdown -i6 -g0 -y”`.

2) Next part of the security upgrade is a process, which entails applying 34 SCO operating system patches. Many require you to reboot the system after application of a patch because it has to rebuild the kernel. Entire process from start to finish will take approximately 1.5 hours. At this time, the patches and associated text files documenting what is included in each patch can be obtained either by cd-rom (from SEC-LEE), downloaded from a server here at SEC-LEE (to be determined) or from the SCO/CALDERA website (<http://www.caldera.com/support/ftplists/uw7list.html>). Basically the patches are installed one by one and you will have to place them in a directory on your server. I suggest a directory called “**scopatches**” (**Note:** If patches are compressed, utilize the “uncompress” command to uncompress them all). After all the patches are in this directory, you will change to that directory and install one at a time. I’ll list each one below and also which patches require a system reboot. For DOIM purposes, more recent patches have superseded some patches and I’ll make note of these at the end of this section. It’s **important** to note, the patches will have to be loaded in the order I list below due to the requirement that some patches require certain ones to be loaded prior to their installation.

- (a) **PTF7603K (Sysdump, VMM Features and Various Fixes Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7603k**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (b) **PTF7701B (Illum Driver and Emergency Recovery Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7701b**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (c) **PTF7715A (Networking and Mem Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7715a**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (d) **PTF7717A (Unixware 7.1.1 Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7717a**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).

- (e) **PTF7710A (ntp Buffer Overflow Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7710a**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (f) **PTF7686A (Audit Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7686a**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (g) **PTF7676A (asyc and iasy Driver).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7676a**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (h) **PTF7664A (cu Security Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7664a**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (i) **PTF7663A (eelsd Security Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7663a**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (j) **PTF7646B (Ip Driver Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7646b**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (k) **PTF7644C (intmap, ldterm and ptem Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7644c**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (l) **PTF7642A (pppGUI Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7642a**” and press enter. Accept all

defaults by pressing enter. No system reboot is required after this patch has been installed.

- (m) **PTF7641D (mc01 Driver Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7641d**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (n) **PTF7634A (mtrr Driver Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7634a**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (o) **PTF7632E (pci Driver Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7632e**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (p) **PTF7627B (osocket Driver Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7627b**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (q) **PTF7624B (diskadd and diskrm Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7624b**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (r) **PTF7620C (fur Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7620c**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (s) **PTF7617C (hw Utility Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7617c**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.

- (t) **PTF7614C (scodb Driver Supplement).** At the command prompt, type “**pkgadd -d /scopatches/ptf7614c**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (u) **PTF7611B (pdimkdev Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7611b**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (v) **PTF7610D (st01 Driver Supplement).** At the command prompt, type “**pkgadd -d /scopatches/ptf7610d**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (w) **PTF7609C (pkgadd Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7609c**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (x) **PTF7607E (libc Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7607e**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (y) **PTF7604G (Hot Plug NIC Supplement).** At the command prompt, type “**pkgadd -d /scopatches/ptf7604g**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (z) **PTF7441E (libmas Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7441e**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (aa) **PTF7426F (ksh Supplement).** Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7426f**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.

- (bb) **PTF7410I (libthread Supplement)**. Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7410i**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (cc) **PTF7130D (sendmail 8.10.1)**. Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7130d**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (dd) **PTF7080D (ticots and ticotsor Supplement)**. At the command prompt, type “**pkgadd -d /scopatches/ptf7080d**” and press enter. Accept all defaults by pressing enter. After the patch has been installed, reboot the system (while rebooting the kernel will be rebuilt).
- (ee) **PTF7045G (Intel Microcode Driver)**. Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7045g**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (ff) **PTF7438G (Unixware 7.X Network Printing Supplement)**. Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/ptf7438g**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.
- (gg) **IAVA A2002-0006 (Buffer Overflow in Common Desktop Environment (CDE) Subprocess Control (SPC) Server)**. This patch can be located at, <ftp://stage.caldera.com/pub/security/openunix/CSSA-2001-SCO.30/> or obtained from SEC-LEE via cd-rom. Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/erg711881**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed
- (hh) **IAVA B2002-0004 (File Globbing Heap Corruption Vulnerability)**. Open a terminal window and change directory to “scopatches”. At the command prompt, type “**pkgadd -d /scopatches/erg501215b**” and press enter. Accept all defaults by pressing enter. No system reboot is required after this patch has been installed.

For DOIM purposes or for your information, the following patches were not applied since they were superseded by new patches above:

- (1) ptf7687a (FTP Server Manager Supplement) has been superseded by ptf7715a for the Unixware 7.1.1 platform only.
- (2) ptf7658c (FTP Service Supplement) has been removed and superseded by ptf7715a.
- (3) ptf7655a (in_telnetd Supplement) has been removed and superseded by ptf7715a.
- (4) ptf7636a (vol Driver Supplement) has been superseded by ptf7717a for Unixware 7.1.1 only.
- (5) ptf7625b (cpio Supplement) has been superseded by ptf7717a for Unixware 7.1.1 only.
- (6) ptf7616b (specfs Driver Supplement) has been removed and is superseded by ptf7717a.
- (7) ptf7612b (ping Supplement) has been removed and is superseded by ptf7715a.
- (8) ptf7608c (sd01 Driver Supplement) has been superseded by ptf7603k.
- (9) ptf7602d (vxfs Driver Supplement) was removed and has been superseded by ptf7717a.
- (10) ptf7601h (inet and socksys Driver Supplement) has been superseded by ptf7603k.
- (11) ptf7058d (mcctl Supplement) was removed and has been superseded by ptf7641d.
- (12) ptf7613a (iasy Driver Supplement) has been superseded by ptf7676a for Unixware 7.1.1 only.
- (13) ptf4141b (ArcserveIT v6.61 Maintenance Supplement) is not required since the ArcServe tool is not utilized by our system.

Disabling System Services:

Several services on your Unixware 7.1.1 server will be disabled: CHARGEN, DAYTIME, DISCARD, ECHO, FINGER, LOGIN, TALK, NETSTAT, NFSD, NTALK, POP-3, SNMP, SMTP, SUNRPC, & SYSTAT.

- (1) Login as the root user and open a terminal window.
- (2) Change directory to `"/etc/inet"`.
- (3) Make backup copies of the `"inetd.conf"` and `"services"` files. (Use the cp (copy) command).
- (4) Then edit the `"inetd.conf"` file and comment out the lines beginning with `"chargen"`, `"daytime"`, `"discard"`, `"echo"`, `"finger"`, `"login"`, `"pop-3"`, `"talk"`, `"netstat"`, `"ntalk"`, & `"systat"`. Save the file.
- (5) Next, edit the `"services"` file and comment out the lines beginning with `"chargen"`, `"daytime"`, `"discard"`, `"echo"`, `"finger"`, `"login"`, `"netstat"`, `"nfsd"`, `"pop-3"`, `"talk"`, `"ntalk"`, `"smtp"`, `"snmp"`, `"sunrpc"`, & `"systat"`. Save the file.
- (6) Change directory to `"/etc/rc2.d"`. Rename `"S73snmp"` to `"s73snmp"`. This will prevent the "SNMP" service from starting when the system is booted up.

