Global Information Assurance Certification Paper

Securing UNIX GCUX Practical Assignment
Version 1.6b

HP-UX 11.0 Installation Checklist

By Della Schmidt

HP-UX 11.0 Installation Checklist

This document is to be used as a guide to help create a secure HP-UX 11.0 Internet ready server. Since this is to be a secure install it is advisable that the server remain off the network/internet until it has been completely configured. You will need to have some way to transfer files so the system will need either a tape drive or a cdrom physically attached. It is also advisable not to have a C compiler installed on the system. (While this won't stop a determined hacker it will make it just a little bit harder for them.) Since the machine will not have a compiler you will need to do the compiles on a different machine and transfer the binaries between them.

HP-UX Minimal OS Installation

To cold-install HP-UX 11.0, you must have the following:

A supported HP 9000 server or workstation (see Appendix A)
64 MB memory, minimum
128 MB swap space, minimum
2GB root disk volume, minimum

You will need the following CD's ready:

HP-UX 11.0 Install/Update/Recovery CD, March 2001 or later.
Core OS Options CD (for technical servers and workstations).
Support Plus CD, March 2001 or later (for hardware/critical patch bundle, diagnostics and iCOD product), is needed.
HP-UX 11.0 Application Software CDs

1. ____ Make sure all peripherals are turned on.
2. ____ Turn on the server or recycle the power.
3. ____ Load the Install and Core OS CDROM into the CD-ROM driver.
4. ____ Interrupt the autoboot process, by pressing any key during the 10 second interval that is given. This is so the system can be booted from the Core OS CDROM.
5. ____ Once autoboot was been interrupted you should now see the autoboot menu.
6. ____ Boot from the device that contains the Core OS CDROM. Usually the alternative boot path is the CDROM drive. But to verify that you can type **search** and view all defined boot devices.
   bo alt OR **bo <device path>**
7. ____ You should now be asked: Interact with IPL (Y or N) ?> Type **n**.
8. ____ The install kernel will take 3-5 minutes to install.
9. ____When that has completed a screen will appear asking for the keyboard language of the console. Respond with the correct number and press ENTER.

10. ____ The Welcome to Ignite-UX screen will be displayed.
11. ____ Tab to Install HP-UX field and press Enter.
12. ____ From the User Interface and Media Options screen, verify that these choices are selected:
    Source Location Options: Media-only installation – installing from the local CD drive.

    User Interface Options: Guided Installation – provides an install wizard with limited choices.
13. ____Now proceed through each screen to configure your system:
    Basic Configuration: Commercial Servers – this will install HP-UX 11.0 Core OS software, required ACE patches, general recommended core (XSWGR1100), latest hardware-enablement and critical (HWCR) patches, diagnostic products and COD Client Product for HP-UX 11.0

    Software Selection: Select needed mass-storage and networking I/O driver products.

    Languages: Click the Languages button to view CDE-languages bundles to be loaded. **Global** is set by default when installing on workstations, resulting in all available CDE-language bundles being installed. **Global (Non-CDE)** is set when installing on servers to indicate that a generic, CDE-language bundle will be installed.

14. ____ Review any messages that Ignite-UX encountered. Resolve any errors before continuing with the installation.
15. ____ Select: **Finish**
16. ____ The system will now configure the disk(s) and load a minimum set of commands and libraries. Software Distributor will download all the products and patches from the CD.
17. ____ As prompted, replace the HP-UX 11.0 Install/Update/Recovery CD with the requested CD from the media box.
18. ____ The system will automatically reboot after all software has been loaded.
19. ____ Set_parms will run and asked you to set
    root password
    date,
    time,
    time zone,
    IP address
    other network parameters.

Updating Applications

After installing HP-UX 11.0, install other needed applications

1. ____Use swinstall to install new software that was not included as part of the basic OS installation. The latest versions of HP-UX software products are provided on the HP-UX Applications CDs. To find the contents of each CD, mount any HP-UX Applications CD and view the TOC file.
2. ____ After installing the software, complete any post-install configuration. This will be explained in the software's release notes or manual. Most documentation for HP-UX applications are either on the HP-UX Instant Information CD or on HP's documentation Web site: docs.hp.com/hpux/os/11.0/

HP-UX Patches Installation

To track down know HP software vulnerabilities and solutions, use the HP Security Archive on the IT Resource Center Web site. Each bulletin contains a description of the problem, which versions of the Operating System are affected and the solution. To access this information go to:

http://itrc.hp.com
Search Technical Knowledge Base
Security Bulletin Archive

You can also subscribe to HP's Security Bulletin Digest. You will receive an email update of new vulnerabilities as they are identified. To sign up for this go to:

http://itrc.hp.com
more…
support information digests

Modification of the Boot Process

Closely review the startup scripts and identify all unnecessary services. You will then want to stop these services from starting up by renaming the startup script file that can be found in /sbin/rc?.d. By renaming the link instead of deleting it, it will be easier if you have to invoke the process in the future. Please pay particular attention to insecure network services. You should be able to eliminate everything in /sbin/rc3.d.

1. ____ Review /etc/rc.log to determine which processes are started on boot
2. ____ Rename NFS-related links
   /usr/bin/mv /sbin/rc2.d/S400nfs.core /sbin/rc2.d/.NOS400nfs.core
   /usr/bin/mv /sbin/rc2.d/S430nfs.client /sbin/rc2.d/.NOS430fns.client
   /usr/bin/mv /sbin/rc3.d/S100nfs.server /sbin/rc3.d/.NOS100nfs.server
3. ____ Rename RPC link

/usr/bin/mv /sbin/rc2.d/S590Rpcd /sbin/rc2.d/.NOS290Rpcd

4. ____ Rename Sendmail links
   /usr/bin/mv /sbin/rc2.d/S540sendmail /sbin/rc2.d/.NOS540sendmail
5. ____ If this is machine not going to be a DNS server, rename DNS link
   /usr/bin/mv /sbin/rc2.d/S370named /sbin/rc2d/.NOS370named
6. ____ Rename everything in /sbin/rc3.d
   /usr/bin/cd /sbin/rc3.d
   for file in S*
   do
   mv $file .NO$file
   done

Create a script to ensure that the startup scripts run with a proper umask [14]

1. ____ /usr/bin/echo 'umask 022' > /sbin/init.d/umask.sh
2. ____ /usr/bin/chmod 744 /sbin/init.d/umask.sh
3. ____ Add umask.sh to startup script directories by running the following script
   /usr/bin/umask 022
   for d in /sbin/rc?.d
   do
   /usr/bin/ln –s /sbin/init.d/umask.sh $d/S000umask.sh
   done

Inetd is the internet daemon that controls access to network services that are started on an as needed basis. Many of the services are considered unsafe. Therefore it is very important to review these services and disable ones that are not absolutely necessary. The Berkley "r" programs have a long history of abuse so make sure that shell and login services are disable. You may also want to consider disabling bootps, exec, ntalk, echo and charge. In fact the ideal situation would be not to run inetd at all. (If inetd is not running you will not have remote access to the machine, until ssh is installed and configured)

1. ____ Disable inetd – Preferred method
   /usr/bin/mv /sbin/rc2.d/S500inetd /sbin/rc2d/.NOS500inetd
   /usr/bin/rm /etc/inetd.conf

2. ____ inetd enabled – but with all unnecessary disabled
   /usr/bin/vi /etc/inetd.conf
   comment out (place # at the beginning of a line) all unnecessary services
   /usr/bin/kill –HUP inetd

Network Tuning

Reconfigure various network parameters to reduce your vulnerability to smurf attacks, SYN floods and ARP spoofing attacks. A description of the listed network parameters can be found in Appendix B. You can use **ndd –h sup** to list all supported network parameters. Use **ndd –h unsup** to list unsupported network parameters. HP recommends that you DO NOT make changes to unsupported parameters.

1. ____/usr/bin/vi /etc/rc.config.d/nddconf
2. ____ Add following entries:

```
TRANSPORT_NAME[0]=ip
NDD_NAME[0]=ip_send_redirects
NDD_VALUE[0]=0
TRANSPORT_NAME[1]=ip
NDD_NAME[1]=ip_ire_flush_interval
NDD_VALUE[1]=60000
TRANSPORT_NAME[2]=arp
NDD_NAME[2]=arp_cleanup_interval
NDD_VALUE[2]=60000
TRANSPORT_NAME[3]=ip
NDD_NAME[3]=ip_forward_directed_broadcast
NDD_VALUE[3]=0
TRANSPORT_NAME[4]=ip
NDD_NAME[4]=ip_forward_src_routed
NDD_VALUE[4]=0
TRANSPORT_NAME[5]=ip
NDD_NAME[5]=ip_forwarding
NDD_VALUE[5]=0
TRANSPORT_NAME[6]=tcp
NDD_NAME[6]=tcp_ip_abort_cinterval
NDD_VALUE[6]=60000
```

3. ____ ndd –c for the changes to take effect

File System Configuration

Some file systems are static in nature and won't change unless you're doing some type of upgrade. Therefore to safeguard against unkown modifications to the files in these file systems and possible addition of trojan horses, it makes sense to mount these files systems read-only. (/usr and /opt are examples) You also want to ensure that setuid programs are not executed in a non-root file system. To do this these file systems must be mounted with the nosuid option. (/var and /home are examples). An example of a secure /etc/fstab can be found in Appendix C.

1. ____ /usr/bin/vi /etc/fstab
2. ____ Add ro option to /opt and /usr
3. ____ Add nosuid to /stand, /var, /home

/usr/local by default has been configured with world-writeable permissions on all directories. Change this to a safer 755.

1. ____ find /usr/local –type d –exec chmod 755 {} \;

Remove write group permissions for /etc/.

1. ____ chmod –R g-w /etc

Remaining Network Services

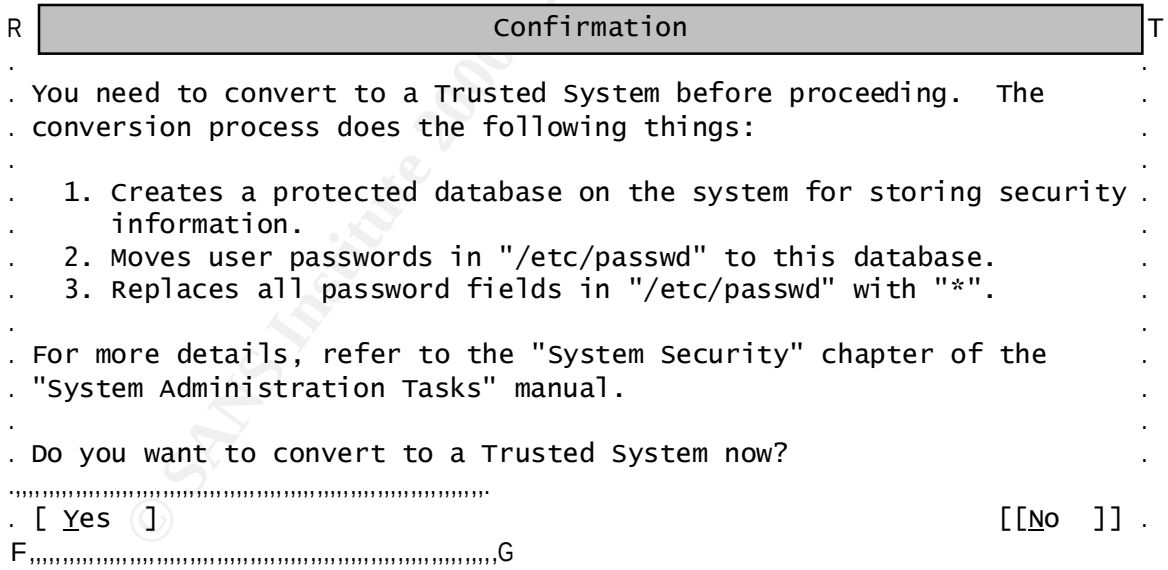
If the machine is to be a DNS client then you'll need to define the domain and it's name server(s). You will have to configure which sources the resolver will use and in which order. You should configure so that the host file is checked first then DNS.

1. ____ /usr/bin/touch /etc/resolv.conf
2. ____ /usr/bin/echo "domain <domain name>" > /etc/resolv.conf
3. ____ /usr/bin/echo "nameserver <ip address>" >> /etc/resolv.conf
4. ____ /usr/bin/chown root:root /etc/resolv.conf
5. ____ /usr/bin/chmod 644 /etc/resolv.conf
6. ____ /usr/bin/cp /etc/nsswitch.files /etc/nsswitch.conf
7. ____ /usr/bin/vi /etc/nsswitch.files
   modify the hosts entry from hosts:files to hosts:files [NOTFOUND=continue] dns
8. ____ /usr/bin/chown root:root /etc/nsswitch.conf
9. ____ /usr/bin/chmod 644 /etc/nsswitch.conf

Convert to a Trusted System

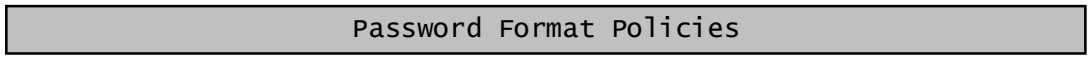
HP-UX offers some additional security features such as, a more stringent authentication system, auditing, terminal access control and time-based access control. These are in addition to the normal Unix security mechanisms that are generally available. But to take advantage of these features the system must be converted to a trusted system.* If security is important, it is recommended this be done. To convert a system you would need to:

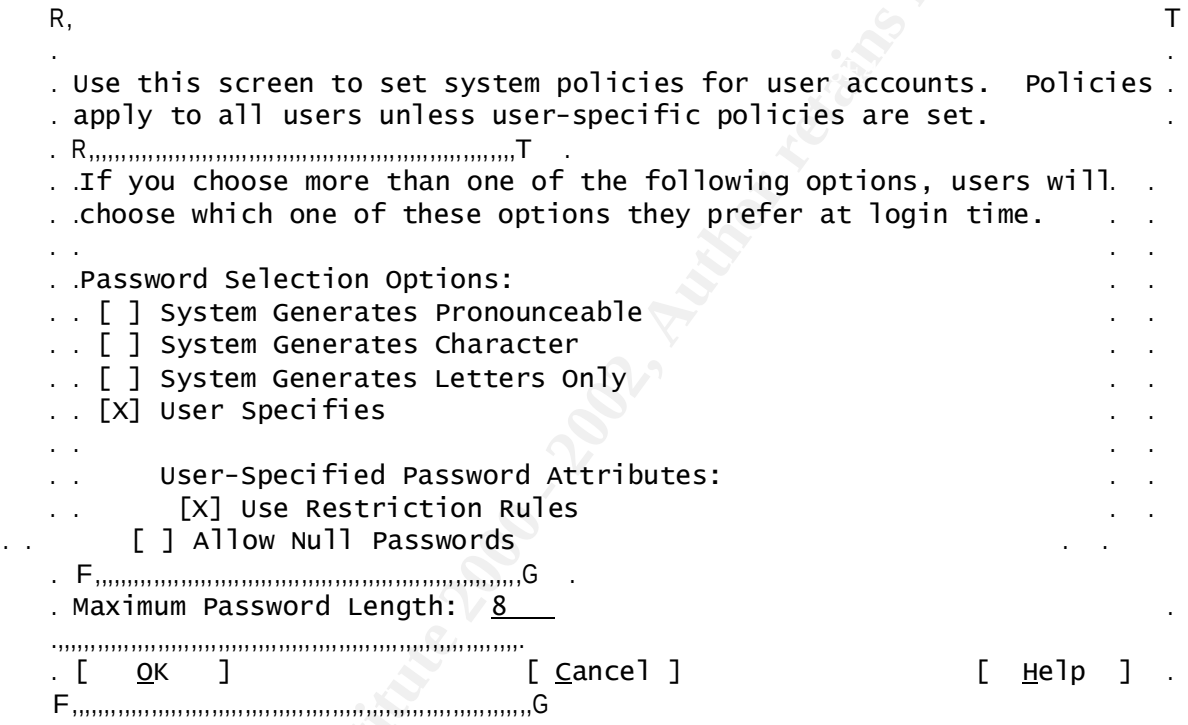
/usr/sbin/sam
Select "Auditing and Security"
Select "System Security Policy"
Select "YES"

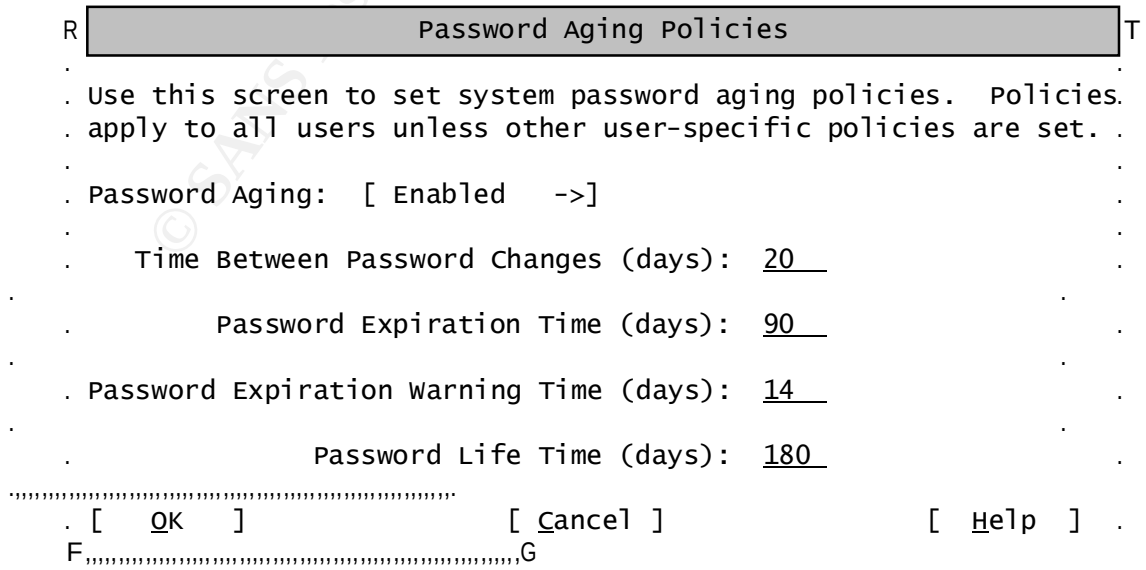


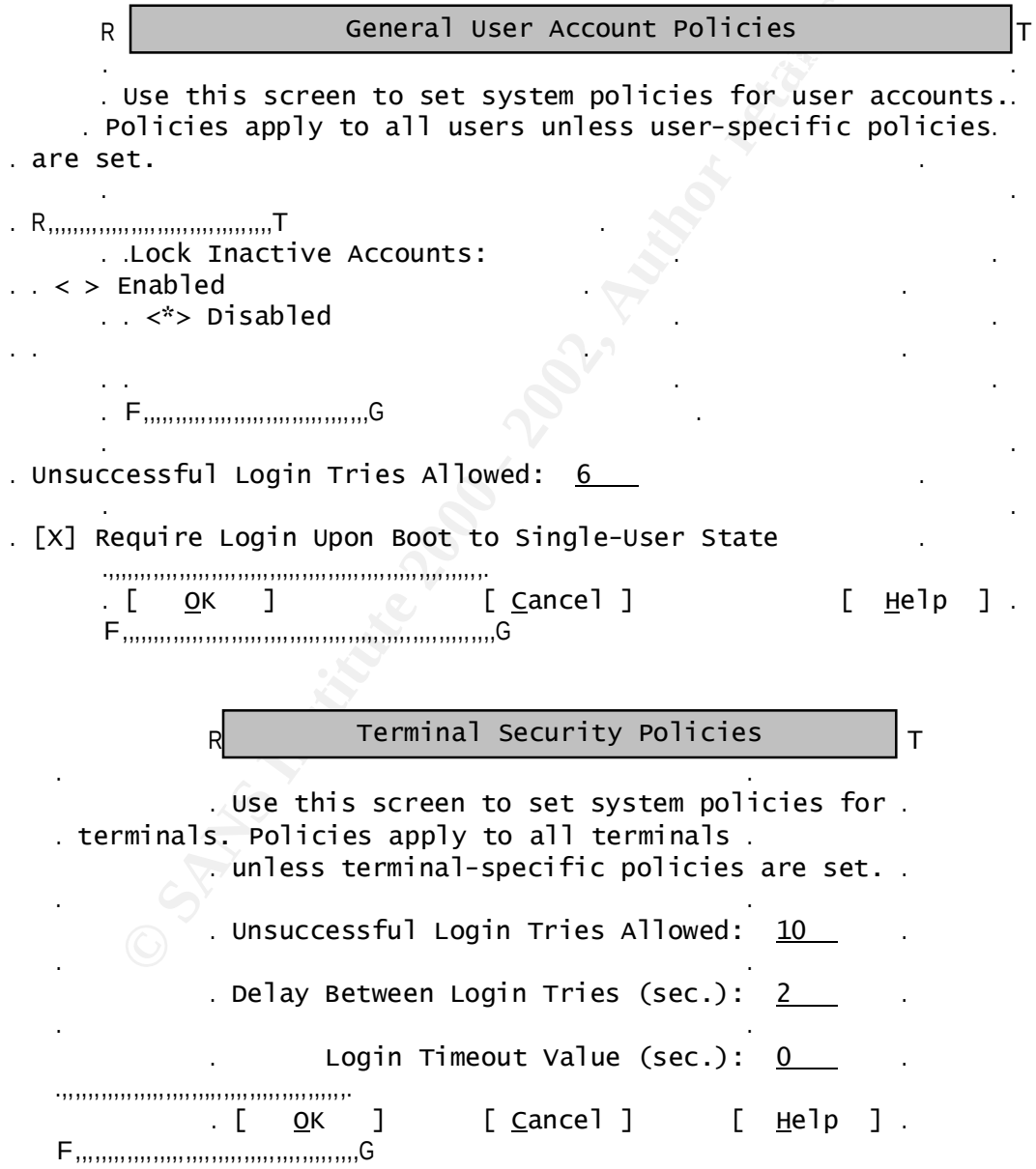
You will then see a message telling you that you're converting to a trusted system...
Next you will receive a "Successfully converted to a trusted system" message. Press OK continue.

Time to setup your security policies. The following are recommendations only. Please curtail yours to fix your environment.







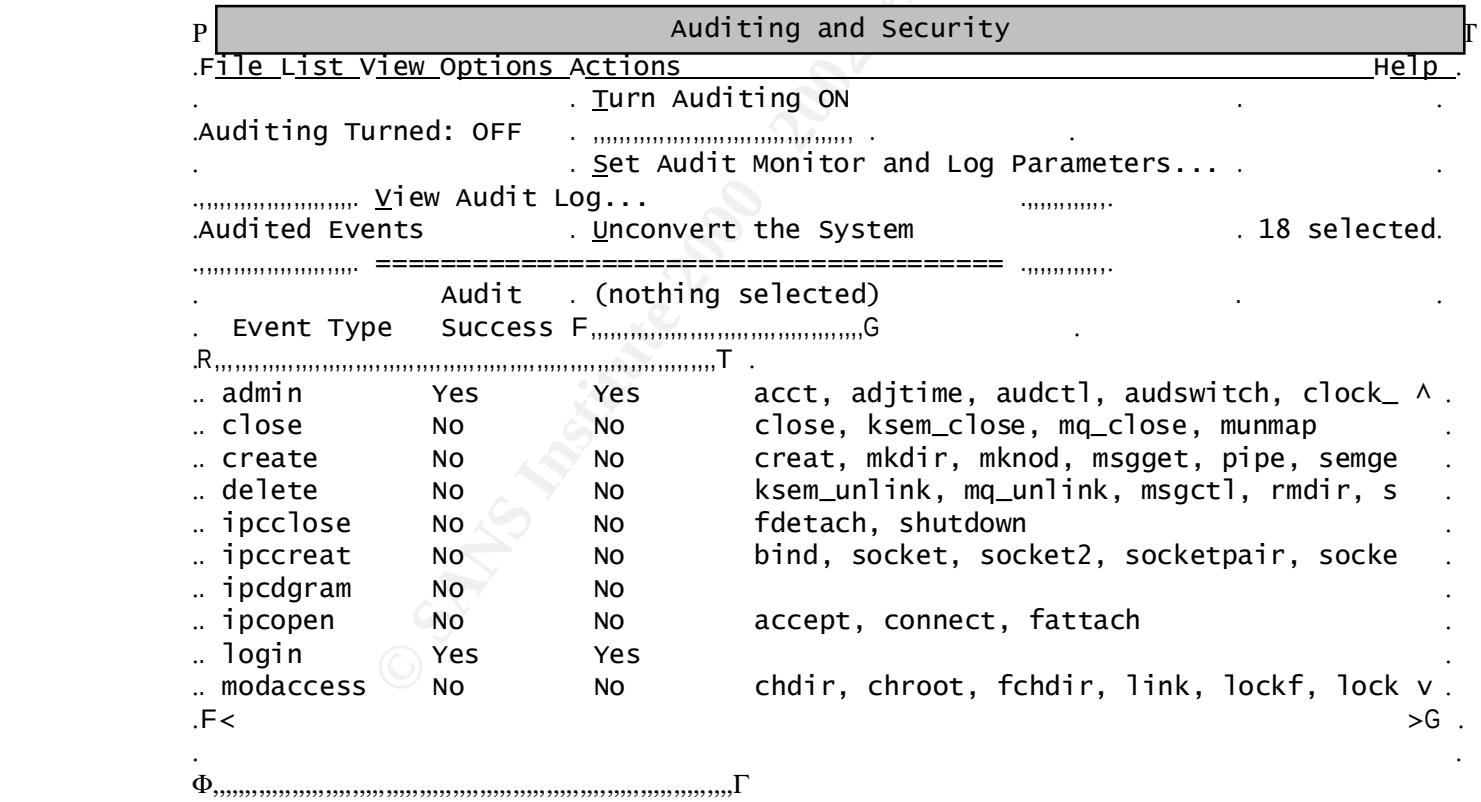


* Network Information Service (NIS) is not supported on a trusted system.

System And Process Auditing

Now that the system has been converted to a trusted system and your security policies have been set. It's time to turn on auditing.

/usr/sbin/sam
Select "Auditing and Security"
Select "Audited Events"
Select "Actions"
Select "Turn Auditing On"



Next you need to select which events you want to audit. At the very minimum you should audit

admin - Logs all administrative and privileged events.
login - Logs all logins and logouts
modaccess - Logs all access modifications other than DAC
moddac - Logs all modifications of object's discretionary access controls

Setup a cron job to collect system diagnostic messages.

1. _____ /usr/bin/crontab –e
2. _____ Insert the following 2 lines
   # log kernel diagnostic messages every 10 minutes
   05,15,25,35,45,55 * * * * /usr/sbin/dmesg - >>/var/adm/messages

User Access Control

Tight controls must be maintained on user's accounts. You should only have accounts on a system that are necessary for the applications that are running.

Restrict root login to just the console. User must use su to login as root.

1. _____ /usr/bin/touch /etc/securetty
2. _____ /usr/bin/echo console > /etc/securetty
3. _____ /usr/bin/chmod 400 /etc/securetty

Enable password history and password reuse. On a trusted systems, the system administrator can enable the password history feature to discourage users from reusing previous passwords

1. _____ /usr/bin/touch /etc/default/security
2. _____ /usr/bin/echo "PASSWORD_HISTORY_DEPTH=10" > /etc/default/security
3. _____ /usr/bin/chown bin:bin /etc/default/security
4. _____ /usr/bin/chmod 444 /etc/default/security

Lock all "pseudo-accounts", including uucp, lp, nnucp, sys, hpdb and www. These are logins that are not associated with individual users and do not have true interactive shells. They are in the password file because they are owners of files.

1. _____ /usr/bin/vi /etc/passwd and change the default shell to /dev/null
2. _____ Lock accounts using /usr/bin/passwd –l <login>
3. _____ Remove any files in /var/spool/cron/crontabs except for root
4. _____ Remove any files in /var/spool/cron/atjobs except for root

Ensure that root is the only login that has access to run crontab and at commands

1. _____ /usr/bin/echo root > /var/admin/cron/cron.allow
2. _____ /usr/bin/echo root > /var/adm/cron/at.allow
3. _____ /usr/bin/chmod 400 /var/adm/cron/cron.allow

4. _____ /usr/bin/chmod 400 /var/adm/cron/at.allow
5. _____ /usr/bin/rm /var/adm/cron/cron.deny
6. _____ /usr/bin/rm /var/adm/cron/at.deny

Restrict ftp access. At a minimum all logins with uid < 100 should not be able to ftp. Also add any other logins that do not need to ftp to /etc/ftpd/ftpusers.

1. _____ /usr/bin/touch /etc/ftpd/ftpusers
2. _____ /usr/bin/chown root:root /etc/ftpd/ftpusers
3. _____ /usr/binchmod 600 /etc/ftpd/ftpusers
4. _____ Add administrative logins to /etc/ftpd/ftpusers

```
for names in root, daemon, bin, sys and adm
do
        echo $names >> /etc/ftpd/ftpusers
done
```

Check for /etc/hosts.equiv, ~/.netrc and ~/.rhost files. The existence of these files can allow selected users to be granted password-free access to a system. There shouldn't be any of these files on your system. But if you have a need for them, check that they are not world-writeable and that there is no + in them. A + means the system will trust all other systems. You can use the following command to search for these files. You should run this command periodically and review the output.

1. _____ /usr/bin/find / \(-name .rhosts –o –name .netrc –o -name hosts.equiv \) -exec ls -ldb {} \; -exec more {} \;

If you are still running inetd and are allowing ftp access you will want to log ftp access to /var/adm/syslog/syslog.log and change the default umask to 022.

1. _____/usr/bin/vi /etc/inetd.conf
2. _____ Add –l and –umask –22 to ftpd

```
ftp         stream tcp nowait root /usr/lbin/ftpd      ftpd -l -umask 022
```

Add umask 022 and TMOUT to /etc/profile. Umask 022 will restrict file permissions. TMOUT will limit how long a session can set idle. But remember these can be easily overwritten in ~/.profile.

1. _____ /usr/bin/vi /etc/profile
2. _____ insert umask 022
3. _____ insert TMOUT=1800 (TMOUT is in seconds)

Statutory Warnings

Add a warning message that machine is for authorized use only and that all activity is subject to monitoring. It is believed that having such a warning, could aid in the prosecution of any computer crimes involving that machine. You should however, consult with legal counsel about the wording of the message. The following is an example of one such message.

This system is the property of the Company ABC. All activities
on this system are subject to monitoring for illegal or unauthorized activity.
Anyone using this system expressly consents to such monitoring and is advised
that if monitoring reveals possible improper or criminal activity, system
personnel may provide the evidence of such monitoring to authorities.

1. ____ /usr/bin/touch /etc/issue
2. ____ /usr/bin/touch /etc/motd.
3. ____ /usr/bin/chown root:root /etc/issue
4. ____ /usr/bin/chown root:sys /etc/motd
5. ____ /usr/bin/chmod 644 /etc/issue
6. ____ /usr/bin/chmod 644 /etc/motd
7. ____ copy warning message to /etc/issue and /etc/motd
8. ____ /usr/bin/vi /etc/inetd.conf *
9. ____ add –b /etc/issue to the end of the telnetd
   telnet stream tcp nowait root /usr/lbin/telnetd telnetd -b /etc/issue

* This is assuming you're running inetd. If not, disregard this step.

Sendmail

Sendmail is very often a security risk. Therefore it is very important that you be running the newest version or at least a fully patched version. Also since most machines only need to send out mail to a relay host, many of sendmail functionalities can be disabled. You can download the latest version of sendmail for http://www.sendmail.org.

1. ____ replace the existing /etc/mail/sendmail.cf [14] with the following
   # Minimal client sendmail.cf
   ### Define macros
   # define the mail hub – Put hostname for local site here.
   DRmailhost

```
# define version
V8
# my name for error messages
DnMAILER-DAEMON
# UNIX initial From header format
DlFrom $g  $d
# delimiter (operator) characters (old $o macro)
Do.:%@!^/[]+
#From of the sender's address
Dq<$g>
# queue directory
OQ/var/spool/mqueue
### Mailer Delivery Agents
#Mailer to forward mail to the hub machine
Mhub,          P=[IPC], S=0, R=0, F=mDFMuCX, A=IPC $h
#Sendmail requires these, but they are not used
Mlocal,        P=/dev/null, F=rlsDFMmnuP, S=0, R=0,A=/dev/null
Mprog,         P=/dev/null, F=lsDFMeuP, S=0, R=0 A=dev/null
### Rule sets
S0
R@S+ $         #error $: Missing user
R$+    $       #hub $@$R $:$1        forward to hub
S3
R$*<>$*        $n       handle <> error address
R$*<$$*>$*     $2       basic RFC822 parsing
```

Since you have removed sendmail from the startup scripts you should schedule a cronjob to run sendmail every hour so any mail can be processed.

1. ____ crontab -e
2. ____ add the following lines

```
## run send mail once an hour
* 0 0 0 0 /usr/sbin/sendmail –q
```

Installation of TCP_WRAPPERS

1. ____ Download from ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz
2. ____ /usr/contrib/bin/gzip -dc tcp_wrappers_7.6.tar.gz | tar xvf –
3. ____ /usr/bin/cd tcp_wrappers_7.6
4. ____ /usr/bin/chmod 644 Makefile
5. ____ /usr/bin/vi Makefile
6. ____ uncomment the REAL_DAEMON_DIR line that refers to HP-UX
   REAL_DAEMON_DIR=/etc
7. ____ Change FACILITY=LOG_MAIL to FACILITY=LOG_AUTH
8. ____ Add –DUSE_GETDOMAIN to the BUGS macro definition if not running NIS
9. ____ Make hp-ux
10. ____ /usr/bin/mkdir –p –m 755 /usr/local/sbin
11. ____ /usr/bin/mkdir –p –m 755 /usr/local/include
12. ____ /usr/bin/mkdir –p –m 755 /usr/local/lib
13. ____ for file in safe_finger tcpd tcpdchk tcpdmatch try-from
    do
    cp $file /usr/local/sbin/$file
    chmod 555 /usr/local/sbin/$file
    chown root:daemon /usr/local/sbin/$file
    done
14. ____ /usr/bin/cp tcpd.h /usr/local/include/tcpd.h
15. ____ /usr/bin/chmod 444 /usr/local/include/tcpd.h
16. ____ /usr/bin/chown root:daemon /usr/local/include/tcpd.h
17. ____ /usr/bin/cp libwrap.a /usr/local/lib/libwrap.a
18. ____ /usr/bin/chmod 555 /usr/local/lib/libwrap.a
19. ____ /usr/bin/chown root:daemon /usr/local/lib/libwrap.a

Installation of Perl

1. ____ Download software HP-UX software porting site
   http://hpux.connect.org.uk/hppd/hpux/Languages/perl-5.6.0/
2. ____ /usr/contrib/bin/gunzip gunzip perl-5.6.0-sd-11.00.depot.gz
3. ____ /usr/sbin/swinstall -s perl-5.6.0-sd-11.00.depot *

Installation of ZLIB

1. ____ Download source from http://hpux.connect.org.uk/hppd/hpux/Misc/zlib-1.1.3/
2. ____ /usr/contrib/bin/gunzip zlib-1.1.3-sd-11.00.depot.gz
3. ____ /usr/sbin/swinstall -s /conv/tara/zlib-1.1.3-sd-11.00.depot *

Installation of OPENSSL

Installation of OPENSSL needs Perl v5 installed on server.

1. ____ Download software from http://hpux.connect.org.uk/hppd/hpux/Languages/openssl-0.9.6/
2. ____ /usr/contrib/bin/gunzip openssl-0.9.6-sd-11.00.depot.gz
3. ____ /usr/sbin/swinstall -s /conv/tara/openssl-0.9.6-sd-11.00.depot *

Installation of OPENSSH

Telnet, rlogin, ftp, and other related programs send a user's password across the Internet unencrypted. Openssh solves this problem by invoking a secure encrypted connection between two untrusted hosts over an insecure network. Openssh is used in place of rlogin and rsh.

1. ____ Download software from
   http://hpux.connect.org.uk/hppd/hpux/Networking/Admin/openssh-2.5.1p1/
2. ____ /usr/contrib/bin/gunzip openssh-2.5.1p1-sd-11.00.depot.gz
3. ____ /usr/sbin/swinstall -s /conv/tara/openssh-2.5.1p1-sd-11.00.depot *

Configuration of TCP-WRAPPERS and OPENSSH

1. ____ for file in /etc/hosts.allow /etc/hosts.deny
   do
   /bin/touch $file
   /bin/chown root:root &file
   /bin/chmod 600 $file
   done
2. ____ /usr//bin/echo 'ALL: <net1>, <net2>, … '> /etc/hosts.allow
   replace net1, net2 with the IP addresses of machines that you want to grant access to

3. ____ /usr/bin/echo 'ALL:ALL: /usr/bin/mailx –s "%s:connection attempt from %a"<ADMIN EMAIL> ' > /etc/hosts.deny
   replace <ADMIN EMAIL> with email address of administrator
4. ____ /usr/bin/cp /opt/openssh/etc/sshd_config /etc/rc.config.d/sshd_config
5. ____ Modify /etc/rc.config.d/sshd_config [14]

```
Port 22
Protocol 2,1
ListenAddress 0.0.0.0
PidFile /opt/openssh2/etc/sshd.pid
HostKey /opt/openssh2/etc/ssh_host_key
HostDSAKey /opt/openssh2/etc/ssh_host_dsa_key
ServerKeyBits 1024
LoginGraceTime 180
KeyRegenerationInterval 900
PermitRootLogin no
IgnoreRhosts yes
IgnoreUserKnownHosts yes
StrictModes yes
X11Forwarding yes
PrintMotd no
KeepAlive no
SyslogFacility AUTH
LogLevel INFO
RhostsAuthentication no
RhostsRSAAuthentication no
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords no
CheckMail nos
UseLogin no
```

6. ____ /usr/bin/chown root:root /etc/rc.config.d/sshd_config
7. ____ /usr/bin/chmod 600 /etc/rc.config.d/sshd_config
8. ____ Generate server key files
   ____ /opt/openssh2/bin/ssh-keygen –b 1024 –N '' –f /opt/openssh2/etc/ssh_host_key
   ____ /opt/openssh2/bin/ssh-keygen –d –N '' –f /opt/openssh2/etc/ssh_host_dsa_key
9. ____ create sshd startup script (See Appendix D for an example)
10. ____ move script to /sbin/init.d/sshd
11. ____/usr/bin/chown root:sys /sbin/init.d/sshd

12. ____/usr/bin/chmod 744 /sbin/init.d/sshd
13. ____ /usr/binln –s /sbin/init.d/sshd /sbin/rc2.d/S75sshd
14. ____ /sbin/init.d/sshd start
15. ____ /usr/sbin/vi /etc/inetd.conf*
16. ____ modify ftp daemon to include tcp_wrappers*
    ftp stream tcp nowait root /usr/local/sbin/tcpd /usr/lbin/ftpd ftpd -l -umask 022
17. ____ modify telnet daemon to include tcp_wrappers*
    telnet stream tcp nowait root /usr/local/sbin/tcpd /usr/lbin/telnetd telnetd -b /etc/issue

* If this system has been configured not to run inetd then you can disregard these steps.

LSOF

This utility is used to list files, sockets, etc opened by processes. It also gives a large amount of other related information that can select by process ID, username or filename.

1. ____ Download 32 bit version of the software from HP-UX Software porting site, http://hpux.connect.org.uk/hppd/hpux/Sysadmin/lsof-4.55/
2. ____ /usr/contrib/bin/gunzip lsof-4.51-sd-11.00.depot.gz
3. ____ /usr/sbin/swinstall -s lsof-4.51-sd-11.00.depot *

1. ____ The 64 bit version binaries can be found at **ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/binaries/hpux/B.11.00/64/9000_800/**
2. ____ /usr/contrib/bin/gunzip lsof_4.55.gz
3. ____ /usr/bin/mv lsof_455 to /opt/lsof/bin

Backups

Create a Golden Image – use make_tape_recovery to create a bootable system recovery tape for an LVM or whole disk system while it is up and running. When a system has a logical volume layout, the recovery tape will only include data from the root volume group, plus data from any Non-root volume group containing /usr. Data not in the root volume group must be backed up and recovered using normal backup utilities. This golden image can be used to restore a non-bootable system with little or not user intervention, restore a system in the event of a hardware failure, clone software from one system to another.

Make_recovery is part of the Ignite-UX product. It can be downloaded from www.software.hp.com/products/IUX/download.html. More detailed installation instructions can be found at www.software.hp.com/products/IUX/install_instructions.html.

Installing Ignite-UX

1. ____ Downloaded software from www.software.hp.com/products/IUX/download.html
2. ____ Copy ignite11_11.00.tar to /tmp
3. ____ /usr/bin/bdf – Make sure you have at least 50 mb of free space in /opt
4. ____ /usr/sbin/swinstall -s /conv/tara/ignite11_11_00.tar *

Create a golden image

5. ____/opt/ignite/bin/make_tape_recovery -AvC -d /dev/rmt/0m

Physical Security

It is extremely important that a unix server be placed in a secure environment. It is a fact that anyone who has physical access to the machine can fairly easily gain root access.

1. ____ The server should be installed in a locked environmentally controlled data center with restricted access to the server.
2. ____ If possible the data center should have cameras installed to monitor all activity.
3. ____ The keyboard should be situated away from any cameras, windows or prying eyes.
4. ____ The system should be attached to a UPS with monitoring software that will shutdown the server when power to the UPS has been interrupted.
5. ____ Backup tapes should be kept in a secure environment.

APPENDIX A – HP-UX 11.0 Supported Systems

Model	32-bit	64-bit
Workstations:		
Series 700: 712, 715/64/80/100/100XC, 725/100	X	
B132L, B132L+, B160L, B180L	X	
B1000, B2000		X
C100, C110, C160L	X	
C160, C180, C180XP, C200, C240, C360	X	X
C3000, C3600		X
J200, J210, J210XC	X	
J280, J282, J2240	X	X
J5000, J5600, J6000, J7000		X
Servers:		
A180, A180C	X	
A400, A5xx		X
Dx10, Dx20, Dx30, Dx50, Dx60	X	
Dx70, Dx80, Dx90	X	X
E, F, G, H, I (all)	X	
Kx00, Kx10, Kx20	X	
Kx50, Kx60, Kx70, Kx80	X	X
L1000, L2000, L3000		X
N4000/360, N4000/440, N4000/550		X
R380, R390	X	X
T500, T520	X	
T6xx	X	X
V22xx, V2500, V2600		X
Enterprise Parallel Servers: EPS22, EPS23, EPS40	X	X

APPENDIX B – Network Parameters [5]

ip_send_redirects – causes the machine not to emit any ICMP redirect Packets. Under normal operation this probably won't have significant security implications.

ip_ire_flush_interval and **arp_cleanup_interval –** control how long information will live in the system's ARP cache. The ARP cache maintains a mapping between Ethernet addresses and IP address. The default values are 10 minutes (?????). Lowering these values can help prevent some ARP spoofing attacks but at the cost of more ARP traffic on your local LAN and possibly reduced performance. Think carefully before you change these variables.

ip_forward_directed_broadcast – caused the machine to not transmit packets which are destined for a broadcast network address. If the machine is being used as a gateway between several networks this can help you from being used as an intermediary network in a "smurf" type network attach. The machine will still respond to broadcast packets directed at any LAN it may be connected to.

ip_forward_src_routed – prevents the machine from forwading any packets that have the source routing option turned on.

ip_forwarding – turning off ip_forwarding prevents the machine from accepting and forwarding on packets that are not destined for one of it's local interface addresses. Such a feature can be used by attackers to bypass other network security measures.

tcp_ip_abort_cinterval – this is how long the kernel will wait for a TCP connection to be completed (in milliseconds). Tuning this value down can also help your system resist SYN flooding attacks.

You can use the following commands to view various information concerning Network parameter.

ndd –h sup – display all the parameters that are supported by HP.
ndd –h unsup – display all the parameter that are not supported by HP. Becareful modifying these!
ndd –c - set tunable parameters

APPENDIX C – Example secure /etc/fstab

```
/dev/vg00/lvol3 /      hfs   defaults   0 1
/dev/vg00/lvol1 /stand hfs   nosuid     0 1
/dev/vg00/lvol4 /tmp   hfs   defaults   0 2
/dev/vg00/lvol5 /home  hfs   nosuid     0 2
/dev/vg00/lvol6 /opt   hfs   ro         0 2
/dev/vg00/lvol7 /usr   hfs   ro         0 2
/dev/vg00/lvol8 /var   hfs   nosuid     0 2
```

APPENDIX D – Sample SSHD Startup Script

```
#!/sbin/sh
#
# start up secure shell deaemon - sshd
#
PATH=/usr/sbin:/usr/bin:/sbin
export PATH
rval=0
case $1 in
'start_msg')
        echo "Starting the sshd"
        ;;
'stop_msg')
        echo "Stopping the sshd"
        ;;
'start')
        if [ -f /etc/rc.config.d/sshd_config ]
        then
                /opt/openssh2/sbin/sshd -f /etc/rc.config.d/sshd_config
        else
                echo "ERROR: /etc/rc.config.d defaults file MISSING"
        fi
        ;;
'stop')
        kill `cat /opt/openssh2/etc/sshd.pid`
        ;;
*)
        echo "usage: $0 {start|stop|start_msg|stop_msg}"
        rval=1
        ;;
esac
exit $rval
```

References:

1. Poniatowski, Marty. HP-UX 10.x SYSTEM ADMINISTRATION "HOW TO" BOOK. Upper Saddle: Prentice Hall PTR, 1996. 1-383.

2. Frisch, Aeleen. Essential System Administration Second Edition. Sebastopol: O'Reilly & Associates, Inc, December 1995. 1-758.

3. Hassell, Bill and Totsch, David. "HP-UX SysAdmin Training Camp". HPWorld '99 August 1999.

4. Farrow, Rik. "HP-UX and Internet Security". HPWORLD '98 August 1998.

5. Brotzman, Lee and Pomeranz. Hal. "UNIX Practicum". SANS Institute February 2001.

6. Pomeranz, Hal. "Common Issues and Vulnerabilities in UNIX Security". SANS Institute February 2001

7. Bishop, Matt. "UNIX Security Tools and Their Uses". SANS Institute". SANS Institute Februray 2001.

8. Netsysco Infrastructure Services. "Networking for System Administrators"

9. HP-UX 11.0 Installation and Update Guide March 2001, HP Part Number: 5971-0642. http://www.docs.hp.com/hpux/onlinedocs/5971-0642/5971-0642.html

10. Installing and Updating HP-UX 11.0 Additional Core Enhancements. November 1999, HP Part Number: B3782-90785 http://www.docs.hp.com/hpux/onlinedocs/B3782-90785/B3782-90785.html

11. HP-UX System Administration Tasks , First Edition. January 1995, HP Part Number: B2355-90672

12. Campione, Jeff. "Solaris 8 Installation Checklist", http://www.sans.org/y2k/practical/Jeff_Campione_GUCX.htm

13. Rhoads, Jason. "HP-UX Security Guide", http://www.sabernet.net/papers/hp-ux10.html

14. The SANS Institute. "Solaris Security Step by Step Version 2"

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**