Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

SANS
Global Information Assurance Certification (GIAC)

GCUX
GIAC Certified UNIX Security Administrator
Practical Assignment, Version 1.9 Option 1

Installing and Securing
Kerberos Key Distribution Center Server on HP-UX 11.11

Ann Adams
June 2003

TABLE of CONTENTS

1   Introduction

Our current environment utilizes UNIX systems utilizing Kerberos V5 authentication to a Windows 2000 Active Directory environment.   This allowed a relatively painless methodology of increasing security for authentication by removing the passwords from NIS maps, while adding little cost to the infrastructure.

Changes in company infrastructure promote further analysis as to the proper hardware platform for the Kerberos KDC (Key Distribution Center).   This analysis must include a security component along with an interoperability component.

The platform we are analyzing is the HP-UX 11i. HP recently released a version of a MIT Kerberos V5 KDC.   This document will define a step-by-step procedure for installing, configuring, and securing a HP Kerberos KDC.

1.1   Architecture

1.1.1   Hardware
For our hardware we are utilizing a HP 3650 workstation with a single RISC process, 2.1 G of RAM and two 18 GB internal hard disk.   Systems backups are an incremental dump to a 10 M tape drive

1.1.2   Software
The system software is HP-UX 11.11, September 2002 release.
The Kerberos KDC software is based on MIT's Systems 5 software.
The SSH and Basilica are both Hp's version.

1.1.3   Network Environment
The assumption is that the Kerberos KDC is on a company wide Wan. The network has a variety of routers and switches with access from the outside only through a firewall.

During the install, the server is connected to an internal network. The Kerberos KDC is not functional without network access.

1.2   Controls Review

1.2.1   Physical Security

The master KDC for each domain will be in a Class A computer room.   The Master KDCs for each realm are the only systems that are allowed administration updates.

The class A computer rooms have very limited access. Only mainframe and server administrators with a valid hardware maintenance need are allowed access to the class A compute room. Access is picture ID card controlled with a scanner at the gate.

Fire safety for the systems is provided by Halogen Fire Suppression system. The fire detection alarms detect the presence of fire, sound an alarm, and trigger the halogen system. The halogen system damps down the fire by the replacement of oxygen with halogen.

Class A computer rooms are very tightly monitored for proper cooling. All equipment is on a raised floor with power and wiring running underneath the systems. The class A computer room can stand extremely high wind velocities.

This class A computer room has a disaster recovery Class A computer room in another building. If a backup server is provided it is placed in the other Class A computer room. If not, the tape backups are placed in the other class A room.

1.2.2   Risk Analysis

The Kerberos KDC is a very high-risk system. This system contains all the names and passwords for your Kerberos realm. Failover is to a Slave KDC, so the users will still be able to login if the Master KDC.   But if hacked all user ids are now available.

For this reason this is a single application system. It is only a Kerberos KDC. It handles key distribution and authentication and that is all. The only logins that need to be allowed onto the system are the system administrators and the Kerberos administrators.

2 Step-by-Step

2.1 Operating System

The HP operating system is installed from either HP distributed media or from a HP-UX Ignite Server. In our environment the servers are installed from CDROM to meet the unique needs of the server environments.   So, the HP-UX 11i base operating system disk 1 of 2 is placed in the CDROM drive.

The HP-UX 11i installation disk group the filesets into "operating environment" bundles The bundle for the base Operating system is "HP-UX 11i MTOE", a 64 bit minimal technical operating environment.

2.1.1. Installation - Step-by-Step

When booting the system "hit any key", at the prompt run ">sea" to find your cdrom, then boot the path or path number. On these systems boot P0, which is the SCSI 2.0 device. When it asks to "Interact with the IPL" answer N. The system then proceeds to the first install screen questions the language, enter 26 for English.

The next screen is a "Welcome to the HP-UX Installation".
> Select the first option [Install HP-UX] and return.

Next is "User Interface and Media Options"
> Select "Media with Network Enabled"
> Select "Guided"
> *It is quicker to configure the system with Network enabled then at the end of the Media enabled installation without networking. The Guided is adequate since our partitioning is not unique.*

Network Configuration
> The network configuration options required the installer to be prepared with the system hostname, IP, gateway, and subnet.

Install HP-UX Wizard: Select an Overall System Configuration
> Select HP-UX B.11.11

Install HP-UX Wizard: Select a System Environment:
> Select HP-UX 11i MTOE – 64 bit
> *The Minimal Technical Operating Environment includes the network item. To install the Base Operating system, additional software would be needed; neither CDE nor Xwindows is included in the Base Operating system install. If the system supports 64 bit, that is the options given. If it is an older system than a 32 bit option for each is also given.*

Install HP-UX Wizard: Select a Root disk
     Select the highlighted disk. In this Case it is a HP18g.2 10/0/15/1.5.0
Install HP-UX Wizard; specify the amount of Root Swap
     Hit return, so root swap is now 4096 while physical memory is 2048.
Install HP-UX Wizard: Select a File System Type
     Select the default Logical Volume Manager (Manager) with VxFs
Install HP-UX Wizard: Specify Root disk
     Number available 2, number of disk 1
     Use Striping <N>
Install HP-UX Wizard: Select Language
     Yes, select English C
     If you utilized set_NULL_Locale the Language variable will return NULL
     instead of English.
Install HP-UX Wizard: Select Additional Software
     Tab, Tab, return to accept
     Looking at All software installs. They cannot be deselected due to
     dependencies. They are:
          Bundle 11i required patch Bundle Feb 2002
          Base VxVM Required due to volume manager selection
          Feature 11-11 Feature enabled for HP-UX 11i Sept 2002
          FDDI-00
          Fiber-Channel-00
          GigEth-00
          GigEth-01
          HP-UX Base Aux
          HW Enable 11i–Hardware Enable patch for HP-UX11i for Sept 02
          Online Diagnostic: HP-UX 11.11. Support
          Raid-00 PCI Raid
     The only exception is the General Patches, they can be deselected.
Install HP-UX Wizard: Preinstall Disk Info
     Tab, Tab, next
Install HP-UX Wizard: System Summary
     Tab, Tab, Return

     When the system responds to install cdrom 2, swap Install cdrom 1 for cdrom 2.

The first disk on the server is now the root disk. Appendix A shows step-by-step
directions for mirroring disk 1 to disk 2 with 2-18 gig disks.   I will then mirror disk1 to
disk2. This allows a bootable disk with my most recent updates for the KDC.

Note, it we did a minimal install we would not have our Xwindows and CDE system. We
are leaving those on the system for ease of use for the Kerberos administrators. The
remote Kerberos administration tool utilizes a GUI interface.

2.1.2 Partitions

There are many methodologies for determining the disk partitioning. Root requires enough space for the base operating system plus updates. Var is frequently setup as a stand alond partition. This way if it grows past its bounds due to excessive logging or poor log maintenance it will not take down your system by filling root. If you want to save your core files, you need root to be twice the size of memory.

 The standard partitioning for the servers is the same across all applications. Disk1 is a dedicated root partition. This allows for a consistent installation on any system with a root disk greater than 4 Gig.

The Standard partitions with the Guided installation are listed below. If a different partition table is preferred, an advanced installation is recommended so the partitions may be modified at installation. Some of the 18Gig disk is not portioned, but it can be as needed at a later date.

```
bdf
Filesystem          kbytes       used       avail    %used     Mounted on
/dev/vg00/lvol3     204800       75776      128040   37%       /
/dev/vg00/lvol1     295024       27680      237840   10%       /stand
/dev/vg00/lvol8     4706304      145368     4525856   3%       /var
/dev/vg00/lvol7     1736704      1137896    594136   66%       /usr
/dev/vg00/lvol4     204800       2416       200872    1%       /tmp
/dev/vg00/lvol6     839680       538462     298904   64%       /opt
/dev/vg00/lvol5     20480        2280       18072    11%       /home
```

2.1.3 Removal of any unnecessary Software

NFS has had many security issues. All of the NFS filesets can be removed except for NFS-CORE NFS-KRN and NFS-SHLIBS.
        Run swremove interactively: swremove –i NFS

```
# swlist -l product | grep NFS

 NFS              B.11.11      ONC/NFS; Network-File System, Information Services ,Utilities

Nothing to remove, running swremove –l NFS results in dependency error s from the NFS-CORE
.
```

Also remove /etc/auto_home, /etc/auto_master,autopush, /etc/dfs/dfstab. Check for any other /etc/auto* files, frequently there are sit specific files called from the master. NFS will not be run on this server.

```
# more /etc/auto_parms.log
Jun 21 07:18:26: DHCP is disabled for: lan0
# ls -l /etc/auto
/etc/auto not found
# ls -l /etc/aut*
-rw-r--r--  1 root      root          49 Jun 21 09:08 /etc/auto_master
-rw-r--r--  1 root      root          44 Jun 21 09:18 /etc/auto_parms.log
# rm /etc/auto_master
# cat /etc/dfs/dfstab

cat: Cannot open /etc/dfs/dfstab: No such file or directory

#
```
There are a number of other **startup scripts** that may be removed from the system.
They are unnecessary at best and a potential security risk.
In startup directory /sbin/rc2.d remove the following Startups:

S006hpfc	K100dtlogin.rc
S30ptydaemon	K200tpc.rc
S370named	K900nfs.serve
S400 nfs.core	
S406nisplus.server	
S408nis plus.client	
S410 nis.server	
S420nis.client	
S430nfs.client	
S440comsec	
S490mrouted	
S510gated	
S522ppp	
S530rwhod	
S540sendmail	
S560Snmpmaster	
S565SnmpHPunixh	
S565SnmpMib2	
S565SnmpTrpDst	
S570dce	
S590Rpcd	
S600iforls	
S620xfs	
S630vt	
S710hparray	
S7201p	
S740supportinfo	
S770audio	
S780slsd	
S870swagentd	
S900hpfcms	

```
# ls S4*
S400nfs.core        S410nis.server      S440comsec
S406nisplus.server  S420nis.client      S462maclan
S408nisplus.client  S430nfs.client      S490mrouted
# pwd
/sbin/rc2.d
# mv S462maclan temp
# rm S4*
# mv temp S462mclan
# ls S5*
S500inetd      S525rarpd      S550ddfa        S565SnmpMib2    S590Rpcd
S510gated      S530rwhod      S560SnmpMaster  S565SnmpTrpDst
S520rdpd       S535inetsvcs   S565OspfMib     S570dce
S522ppp        S540sendmail   S565SnmpHpunix  S576SnmpFddi4
# rm S510*
# rm S522*
# rm S530*
# rm S540*
# rm S560*
# rm S565*
# rm S570
rm: S570 non-existent
# rm S590
…. Continue removal till through above list.
```

Remove the software-programming environment, start swremove interactively and un-
select **ProgSupport.C-INC**. This fileset is necessary for kernel rebuilds, with its
removal a kernel recreation is not possible.

> Swremove –I CPS Perl5 ProgSupport SourceControl Jul-lib \
> KernDevKit Networking.NET-PRG InternetSrvcs.INETSVCS-INC \
> Networking.LAN-PRG
>
> example: swremove –I ProgSupport.C-INC
> Watch for depencies, to remove ProgSupport.C, it was necessary to
> remove GraphisSbaseDK If you can't resolve dependencies, may want to
> unselect enforce dependencies under options for certain packages.

Many of the **serial data communication** products may be removed
> Swremove UUCP SystemComm Terminal Mngr NonHP-Terminfo KeyShell \
> Curses-Color

Remove the **Mail utility** since this is not a system for reading or sending mail and it is frequently a security hole: Swremove Mail Utilities

```
        swlist -l product | grep Mail
          MailUtilities       B.11.11       User mail agents and related tools
        # swremove MailUtilities

        ======= 06/24/03 07:39:24 EDT  BEGIN swremove SESSION
              (non-interactive) (jobid=sic76048.fsic.ford.com-0012)

           * Session started for user "root@sic76048.fsic.ford.com".

           * Beginning Selection
           * Target connection succeeded for "sic76048.fsic.ford.com:/".
           * Software selections:
               MailUtilities.MAIL-ENG-A-MAN,l=/,r=B.11.11,a=HP-
        UX_B.11.11_32/64,v=HP,fr=B.11.11,fa=HP-UX_B.11.11_32/64
        .
```

2.2   File Permissions

Remove unneeded **Set-ID** Programs.
Many programs have Set-ID programs there are not needed. Most servers do not have end users running applications, if so they are not needed.

To obtain a list of all files with the set-uid or set-gid bit execute
find / -perm -4000 -o -perm -2000 –print

```
        /etc/wall /etc/sysdef /etc/lanscan /usr/bin/iostat /usr/bin/netstat /usr/bin/vmstat
        /usr/bin/ipcs /usr/bin/top /usr/bin/uptime /usr/bin/w /usr/bin/strdb /usr/bin/X11/xfs
        /usr/bin/elm /usr/bin/stmkfont /usr/sbin/wall /usr/sbin/lanscan /usr/sbin/sysdef
        /usr/lbin/fs/vxfs/diskusg /usr/lbin/fs/hfs/diskusg /usr/lbin/rmmail
        /usr/contrib/bin/X11/xload/usr/dt/bin/dtmail  /usr/dt/bin/dtmailpr etc
        # ls -l /usr/bin/w
        -r-xr-sr-x  2 bin       sys      16384 Nov 14 2000 /usr/bin/w
        #So remove the set-uid and set-gid and add the bit back to the files that require it.

        #  find / -perm -4000 -type f -exec chmod u-s {} \;
        # find /  -perm -2000 -type f -exec chmod g-s {} \;[1]
        ls # -l /usr/bin/w
        -r-xr-xr-x  2 bin       sys      16384 Nov 14 2000 /usr/bin/w
        # ls -l /usr/bin/su
        -r-xr-xr-x  1 root      bin      24576 Nov 14 2000 /usr/bin/su

        # chmod u+s /usr/bin/su
        # chmod u+s /usr/bin/passwd
        # ls -l /usr/bin/su
        -r-sr-xr-x  1 root      bin      24576 Nov 14  2000
```

---

[1] Pipkin, page 270

2.3 Account Security

2.3.1 Remove unused system accounts.
This can be a potential login for a hacker. Default users could include uucp,lp, nuuccp, hpdb,www, and daemon. Default groups can include lp, nuucp, and daemon. Utilize SAM to cleanly remove the accounts or edit /etc/passwd and run pwconv if it is a trusted host or if the shadow password package is installed.

2.3.2 Remove unused user accounts.
Utilize SAM to remove the unused user accounts. The only users that will login to this server is a system administrator or a Kerberos administrator. No end user will login to this server.

2.3.3 Disable pseudo-accounts
They should be configured so no user can gain access with the account, so disable them. The NP in the password field guarantees no password will HASH fro login. They should also have an invalid shell program and invalid home directory. This will disable remote connections.

Only HP the needed pseudo-accounts are: bin, sys, and adm
Bin:*2:2: NP:/bin/false:/dev/null
Sys:*:2:2:NP:/bin/false:/dev/null
Adm:*:2:2:NP:/bin/false:/dev/null[2]

2.3.4 Root's Home
Move root's home from root and build a new home directory, this will prevent root accidentally placing files in the root directory.
Mkdir /root
Chown root:root /root
Chmod 700 /root
Mv /.profile /root
Pwconv(Only needed if in trusted mode)

```
# cat /etc/passwd
root:qqlSWA3/aNuRY:0:3::/root:/sbin/sh
bin:*:2:2:NO LOGIN:/usr/bin:/sbin/sh
sys:*:3:3:NO LOGIN:/:
adm:*:4:4:NO LOGIN:/var/adm:/sbin/sh
nuucp:*:11:11::/var/spool/uucppublic:/usr/lbin/uucp/uucico
nobody:*:-2:-2::/:
webadmin:*:40:1::/usr/obam/server/nologindir:/usr/bin/false
user1:NP:101:20:,,,:/home/user1:/usr/bin/sh
user2:7NP:,,,:/home/user2:/usr/bin/sh
user3:8qjllROWJ5BCU:103:20:,,,:/home/user3:/usr/bin/sh
+:*:-2:-2::/:
#
```

---

[2] Pipkin, Page 274

2.4   System Access

2.4.1 Console Root Login
 Restrict root login to the console. So the entry in /etc/securetty place console, and set the permissions
>   Echo console > /etc/securetty
>   chown bin:bin /etc/securetty
>   Chmod 400 /etc/securetty

2.4.2 Hosts.equiv and .rhost
Remove hosts.equiv and rhosts. No system is trusted enough to be allowd access without a password. In our Kerberos environment if the user already has a credential from a previous login, no password is required after the initial authentication.

2.5   Internet Services

As a Kerberos server only the administrators will be logging onto the system. They will utilize the local password file for their uid, gid, etc, but NP will be in place of their password. They will utilize their Kerberos password stored in the KDC database. They must do a kerberized login as themselves from a remote location or they may login as root from the console.

2.5.1 Cleanup Inetd.conf
        Remove all unnecessary entries. For the server only we will just retain the kerberized SSH. The other kerberized services are secure, but for the KDC we want to minimize access point. Utilizing kerberized SSH provides both authentication security through Kerberos and encryption.

 Run either "kill –HUP #inetd" on the inetd service or reboot the system. This is necessary for inetd.conf to be reread.

2.5.2 Configure Pam.conf
        Remove all unnecessary entries. In our scenario, end user authentication will only be through the Kerberos module. The user will still need to be in /etc/passwd for authorization, the user's uid/gid is in /etc/passwd, but no authentications will be done through the password file. All user passwords will be NP.

The exception is root. Root must retain a local password on the system for system administration. The other negative feature of root in a Kerberos KDC is root is then the effectively the same login across all systems within the Kerberos Realm.

With sufficient on the Pam-Kerberos module , the Kerberos login will always be tried first. If it fails it will fall through to the standard Pam-unix module. If it succeeds it will be sufficient with no other authentication required.

The default pam.conf authentication sections of pam.conf is below:
vi /etc/pam.conf
PAM configuration
Authentication management
#
login   auth required   /usr/lib/security/libpam_unix.1
su   auth required   /usr/lib/security/libpam_unix.1
dtlogin auth required   /usr/lib/security/libpam_unix.1
dtaction auth required   /usr/lib/security/libpam_unix.1
ftp   auth required   /usr/lib/security/libpam_unix.1
OTHER   auth required   /usr/lib/security/libpam_unix.1
#

Note that the standard pam.conf utilized the standard pam_unix module, which utilizes passwd, NIS, or NIS+ for UNIX authentication. OTHER is also an available access utilizing standard UNIX authentication.

With our new pam.conf authentication module below. Rlogin and ftp have been removed since we have a kerberized SSH on the system. Login and dtlogin are still available in pam.conf for console logins.

The libpam_krb5 module is listed as sufficient so access to the system will attempt a kerberized authentication, if this fails it will fall through to the required UNIX login.   The backup UNIX login is for system accounts that cannot be kerberized. Some local system accounts cannot be placed in the Kerberos KDC.
...

Pam.conf auth section

login   auth sufficient /usr/lib/security/libpam_krb5.1 forwardable renewable=7d krb_prompt
login   auth required   /usr/lib/security/libpam_unix.1 use_first_pass
#
dtlogin   auth sufficient /usr/lib/security/libpam_krb5.1 forwardable renewable=7d krb_prompt
dtlogin   auth required   /usr/lib/security/libpam_unix.1 use_first_pass
#
dtsession   auth sufficient /usr/lib/security/libpam_krb5.1 forwardable renewable=7d krb_prompt
dtsession   auth required   /usr/lib/security/libpam_unix.1 use_first_pass
#
su   auth sufficient /usr/lib/security/libpam_krb5.1 forwardable renewable=7d krb_prompt
su   auth required   /usr/lib/security/libpam_unix.1 use_first_pass
#
ssh   auth sufficient /usr/lib/security/libpam_krb5.1 forwardable renewable=7d krb_prompt
ssh   auth required   /usr/lib/security/libpam_unix.1 use_first_pass
#

Pam_updb.conf

A rather unique Hp configuration file. This file says to ignore the particular user for that module. This works great when you have a user, such as root, that cannot be in the Kerberos KDC and must stay local on the system. The pam_updb module allows root to ignore the Kerberos authentication module and drop to the next authentication module, the pam_unix module, which will rely on /etc/passwd.

2.6 Miscellaneous Daemons

2.6.1 Disable SNMP daemons
Due to the potential of a hacker accessing system information through SNMP, SNMP(Simple Network Management Protocol) is a potential hole.
On HP-UX many of the filesets are dependent on SNMP, therefore you can only disable the service, not remove it.
In /etc/rc.config.d/SnmpMaster
> SNMP_HPUNIX_START=0
> IN /etc/rc.clonfi.d/SnmpMaster
> SNMP_MASTER_START=0
> In /etc/rc.config.d/SnmpMib2
> SNMP_MIB2_START=0
> In /etc/rc.config.d/SnmpTrpDst
> SNMP_TRAPDEST_START=0[3]

2.6.2 Disable swagentd Daemon
The swagentd script does need to run as part of the boot-up start sequence. When it is run from S120swconfig it will complete any cleanup work from an install which required a reboot, such as remove the files listed in /var/adm/sw/cleanupfile.

 But the startup file, /etc/rc2.d/S870 swagentd should be removed to keep the daemon from running. [4]

2.6.3 Disable Password and group caching daemon.
HP_UX had introduced a password and group-caching daemon, pwgrd, to improve the performance of accessing user and group IDS. It utilized a UNIX domain socket for client request, the daemons should be disabled. Edit the following line in the file /etc/rc.config.d/pwgr: PWGR=0
> The sockets used by the password and group-caching daemon should be removed
> Rm /var/spool/pwgr/*
> Rm /var/spool/sockets/pwgr/*[5]

---

[3] Pipkin, Page 273
[4] Pipkin, Page 274

2.6.4 Disable pty Daemon
The ptydaemon is a carry-over from the proprietary networking days at HP. It supports vt and dscopy commands. Vt is for a MAC level terminal connection and dscopy is no longer supported. So change PTYDAEMON_START=0 [6]

2.6.5 Disable RPC services
RPC services are the basis for NIS and NFS. On our Kerberos KDC server there is no reason to run either NIS or NFS. ON HP-UX 11i rpcbind provide the RPC services. Rpcbind is started from the nfs.core script. Setting their permission to 0 will assure no accidental startups.

> Chmod - /sbin/rc1.d/K600nfs.core
> Chmod 0 /sbin/rc2.d/S400nfs.core
> Chmod 0 /usr/sbin/rpcbind

2.7 Log files

The majority of the log files are in the /var/adm directory. Log files for a specific product are stored in /var/adm/$product.

Any errors from the installs will be in /var/adm/sw/swagent.log. Verify that all installations went smoothly.

The btmp logfile contains bad login attempts. The login process, rather than syslogd writes to the btmp file. Only root can read and write it. The bmp file contains two entries for every bad login attempt(327,wong)

The /var/adm/sulog log file records all successful and unsuccessful use of su

The syslog daemon,syslogd accepts messages from programs and determines where to log the informations based on syslog.conf.

```
cat /etc/syslog.conf
# @(#)B.11.11_LR
#
# syslogd configuration file.
#
# See syslogd(1M) for information about the format of this file.
#
mail.debug          /var/adm/syslog/mail.log
*.info;mail.none       /var/adm/syslog/syslog.log
*.alert           /dev/console
*.alert           root
*.emerg            *
#
```

---

[5] Pipkin, Page 276
[6] Pipkin, Page 274

The system logger, syslog, records kernel, system, and application log messages. It also will accept messages from other systems on the network. This feature should be disable so that other systems cannot utilize allocated resources. Change syslogd startups to include the –D option to avoid this, /usr/bin/syslogd -DN

Non-privilege users are not allowed to change the ownership of files.   HP-UX restricts the access to changing ownership through the privileged group mechanism. By default the "CHOWN" privilege is a global privilege and applies to all groups. The file /etc/privgroup should be created with permissions set at 400 and containing –n. This will disable any privileged group[7].

More verbage can be associated with the pam.conf logging. Simply add In /etc/pam_debug, put "1" through "4" as the only character in the file. "1" for basic logging, "4" for extensive verbage. Add "debug.* /var/adm/messages" to /etc/syslog.conf, and restart syslogd. Once you've done that, all PAM logins will be generating traces into syslog

2.8   SSH

HP-SSH is Open SSH Secure Shell. HP made it available in their Sept 2002 release. This is a compiled, supported version with no other packages required. It provides a ssh_keyen for manually generating keys.   It also can utilize KerberosV5 authentication, utilizing the KDC for the user's password.

---
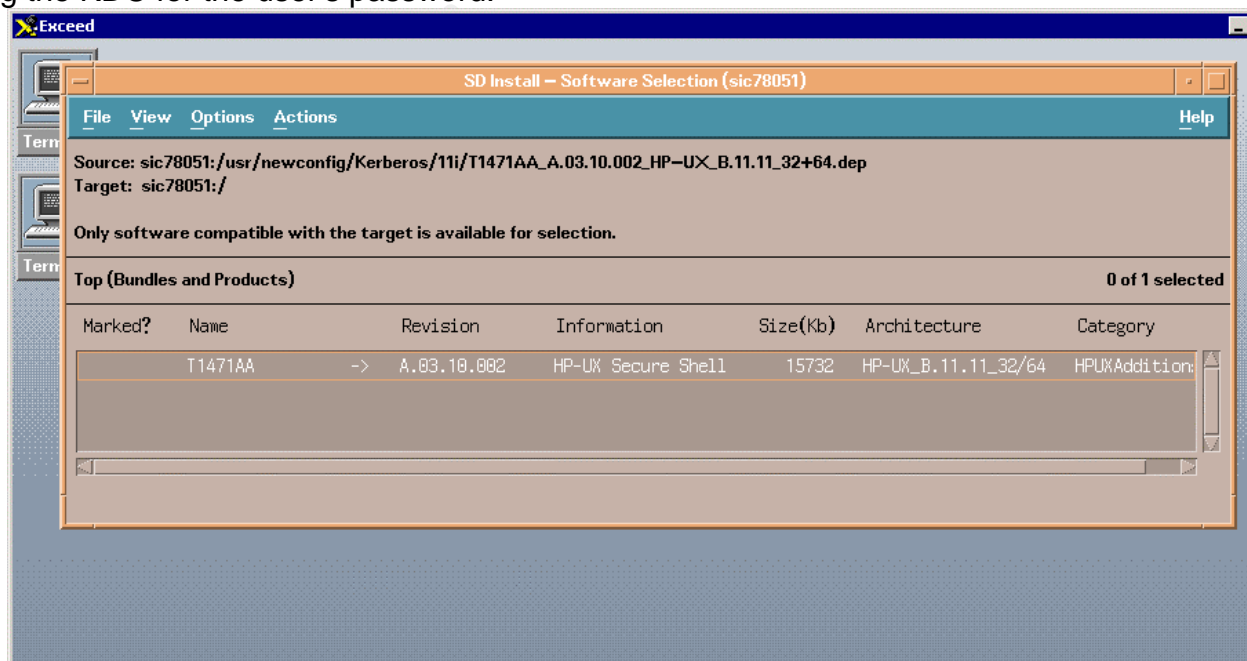
[7] Pipkin, Page 276:

hostname

sic78051

ssh sic78051

The authenticity of host 'host (11.11.78.51)' can't be established.

RSA key fingerprint is 0e:e9:04:ce:a6:33:55:ae:46:66:4d:24:af:1a:90:c8.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added 'sic78051' (RSA) to the list of known hosts.

root@sic78051's password:

Last login: Sun Jun 22 17:58:04 2003 from sic78051

(c)Copyright 1983-2000 Hewlett-Packard Co., All Rights Reserved.

Value of TERM has been set to "dtterm".
WARNING: YOU ARE SUPERUSER !
ssh sic76048

2.9   Security Patches

Check the vendor patch list. Only apply the patches necessary for your hardware or software. The Support Plus CD contains the General Release patches. This is the accumulation of the patches that have been released since the last release. Mount the support plus CD and use swinstall.

One advantage of patches versus the code as part of the images is the ability to remove the patches.   Rollback copies of the patch files are saved in /var/adm/sw/save. Once you are satisfied with the patch you can commit the patches or patches with swmodify – x patch_commit=true '*.*'. Once they are committed they are no longer removable with swremove..

If you have a good Perl installation and want a complete security patch check run the patch check script available for HP-UX. "security_patch_check: must have access to a catalog of patches. To download the patch catalog from HP security_patch_check –r (Once security_patch_check has access to a security patch catalog, it will create a list of the patches, which are applicable to your file system and not install.

Appendix B has a trace from running security_patch_check. Some of the patches are not on the system, due to the fact that we already removed the service. With the application of any kernel patch, communications service, DCE or Kerberos file your Kerberos test matrix should be rerun

The latest security patches are available from ftp://ftp.itrc.hp.com/hp-ux patches.
To track known the know vulnerabilities and solutions use the HP Security Archive on the IT Resource Center Web site.

2.10 Convert to a trusted system

 This implements "C2" level security. This includes password shadowing and system auditing. Run:

        /usr/lbin/tsconvert
        password root

When a trusted system is implemented, the passwords are removed from /etc/passwd and placed in a password shadow file. This file is readable only by root.

Other pluses of the trusted systems are:
        Auditing
        Terminal restrictions
        Serial port restrictions
        Access time restrictions
        Password generation
        Password aging

One of the negatives of the trusted systems is the login restrictions. If you fail to login as root 3 x, due to a bad password, the administrator is now locked out of the system as toot. Recovery must be done by booting to single user mode.

If the system cannot be converted to a trusted system, the administrator should at minimal install HP's shadow password package, this will pull the passwd from /etc/passwd.. To install this package swinstall –s /var/tmp/ShadowPassword_B01.00.00_HP-UX_B.11.11_21+64.depot
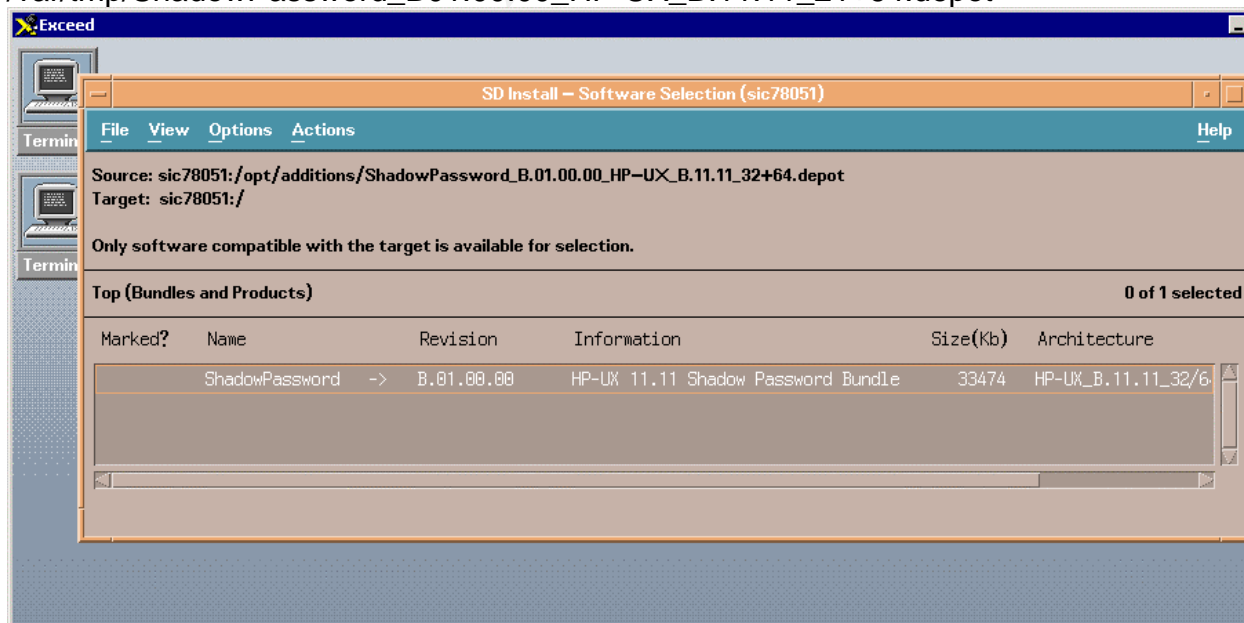
2.11 System Hardening Tool - Bastille

HP-UX Bastille is a security hardening/lockdown tool. It provides customized lockdown on ad system by systems.   Hp is participating with the open source community by providing HP-UX Bastille.

HP-UX Bastille configures daemons and system setting to increase security, turns off unneeded services, creates chroot jails, configures Security PatchCheck to run automatically, configures an IPFilter-based firewall. The "revert features" returns the security configuration to the state before Bastille was run.

Bastille can be ran interactively through the user interface as seen in Appendix C. It performs the actions in can perform and produces a "to do" list of the manual steps that are needed.

This configuration can be saved to be used non-interactively on other systems.

Before installing Bastille you must have a good version of Perl. The HP package of Bastille, B6849AA version 2.01, requires Perl 5.6.1 e or higher. It is also available for download from HP's software depot, www.software.hp.com. Verify your current version with Perl –v.

When running Bastille, my configuration is "no" for "running the security patch check" . We do not allow automated scripts through the firewall. Patch check will be manually ran, after downloading the most recent catalogue file to another systems. Also, the configuration does not disable the Xwindows ability, since the system administrator may have to login through his/her portable with Exceeds.

swlist -l product | grep Sec

 Bastille   B.02.00.05   HP-UX Security Hardening Tool
SecPatchChk   B.01.01   HP-UX Security Check Tools

```
# /opt/sec_mgmt/bastille/bin/bastille
```

/opt/sec_mgmt/bastille/bin/bastille
Using Tk user interface module.
Only displaying questions relevant to the current configuration.
Could not open config: /etc/opt/sec_mgmt/bastille/config, defaults used.
Entering Critical Code Execution.
Bastille has disabled keyboard interrupts.
Bastille is now locking down your system in accordance with your
answers in the "config" file. Please be patient as some modules
may take a number of minutes, depending on the speed of your machine.
Executing File Permissions Specific Configuration
Executing Account Security Specific Configuration
Executing Inetd Specific Configuration
Executing Daemon Specific Configuration
Executing Sendmail Specific Configuration
Executing DNS Specific Configuration
Executing FTP Specific Configuration
Executing HP-UX Specific Configuration

Executing HP-UX's Security Patch Check Configuration

Please check
/var/opt/sec_mgmt/bastille/TODO.txt
for further instructions on how to secure yoursystem

2.12 Kerberos Key Distribution Center

2.12.1 Configure NTP

The Network Time Protocol(NTP) package is bundled with HP_UX. The xntpd daemon is responsible for synchronization of time. The daemon utilized the configuration file /etc/ntp.conf

NTP keeps track of any drift in the local systems clock and synchronized itself. This is necessary for Kerberos, since the packets have a maximum of 5 minutes skew allowed to avoid spoofing.

Check that xntpd is running and that /etc/ntp.conf points to a local router/switch. It then syncs up with the primary DNS server.
()Copyright 1983-1997 Hewlett-Packard Co., All Rights Reserved.

```
# ps -elf | grep ntp

 41 S    root  1000    1  0 120 20       48d5b500  95 400003fffff0000 Jun 18  ?       0:12
/usr/sbin/xntpd

# cat /etc/ntp.conf

server sic.example.com
```

2.12.2 Installation
The Kerberos server installation is a stand HP-UX 11.11 package, and can be installed with swinstall. All four Kerberos packages must be installed including the Kerberos client package.

They are:

KRB-Support	B.11.11	Kerberos Support for HP-UX and DCE
KRB5-Client	B.11.11	Kerberos V5 Client Version 1.0
KRB5-Server	B.11.11.02	Kerberos Server Daemons Version 2.0
KRB5-Srv-Admin	B.11.11.02	Kerberos V5 Server Admin Utilities Version 2.0

2.1.3 Configure with krbsetup

Hp now provides its own configuration script.

To configure the master server you must have the following information:

Realm name =	??	(KERBEROS.COM)
DNS domain name =	??	(central.com)
Master KDC =	??	(This server.central.com)
Admin principal =	kws/admin	

The server must have its own fully qualified domain name in /etc/hosts.

© SANS Institute 2003,   As part of GIAC practical repository.   Author retains full rights.

The Security Sever files that require Configuration are:

Krb.conf: Describes the default realm of the primary server and the tools of each server for that realm.

Krb.realms: provides a map for the domain name to the realm name

Admin_acl_file: Controls the administrative permissions for administrators

Password.policy Controls password policy for the entire secure network

Kpropd.ini: Contain the propogation information.

A tool name krbsetup has been provided by HP to auto configure the Kerberos Server. Using this tool you can configure, unconfigure, start, and stop the Kerberos Key Distribution Center(KDC) and the kadmind daemons. This tool is ran from /opt/krb5/sbin..

Krbsetup will create your krb.conf and krb.realms files and placed then in the /opt/krb5 directory. This tool allow you to specify whether the Kerberos server is a Primary or secondary server, customize your realm name, allows the creation of a stash file, and allows you to specify the encryption type.
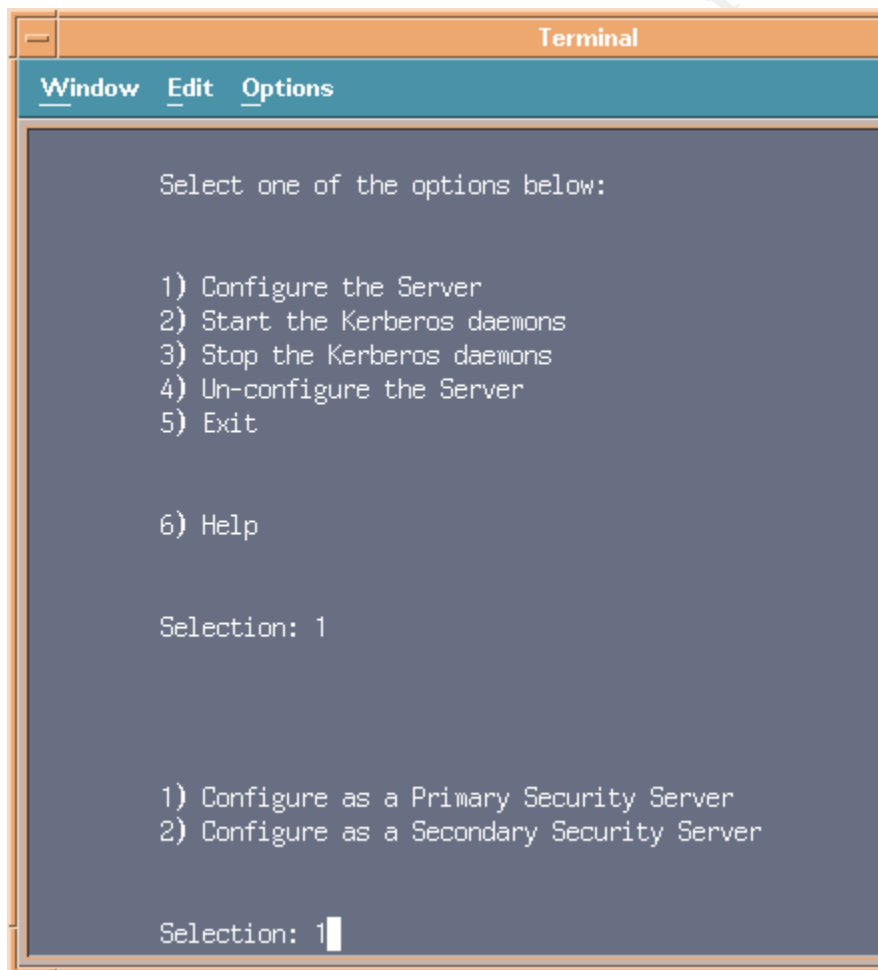
```
# cd /etc/rc.config.d
#
```
 # cat krbsrv
```
#!/sbin/sh -p
#           The Kerberos server maintains this file
#           to reflect the current Kerberos configuration of this system.
# Config Flags for Kerberos Server
# KDC == 1 Indicates that the kdcd has to be started
# ADMD == 1 Indicates that the kadmind has to be started
KDC=1
ADMD=1
#
```

The Kerberos daemons may be started with /stin/init.d/krbsrv start or by typing /opt/krb5/sbin/kdcd and /opt/krb5/sbin/kadmid. The configurations script has placed a Kerberos startup script in /etc/rc.config.d so Kerberos restarts at boot up.

```
ls -l *kr*
lrwxr-xr-x  1 bin      bin           19 May 21 18:54 S395krbsrv -> /sbin/init.d/krbsrv
# pwd
/sbin/rc2.d
#
```

2.13.3   Manual Configuration

Looking at the files after running krbsetup, it configured the system cleanly. This is a walk through as to what the configuration was, skip over if this is uneccessary informations, since krbsetup already configured cleanly.

Krb.conf defines the realm and the Master KDC; while krb.realm associates the DNS domain to a Kerberos Realm.
```
# cd /opt/krb
```

 # cat krb.conf
```
KERBEROS.COM
KERBEROS.COM sic78051.central.com admin server
```

 # cat krb.realms
```
Central.com KERBEROS.COM
```

Krbsetup adds the Kerberos services to the /etc/services files. These entry allows client application to establish socket connections to the KDC.

 # grep Ker /etc/services

.
klogin   543/tcp   # Kerberos rlogin -kfall
kshell   544/tcp krcmd   # Kerberos remote shell -kfall
ekshell   545/tcp krcmd   # Kerberos encrypted remote shell -kfall
krbupdate   760/tcp kreg   # Kerberos registration -kfall
kpasswd   761/tcp kpwd   # Kerberos "passwd" -kfall
eklogin   2105/tcp   # Kerberos encrypted rlogin -kfall
HP Kerberos ADDITIONS START HERE
kerberos5   88/udp   kdc   # Kerberos authentication
kerberos5   88/tcp   kdc   # Kerberos authentication
kerberos-adm 749/tcp   kerberos_adm   # Kerberos admin/changepw
kerberos-cpw 751/tcp   kerberos_master # Kerberos changepw
krb5_prop   754/tcp   # Kerberos slave propagation
HP Kerberos ADDITIONS END HERE
#

The four basic tasks after the confiruation file are setup:
   1) Create the Principal Database
   2) Add an administrative principal
   3) Create a host principal and extract its service
   4) Start the Kerberos daemon

 It runs **krb_create -s to create the Kerberos Distribution Center(KDC) database.**
The script edits the Kerberos Access file /etc/krb5/kadm5.acl, the default Kerberos
admin is kws/admin@CENTRAL.COM. This user is the only user that can modify the
Kerberos database, until other administrative users are added.

Lastly, it creates administration principals(a principal can be a user or a service).
/usr/krb5/ssbin/kadmin.local
kadmin.local: addprinc kwd/admin
Enter password for principal kws/admin@CENTRAL.COM
Reenter password for principal
            kws/admin@CENTRAL.COM
Principal kws/admin@CENTRAL.COM created.
Kadmin.local: ktadd –k /etc/krb5/kadm5.keytab
       Kadmin/central.com
Entry for principal kadmin/central.com
Kadmin.local: ktadd –k /etc/krb5/kadm5.keytab
       Changepw/central.com
Entry for principal changempw/central.com
Kadmin.local:quit

Kadmin and kdcd are both running. The administrative principal is kws/admin with full privileged. A host principal was created and extracted.

```
# ps -elf | grep kdcd
 1 S    root 3636    1 0 158 20       42ed50c0  88      42f88040 Jun 22 ?      0:00
/opt/krb5/sbin/kdcd
 1 S    root 3645 3636 0 154 20       42f16940  316        aaa280 Jun 22 ?      0:00
/opt/krb5/sbin/kdcd
# ps -elf | grep kadmin
 1 S    root 3647    1 0 154 20       42f166c0  475        aaa280 Jun 22 ?      0:15
/opt/krb5/sbin/kadmind
#
```

2.1.5 Securing the Kerberos Installation

Krb.conf must reside in the /opt/krb5 directory and must have -rw-r—r—root 3 for permissions.   The krb.conf file allowed the clients to locate servers on the network for authentication requests.

Security Policies

There are two files that are directly related to the security for the network of your organization. Namely password policy file and admin_acl_file.

Password Policy File
This file controls password rules such as password length, number of character types, and the lifetime of a password. This file is locate on each Primary and all the Secondary security Servers. Using the password policy file you can specify rules that force users to build good pass

/opt/krb5/password.policy

*.MaxRepeatChars	3
*.MaxRepeatClasses	4
*.Maximum Match	4,
*.MinimumLength	6
*.MinimumClasses	2
*.Expiration	90d
*.MinimuAge	None
*.NotifyTime	7d
*.dictionaries	None
*.MaxFailAuthCnt	10
*.NoReqChangePwd	0
*.MaximumHistory	3

User principals must provide their passwords during authentication to create their secret keys. For security users should be required to periodically change their passwords. If the system administrator enable the "Password Change Required attribute",   the user principal must change their passwords at next login.

The password expiration date is exceeded. If the password has expired, the user principal must change its passwords. The user can change their password with utilizing kpasswd. The administrator can also change a usr principal's password The "change password required" attribute is automatically enable.

Admin_acl file

The admin_acl file lists the various administrators along with their respective administrative permissions. It also lists the principals whose attributes cannot be changed without explicit privileges.   It must be protected with appropriate read write privileges and must be accessible only by a root user.

It must be protected with the appropriate read-write privileges and must be accessible only by the root user.

Kadmind checks for the principal's permissions in the admin_acl_file. The admin_acl_file can be edited directly on the primary servers, or can be edited remotely used the "administrative Permissions" window of the Administrator.

 By restricting the permissions setting, various administrators can have different privileges. The are broke into a, c, d, l, m for add, change, delete, list, and delete principals. The   X option allows extracting Keys. R is the restricted administrator, used in combination with the others it allow only the listed privilege

You can add any principal name to the admin_acl_File as an entry with or without assigned administrative permissions.

Reserved Principals

These principals are required on the Kerberos server. They are added when the database Is created.

Reserved special principal K/M@REalm The K/M@REALM principal contain the secret key of the principal database. When the database is created, this principal is added to the server's default realm to store the database secret key. All records in the principal database are encrypted using this key. The key for the principal is store in a file named. K5.realm .

The default@REALM principal contains the default group principals attributes for REALM. This principal is required in each realm. This principal is locked by default eliminating the security risk of an attacker attempting to authenticate using this principal account.

krbtgt@ERALM@REALM the krbtgt principal's secret key is used to encrypt and decrypt TGTs issued by the issued by the security server for principals in the realm

The kadmin/changepw@REALM is required for the Kerberos v5 standard password protocol.

The kcpwd/REALM@REALM is change passwd services for Kerberos.

2.1.6 Kerberos Administration

The Kerberos database utility can be used to globally manage the principals and their utilized with the Administrator or Command-Line-Administrator. The Administrator is the graphical-user interface that can be used to manage your principals and realms

The GUI Administrator can be used with the remote administrator, kadmind, or the local administrator, kadmin_ui. The remote kadmin must utilized Kerberos authentication before hand.

3.   CONCLUSIONS

At this point the server should be secure and functional.

The patches on the system are up-to-date. Many unneeded services are either removed, turned off, or disabled. NFS, NIS, and sendmail all with major security issues are disabled. Most serial communications are shutdown an Kernel rebuilds are not possible.

Root can only login directly to the console, all other access will be through a kerberized ssh and then su to root on the system. The only users on the system are either Kerberos or system administrators.

System Verification

- Running kinit from a kerberized client that points to this KDC should return a reusable credential

```
# kinit aadams1/sic78051@KTEST.EXAMPLE.COM
Password for aadams1/sic78051@EXAMPLE.COM:
```

```
# klist
Ticket cache: /tmp/krb5cc_102
Default principal: aadams1/sic78051@EXAMPLE.COM

Valid starting                    Expires                    Service
principal
Wed May 27 16:20:33 2000  Wed May 27 16:49:37 2000
krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

- Attempt to connect with a disabled service
    Try rlogin
    rlogin sic78051
    rcmd: connect: sic78051: Connection refused

- Verify that NIS is disabled
    # domainname kerb.com
    # ypcat passwd
    ypcat: can't bind to an NIS server for domain kerb.com.
     Reason: can't communicate with ypbind

- Check services with netstat
    Netstat will show the services that are running on the system
    One uniqueness in this one is the kshell and klogin, those are kerberized
    services that were left in inetd, since they are secure. They will run on the
    Kerberos clients, but will disalb ethem from the server.

    Nestat –af inet

    Proto Recv-Q Send-Q Local Address   Foreign Address   (state)
    tcp   0   0 *.portmap   *.*   LISTEN
    tcp   0   0 *.ident   *.*   LISTEN
    tcp   0   0 *.time   *.*   LISTEN
    tcp   0   0 *.discard   *.*   LISTEN
    tcp   0   0 *.echo   *.*   LISTEN
    tcp   0   0 *.2121   *.*   LISTEN
    tcp   0   0 *.kshell   *.*   LISTEN
    tcp   0   0 *.klogin   *.*   LISTEN
    tcp   0   0 *.49194   *.*   LISTEN
    tcp   0   0 *.53357   *.*   LISTEN
    tcp   0   0 *.49196   *.*   LISTEN

29
```

```
udp     0    0 *.*              *.*
udp     0    0 *.*              *.*
udp     0    0 *.syslog            *.*
udp     0    0 *.echo             *.*
udp     0    0 *.discard            *.*
udp     0    0 *.daytime            *.*
udp     0    0 *.chargen            *.*
udp     0    0 *.egb-daemon          *.*
udp     0    0   *.portmap      *.*
```

- Check processes with system versionof ps..
  Ps –ef

  Another look at the processes table. Note the getty console is for the
  dtlogins from the console for root

  ```
  root   0   0 0 Jun 21 ?        0:22 swapper
    root   9    0 0 Jun 21 ?       0:00 strmem
    root  10    0 0 Jun 21 ?       0:00 strweld
    root  11    0 0 Jun 21 ?       0:00 strfreebd
    root   3    0 0 Jun 21 ?       2:12 statdaemon
    root   4    0 0 Jun 21 ?       0:01 unhashdaemon
    root  12    0 0 Jun 21 ?       0:00 ttisr
    root   1    0 0 Jun 21 ?       0:00 init
    root  19    0 0 Jun 21 ?       0:00 lvmkd
    root  20    0 0 Jun 21 ?       0:00 lvmkd
    root  21    0 0 Jun 21 ?       0:00 lvmkd
    root  22    0 0 Jun 21 ?       0:00 lvmkd
    root  23    0 0 Jun 21 ?       0:00 lvmkd
    root  24    0 0 Jun 21 ?       0:00 lvmkd
    root 2972   1 0 Jun 21 console  0:00 /usr/sbin/getty console console
    root  855   1 0 Jun 21 ?        0:11 /usr/sbin/syncer
    root 10265 10263 0 07:04:12 pts/6   0:00 /sbin/sh
    root  31    0 0 Jun 21 ?       1:55 vxfsd
    root 1017   1 0 Jun 21 ?        0:00 /usr/sbin/syslogd -D
    root 1237   1 0 Jun 21 ?        0:00 /usr/sbin/rpcbind
    root 1060   1 0 Jun 21 ?        0:00 /usr/lbin/nktl_daemon 0 0 0 0 0 1
  -2
    root 1064   1 0 Jun 21 ?        0:00 /usr/lbin/ntl_reader 0 1 1 1 1000
  2 /var/adm/nettl /var/adm/con
    root 6298 6287 0 Jun 22 ttyp1   0:03 /opt/perl/bin/perl
  /opt/sec_mgmt/bastille/bin/InteractiveBastil
    root 2139   1 0 Jun 21 ?        0:00 /var/dmi/bin/hpuxci
    root 1414   1 0 Jun 21 ?        0:02 /usr/sbin/inetd
    r
  ```

3   ONGOING MAINTENANCE

Hp's security bulletin digest will send a update of new vulnerabilities as they arrive. Monthly, download the newest patch catalogue and rerun Patch Check to check for new vulnerabilities. Add patches as needed.

Since this is a Kerberos server, signup with MIT for their MIT updates also the Cert Advisory Mailing list http://www.cert.org/contact_cert/cermaillist.html, scan for any updates to Kerberos V(krb5). Also, sign up for Hp's atch update, that also is released monthly.

Continue to run Bastille on a weekly basis. Changes to file ownership or flagrant modifications in secure files should be detected though changes in what Bastille is flagging.

Run netstat and ps nightly, checking for changes in the morning.

Maintain the log files, choose one of many rolling routines. Two in the morning is optimal, since that is the quiet time. The KDC realms are broke up geographically, so Europe would not have U.S. users authentications. System maintenance and full backups can be done monthly when there is a Sunday morning maintenance window.

The KDC is propagated to a Slave KDC so there is a continous backup. Nightly a Kerberos database should be done and backed off to its own tape, Save off one tape a month for a long term snapshot. The others can be on a monthly rotation schedule.

Example—Backing Up the Kerberos Database
In the following example, the Kerberos database is backed up to a file called dumpfile. Because the -verbose option is specified, each principal is printed as it is backed up.
        # kdb5_util dump –f dump.dtatbase.txt
        kadmin/kdc1.eng.example.com@ENG.EXAMPLE.COM
        krbtgt/eng.example.com@ENG.EXAMPLE.COM
        kadmin/history@ENG.EXAMPLE.COM
        pak/admin@ENG.EXAMPLE.COM
        pak@ENG.EXAMPLE.COM
        changepw/kdc1.eng.example.com@ENG.EXAMPLE.COM

Make sure you have copies of admin_acl_file, password.policy, principal database files, and krb.conf. Do not make copies of .k5.REALM,instead recreate with master password, or v5srvtab, since they are the systems keytab just recreate them if needed.

Document any system changes both on the system an offloaded onto another system. Retain a binder hard copy.

BIBLIOGRAPHY

1) <u>Halting the Hacker: A practical to Computer Security</u> second edition ,
    Donald L. Pippin, Prentice Hall, New Jersey, 2002

2) <u>HP-UX 11i Security</u> ,Chris Wong, Prentice Hall, New Jersey, 2002.

3) "HP_UX Computer Security Checklist: by Lorraine Venner, 2001.
    URL: http://www.idio.com/~lorraine/securecheck.html

4) "Securing HP-UX 11" by Larry Harker, May 30,2001. Sans InfoSec Reading Room
    URL: http://www.sans.org/rr/unix/HP-UX11.php

5) "Network Security Features of HP-UX 11i: An HP-UX 11i. White Paper from Hewlett-
    Packard", Hewlett-Packard Company, February 2002
    URL: http://docs.hp.com

6) "Securing HP-UX Services" by Fernando Espinoza Sals, July 28,2001
    . URL: http://www.sans.org/rr/unix/sec_HPUX.php

7) "HP-UX Computer Security checklist"
    URL: http://www.idiom.com/~lorraine/securecheck.html

8) "HP-UX 11.0 Installation Checklist" by Deall Schmidt, April 6, 2001
    URL:http://www.sansorg/rr/unix/HPUX_check.php

9) "Network Security Features of HP=UX 11i:An HP-UX 11i White Paper form Hewlett-
    Packard", February 2002. URL: http://docs.hp.com

10) "Installing, Configuring, and Administering the Kerberos Server V 2.0 on HP-UX 11i",
    HP 9000 Networking, #T1417-90003, 2002

APPENDIX A: Step by Step mirroring of the root disk

```
# script /tmp/mkboot.out
#
# lvlnboot -v
Boot Definitions for Volume Group /dev/vg00:
Physical Volumes belonging in Root Volume Group:
      /dev/dsk/c3t5d0 (10/0/15/1.5.0) -- Boot Disk
Boot: lvol1 on:   /dev/dsk/c3t5d0
Root: lvol3 on:   /dev/dsk/c3t5d0
Swap: lvol2 on:   /dev/dsk/c3t5d0
Dump: lvol2 on:   /dev/dsk/c3t5d0, 0


# pvcreate -Bf /dev/rdsk/c3t6d0
# pvcreate -Bf
Physical volume "/dev/rdsk/c3t6d0" has been successfully created.


#
# vgextend /dev/vg00 /dev/dsk/c3t6d0
Volume group "/dev/vg00" has been successfully extended.
Volume Group configuration for /dev/vg00 has been saved in
/etc/lvmconf/vg00.conf


# mkboot -a "hpux" /dev/dsk/c3t6d0

# lvlnboot -v
Boot Definitions for Volume Group /dev/vg00:
Physical Volumes belonging in Root Volume Group:
      /dev/dsk/c3t5d0 (10/0/15/1.5.0) -- Boot Disk
      /dev/dsk/c3t6d0 (10/0/15/1.6.0) -- Boot Disk
Boot: lvol1 on:   /dev/dsk/c3t5d0
Root: lvol3 on:   /dev/dsk/c3t5d0
Swap: lvol2 on:   /dev/dsk/c3t5d0
Dump: lvol2 on:   /dev/dsk/c3t5d0, 0

#
# vgdisplay -v | more
--- Volume groups ---
VG Name                   /dev/vg00
VG Write Access           read/write
VG Status                 available
Max LV                    255
Cur LV                    7
Open LV                   7
Max PV                    16
Cur PV                    2
Act PV                    2
Max PE per PV             4350
VGDA                      4
PE Size (Mbytes)          4
```

```
Total PE                    8680
Alloc PE                    1892
Free PE                     6788
Total PVG                   0
Total Spare PVs             0
Total Spare PVs in use      0

    --- Logical volumes ---
    LV Name                 /dev/vg00/lvol1
    LV Status               available/syncd
    LV Size (Mbytes)        200
    Current LE              50
     Allocated PE            50
     Used PV                 1

     LV Name                /dev/vg00/lvol2
     LV Status              available/syncd
     LV Size (Mbytes)       1024
     Current LE             256
     Allocated PE           256
     Used PV                1

     LV Name                /dev/vg00/lvol3
     LV Status              available/syncd
     LV Size (Mbytes)       200
     Current LE             50
     Allocated PE           50
     Used PV                1

     LV Name                /dev/vg00/lvol4
     LV Status              available/syncd
     LV Size (Mbytes)       1024
     Current LE             256
     Allocated PE           256
     Used PV                1

     LV Name                /dev/vg00/lvol5
     LV Status              available/syncd
     LV Size (Mbytes)       1024
     Current LE             256
     Allocated PE           256
     Used PV                1

     LV Name                /dev/vg00/lvol6
     LV Status              available/syncd
     LV Size (Mbytes)       2048
     Current LE             512
     Allocated PE           512
     Used PV                1

     LV Name                /dev/vg00/lvol7
     LV Status              available/syncd
     LV Size (Mbytes)       2048
     Current LE             512
     Allocated PE           512
     Used PV                1
```

```
    --- Physical volumes ---
    PV Name                         /dev/dsk/c3t5d0
    PV Status                       available


# for i in 1 2 3 4 5 6 7
> do
>   lvextend -m 1 /dev/vg00/lvol$i /dev/dsk/c3t6d0
> done
The newly allocated mirrors are now being synchronized. This operation will
t e some time. Please wait ....
Logical volume "/dev/vg00/lvol1" has been successfully extended.
Volume Group configuration for /dev/vg00 has been saved in
/etc/lvmconf/vg00.conf
The newly allocated mirrors are now being synchronized. This operation will
t e some time. Please wait ....
Logical volume "/dev/vg00/lvol2" has been successfully extended.
Volume Group configuration for /dev/vg00 has been saved in
/etc/lvmconf/vg00.conf
The newly allocated mirrors are now being synchronized. This operation will
t e some time. Please wait ....
Logical volume "/dev/vg00/lvol3" has been successfully extended.
Volume Group configuration for /dev/vg00 has been saved in
/etc/lvmconf/vg00.conf
The newly allocated mirrors are now being synchronized. This operation will
t e some time. Please wait ....
Logical volume "/dev/vg00/lvol4" has been successfully extended.
Volume Group configuration for /dev/vg00 has been saved in
/etc/lvmconf/vg00.conf
The newly allocated mirrors are now being synchronized. This operation will
t e some time. Please wait ....
Logical volume "/dev/vg00/lvol5" has been successfully extended.
Volume Group configuration for /dev/vg00 has been saved in
/etc/lvmconf/vg00.conf
The newly allocated mirrors are now being synchronized. This operation will
t e some time. Please wait ....
Logical volume "/dev/vg00/lvol6" has been successfully extended.
Volume Group configuration for /dev/vg00 has been saved in
/etc/lvmconf/vg00.conf
The newly allocated mirrors are now being synchronized. This operation will
t e some time. Please wait ....
Logical volume "/dev/vg00/lvol7" has been successfully extended.
Volume Group configuration for /dev/vg00 has been saved in
/etc/lvmconf/vg00.conf
#
#
#
# lvlnboot -v

Boot Definitions for Volume Group /dev/vg00:
Physical Volumes belonging in Root Volume Group:
      /dev/dsk/c3t5d0 (10/0/15/1.5.0) -- Boot Disk
      /dev/dsk/c3t6d0 (10/0/15/1.6.0) -- Boot Disk
Boot: lvol1 on:   /dev/dsk/c3t5d0
                  /dev/dsk/c3t6d0
Root: lvol3 on:   /dev/dsk/c3t5d0
```

```
                       /dev/dsk/c3t6d0
Swap: lvol2 on:    /dev/dsk/c3t5d0
                       /dev/dsk/c3t6d0
Dump: lvol2 on:    /dev/dsk/c3t5d0, 0

# setboot
Primary bootpath : 10/0/15/1.5.0
Alternate bootpath : 10/0/15/0.6.0

Autoboot is ON (enabled)
Autosearch is ON (enabled)

#
#
# ioscan -funC disk
Class    I  H/W Path        Driver S/W State   H/W Type     Description
=========================================================================
disk     0  10/0/15/0.2.0  sdisk CLAIMED      DEVICE        TOSHIBA CD-ROM XM-
5401TA
                           /dev/dsk/c2t2d0   /dev/rdsk/c2t2d0
disk     1  10/0/15/1.5.0  sdisk CLAIMED      DEVICE        HP 18.2GST318406LC
                           /dev/dsk/c3t5d0   /dev/rdsk/c3t5d0
disk     2  10/0/15/1.6.0  sdisk CLAIMED      DEVICE        HP 18.2GST318406LC
                           /dev/dsk/c3t6d0   /dev/rdsk/c3t6d0
# setboot -a 10/0/15/1.6.0
# setboot
Primary bootpath : 10/0/15/1.5.0
Alternate bootpath : 10/0/15/1.6.0

Autoboot is ON (enabled)
Autosearch is ON (enabled)
```

Appendix B

```
# ./security_patch_check -c /usr/11i/11i/security_catalog

WARNING: There are group- and world-writable directories in your path

        to perl and/or your PATH environment variable.  This represents a

        security vulnerability (especially if running as root) that may

        compromise the effective use of this tool.  Please use the command:

        chmod og-w <directory name>

        to ensure this tool can be used safely in the future.  A list of the

        vulnerable directories follows:

            /usr/local

            /usr/local/bin


HP SECURITY PATCH CHECK (SPC) SOFTWARE TOOL DISCLAIMER.

Use of the SPC software tool can help efficiently optimize system security,
but

does not guarantee system security. Information about security patches
obtained

through use of the SPC software tool is provided on an "AS-IS" basis only and

is subject to change without notice.  HP DISCLAIMS ALL WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF
MERCHANTABILITY

AND FITNESS FOR A PARTICULAR PURPOSE.  Customer acknowledges that the
customer

is responsible for their system's security.

You must accept the terms of this disclaimer to use security_patch_check.
Type

"accept" (without quotes) within 2 minutes to accept the terms of the above

disclaimer

> accept

This disclaimer will not appear again for users on localhost whose home
```

directory is /. To suppress the disclaimer on other machines, use

security_patch_check's -d flag (example: security_patch_check -d -r).

WARNING: /usr/11i/11i/ is group/world writable and the sticky bit is not on.

WARNING: /usr/11i/ is group/world writable and the sticky bit is not on.

WARNING: /usr/11i/11i/security_catalog is over 2 days old and should be

updated. To get the latest catalog, run "security_patch_check -r", or

if running security_patch_check from within ServiceControl Manager,

run the "Get Patch Catalog" tool.

WARNING: Recalled patch PHCO_27099 is active on the target system. Its record,

including the Warn field, is available from

/usr/11i/11i/security_catalog, through the Patch Database area of the

ITRC or by using the -m flag (security_patch_check -m ...).

WARNING: No patch is currently on the target system to address the issues

described in security bulletin(s) 264 . No General Release patch or

replacement is currently available. The patch PHNE_28895 is listed as

being the best available patch, but has been recalled and is not

generally recommended by Hewlett-Packard.

The security bulletin and recall notice information should be

reviewed. Each customer should respond in a manner appropriate to

their environment.

Security bulletins can be found by number at

http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin

Patch recall notices can be seen using the security_patch_check -m

option, through the Patch Database area of the ITRC, or from within

/usr/11i/11i/security_catalog.

*** BEGINNING OF SECURITY PATCH CHECK REPORT ***

Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root

Analyzed localhost (HP-UX 11.11) from sic76048.fsic.ford.com

Security catalog: /usr/11i/11i/security_catalog

Security catalog created on: Sat Jun 21 22:59:15 2003

Time of analysis: Tue Jun 24 10:31:17 2003

List of recommended patches for most secure system:

Recommended Bull(s) Spec? Reboot? PDep? Description

#	Recommended	Bull(s)	Spec?	Reboot?	PDep?	Description
1	PHCO_27020	213	Yes	No	No	lpspool subsystem cumulative
2	PHCO_28719	258	No	No	No	wall(1M)
3	PHNE_25184	179	Yes	No	No	sendmail(1m) 8.9.3
4	PHNE_27765	162	No	No	No	ftpd(1M)
5	PHNE_28103	215 242	Yes	Yes	Yes	ONC/NFS General Release/Performance
6	PHNE_28450	209	No	No	No	Bind 8.1.2
7	PHSS_27258	196	Yes	No	Yes	HP DCE/9000 1.8 DCE Client IPv6

*** END OF REPORT ***

```
NOTE: Security bulletins can be found ordered by number at
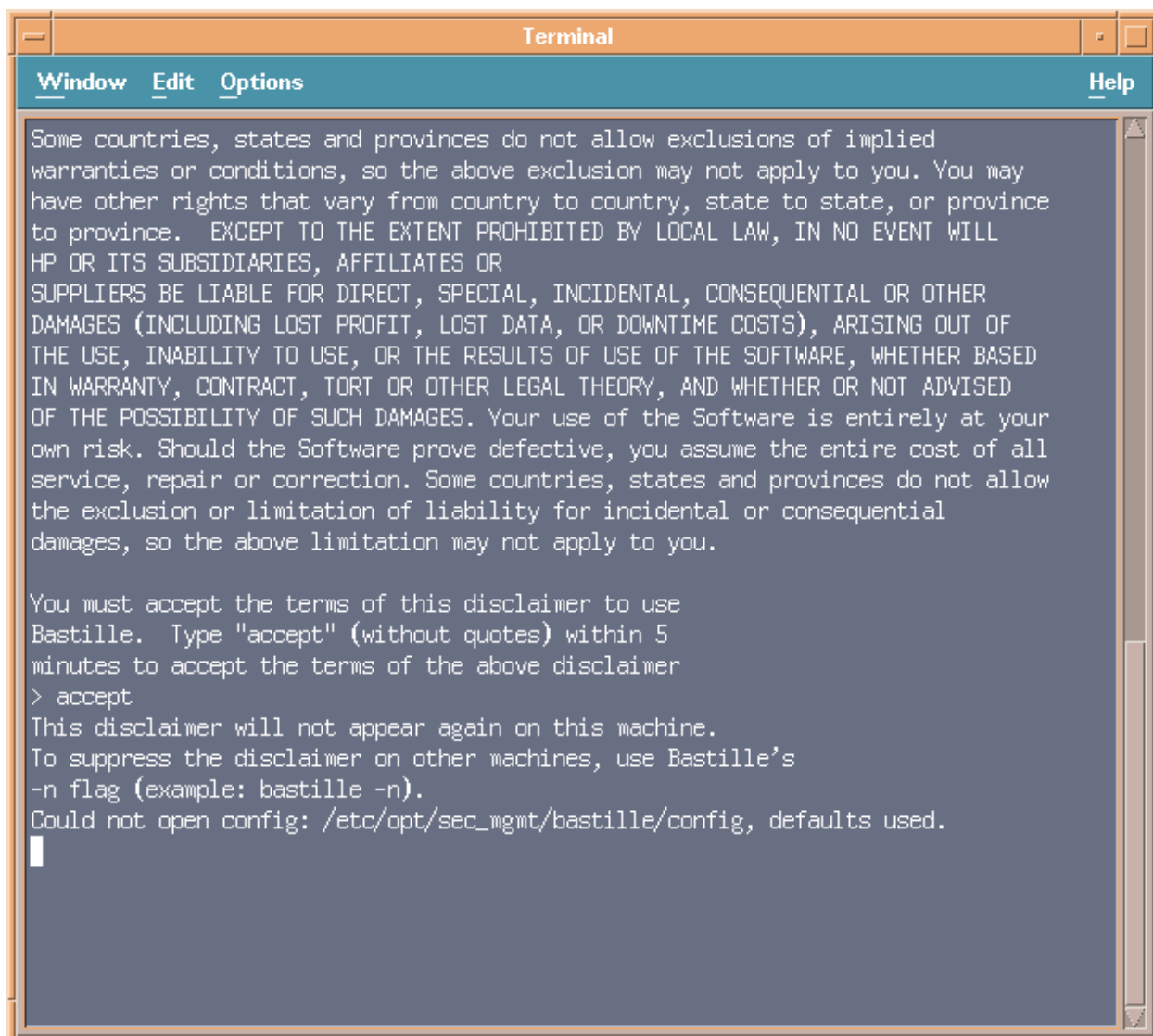
        http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin


# exit
```

Appendix C: Bastille Interactive Configuration

Terminal

Window   Edit   Options   Help

Some countries, states and provinces do not allow exclusions of implied
warranties or conditions, so the above exclusion may not apply to you. You may
have other rights that vary from country to country, state to state, or province
to province.   EXCEPT TO THE EXTENT PROHIBITED BY LOCAL LAW, IN NO EVENT WILL
HP OR ITS SUBSIDIARIES, AFFILIATES OR
SUPPLIERS BE LIABLE FOR DIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR OTHER
DAMAGES (INCLUDING LOST PROFIT, LOST DATA, OR DOWNTIME COSTS), ARISING OUT OF
THE USE, INABILITY TO USE, OR THE RESULTS OF USE OF THE SOFTWARE, WHETHER BASED
IN WARRANTY, CONTRACT, TORT OR OTHER LEGAL THEORY, AND WHETHER OR NOT ADVISED
OF THE POSSIBILITY OF SUCH DAMAGES. Your use of the Software is entirely at your
own risk. Should the Software prove defective, you assume the entire cost of all
service, repair or correction. Some countries, states and provinces do not allow
the exclusion or limitation of liability for incidental or consequential
damages, so the above limitation may not apply to you.

You must accept the terms of this disclaimer to use
Bastille. Type "accept" (without quotes) within 5
minutes to accept the terms of the above disclaimer
> accept
This disclaimer will not appear again on this machine.
To suppress the disclaimer on other machines, use Bastille's
-n flag (example: bastille -n).
Could not open config: /etc/opt/sec_mgmt/bastille/config, defaults used.

Bastille

Modules
✔ Title Screen
  Patches
  FilePermissions
  AccountSecurity
  SecureInetd
  MiscellaneousDaemons
  Sendmail
  DNS
  FTP
  HP_UX
  End Screen

Question

Explanation

(Tk User Interface)

v2.0.5

Please answer all the questions to build a more secure system.

The OK and Back buttons navigate forward and backward in the
questions database. Changes made in the Answer field are *only*
saved when you push the Ok button! The "modules" in the
questions database are listed to the left. You can jump to
the start of any module simply by clicking on its name.

Some questions have two levels of explanatory text, which you
can adjust with the Explain Less/More button.

Current support information for HP-UX Bastille is provided on the
HP-UX Bastille product page at http://software.hp.com

HP-UX Bastille has the potential to make changes which will affect
the functionality of other software. If you experience problems after
applying Bastille changes to your machine, be sure to inform anyone
you ask for help that you have run Bastille on this machine.

Helpful diagnostic tips:
- 'bastille -r' will revert your system to a pre-Bastille state.
  so you can better track down the cause of the problem
- A list of all actions Bastille has taken is located in.
     /var/opt/sec_mgmt/bastille/log/action-log
- If you suspect Bastille, the following files will be
  helpful to others in diagnosing your problem:
     /var/opt/sec_mgmt/bastille/log/action-log
     /var/opt/sec_mgmt/bastille/log/error-log
     /etc/opt/sec_mgmt/bastille/config

Available resources include:
- the itrc hp-ux security forum at http://www.itrc.hp.com
- the Bastille discussion group at
     bastille-linux-discuss@lists.sourceforge.net

Answer

←- Back   Restore Default   Explain Less   OK →

Modules

✔ Title Screen
✔ Patches
  FilePermissions
  AccountSecurity
  SecureInetd
  MiscellaneousDaemons
  Sendmail
  DNS
  FTP
  HP_UX
  End Screen

Question

Should Bastille scan for world-writeable directories?

Explanation

bit instead (what this script will do by default) did not have the same effects.

 - There are several other directories which have world-writeable permissions. Some of these are shipped with HP-UX, others are shipped with 3rd party products, and others may have been created by users without an appropriate umask set. Bastille will help you find those directories so that you can make appropriate decisions for your environment. The full impact of making these changes has not been analyzed.

As you run the script, it will create a "revert-directory-perms.sh" script which will allow you to revert to a supported state (independent of the rest of the HP-UX Bastille configurations, which are supported). Because of the potential for very subtle breakages, you should also keep a record of any changes which you make manually to your system so that you can revert them to help debug any problems which you run into. Running \'bastille -r\' will revert all bastille changes, including running the revert-directory-perms.sh script, but it may not revert changes you have made manually.

The fact that a directory is world-writeable does not imply that a vulnerability exists, because it depends on how the data stored in that directory is used. Still, it is a security best-practice to allow all users to write to ONLY temporary directories, such as /tmp and /var/tmp, and to set the "sticky" bit on those directories. By default, the generated script will set the "sticky" bit on all world-writeable directories.

If the "sticky" bit is set on a directory, only the file owner, directory owner, and superuser are allowed to rename or delete (and thus replace) the file, regardless of the group and world write permissions on the directory. The ownerships and permissions of the files and subdirectories in that directory determine how those files and subdirectories can be modified, respectively. You can tell that the "sticky" bit is set if there is a "t" in the last permissions column. (e.g.: drwxrwxrwt). Left unedited, the created script will set the "sticky" bit on any world-writeable directory.

(MANUAL ACTION REQUIRED TO COMPLETE THIS CONFIGURATION, see TODO list for details)

Answer

◇ No ◆ Yes

[← Back]   [Restore Default]   [Explain Less]   [OK →]

As part of GIAC practical repository.

Bastille

Modules
- ✔ Title Screen
- ✔ Patches
- ✔ FilePermissions
- ✔ AccountSecurity
- SecureInetd
- MiscellaneousDaemons
- Sendmail
- DNS
- FTP
- HP_UX
- End Screen

Question

Explanation

A default login/telnet/ftp "Authorized Use Only" banner will be created, and will be found in /etc/issue. You should modify this banner to apply more specifically to your organization (for instance, adding any site-specific information to the default warnings). If this is a corporate site, check with your corporate counsel to determine the most appropriate warning for the banner. These banners, according to CIAC's bulletin

    (http://ciac.llnl.gov/ciac/bulletins/j-043.shtml)

may make it much easier to prosecute intruders. By including this default banner, neither the Bastille development team nor Hewlett-Packard Company take any responsibility for your ability to prosecute system crackers. Please, especially if you run a corporate site, review/replace this with more specific language.

Answer

<-- Back   Restore Default   Explain Less   OK -->

© SANS Institute

Bastille

Modules
- ✔ Title Screen
- ✔ Patches
- ✔ FilePermissions
- ✔ AccountSecurity
- ✔ SecureInetd
- MiscellaneousDaemons
- Sendmail
- DNS
- FTP
- HP_UX
- End Screen

Question

Would you like to deactivate the NFS server on this system?

Explanation

An NFS (Network File System) server allows it's host machine to export file systems onto other designated machines on a network. NFS has a history of major security vulnerabilities, as well as being a clear-text protocol and relying on the presented username for authentication. Any data transferred by NFS can be monitored by any other network machine. Transferred data includes file handles, which can then be used to modify files.

This service can be made safer if it is locked behind a firewall that will block NFS packets from entering or leaving your network. It is best to deactivate it until you can investigate whether or not you need NFS and how to best secure it.

One alternative is CIFS/9000 (similar to Samba). It is still a cleartext, shared file system and therefore still raises security concerns, but unlike NFS, CIFS/9000 at least requires the user to authenticate (prove they are who they say they are) before reading or writing to files. Other alternatives include tunneling NFS through IPSec or Secure Shell, but this can take quite a bit of effort to setup and may degrade performance.

Answer

◇ No ◆ Yes

[← Back] [Restore Default] [Explain Less] [OK →]

As part of GIAC practical repository.

Bastille

Modules
- ✔ Title Screen
- ✔ Patches
- ✔ FilePermissions
- ✔ AccountSecurity
- ✔ SecureInetd
- MiscellaneousDaemons
- Sendmail
- DNS
- FTP
- HP_UX
- End Screen

Question

Would you like to deactivate NFS client daemons?

Explanation

NFS (Network File System) client daemons are by default running on the system. These include automount, which allows normal users to mount nfs file systems, and biod, block I/O daemons which are used on an NFS client to handle read-ahead and write-behind buffer caching. Automount for example, allows any user to perform an operation that is normally restricted to root. There is an inherent security benefit to removing privileges from non root accounts. NFS has a history of major security vulnerabilities, as well as being a clear-text protocol. Any data transferred by NFS can be monitored by any other network machine. Transferred data includes file handles, which can then be used to modify files.

The daemons to be deactivated are automount, autofs. and biod. These services can be made safer if they are locked behind a firewall that will block NFS packets from entering or leaving your network. It is best to deactivate them until you can investigate whether or not you need NFS and how to best secure it.

Answer

◇ No ◆ Yes

[← Back] [Restore Default] [Explain Less] [OK →]

As part of GIAC practical repository.

Bastille

Modules
- ✔ Title Screen
- ✔ Patches
- ✔ FilePermissions
- ✔ AccountSecurity
- ✔ SecureInetd
- MiscellaneousDaemons
- Sendmail
- DNS
- FTP
- HP_UX
- End Screen

Question

Would you like to deactivate NIS server programs?

Explanation

An NIS (Network Information System) server is used to distribute network naming and administration information to other machines on a network

NIS is a system used for synchronizing key host information, including account names and passwords. It is a clear-text protocol, and can be easily compromised to gain access to accounts on the system. If you are really interested in using NIS, you should configure your firewall to block NIS traffic going in or out of the network.

On many systems, including trusted-mode HP-UX systems, passwords are not only encrypted but also readable only by the super-user. This defense measure was taken because encrypted passwords can be decrypted fairly quickly with today's computers. When you use NIS, the encrypted password is transmitted in clear-text and made available to anyone on the network, compromising this defense measure. Because of this, HP-UX trusted mode, a security feature that Bastille can enable, is incompatible with NIS. If you choose to convert to trusted-mode, you should also disable NIS.

We recommend that you deactivate NIS server programs. Alternatives include NIS+, LDAP, and Kerberos servers.

Answer

◇ No ◆ Yes

<- Back   Restore Default   Explain Less   OK ->

Bastille

Modules

✔ Title Screen
✔ Patches
✔ FilePermissions
✔ AccountSecurity
✔ SecureInetd
  MiscellaneousDaemons
  Sendmail
  DNS
  FTP
  HP_UX
  End Screen

Question

Should Bastille deactivate rbootd?

Explanation

The rbootd daemon is used for a protocol called RMP, which is a predecessor to the "bootp" protocol (which serves DHCP). Basically, unless you are using this machine to serve dynamic IP addresses to very old HP-UX systems (prior to 10.0, or older than s712's), you have no reason to have this running.

Answer

◆ No ◆ Yes

←Back   Restore Default   Explain Less   OK →

As part of GIAC practical repository.

Bastille

Modules

✔ Title Screen
✔ Patches
✔ FilePermissions
✔ AccountSecurity
✔ SecureInetd
✔ MiscellaneousDaemons
  Sendmail
  DNS
  FTP
  HP_UX
  End Screen

Question

Would you like to run sendmail via cron to process the queue?

Explanation

Should sendmail run every 15 minutes to process the mail queue, processing and sending out e-mail? If this machine does not run sendmail in daemon mode, you may want to do this to make your outbound mail more reliable.

Most of the time, this is not required since most mailer programs activate sendmail to process their particular message. A message usually only gets written to the queue (and thus needs a cron entry) if sendmail has trouble delivering it. Example: the receiving mail server is down.

Please note that the 15 min. interval can be easily changed later, see crontab(1).

Answer

◇ No ◆ Yes

← Back   Restore Default   Explain Less   OK →

© SANS Institute 2003,

Bastille

Modules
- ✔ Title Screen
- ✔ Patches
- ✔ FilePermissions
- ✔ AccountSecurity
- ✔ SecureInetd
- ✔ MiscellaneousDaemons
- Sendmail
- DNS
- FTP
- HP_UX
- End Screen

Question

Would you like to disable the VRFY and EXPN sendmail commands?

Explanation

An attacker can use sendmail's vrfy (verify recipient existence) and expn (expand recipient alias/list contents) commands to learn more about accounts on the system. The expn command, for instance, could be used to find out who the "postmaster" and "abuse" aliases redirect mail to, which identifies which user account belongs to the system administrator.

These sendmail commands can probably be disabled without breaking anything and will make the system cracker's job more difficult. The only reasons to leave them on are (1) you are running an old-fashioned, friendly site, (2) you are using them to debug your own mail server, or (3) the very small chance that some software you use relies on this.

Answer

◆ No ◆ Yes

[← Back] [Restore Default] [Explain Less] [OK →]

67

Bastille

Modules
- ✔ Title Screen
- ✔ Patches
- ✔ FilePermissions
- ✔ AccountSecurity
- ✔ SecureInetd
- ✔ MiscellaneousDaemons
- ✔ Sendmail
- ✔ DNS
- FTP
- HP_UX
- End Screen

Question

Would you like to chroot named and set it to run as a non-root user?

Explanation

The name server, "named", needs to run with privileged access, and was traditionally given full root access. This allows "named" to function correctly, but increases the security risk if any vulnerabilities are found. We can decrease this risk by running "named" as a non-privileged user and by putting its files in a restricted file system (called a chroot jail).

For security reasons, it would be ideal to restrict every process which is listening to untrusted data as much as possible. This is especially true of network daemons, such as bind. If a vulnerability is found in the daemon, then a chroot jail will contain any intrusions.   Only a root process can break out of a chroot jail, so Bastille will ensure that "named" is not running as root. A successful attack on "named" in a chroot jail running as a non-privileged user will allow the attacker to modify only files owned or writeable by that non-privileged user and protect the rest of the system.

HP-UX Note: The general structure of the jail will be created but several entries will be added to Bastille's generated TODO list which require MANUAL ACTION on your part. (HP-UX does not ship with a name server configured by default, so much of this depends on how your system's name server is configured.)

(MANUAL ACTION REQUIRED TO COMPLETE THIS CONFIGURATION, see TODO list for details)

Answer

◇ No ◆ Yes

[←– Back]   [Restore Default]   [Explain Less]   [OK –→]

68

Bastille

Modules
- ✔ Title Screen
- ✔ Patches
- ✔ FilePermissions
- ✔ AccountSecurity
- ✔ SecureInetd
- ✔ MiscellaneousDaemons
- ✔ Sendmail
- ✔ DNS
- ✔ FTP
- HP_UX
- End Screen

Question

Would you like to enable kernel-based stack execute protection?

Explanation

A common way to gain privileged access is to provide some type of out-of-bounds input that is not checked by a program. This input can be used to overflow the stack in a way that leaves some cleverly written instructions stored in a place that will be executed by the program. The HP-UX kernel has the ability to disallow execution of commands from the stack. This will contain many of these types of attacks, making them completely useless. Because this is done at the kernel level, it is independent of any application which may have a vulnerability of this type. Note that this will also break some applications (Example: Java 1.2 programs will fail if using JDK/JRE 1.2.2 versions older than 1.2.2.06) which were designed to execute code off of the stack. However, you can run "chatr +es <executeable_file>" to override this for individual programs if they break.

Changing the kernel parameter "executable_stack" requires Bastille to recompile the kernel. Ensure that the current running kernel is /stand/vmunix. A backup of the old kernel will be placed in /stand/vmunix.prev and /stand/dlkm.vmunix.prev. If you answer yes to this question, you must reboot your system for this change to take effect.

(MANUAL ACTION REQUIRED TO COMPLETE THIS CONFIGURATION, see TODO list for details)

Answer

◇ No ◆ Yes

[← Back]   [Restore Default]   [Explain Less]   [OK →]

Bastille

Modules

✔ Title Screen
✔ Patches
✔ FilePermissions
✔ AccountSecurity
✔ SecureInetd
✔ MiscellaneousDaemons
✔ Sendmail
✔ DNS
✔ FTP
   HP_UX
   End Screen

Question

Would you like Bastille to make the suggested ndd changes?

Explanation

ndd is a utility for getting and setting network device parameters.

The following is a list of some ndd parameters which the "HP-UX Bastion Host Whitepaper" suggests that you change for greater security:

	Default => Suggested		
ip_forward_directed_broadcasts	1	=>	0
ip_forward_src_routed	1	=>	0
ip_forwarding	2	=>	0
ip_ire_gw_probe	1	=>	0
ip_pmtu_strategy	2	=>	1
ip_send_redirects	1	=>	0
ip_send_source_quench	1	=>	0
tcp_conn_request_max	20	=>	4096
tcp_syn_rcvd_max	500	=>	1000

For more information on each of these parameters, run

ndd -h

Note: If you already have some non-default settings in effect, you will need to merge the settings manually, and a reminder will be added to your TODO list.

(MANUAL ACTION MAY BE REQUIRED TO COMPLETE THIS CONFIGURATION, see TODO list for details)

Answer

◇ No ◆ Yes

| ← Back | Restore Default | Explain Less | OK → |