Global Information Assurance Certification Paper

Abstract

Pre-approval was sought by me to utilize this format for my GSEC practical. This was approved by SANS on March 25th, 2003. This report documents findings and recommendations following a review of the information security policies and procedures currently in place at University of Test Case in addition to analyzing a single systems configuration.

Author

Colleen Bolan

Purpose

The purpose of this documentation is to ascertain vulnerabilities in the company's information security implementation and to communicate best practices for security management in a distributed computing environment. The document addresses specific concerns for the operation of world-class industry standards for centralized management of midrange (HP-UX) computing systems.

Limitations

The following areas have not been addressed within this document:

- Application security and controls.
- Operating system security for systems not specifically described in this report.

Security of the network, including bridges, routers, switches, and firewall

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Introduction

This report is a result of my findings from an Information Security Review, which was performed at University of Test Case on Monday, March 31st, 2003.

The goal of this Security Review is to reduce our customers' risk of financial and public image losses due to intrusion, system misuse, privilege abuse, tampering, fraud, and service interruption. My focus is on providing strategies, policies and technical solutions to counter external threats (e.g. hackers, competitive adversaries, and the criminal element) and internal abuse (e.g., unstable or unscrupulous employees). I provide a combination of services that will allow customers to address the business issue of enterprise computing security. Using a combination of technical, human, and process controls, the security risks can be removed or reduced to a well-understood and manageable level.

The goal of the company's information security solution should be to provide a comprehensive set of security services that ensure the availability, integrity and confidentiality of corporate information assets.

A comprehensive security solution includes the concept of end-to-end security of network and transaction traffic wherein the introduction of a single, inherently non-secure component cannot compromise the security of the networked system as a whole.

Security services are comprised of five components:

- Authentication - the ability to prove one's identity
- Authorization - the ability to regulate access based on identity,
- Confidentiality - the ability to protect data from unauthorized disclosure
- Integrity - the ability to protect data from unauthorized modification,
- Audit - the ability to track usage based on identity.

These services should be as unobtrusive to the end-user as possible, providing the user with enhanced, not degraded productivity. Security services should be designed to be manageable; that is, they should be logically centralized and integrated within a common system and network management framework.

Scope

The scope of this security review was to examine the policies and procedures of University of Test Case, both written and practiced, and to analyze one of University of Test Case servers for appropriate security configuration and safeguards. The system used for this review was a HP 9000 N Series, identified as SERVER1, which is thought to be representative of the other servers in the University of Test Case environment.

The objective of the review was to help ensure the integrity of the applications and information. The intent was to discover security problem areas, and to suggest solutions to problems uncovered.

As part of this review, personnel from the following job categories at University of Test Case were interviewed:

- Susie Testcase – Security Manager
- Bricker Case - Administration Team

Review Methodology

The information security review involved the review of active controls, an analysis of audit trail data, and a review of the computing procedures and policies. The information security review also analyzed the adherence of University of Test Case to policy and established security guidelines. The essence of a review is to perform an independent analysis of a given subject, and to produce a report detailing the findings. This security review report is an analysis of how the current computing environment measures up against an acceptable set of standards.

The system's analysis was divided into the following eight specific areas:

- Policies, Procedures and Documentation
- Physical Security
- Security of Root user
- Security of Normal Users
- Security of Files
- Security of Modems
- Overall Security of the System
- Periodic Testing

Recommendations for changes to the computing environment are included.

Conclusions

Following is a summary of the findings of the security review. For a detailed analysis of the security review, refer to the "Findings and Recommendations" section and the "Interview Questions" of this document.

This summary will cover some areas where University of Test Case is demonstrating good or adequate security practices and areas where improvements could be made. Not all strengths or weaknesses are listed in this Executive Summary. Therefore, it is STRONGLY RECOMMENDED that the "Findings and Recommendations" section is reviewed in detail, and that the recommendations are implemented within the I.T. department at University of Test Case.

In working through this Security Review with the staff at the University of Test Case it is my understanding that efforts have been made to establish security polices and procedures for the IT environment. These polices, procedures provide a building block for good security practices however they need to be enhanced further. The following are my recommendations:

Policies, Procedures and Documentation

Incident Plan – currently the plan in place provides for names of managers and administrators who should be contacted when an incident occurs, and the method for contacting them. It also provides a plan to protect the system from further loss if a problem is discovered. This is a foundation but by incorporating the following your incident plan would become stronger.

- Documentation should be created, published and reviewed regularly so that everyone knows the immediate actions that should be taken by operators in case of a security incident. This should be created in a step-by-step process.
- Steps on how to protect information concerning an incident so that it can be used to determine what occurred and later used as legal evidence if need be.
- Part of this documentation needs to incorporate procedures for when to notify law enforcement and corporate counsel.
- Plan should define when it is appropriate for an incident to be reported to CERT.

Recovery Plan – Implementation of a written recovery plan should be published. Even though a recovery plan resides in everyone's mind of the steps they would need to take in case of a severe security incident, it is best served if it is written step-by-step and published so that nothing gets missed if a crisis occurs. Taking this plan further to guarantee success in a crisis would be to practice the procedures at a minimum of one time per year. Policies continually need to be improved but if they aren't practiced you won't know if they really work.

The University of Test Case should consider having their policies and procedures reviewed by HP in the form of yearly security audits and vulnerability assessments.

Physical Security

Computer Room Access – This facility is older in nature and doesn't have all the latest controlled access devices. It does on the second level of the building, have solid walls that run from the floor to the ceiling, and a doorway into the room. The following recommendations would allow for tighter security of the systems without the undertaking of a full room renovation.

- Provide controls for logging visitor's in/out of the computer room
- Visitors should be escorted, and provided with a badge that identifies them as a visitor
- Door should be locked at all times. If agreed to by management, install a coded entry lock instead of having door keys. Door keys can be easily lost, and even more easily duplicated. Coded entry lock combinations can be changed at random, making it easier and cost effective if personnel changes occur.

Server Security – The system console is the most powerful, and potentially the most vulnerable point of access to your IT environment. The following recommendations should be considered:

- Disable Service Mode on your servers' CPU's. (Some HP systems have this feature check with your hardware engineer to see if your equipment has it)

- Once physical access is established, powering down the server via the power switch, or pulling the plug and then trying to bring the system up into single-user mode is easy. Implement password usage in Single-User mode to restrict access to your system.

Install, Support and Backup Media – All media should be available in case of emergencies to allow for quick restoration of your system. However, they should be secured in a locked cabinet or another locked area away from the server during off hours.

Overall Security of the System

During the Security Review I ran an application called "Medusa". This application produced three output files that provided detailed information on file system security structures. Each problem I found was classified as either A, B, or C depending on the severity of the security risk and is detailed more thoroughly in the findings and recommendations section of this report. In short the findings pointed to these areas of concern:

- System Files and Directories are publicly writable
- inetd logging is disabled
- Inconsistencies in password entries
- Non-administrative UID/GID writable files/directories exist in users path
- Non-standard SUID and/or SGID files
- Improper users' parent directory(s) ownerships/permissions

- Non-standard ownerships
- Improper ownerships/permissions with users' $HOME directory and/or files
- Implement a global umask of 022
- Compromised fileset integrity in SD-installed software
- Root messaging is enabled

Periodic Testing

Remember it is far easier to prevent unauthorized access to your system than to fix up after the fact. With that said it is very important to periodically test the security practices and procedures within your environment to ensure success if and when they may need to be put into action. The following recommendations will only improve upon the foundations of the University of Test Case's security practices.

- Implement usage of HP's swverify command or a public domain application like COPS that would check the integrity of the system files. This practice should be automated and periodically run manually by system operators. Doing both steps allows for verification of accuracy in the findings.
- Implement periodic checks of /etc/passwd file, to verify UID 0 is not set in any user logins. This can be done in a cron job and as well should be run manually by system operators. Doing both steps allows for verification of accuracy in the findings.
- Once IDS/9000 is fully functional this application must also be tested to verify it is working properly. Create a mock incident.
- Implement HP's Security Patch Check tool to analyze the currency of a system with respect to security patches. It recommends patches for security vulnerabilities that have not been fixed by other patches currently on the system.

By addressing the areas mentioned above, University of Test Case will have a good start toward increasing the security of its information systems. As stated before, in the "Findings and Recommendations" section of this report you will find details of changes that should be made in these areas, as well as other areas that are not listed in this Executive Summary.

It should be noted that information systems security is an ongoing task. By securing areas you have control over and preparing for unplanned events, you are better able to provide a more secure computing environment for your users.

This concludes the executive summary.

FINDINGS AND RECOMMENDATIONS

Security Assessment Report

The following security problems were noted on server1. Each noted problem is classified as either A, B, or C depending on the severity of the security risk.

Classifications

A: Critical, should be remedied immediately.
B: Serious, should be addressed as soon as is reasonable.
C: Minor, but should be fixed when time permits.

General Comments

Many security-related problems can be avoided by making the global umask setting sufficient in both /etc/profile and /etc/csh.login. The umask defines the file mode creation mask value for the default permissions of newly created files. It is good practice to enable the umask to prevent group and public write permission bits from being set. This can be accomplished by using the following command line within both /etc/profile and /etc/csh.login: umask 022 this will, by default, cause all newly created files to have the following permissions: -rw-r--r--

Security Analysis

Class A Problems

- Essential system files/directories publicly writable:

```
-rw-rw-rw-   1 root     sys          55 Jun  3 14:38     /usr/bin/system_db
-rwxrwxrwx   1 bin      bin      268320 May 17  1994     /usr/lbin/udf_ccdc
-rwxrwxrwx   1 bin      bin      419760 May 17  1994     /usr/lbin/udf_big5
```

Explanation

As a general rule, a file or directory should have public write permission turned on only if there is a need to do so. Nearly all system files should not be publicly writable, both as a matter of good practice and to prevent accidental (or intentional) unauthorized over-writing. The files and directories listed here are the essential OS commands, sensitive files, and trees (such as /sbin, /usr/bin) that do not need public write permissions.

Corrective Action

Execute the following:

chmod o-w <file_or_dir> ***or*** ***chmod g-w <file_or_dir>***

- Inetd was started with logging disabled

Explanation

The Internet daemon, /usr/sbin/inetd, invokes Internet server processes as needed by the system and is usually invoked on boot-up by /sbin/init.d/inetd. The logging option of inetd should be turned on as a debugging aid as well as a way of monitoring or tracing access to network services when starting the inetd daemon.

Corrective Action

Edit "/etc/rc.config.d/netdaemons" and add "-l" in the INETD_ARGS variable like:

export INETD_ARGS="-l"

Restart inetd manually by executing:

/sbin/init.d/inetd stop
/sbin/init.d/inetd start

Class B Problems

- Inconsistencies with the following /etc/passwd entries

webadmin:*:40:1:*:/usr/obam/server/nologindir Login directory not found
smbnull:*:101:101:*:/home/smbnull:/sbin/sh Login directory not found

Explanation

This verification includes a validation of the number of fields, login name, user ID, group ID, and whether the login directory and optional program name exist.

Corrective Action

Corrective action is indicated within the diagnostic message.

- Non-administrative UID/GID writable files/directories exist in bevb's $PATH

drwxrwxrwx 2 bin bin 96 Aug 26 09:59 /usr/local/bin

```
-rwxr-xr-x    1 oracle    sys         2512 Jun 14 18:21      /usr/local/bin/oraenv
-rwxr-xr-x    1 oracle    sys         2417 Jun 14 18:21      /usr/local/bin/dbhome
-rwxr-xr-x    1 oracle    sys         2316 Jun 14 18:21      /usr/local/bin/coraenv
```

- Non-administrative UID/GID writable files/directories exist in nanf's $PATH

```
drwxrwxrwx   2 bin       bin           96 Aug 26 09:59      /usr/local/bin
-rwxr-xr-x    1 oracle    sys         2512 Jun 14 18:21      /usr/local/bin/oraenv
-rwxr-xr-x    1 oracle    sys         2417 Jun 14 18:21
      /usr/local/bin/dbhome
-rwxr-xr-x    1 oracle    sys         2316 Jun 14 18:21
      /usr/local/bin/coraenv
```

- Non-administrative UID/GID writable files/directories exist in dianemcd's $PATH

```
drwxrwxrwx   2 bin       bin           96 Aug 26 09:59      /usr/local/bin
-rwxr-xr-x    1 oracle    sys         2512 Jun 14 18:21      /usr/local/bin/oraenv
-rwxr-xr-x    1 oracle    sys         2417 Jun 14 18:21      /usr/local/bin/dbhome
-rwxr-xr-x    1 oracle    sys         2316 Jun 14 18:21      /usr/local/bin/coraenv
```

- Non-administrative UID/GID writable files/directories exist in oracle's $PATH

```
drwxrwxrwx   2 bin       bin           96 Aug 26 09:59      /usr/local/bin
```

Explanation

All users should not have any non-administrative (UIDs below 100) writable directories in their $PATH variable unless the path is a subordinate directory of their $HOME directory. Otherwise, users are vulnerable to possible Trojan horses and other security breaching tactics.

Corrective Action

Correct $PATH for the user to include only administrative UID writable directories, preferably at the head of the $PATH string, and/or subdirectories of user's $HOME.

- User "root" does not have mesg capability turned off

Explanation

mesg capability should be turned off on all UID-0 shells. Other users should not be allowed to write to a terminal or window in which a super-user is active. This capability can be abused to read keystrokes and possibly capture sensitive information, or otherwise cause mischief.

Corrective Action

Add the following to root's .profile, .kshrc, .cshrc, or .login: mesg n

- Non-standard SUID and/or SGID files

```
 -r-sr-x---  1 root      ids         266240 Mar 22 09:47  /opt/ids/lbin/idssysdsp
 -r-sr-x---  1 root      ids         274432 Mar 22 10:01  /opt/ids/lbin/updaterc
 -r-sr-xr-x  1 root      bin          16384 Dec 17  200   /opt/webadmin/parmgr/startParMgr.cgi
 -r-sr-xr-x  1 root      bin          16384 Jun 19  2001  /usr/lib/lanadmin/libdsfddi4.1
 -r-sr-xr-x  1 root      bin          20480 Nov 14  20    /var/adm/sw/save/PHNE_22727/100BT
RUN/usr/lib/lanadmin/libdsbtlan.1

 -r-sr-xr-x  1 root      bin         20480 Sep  3  2001 /opt/webadmin/mx/startMUXPlex.cgi
 -r-sr-xr-x  1 root      bin         28672 Feb  2  2001 /var/adm/sw/save/PHNE_23465/100BT-
RUN/usr/lib/lanadmin/libdsbtlan.1

 -r-sr-xr-x  1 root      bin          139264 Oct  2  2000  /usr/lib/lanadmin/libdsgelan.1
 -r-sr-xr-x  1 root      bin         2305720 Sep  3  2001 /opt/mx/bin/scmgr
 -r-sr-xr-x  1 root      sys          798720 Apr 12  2001 /sbin/sdstolvm
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/bin/mxauth
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/bin/mxexec
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/bin/mxngroup
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/bin/mxnode
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/bin/mxrole
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/bin/mxtool
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/bin/mxuser
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/lbin/.mxcli
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/lbin/mxconfigdirectory
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/lbin/mxconfigproperties
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/lbin/mxconfigschema
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/lbin/mxgetlocalhostname
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/lbin/mxinit
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/lbin/mxinitialization
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/lbin/mxpassword
 -r-sr-xr-x 16 root      bin         200704 Sep  3  2001  /opt/mx/lbin/mxshutdown
 -r-sr-xr-x 31 root      sys         544768 May 16 10:06 /usr/sbin/pvremove
 -r-sr-xr-x 31 root      sys         544768 May 16 10:06 /usr/sbin/vgchgid
 -r-sr-xr-x 31 root      sys         823296 May 16 10:06 /sbin/pvremove
 -r-sr-xr-x 31 root      sys         823296 May 16 10:06 /sbin/vgchgid
 -r-xr-sr-x  1 bin       sys          16384 Mar 22  2001  /var/adm/sw/save/PHCO_25008/CMDS-
AUX/usr/bin/pipcs

 -r-xr-sr-x    1 bin     sys          16384    Nov 15  2001   /usr/bin/pipcs
 -rwsr-xr-x  1 root      bin          356352 Oct  8  2001    /usr/sbin/vxprint
 -rwsr-xr-x  1 root      bin          622592 Oct  8  2001    /etc/vx/type/static/vxprint
 -rwsr-xr-x  1 root      users         49152 Mar 28  2001   /opt/cifsclient/bin/cifslist
 -rwsr-xr-x  1 root      users         49152 Mar 28  2001   /opt/cifsclient/bin/cifslogout
 -rwsr-xr-x  1 root      users         53248 Mar 28  2001   /opt/cifsclient/bin/cifslogin
```

Explanation

Generally speaking, when a program is invoked, it executes as, and with the permissions of, the executing user, which is independent of the ownership of the

executable file. This is changed when the "set user ID" (SUID) bit is set in the file permissions of the executable. When the SUID bit is set the program is executed as, and with the permissions of, the *owner* of the executable file.

For example, a non-root user generally cannot modify /etc/passwd since the file permissions are protective of such activity. However, the same non-root user can change their password using /usr/bin/passwd. This is because /usr/bin/passwd is a SUID program whereby it is owned by root and, as consequence of the SUID bit, when executed, it runs as if root is executing the program. As a result, the non-root user is able to modify /etc/passwd. This analysis applies to SGID files as well.

Any SUID file that is owned by an administrative user (UID < 100) must be examined closely to assure that it doesn't create a security threat (allowing SUID or SGID capabilities).

Corrective Action

If the file does not need to be SUID, the best action is to execute: chmod u-s <filename>

If the file does not need to be SGID, the best action is to execute: chmod g-s <filename>

- Confidential/critical files with improper ownership/permissions: [file permissions should not be publicly writable nor readable and should be owned by administrative UIDs/GIDs.]

```
crw-rw-rw-  1 bin      bin      14 0x000000 May 15 08:21 /dev/lan0
crw-rw-rw-  1 bin      bin      14 0x000001 May 15 08:21 /dev/ether0
crw-rw-rw-  1 bin      bin      14 0x010000 May 15 08:21 /dev/lan1
crw-rw-rw-  1 bin      bin      14 0x010001 May 15 08:21 /dev/ether1
crw-rw-rw-  1 bin      bin      14 0x020000 May 15 08:21 /dev/lan2
crw-rw-rw-  1 bin      bin      14 0x020001 May 15 08:21 /dev/ether2
```

Explanation

This message refers to files, which contain sensitive information in plain text and therefore should not be publicly and/or group readable or writable. By default these files include confidential key files for uucp as well as the mail directories: Systems, and Permissions, usr/mail/*. Systems, and Permissions are located in the /etc/uucp/ directory, which contain sensitive information in plain text. /var/mail/* files refer to the system mailboxes. All of these files should not be publicly and/or group readable or writable.

Corrective Action

Execute the following: chmod o-rw <filename> or chmod g-rw <filename>

- Improper users' parent directory(s) ownerships/permissions: [directory permissions should not be publicly writable and have appropriate administrative ownerships.]

drwxr-xr-x 14 dsc dba 1024 Jul 9 09:44 /home/

Explanation

In general, a user should have sole control over the files in their $HOME directory. This principle can be compromised if the parent directory(s) of the user $HOME directory (ancestry directories) is owned by a non-administrative login and/or if the ancestry directories' permissions are set improperly. Permissions should be at least mode 755 on any users' ancestry directory(s).

Corrective Action

Execute the following: **chown root /home**
chgrp root /home
chmod 755 /home

(Substitute the appropriate parent directory(s) for the users' directory of your system.)

- Non-standard ownerships: [files should have appropriate administrative ownerships.]

```
-r-------- 1 ids ids 60 Oct 5 2000 /opt/ids/newconfig/etc/opt/ids/critical_files
-r-------- 1 ids ids 89 Oct 6 2000 /opt/ids/bin/gui/Images/cut.gif
-r-------- 1 ids ids 90 Oct 6 2000 /opt/ids/bin/gui/Images/about.gif
-r-------- 1 ids ids 90 Oct 6 2000 /opt/ids/bin/gui/Images/new.gif
-r-------- 1 ids ids 102 Oct 6 2000 /opt/ids/bin/gui/Images/save.gif
-r-------- 1 ids ids 104 Oct 6 2000 /opt/ids/bin/gui/Images/copy.gif
-r-------- 1 ids ids 112 Oct 6 2000 /opt/ids/bin/gui/Images/open.gif
-r-------- 1 ids ids 134 Oct 6 2000 /opt/ids/bin/gui/Images/paste.gif
-r-------- 1 ids ids 183 Oct 6 2000 /opt/ids/bin/gui/Images/Info.gif
-r-------- 1 ids ids 379 Oct 11 2001 /opt/ids/README
-r-------- 1 ids ids 597 Oct 8 2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/login_logout.template

-r-------- 1 ids ids 629 Oct 8 2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/suid.template

-r-------- 1 ids ids 649 Oct 8 2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/sulogFailedsu.template

-r-------- 1 ids ids 650 Oct 8 2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/bufferOverflow.template
```

```
  -r--------  1 ids      ids          663 Oct  6  2000 /opt/ids/bin/gui/Images/notice.jpg

-r--------  1 ids      ids          699 Oct  8  2001
 /opt/ids/newconfig/var/opt/ids/gui/Templates/logins.template

  -r--------  1 ids      ids          715 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/failedLogin.template

  -r--------  1 ids      ids          730 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/TOCTTOU.template

  -r--------  1 ids      ids          769 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/appendOnly_files.template

  -r--------  1 ids      ids          861 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/worldWritable.template
  -r--------  1 ids      ids          890 Oct  6  2000 /opt/ids/bin/gui/Images/disable_add.jpg
  -r--------  1 ids      ids          916 Oct  6  2000 /opt/ids/bin/gui/Images/right_arrow.gif
  -r--------  1 ids      ids          917 Oct  6  2000 /opt/ids/bin/gui/Images/left_arrow.gif
  -r--------  1 ids      ids          924 Oct  6  2000 /opt/ids/bin/gui/Images/redBullet.gif
  -r--------  1 ids      ids          924 Oct  6  2000 /opt/ids/bin/gui/Images/yellowBullet.gif
  -r--------  1 ids      ids          926 Oct  6  2000 /opt/ids/bin/gui/Images/blueBullet.gif

  -r--------  1 ids      ids          945 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/modify_non_owned_files.template

  -r--------  1 ids      ids          972 Oct  6  2000 /opt/ids/bin/gui/Images/error.gif

  -r--------  1 ids      ids         1036 Oct  6  2000 /opt/ids/bin/gui/Images/disable_delete.jpg

  -r--------  1 ids      ids         1068 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceSchedules/FileLoginMixture.sched

  -r--------  1 ids      ids         1075 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceSchedules/LoginMonitoringAlwaysOn.sched

  -r--------  1 ids      ids         1077 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceSchedules/FileModificationsWeekdays.sched

  -r--------  1 ids      ids         1077 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceSchedules/FileModificationsWeekends.sched

  -r--------  1 ids      ids         1078 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceSchedules/FileModificationsWorkHours.sched

  -r--------  1 ids      ids         1082 Jun 13 07:14 /etc/opt/ids/certs/admin/cacert.pem
  -r--------  1 ids      ids         1082 Jun 13 07:15 /etc/opt/ids/certs/agent/cacert.pem

  -r--------  1 ids      ids         1082 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceSchedules/FileAndLoginMonitoringAlwaysOn.sched

  -r--------  1 ids      ids         1157 Oct  6  2000 /opt/ids/bin/gui/Images/find.jpg
  -r--------  1 ids      ids         1178 Oct  6  2000 /opt/ids/bin/gui/Images/add.jpg

  -r--------  1 ids      ids         1265 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/Templates/megaReadOnly.template
```

```
-r--------  1 ids      ids         1269 Oct  6  2000 /opt/ids/bin/gui/Images/alerts.jpg
-r--------  1 ids      ids         1316 Oct  6  2000 /opt/ids/bin/gui/Images/delete.jpg
-r--------  1 ids      ids         1360 Oct  6  2000 /opt/ids/bin/gui/Images/hosts.jpg
-r--------  1 ids      ids         1401 Oct  6  2000 /opt/ids/bin/gui/Images/report.jpg
-r--------  1 ids      ids         1439 Oct  6  2000 /opt/ids/bin/gui/Images/System.jpg
-r--------  1 ids      ids         1500 Oct  6  2000 /opt/ids/bin/gui/Images/find_next.jpg
-r--------  1 ids      ids         1667 Oct  6  2000 /opt/ids/bin/gui/Images/disable_stop.jpg
-r--------  1 ids      ids         1713 Oct  6  2000 /opt/ids/bin/gui/Images/disable_start.jpg
-r--------  1 ids      ids         1809 Oct  6  2000 /opt/ids/bin/gui/Images/disable_status.jpg
-r--------  1 ids      ids         1842 Oct  6  2000 /opt/ids/bin/gui/Images/disable_remove.jpg
-r--------  1 ids      ids         1885 Oct  6  2000 /opt/ids/bin/gui/Images/disable_download.jpg
-r--------  1 ids      ids         1969 Jun 13 07:14 /etc/opt/ids/certs/admin/caprivkey.pem
-r--------  1 ids      ids         2219 Oct  8  2001 /opt/ids/lbin/host_lookup
-r--------  1 ids      ids         2280 Oct  6  2000 /opt/ids/bin/gui/Images/start.jpg
-r--------  1 ids      ids         2331 Jun 27  2001 /opt/ids/bin/gui/Images/status.jpg
-r--------  1 ids      ids         2374 Oct  6  2000 /opt/ids/bin/gui/Images/remove.jpg
-r--------  1 ids      ids         2435 Jun 13 07:14 /etc/opt/ids/certs/admin/sslc-default.cnf
-r--------  1 ids      ids         3027 Jun 13 07:14 /etc/opt/ids/certs/admin/IDS_Admin_KeyStore
-r--------  1 ids      ids         3059 Jun 13 07:15 /etc/opt/ids/certs/agent/agent.pem
-r--------  1 ids      ids         3539 Oct  4  2001 /opt/ids/share/man/man1m/idsgui.1m
-r--------  1 ids      ids         3576 Oct  4  2001 /opt/ids/share/man/man1m/IDS_importAgentKeys.1m
-r--------  1 ids      ids         4067 Oct  6  2000 /opt/ids/bin/gui/Images/doglook.gif

-r--------  1 ids      ids         4684 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceGroups/AdvancedGroup.grp

-r--------  1 ids      ids         4705 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceGroups/LoginMonitoringGroup.grp

-r--------  1 ids      ids         4911 Oct  1  2001 /opt/ids/share/man/man1m/IDS_genAdminKeys.1m

-r--------  1 ids      ids         4977 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceGroups/FileModificationGroup.grp

-r--------  1 ids      ids         5032 Oct  8  2001
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceGroups/AllTemplateGroup.grp

-r--------  1 ids      ids         5153 Oct  4  2001 /opt/ids/share/man/man1m/IDS_genAgentCerts.1m
-r--------  1 ids      ids         5832 Oct  4  2001 /opt/ids/share/man/man1m/idsadmin.1m
-r--------  1 ids      ids         6093 Sep 21  2001 /opt/ids/share/man/man1m/idsagent.1m
-r--------  1 ids      ids         6120 Oct  6  2000 /opt/ids/bin/gui/Images/ErrorIcon.jpg
-r--------  1 ids      ids         6470 Oct  6  2000 /opt/ids/bin/gui/Images/MarkUnseen.jpg
-r--------  1 ids      ids         6808 Oct  6  2000 /opt/ids/bin/gui/Images/MarkSeen.jpg
-r--------  1 ids      ids         7045 Oct  6  2000 /opt/ids/bin/gui/Images/Dragon.jpg
-r--------  1 ids      ids         7228 Jun 27  2001 /opt/ids/bin/gui/Images/Help.jpg
-r--------  1 ids      ids         7308 Jun 27  2001 /opt/ids/bin/gui/Images/redo.jpg
-r--------  1 ids      ids         7370 Jun 27  2001 /opt/ids/bin/gui/Images/stop.jpg
-r--------  1 ids      ids         7370 Jun 27  2001 /opt/ids/bin/gui/Images/undo.jpg
-r--------  1 ids      ids         7522 Jun 27  2001 /opt/ids/bin/gui/Images/save.jpg
-r--------  1 ids      ids         7622 Jun 28  2001 /opt/ids/bin/gui/Images/download.jpg
-r--------  1 ids      ids         7733 Jun 27  2001 /opt/ids/bin/gui/Images/cancelAll.jpg
-r--------  1 ids      ids         7932 Jun 27  2001 /opt/ids/bin/gui/Images/resync.jpg
-r--------  1 ids      ids         8319 Oct  6  2000 /opt/ids/bin/gui/Images/AllNotSeen.jpg
-r--------  1 ids      ids         9013 Oct  6  2000 /opt/ids/bin/gui/Images/AllSeen.jpg
-r--------  1 ids      ids         9299 Mar 18 14:09 /opt/ids/lbin/ids_checkJavaVersion
```

```
-r--------  1 ids      ids       9369 Oct  6  2000 /opt/ids/bin/gui/Images/NextIcon.jpg
-r--------  1 ids      ids      14491 Feb 22  2002 /opt/ids/share/man/man5/ids.cf.5
-r--------  1 ids      ids      16849 Jul 25 10:04 /etc/opt/ids/ids.cf
-r--------  1 ids      ids      16870 Feb 21  2002 /opt/ids/newconfig/etc/opt/ids/ids.cf
-r--------  1 ids      ids      75743 Oct  6  2000 /opt/ids/bin/gui/symlib/jsdk.jar
-r--------  1 ids      ids     105663 Oct 23  2000 /opt/ids/bin/gui/symlib/templates.jar
-r--------  1 ids      ids     115061 Oct 23  2000 /opt/ids/bin/gui/symlib/symtools.jar
-r--------  1 ids      ids     124068 Oct  6  2000 /opt/ids/bin/gui/symlib/icebrowserbean.jar
-r--------  1 ids      ids     176659 Jun 21  2001 /opt/ids/bin/gui/javaHelp/jsearch.jar
-r--------  1 ids      ids     184564 Jun 21  2001 /opt/ids/bin/gui/javaHelp/jhtools.jar
-r--------  1 ids      ids     210514 Jun 21  2001 /opt/ids/bin/gui/javaHelp/jhbasic.jar
-r--------  1 ids      ids     236799 Oct  6  2000 /opt/ids/bin/gui/symlib/Olite35.jar
-r--------  1 ids      ids     240568 Oct  6  2000 /opt/ids/bin/gui/symlib/collections.zip
-r--------  1 ids      ids     343864 Jun 21  2001 /opt/ids/bin/gui/javaHelp/jh.jar
-r--------  1 ids      ids     354106 Oct  6  2000 /opt/ids/bin/gui/symlib/dbaw.zip
-r--------  1 ids      ids     394331 Jun 21  2001 /opt/ids/bin/gui/javaHelp/jhall.jar
-r--------  1 ids      ids     868731 Oct  6  2000 /opt/ids/bin/gui/symlib/sfc.jar
-r--------  1 ids      ids    1656792 Oct 23  2000 /opt/ids/bin/gui/symlib/symbeans.jar
-r--------  1 ids      ids    2420388 Oct  6  2000 /opt/ids/bin/gui/symlib/swingall.jar
-r--------  1 ids      ids    5121484 Oct 23  2000 /opt/ids/bin/gui/symlib/symclass.zip
-r--------  1 ids      ids    8806125 Oct  6  2000 /opt/ids/bin/gui/symlib/classes.zip
-r-sr-x---  1 root     ids     266240 Mar 22 09:47 /opt/ids/lbin/idssysdsp
-r-sr-x---  1 root     ids     274432 Mar 22 10:01 /opt/ids/lbin/updaterc
-r-x------  1 ids      ids        267 Mar  5  2001 /opt/ids/share/examples/progsuid
-r-x------  1 ids      ids        316 Mar  5  2001 /opt/ids/share/examples/progfailedLogin
-r-x------  1 ids      ids        423 Mar  5  2001 /opt/ids/share/examples/progsufl
-r-x------  1 ids      ids        569 Mar  5  2001 /opt/ids/share/examples/prog2
-r-x------  1 ids      ids        573 Aug 23  2001 /opt/ids/response/send_alert_to_vpo.sh
-r-x------  1 ids      ids        615 Mar  5  2001 /opt/ids/share/examples/progmegaReadOnly
-r-x------  1 ids      ids        677 Mar  5  2001 /opt/ids/share/examples/prog3sigs
-r-x------  1 ids      ids       1641 Mar  5  2001 /opt/ids/share/examples/allSigsEveryday
-r-x------  1 ids      ids       1751 Sep 28  2001 /opt/ids/lbin/idsConvert
-r-x------  1 ids      ids       1756 Oct  9  2001 /opt/ids/bin/IDS_checkAdminCert
-r-x------  1 ids      ids       1958 Oct  9  2001 /opt/ids/bin/IDS_checkAgentCert
-r-x------  1 ids      ids       2578 Feb 15  2002 /opt/ids/share/examples/ids_alertResponse.c
-r-x------  1 ids      ids       2820 Feb 20  2002 /sbin/init.d/idsagent
-r-x------  1 ids      ids       2879 Feb 15  2002 /opt/ids/bin/IDS_checkInstall
-r-x------  1 ids      ids       3098 Jul 17  2001 /opt/ids/bin/gui/jnet.jar
-r-x------  1 ids      ids       3248 Oct 15  2001 /opt/ids/bin/IDS_importAgentKeys
-r-x------  1 ids      ids       5559 Jul 18  2001 /opt/ids/bin/gui/License/License.txt
-r-x------  1 ids      ids       7100 Jul 25 08:08 /opt/ids/bin/idsgui
-r-x------  1 ids      ids       7637 Jul 17  2001 /opt/ids/bin/gui/jcert.jar
-r-x------  1 ids      ids       9668 Mar  5  2001 /opt/ids/share/examples/allSigsMonSatEachday
-r-x------  1 ids      ids      12318 Oct  6  2000 /opt/ids/lib/libecsMDL.sl
-r-x------  1 ids      ids      14486 Oct 12  2001 /opt/ids/bin/IDS_genAgentCerts
-r-x------  1 ids      ids      16384 Mar 22 09:45 /opt/ids/response/ids_alertResponse
-r-x------  1 ids      ids      16384 Mar 22 09:47 /opt/ids/response/vpo/ids_vpoalert
-r-x------  1 ids      ids      18941 Oct 12  2001 /opt/ids/bin/IDS_genAdminKeys
-r-x------  1 ids      ids      24576 Aug 16  2001 /opt/ids/lbin/getservbyname
-r-x------  1 ids      ids      40366 Oct  6  2000 /opt/ids/templates/unusualSystemState.eco
-r-x------  1 ids      ids      40960 Mar 22 09:45 /opt/ids/lbin/idssc
-r-x------  1 ids      ids      42444 Mar 22 09:47 /opt/ids/lib/mdl.md
-r-x------  1 ids      ids      71726 Oct  6  2000 /opt/ids/templates/logins.eco
-r-x------  1 ids      ids      74841 Oct 23  2000 /opt/ids/templates/sulogFailedsu.eco
-r-x------  1 ids      ids      78770 Oct  6  2000 /opt/ids/templates/login_logout.eco
-r-x------  1 ids      ids      87435 Oct  6  2000 /opt/ids/templates/failedLogin.eco
```

```
-r-x------  1 ids      ids      228194 Oct 23  2000 /opt/ids/templates/appendOnly_files.eco
-r-x------  1 ids      ids      229176 Oct  6  2000 /opt/ids/templates/suid.eco
-r-x------  1 ids      ids      259035 Oct  6  2000 /opt/ids/templates/worldWritable.eco
-r-x------  1 ids      ids      346315 Oct  6  2000 /opt/ids/templates/bufferOverflow.eco
-r-x------  1 ids      ids      385024 Mar 22 09:47 /opt/ids/lbin/idskerndsp
-r-x------  1 ids      ids      391106 Oct  6  2000 /opt/ids/templates/megaReadOnly.eco
-r-x------  1 ids      ids      401746 Oct 23  2000 /opt/ids/templates/TOCTTOU.eco
-r-x------  1 ids      ids      408922 Oct  6  2000 /opt/ids/templates/modify_non_owned_files.eco
-r-x------  1 ids      ids      463863 Jul 17  2001 /opt/ids/bin/gui/jsse.jar
-r-x------  1 ids      ids      622592 Mar 22 09:49 /opt/ids/bin/idsadmin
-r-x------  1 ids      ids      741376 Mar 22 09:45 /opt/ids/bin/idsagent
-r-x------  1 ids      ids     1095172 Jun 29  2001 /opt/ids/lbin/sslc
-r-x------  1 ids      ids     1478656 Mar 22 09:46 /opt/ids/lbin/idscor
-r-x------  1 ids      ids     4082036 Mar 22 10:10 /opt/ids/bin/gui/idsgui.jar
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmcksum
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmdiag
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmdown
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmhostid
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmremove
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmreread
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmstat
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmswitchr
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmutil
-r-xr-xr-x 10 bevb     adm      264192 Jun 20 15:46 /usr/local/flexlm/bin/lmver
-rw-------  1 ids      ids           0 Jul 29 14:37 /etc/opt/ids/gui/config/HostTags.txt
-rw-------  1 ids      ids           9 Jun 13 07:15 /etc/opt/ids/certs/admin/serial.ids
-rw-------  1 ids      ids          60 Oct  5  2000 /etc/opt/ids/critical_files
-rw-------  1 ids      ids          64 Jul 29 08:58 /etc/opt/ids/gui/config/sentinal.hosts
-rw-------  1 ids      ids         905 Jun 24 13:44 /etc/opt/ids/gui/config/sentinal.props
-rw-------  1 ids      ids        1114 Jun 13 07:15 /etc/opt/ids/certs/admin/index.ids
-rw-r--r--  1 root     users       636 Jan 10  2000 /opt/cifsclient/README
-rw-r--r--  1 root     users      2159 Dec  9  1999 /etc/opt/samba/smb.conf
-rw-r--r--  1 root     users      2159 Dec  9  1999 /etc/opt/samba/smb.conf.default
-rw-r--r--  1 root     users      2159 Dec  9  1999 /opt/samba/newconfig/etc/opt/samba/smb.conf
-rw-r--r--  1 root     users      2784 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapNeXT.cfg
-rw-r--r--  1 root     users      2994 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap8859-6.cfg
-rw-r--r--  1 root     users      3099 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap8859-8.cfg
-rw-r--r--  1 root     users      3156 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapJIS201.cfg
-rw-r--r--  1 root     users      3573 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap8859-3.cfg
-rw-r--r--  1 root     users      3578 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap8859-7.cfg
-rw-r--r--  1 root     users      3670 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap8859-9.cfg
-rw-r--r--  1 root     users      3671 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap8859-5.cfg
-rw-r--r--  1 root     users      3683 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap8859-1.cfg
-rw-r--r--  1 root     users      3683 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap8859-2.cfg
-rw-r--r--  1 root     users      3684 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap8859-4.cfg
-rw-r--r--  1 root     users      3725 Jun 21  2000 /etc/opt/cifsclient/unitables/unimap8859-15.cfg
-rw-r--r--  1 root     users      4205 Sep 12  2000 /etc/opt/cifsclient/unitables/README
-rw-r--r--  1 root     users      4629 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP737.cfg
-rw-r--r--  1 root     users      4630 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP862.cfg
-rw-r--r--  1 root     users      4630 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP865.cfg
-rw-r--r--  1 root     users      4631 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP863.cfg
-rw-r--r--  1 root     users      4632 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP437.cfg
-rw-r--r--  1 root     users      4632 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP855.cfg
-rw-r--r--  1 root     users      4633 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP861.cfg
-rw-r--r--  1 root     users      4634 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP775.cfg
-rw-r--r--  1 root     users      4634 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP860.cfg
```

```
  -rw-r--r--  1 root     users        4635 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP850.cfg
  -rw-r--r--  1 root     users        4635 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP852.cfg
  -rw-r--r--  1 root     users        4640 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP866.cfg
  -rw-r--r--  1 root     users        4643 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP857.cfg
  -rw-r--r--  1 root     users        4654 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP864.cfg
  -rw-r--r--  1 root     users        4667 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP869.cfg
  -rw-r--r--  1 root     users        4756 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapCP874.cfg
  -rw-r--r--  1 root     users       14116 Mar 28  2001 /etc/opt/cifsclient/cifsclient.cfg
  -rw-r--r--  1 root     users       14116 Mar 28  2001 /etc/opt/cifsclient/cifsclient.cfg.default
  -rw-r--r--  1 root     users       14116 Mar 28  2001
/opt/cifsclient/newconfig/etc/opt/cifsclient/cifsclient.cfg
  -rw-r--r--  1 root     users       38468 Jul 21  1999 /etc/opt/cifsclient/unitables/unicase.cfg
  -rw-r--r--  1 root     users       95746 Mar 28  2001
/opt/cifsclient/HP_Docs/CIFS9k_Client_Rel_Notes.pdf
  -rw-r--r--  1 root     users      161593 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapShiftJIS-std.cfg
  -rw-r--r--  1 root     users      161893 Jul 21  1999 /etc/opt/cifsclient/unitables/unimap-eucJP.cfg
  -rw-r--r--  1 root     users      161985 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapShiftJIS.cfg
  -rw-r--r--  1 root     users      191947 Sep 12  2000 /etc/opt/cifsclient/unitables/unimap-eucKR.cfg
  -rw-r--r--  1 root     users      298617 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapJIS.cfg
  -rw-r--r--  1 root     users      302409 Jul 21  1999 /etc/opt/cifsclient/unitables/unimapBig5.cfg
  -rw-r--r--  1 root     users      607332 Mar 28  2001 /opt/cifsclient/HP_Docs/CIFS9k_Client_Manual.pdf

  -rw-rw-r--  1 20000    12064        131 Jul 13  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/4/4aedbe38.002

  -rw-rw-r--  1 20000    12064        131 Jun 19  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/4/4aedbe38.001

  -rw-rw-r--  1 20000    12064        159 Jul 13  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2d6c22d4.002

  -rw-rw-r--  1 20000    12064        159 Jun 19  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2d6c22d4.001

  -rw-rw-r--  1 20000    12064        245 Jul 13  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2c1ea82a.002

  -rw-rw-r--  1 20000    12064        245 Jun 19  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2c1ea82a.001

  -rw-rw-r--  1 20000    12064        249 Jul 13  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2d0d1e06.002

  -rw-rw-r--  1 20000    12064        249 Jun 19  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2d0d1e06.001

  -rw-rw-r--  1 20000    12064        270 Jul 13  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2afd7d40.002

  -rw-rw-r--  1 20000    12064        270 Jun 19  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2afd7d40.001

  -rw-rw-r--  1 20000    12064        298 Jul 13  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2aa09af8.002
```

-rw-rw-r-- 1 20000 12064 298 Jun 19 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2aa09af8.001

-rw-rw-r-- 1 20000 12064 309 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2cddcdc2.002

-rw-rw-r-- 1 20000 12064 309 Jun 19 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2cddcdc2.001

-rw-rw-r-- 1 20000 12064 392 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2a71926c.002

-rw-rw-r-- 1 20000 12064 392 Jun 19 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2a71926c.001

-rw-rw-r-- 1 20000 12064 476 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2cae2a2c.002

-rw-rw-r-- 1 20000 12064 476 Jun 19 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2cae2a2c.001

-rw-rw-r-- 1 20000 12064 518 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2d3d292a.002

-rw-rw-r-- 1 20000 12064 518 Jun 19 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2d3d292a.001

-rw-rw-r-- 1 20000 12064 577 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2aceee76.002

-rw-rw-r-- 1 20000 12064 577 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2dca6362.002

-rw-rw-r-- 1 20000 12064 577 Jun 19 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2aceee76.001

-rw-rw-r-- 1 20000 12064 577 Jun 19 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2dca6362.001

-rw-rw-r-- 1 20000 12064 598 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2beb6546.002

-rw-rw-r-- 1 20000 12064 598 Jun 19 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2beb6546.001

-rw-rw-r-- 1 20000 12064 724 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2dfd674e.002

-rw-rw-r-- 1 20000 12064 724 Jun 19 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2dfd674e.001

-rw-rw-r-- 1 20000 12064 1500 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/instr.map

-rw-rw-r-- 1 20000 12064 1571 Jul 13 2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2d9aabb8.002

```
  -rw-rw-r--   1 20000      12064        1571 Jun 19  2001
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2/2d9aabb8.001

  -rw-rw-r--   1 oracle     dba           27 Aug  2 13:11 /etc/oratab
  -rw-rw-rw-   1 bevb       adm          1520 Jun 21 10:07 /usr/local/flexlm/bin/logfile
  -rwsr-xr-x   1 root       users       49152 Mar 28  2001 /opt/cifsclient/bin/cifslist
  -rwsr-xr-x   1 root       users       49152 Mar 28  2001 /opt/cifsclient/bin/cifslogout
  -rwsr-xr-x   1 root       users       53248 Mar 28  2001 /opt/cifsclient/bin/cifslogin
  -rwxr-xr-x   1 oracle     sys          2316 Jun 14 18:21 /usr/local/bin/coraenv
  -rwxr-xr-x   1 oracle     sys          2417 Jun 14 18:21 /usr/local/bin/dbhome
  -rwxr-xr-x   1 oracle     sys          2512 Jun 14 18:21 /usr/local/bin/oraenv
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/client/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/codepages/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/nmbd/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/printing/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/rpc_parse/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/rpc_server/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/script/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/smbd/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/tests/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul  7  1999 /opt/samba_src/samba/source/web/.cvsignore
  -rwxr-xr-x   1 root       users           0 Jul 21  2000 /opt/samba_src/samba/source/bin/.dummy
  -rwxr-xr-x   1 root       users           8 Jun 21  2001 /etc/opt/samba/codepages/codepage.932
  -rwxr-xr-x   1 root       users           8 Jun 21  2001 /etc/opt/samba/codepages/codepage.936
  -rwxr-xr-x   1 root       users           8 Jun 21  2001 /etc/opt/samba/codepages/codepage.949
  -rwxr-xr-x   1 root       users           8 Jun 21  2001 /etc/opt/samba/codepages/codepage.950
  -rwxr-xr-x   1 root       users           8 Jun 23  2000 /opt/samba_src/samba/source/include/.cvsignore
  -rwxr-xr-x   1 root       users          11 Nov 12  1999 /opt/samba/docs/yodldocs/.cvsignore
  -rwxr-xr-x   1 root       users          13 Jul  7  1999 /opt/samba_src/samba/source/lib/.cvsignore
  -rwxr-xr-x   1 root       users          13 Jul  7  1999 /opt/samba_src/samba/source/libsmb/.cvsignore
  -rwxr-xr-x   1 root       users          13 Jul  7  1999 /opt/samba_src/samba/source/param/.cvsignore
  -rwxr-xr-x   1 root       users          13 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/.cvsignore
  -rwxr-xr-x   1 root       users          21 Jul  7  1999 /opt/samba_src/samba/source/tests/trivial.c
  -rwxr-xr-x   1 root       users          24 May 16  2001 /opt/samba_src/samba/source/include/version.h
  -rwxr-xr-x   1 root       users          29 Jul 22  1999 /opt/samba_src/samba/source/include/stamp-h.in
  -rwxr-xr-x   1 root       users          44 Jul  7  1999 /opt/samba/examples/simple/README
  -rwxr-xr-x   1 root       users          44 Jun 21  2001 /opt/samba/swat/include/footer.html
  -rwxr-xr-x   1 root       users          46 Jul  7  1999 /opt/samba/examples/tridge/smb.conf.vittjokk
  -rwxr-xr-x   1 root       users          55 Jul  7  1999 /opt/samba/examples/tridge/smb.conf.WinNT
  -rwxr-xr-x   1 root       users          55 Jul  7  1999 /opt/samba/examples/tridge/smb.conf.lapland
  -rwxr-xr-x   1 root       users          60 Jul  7  1999 /opt/samba_src/samba/source/smbwrapper/.cvsignore
  -rwxr-xr-x   1 root       users          63 Jun 23  2000 /opt/samba_src/samba/source/.cvsignore
  -rwxr-xr-x   1 root       users         114 Jul  7  1999 /opt/samba/examples/printer-accounting/acct-all
  -rwxr-xr-x   1 root       users         120 Jul 21  2000 /opt/samba_src/samba/source/configure.developer
  -rwxr-xr-x   1 root       users         122 Jul  7  1999 /opt/samba/docs/Win95_PlainPassword.reg
  -rwxr-xr-x   1 root       users         122 Jul  7  1999 /opt/samba/docs/Win98_PlainPassword.reg
  -rwxr-xr-x   1 root       users         131 May 16  2001 /opt/samba/docs/textdocs/MIRRORS.txt
  -rwxr-xr-x   1 root       users         132 Jun 21  2001 /etc/opt/samba/codepages/codepage.850
  -rwxr-xr-x   1 root       users         140 Jun 21  2001 /etc/opt/samba/codepages/codepage.1251

  -rwxr-xr-x   1 root       users         148 Jul  7  1999
/opt/samba_src/samba/source/script/extract_allparms.sh

  -rwxr-xr-x   1 root       users         148 Jun 21  2001 /etc/opt/samba/codepages/codepage.737
  -rwxr-xr-x   1 root       users         150 Jul  7  1999 /opt/samba/examples/tridge/smb.conf.fjall
```

```
  -rwxr-xr-x   1 root      users         155 Jul  7  1999 /opt/samba/examples/dce-dfs/README
  -rwxr-xr-x   1 root      users         172 Jun 21  2001 /etc/opt/samba/codepages/codepage.852
  -rwxr-xr-x   1 root      users         190 Jul  7  1999 /opt/samba/docs/Win9X-CacheHandling.reg
  -rwxr-xr-x   1 root      users         196 Jun 21  2001 /etc/opt/samba/codepages/codepage.437
  -rwxr-xr-x   1 root      users         199 Nov 12  1999 /opt/samba_src/samba/source/include/interfaces.h
  -rwxr-xr-x   1 root      users         205 Jul  7  1999
/opt/samba_src/samba/source/script/mksmbpasswd.sh
  -rwxr-xr-x   1 root      users         213 May 16  2001 /opt/samba/docs/textdocs/Support.txt
  -rwxr-xr-x   1 root      users         217 Nov 12  1999 /opt/samba_src/samba/source/web/po/swatlang.h
  -rwxr-xr-x   1 root      users         230 Nov 12  1999 /opt/samba/docs/WindowsTerminalServer.reg
  -rwxr-xr-x   1 root      users         270 Jul  7  1999 /opt/samba_src/samba/source/script/revert.sh
  -rwxr-xr-x   1 root      users         283 Jul  7  1999 /opt/samba/examples/README
  -rwxr-xr-x   1 root      users         287 Jul  7  1999 /opt/samba_src/samba/source/include/clitar.h

  -rwxr-xr-x   1 root      users         292 Dec  9  1999
/opt/samba_src/samba/source/configure_hp_options.sh

  -rwxr-xr-x   1 root      users         297 Jun 21  2001 /opt/samba/swat/include/header.html
  -rwxr-xr-x   1 root      users         303 Jul  7  1999 /opt/samba/docs/NT4_PlainPassword.reg
  -rwxr-xr-x   1 root      users         303 Jul 22  1999 /opt/samba/docs/Win2000_PlainPassword.reg
  -rwxr-xr-x   1 root      users         320 Jun 21  2001 /opt/samba/swat/using_samba/gifs/txthome.gif
  -rwxr-xr-x   1 root      users         321 Jul  7  1999 /opt/samba_src/samba/source/tests/README

  -rwxr-xr-x   1 root      users         322 Jul  7  1999
/opt/samba_src/samba/source/script/updatesmbpasswd.sh

  -rwxr-xr-x   1 root      users         341 Jul  7  1999 /opt/samba/examples/tridge/README
  -rwxr-xr-x   1 root      users         388 Jun 21  2001 /etc/opt/samba/codepages/codepage.775
  -rwxr-xr-x   1 root      users         390 Jul  7  1999 /opt/samba_src/samba/source/tests/ftruncate.c
  -rwxr-xr-x   1 root      users         419 Jun 21  2001 /opt/samba/swat/using_samba/gifs/txtnexta.gif
  -rwxr-xr-x   1 root      users         436 Nov 12  1999 /opt/samba/examples/wins_hook/README

  -rwxr-xr-x   1 root      users         446 Jul  7  1999
/opt/samba_src/samba/source/script/convert_smbpasswd

  -rwxr-xr-x   1 root      users         446 Jun 21  2001 /opt/samba/bin/convert_smbpasswd
  -rwxr-xr-x   1 root      users         446 Jun 21  2001 /opt/samba/script/convert_smbpasswd
  -rwxr-xr-x   1 root      users         460 Jun 21  2001 /etc/opt/samba/codepages/codepage.861
  -rwxr-xr-x   1 root      users         497 Nov 12  1999 /opt/samba/examples/autofs/README
  -rwxr-xr-x   1 root      users         560 Jul  7  1999 /opt/samba/examples/printer-accounting/printcap
  -rwxr-xr-x   1 root      users         562 Apr  4  2000 /opt/samba_src/samba/source/script/installexs.sh
  -rwxr-xr-x   1 root      users         565 Jun 21  2001 /opt/samba/swat/using_samba/gifs/index.gif
  -rwxr-xr-x   1 root      users         569 Jun 21  2001 /opt/samba/swat/images/shares.gif
  -rwxr-xr-x   1 root      users         578 Jun 21  2001 /opt/samba/swat/images/status.gif
  -rwxr-xr-x   1 root      users         580 Jun 21  2001 /opt/samba/swat/images/home.gif
  -rwxr-xr-x   1 root      users         584 Oct 10  2000 /opt/samba/script/samba_init
  -rwxr-xr-x   1 root      users         588 Jun 21  2001 /etc/opt/samba/codepages/codepage.866
  -rwxr-xr-x   1 root      users         588 Jun 21  2001 /opt/samba/swat/using_samba/gifs/txtpreva.gif
  -rwxr-xr-x   1 root      users         610 Jul  7  1999 /opt/samba/docs/faq/sambafaq-5.html
  -rwxr-xr-x   1 root      users         613 Jun 21  2001 /opt/samba/swat/images/passwd.gif
  -rwxr-xr-x   1 root      users         628 Jun 21  2001 /opt/samba/swat/images/globals.gif
  -rwxr-xr-x   1 root      users         638 Jul  7  1999 /opt/samba/docs/faq/Samba-meta-FAQ-6.html
  -rwxr-xr-x   1 root      users         663 Jul  7  1999 /opt/samba/examples/svr4-startup/README
  -rwxr-xr-x   1 root      users         671 Nov  3  1999 /opt/samba_src/samba/source/script/uninstallexs.sh
  -rwxr-xr-x   1 root      users         675 Nov  3  1999 /opt/samba_src/samba/source/script/uninstallsrc.sh
  -rwxr-xr-x   1 root      users         686 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/README.UBI
```

```
  -rwxr-xr-x   1 root      users         695 Jul  7  1999 /opt/samba/examples/printer-accounting/acct-sum
  -rwxr-xr-x   1 root      users         705 Jun 21  2001 /opt/samba/swat/images/printers.gif

  -rwxr-xr-x   1 root      users         719 Jul  7  1999
/opt/samba_src/samba/source/script/mknissmbpasswd.sh

  -rwxr-xr-x   1 root      users         726 Jul  7  1999 /opt/samba_src/samba/source/include/vt_mode.h
  -rwxr-xr-x   1 root      users         744 Jun 21  2001 /opt/samba/man/man8/smbumount.8
  -rwxr-xr-x   1 root      users         744 May 16  2001 /opt/samba/docs/manpages/smbumount.8
  -rwxr-xr-x   1 root      users         746 Jul 22  1999 /opt/samba/examples/printer-accounting/lp-acct
  -rwxr-xr-x   1 root      users         772 Jan 10  2000 /opt/samba/README
  -rwxr-xr-x   1 root      users         777 Jul  7  1999 /opt/samba/docs/NT4-Locking.reg
  -rwxr-xr-x   1 root      users         777 Jul  7  1999 /opt/samba_src/samba/source/script/uninstallman.sh
  -rwxr-xr-x   1 root      users         793 Jul  7  1999 /opt/samba/examples/dce-dfs/smb.conf
  -rwxr-xr-x   1 root      users         796 May 16  2000 /opt/samba_src/samba/source/script/installdocs.sh
  -rwxr-xr-x   1 root      users         798 Mar 27  2001 /etc/opt/cifsclient/pam/smb.conf
  -rwxr-xr-x   1 root      users         798 Mar 27  2001 /etc/opt/cifsclient/pam/smb.conf.default

  -rwxr-xr-x   1 root      users         798 Mar 27  2001
/opt/cifsclient/pam/newconfig/etc/opt/cifsclient/pam/smb.conf

  -rwxr-xr-x   1 root      users         807 May 16  2001 /opt/samba/docs/textdocs/SCO.txt
  -rwxr-xr-x   1 root      users         812 May 16  2001 /opt/samba/docs/textdocs/CRLF-LF-
Conversions.txt
  -rwxr-xr-x   1 root      users         820 Jun 21  2001 /opt/samba/swat/images/viewconfig.gif

  -rwxr-xr-x   1 root      users         840 Jul  7  1999
/opt/samba_src/samba/source/script/mknissmbpwdtbl.sh

  -rwxr-xr-x   1 root      users         862 Jul  7  1999 /opt/samba_src/samba/source/smbwrapper/init.c
  -rwxr-xr-x   1 root      users         865 Jul 21  2000 /opt/samba_src/samba/source/tests/sgi_sysv_hack.c
  -rwxr-xr-x   1 root      users         869 Jul  7  1999 /opt/samba_src/samba/source/script/uninstallcp.sh
  -rwxr-xr-x   1 root      users         880 Jul  7  1999 /opt/samba/examples/svr4-startup/samba.server
  -rwxr-xr-x   1 root      users         896 Jul  7  1999
/opt/samba_src/samba/source/script/uninstallscripts.sh
  -rwxr-xr-x   1 root      users         897 Jan 20  2000 /etc/rc.config.d/samba
  -rwxr-xr-x   1 root      users         897 Jan 20  2000 /opt/samba/newconfig/etc/rc.config.d/samba
  -rwxr-xr-x   1 root      users         897 Jan 20  2000 /opt/samba/script/samba_config
  -rwxr-xr-x   1 root      users         915 Nov 12  1999 /opt/samba_src/samba/source/web/po/Makefile
  -rwxr-xr-x   1 root      users         937 Jul  7  1999 /opt/samba_src/samba/source/script/uninstallbin.sh
  -rwxr-xr-x   1 root      users         950 Jul 21  2000 /opt/samba/docs/samba.lsm

  -rwxr-xr-x   1 root      users         955 Jul  7  1999
/opt/samba_src/samba/source/codepages/codepage_def.932

  -rwxr-xr-x   1 root      users         960 Jul  7  1999 /opt/samba/docs/textdocs/INSTALL.sambatar
  -rwxr-xr-x   1 root      users         967 May 16  2000
/opt/samba_src/samba/source/script/uninstalldocs.sh
  -rwxr-xr-x   1 root      users         998 Jul 22  1999 /opt/samba/examples/printer-accounting/hp5-redir
  -rwxr-xr-x   1 root      users        1003 Nov  3  1999 /opt/samba_src/samba/source/script/installsrc.sh

  -rwxr-xr-x   1 root      users        1013 Jul  7  1999
/opt/samba_src/samba/source/codepages/codepage_def.949

  -rwxr-xr-x   1 root      users        1013 Jul 21  2000 /opt/samba_src/samba/source/include/talloc.h
```

```
  -rwxr-xr-x  1 root     users       1019 Jul  7  1999
/opt/samba_src/samba/source/codepages/codepage_def.936

  -rwxr-xr-x  1 root     users       1019 Jul  7  1999
/opt/samba_src/samba/source/codepages/codepage_def.950

  -rwxr-xr-x  1 root     users       1031 Nov 12  1999 /opt/samba_src/samba/source/script/installbin.sh
  -rwxr-xr-x  1 root     users       1043 Jul 21  2000 /opt/samba_src/samba/source/script/installcp.sh
  -rwxr-xr-x  1 root     users       1046 Jul  7  1999 /opt/samba_src/samba/source/smbwrapper/smbsh.in
  -rwxr-xr-x  1 root     users       1079 Jul 22  1999 /opt/samba/docs/NT4-Locking.txt
  -rwxr-xr-x  1 root     users       1090 Jun 21  2001 /opt/samba/man/man8/smbmnt.8
  -rwxr-xr-x  1 root     users       1090 May 16  2001 /opt/samba/docs/manpages/smbmnt.8
  -rwxr-xr-x  1 root     users       1109 Nov 12  1999
/opt/samba_src/samba/source/script/installscripts.sh
  -rwxr-xr-x  1 root     users       1115 Nov 12  1999 /opt/samba_src/samba/source/tests/summary.c
  -rwxr-xr-x  1 root     users       1121 May 16  2001 /opt/samba/docs/textdocs/Macintosh_Clients.txt
  -rwxr-xr-x  1 root     users       1124 Jul 21  2000 /opt/samba/docs/yodldocs/smbmnt.8.yo
  -rwxr-xr-x  1 root     users       1152 Jul  7  1999 /opt/samba/docs/textdocs/README.sambatar
  -rwxr-xr-x  1 root     users       1155 Jul  7  1999 /opt/samba_src/samba/source/tests/ftruncroot.c
  -rwxr-xr-x  1 root     users       1171 Jul  7  1999 /opt/samba/docs/faq/sambafaq-4.html
  -rwxr-xr-x  1 root     users       1173 Jul 22  1999 /opt/samba_src/samba/source/tests/shared_mmap.c
  -rwxr-xr-x  1 root     users       1190 Jul  7  1999 /opt/samba/docs/faq/Samba-meta-FAQ-5.html
  -rwxr-xr-x  1 root     users       1295 Jul 21  2000 /opt/samba_src/samba/source/include/profile.h
  -rwxr-xr-x  1 root     users       1307 Jul  7  1999 /opt/samba_src/samba/source/smbd/noquotas.c
  -rwxr-xr-x  1 root     users       1325 Jul  7  1999 /opt/samba_src/samba/source/tests/getgroups.c
  -rwxr-xr-x  1 root     users       1328 Jun 21  2001 /opt/samba/swat/using_samba/this_edition.html
  -rwxr-xr-x  1 root     users       1355 Jul  7  1999
/opt/samba_src/samba/source/smbwrapper/realcalls.c
  -rwxr-xr-x  1 root     users       1360 Jul  7  1999 /opt/samba_src/samba/source/tests/crypttest.c
  -rwxr-xr-x  1 root     users       1539 Jul  7  1999 /opt/samba_src/samba/source/smbwrapper/smbw.h
  -rwxr-xr-x  1 root     users       1539 Jul  7  1999 /opt/samba_src/samba/source/tests/sysv_ipc.c
  -rwxr-xr-x  1 root     users       1550 Jul 21  2000 /opt/samba/docs/htmldocs/smbmnt.8.html
  -rwxr-xr-x  1 root     users       1550 Jun 21  2001 /opt/samba/swat/help/smbmnt.8.html
  -rwxr-xr-x  1 root     users       1566 Jul  7  1999 /opt/samba_src/samba/source/script/installman.sh
  -rwxr-xr-x  1 root     users       1590 Jul  7  1999 /opt/samba_src/samba/source/include/dlinklist.h
  -rwxr-xr-x  1 root     users       1597 Jul  7  1999 /opt/samba_src/samba/source/lib/slprintf.c
  -rwxr-xr-x  1 root     users       1646 Jun 21  2001 /opt/samba/man/man1/stopsmb.1
  -rwxr-xr-x  1 root     users       1646 Mar 22  2000 /opt/samba/docs/manpages/stopsmb.1
  -rwxr-xr-x  1 root     users       1682 Jun 21  2001 /opt/samba/man/man1/startsmb.1
  -rwxr-xr-x  1 root     users       1682 Mar 22  2000 /opt/samba/docs/manpages/startsmb.1
  -rwxr-xr-x  1 root     users       1697 Jul 22  1999 /opt/samba_src/samba/source/tests/fcntl_lock.c
  -rwxr-xr-x  1 root     users       1708 Jul  7  1999 /opt/samba_src/samba/source/script/addtosmbpass
  -rwxr-xr-x  1 root     users       1708 Jun 21  2001 /opt/samba/bin/addtosmbpass
  -rwxr-xr-x  1 root     users       1708 Jun 21  2001 /opt/samba/script/addtosmbpass
  -rwxr-xr-x  1 root     users       1716 May 16  2001 /opt/samba/docs/textdocs/DNIX.txt
  -rwxr-xr-x  1 root     users       1731 Jul  7  1999 /opt/samba/docs/textdocs/SMBTAR.notes
  -rwxr-xr-x  1 root     users       1735 Jul  7  1999 /opt/samba_src/samba/source/web/diagnose.c
  -rwxr-xr-x  1 root     users       1814 Mar 22  2000 /opt/samba/docs/yodldocs/stopsmb.1.yo
  -rwxr-xr-x  1 root     users       1817 Jul  7  1999 /opt/samba_src/samba/source/tests/trapdoor.c
  -rwxr-xr-x  1 root     users       1837 Jul  7  1999 /opt/samba/examples/printing/smbprint.sysv
  -rwxr-xr-x  1 root     users       1837 Jul 21  2000 /opt/samba_src/samba/source/tests/fcntl_lock64.c
  -rwxr-xr-x  1 root     users       1850 Mar 22  2000 /opt/samba/docs/yodldocs/startsmb.1.yo
  -rwxr-xr-x  1 root     users       1852 Feb 21  2001 /opt/samba_src/samba/source/script/startsmb
  -rwxr-xr-x  1 root     users       1852 Jun 21  2001 /opt/samba/bin/startsmb
  -rwxr-xr-x  1 root     users       1852 Jun 21  2001 /opt/samba/script/startsmb
```

```
  -rwxr-xr-x  1 root     users       1876 Jul  8  1999
/opt/samba_src/samba/source/script/makeyodldocs.sh
  -rwxr-xr-x  1 root     users       1917 Jul  7  1999 /opt/samba_src/samba/source/smbadduser
  -rwxr-xr-x  1 root     users       1924 Jul  7  1999 /opt/samba/examples/tridge/smb.conf
  -rwxr-xr-x  1 root     users       1935 Jul 21  2000 /opt/samba_src/samba/source/ubiqx/sys_include.h
  -rwxr-xr-x  1 root     users       1939 Jul  7  1999 /opt/samba/examples/misc/wall.perl
  -rwxr-xr-x  1 root     users       1944 Jul  7  1999 /opt/samba_src/samba/source/web/startstop.c
  -rwxr-xr-x  1 root     users       1957 Jul  7  1999 /opt/samba_src/samba/source/utils/testprns.c
  -rwxr-xr-x  1 root     users       1980 May 16  2001 /opt/samba/docs/textdocs/Passwords.txt
  -rwxr-xr-x  1 root     users       1981 May 16  2001 /opt/samba/docs/textdocs/UNIX_SECURITY.txt
  -rwxr-xr-x  1 root     users       2019 Jun 21  2001 /opt/samba/man/man1/smbstatus.1
  -rwxr-xr-x  1 root     users       2019 May 16  2001 /opt/samba/docs/manpages/smbstatus.1
  -rwxr-xr-x  1 root     users       2073 Jul  7  1999 /opt/samba_src/samba/source/utils/smbrun.c
  -rwxr-xr-x  1 root     users       2110 May 16  2001 /opt/samba/docs/textdocs/NT-Guest-Access.txt
  -rwxr-xr-x  1 root     users       2155 Jun 21  2001 /opt/samba/man/man1/smbrun.1
  -rwxr-xr-x  1 root     users       2155 May 16  2001 /opt/samba/docs/manpages/smbrun.1
  -rwxr-xr-x  1 root     users       2160 Jul  7  1999
/opt/samba_src/samba/source/smbwrapper/PORTING
  -rwxr-xr-x  1 root     users       2173 May 16  2001 /opt/samba/docs/textdocs/Application_Serving.txt
  -rwxr-xr-x  1 root     users       2205 Feb 21  2001 /opt/samba_src/samba/source/script/stopsmb
  -rwxr-xr-x  1 root     users       2205 Jun 21  2001 /opt/samba/bin/stopsmb
  -rwxr-xr-x  1 root     users       2205 Jun 21  2001 /opt/samba/script/stopsmb
  -rwxr-xr-x  1 root     users       2218 Jul  7  1999
/opt/samba_src/samba/source/mem_man/mem_man.h
  -rwxr-xr-x  1 root     users       2255 Jul  7  1999 /opt/samba_src/samba/source/include/rpc_wkssvc.h
  -rwxr-xr-x  1 root     users       2285 Nov 12  1999 /opt/samba/examples/wins_hook/dns_update
  -rwxr-xr-x  1 root     users       2325 Jul  7  1999 /opt/samba_src/samba/source/lib/fault.c
  -rwxr-xr-x  1 root     users       2334 Jun 21  2001 /opt/samba/swat/help/stopsmb.1.html
  -rwxr-xr-x  1 root     users       2334 Mar 22  2000 /opt/samba/docs/htmldocs/stopsmb.1.html
  -rwxr-xr-x  1 root     users       2355 Jun 21  2001 /opt/samba/man/man1/samba_setup.1
  -rwxr-xr-x  1 root     users       2355 Mar 22  2000 /opt/samba/docs/manpages/samba_setup.1
  -rwxr-xr-x  1 root     users       2357 May 16  2001 /opt/samba/docs/textdocs/Speed2.txt
  -rwxr-xr-x  1 root     users       2371 Jun 21  2001 /opt/samba/swat/help/startsmb.1.html
  -rwxr-xr-x  1 root     users       2371 Mar 22  2000 /opt/samba/docs/htmldocs/startsmb.1.html
  -rwxr-xr-x  1 root     users       2372 Jul 21  2000 /opt/samba/docs/yodldocs/smbstatus.1.yo

  -rwxr-xr-x  1 root     users       2376 Jul  7  1999
/opt/samba_src/samba/source/codepages/codepage_def.850

  -rwxr-xr-x  1 root     users       2379 Jul  7  1999 /opt/samba/examples/printer-accounting/README
  -rwxr-xr-x  1 root     users       2385 Jul 21  2000 /opt/samba_src/samba/source/script/mkproto.awk
  -rwxr-xr-x  1 root     users       2391 Jul  7  1999 /opt/samba/examples/misc/extra_smbstatus
  -rwxr-xr-x  1 root     users       2394 Jun 21  2001 /opt/samba/swat/help/welcome.ja_JP.ujis.html
  -rwxr-xr-x  1 root     users       2398 Apr 16  2001 /opt/samba/HA/active_standby/samba.mon
  -rwxr-xr-x  1 root     users       2402 Jul  7  1999 /opt/samba/docs/textdocs/README.smbmount
  -rwxr-xr-x  1 root     users       2402 Jul  7  1999 /opt/samba/examples/autofs/mount-smb.doc
  -rwxr-xr-x  1 root     users       2413 Nov 12  1999 /opt/samba_src/samba/source/include/fnmatch.h
  -rwxr-xr-x  1 root     users       2417 Jul 21  2000 /opt/samba_src/samba/source/lib/talloc.c
  -rwxr-xr-x  1 root     users       2423 Apr 16  2001 /opt/samba/HA/active_active/samba.mon
  -rwxr-xr-x  1 root     users       2438 Jul  7  1999
/opt/samba_src/samba/source/rpcclient/cmd_wkssvc.c
  -rwxr-xr-x  1 root     users       2453 Jun 21  2001 /opt/samba/man/man1/smbsh.1
  -rwxr-xr-x  1 root     users       2453 May 16  2001 /opt/samba/docs/manpages/smbsh.1
  -rwxr-xr-x  1 root     users       2458 Jul 21  2000 /opt/samba/docs/yodldocs/smbrun.1.yo
  -rwxr-xr-x  1 root     users       2469 Jul 21  2000 /opt/samba/docs/yodldocs/smbmount.8.yo
```

```
  -rwxr-xr-x   1 root      users        2474 Jul 21  2000
/opt/samba_src/samba/source/codepages/codepage_def.1251

  -rwxr-xr-x   1 root      users        2485 Jul  7  1999
/opt/samba_src/samba/source/rpc_client/cli_wkssvc.c
  -rwxr-xr-x   1 root      users        2502 Jul 21  2000 /opt/samba/docs/yodldocs/smbsh.1.yo
  -rwxr-xr-x   1 root      users        2509 Jul 21  2000 /opt/samba_src/samba/source/include/hash.h
  -rwxr-xr-x   1 root      users        2509 Mar 22  2000 /opt/samba/docs/yodldocs/samba_setup.1.yo
  -rwxr-xr-x   1 root      users        2553 Jun 21  2001 /opt/samba/man/man8/smbmount.8
  -rwxr-xr-x   1 root      users        2553 May 16  2001 /opt/samba/docs/manpages/smbmount.8

  -rwxr-xr-x   1 root      users        2565 Jul  7  1999
/opt/samba_src/samba/source/codepages/codepage_def.737

  -rwxr-xr-x   1 root      users        2565 May 16  2001 /opt/samba/docs/textdocs/RoutedNetworks.txt
  -rwxr-xr-x   1 root      users        2573 May 16  2001 /opt/samba/docs/textdocs/NTDOMAIN.txt
  -rwxr-xr-x   1 root      users        2594 Nov 12  1999 /opt/samba/examples/printing/smbprint
  -rwxr-xr-x   1 root      users        2619 Jun 21  2001 /opt/samba/man/man8/smbspool.8
  -rwxr-xr-x   1 root      users        2619 May 16  2001 /opt/samba/docs/manpages/smbspool.8
  -rwxr-xr-x   1 root      users        2622 Nov 12  1999 /opt/samba_src/samba/source/include/charset.h
  -rwxr-xr-x   1 root      users        2648 Jul  7  1999 /opt/samba/examples/validchars/validchr.c
  -rwxr-xr-x   1 root      users        2649 Jul 21  2000 /opt/samba_src/samba/source/aclocal.m4
  -rwxr-xr-x   1 root      users        2673 Jul 21  2000 /opt/samba/docs/yodldocs/smbspool.8.yo
  -rwxr-xr-x   1 root      users        2679 Jul  7  1999 /opt/samba/docs/faq/Samba-Server-FAQ-1.html
  -rwxr-xr-x   1 root      users        2683 Jul  7  1999
/opt/samba_src/samba/source/smbwrapper/README
  -rwxr-xr-x   1 root      users        2687 Jul  7  1999 /opt/samba/docs/textdocs/README.DCEDFS
  -rwxr-xr-x   1 root      users        2725 Jul 22  1999 /opt/samba_src/samba/source/lib/pidfile.c
  -rwxr-xr-x   1 root      users        2732 May 16  2001 /opt/samba/docs/textdocs/OS2-Client-HOWTO.txt
  -rwxr-xr-x   1 root      users        2799 May  3  2001 /opt/samba_src/samba/source/acconfig.h
  -rwxr-xr-x   1 root      users        2802 Jun 21  2001 /opt/samba/man/man5/lmhosts.5
  -rwxr-xr-x   1 root      users        2802 May 16  2001 /opt/samba/docs/manpages/lmhosts.5
  -rwxr-xr-x   1 root      users        2809 Jul  7  1999 /opt/samba_src/samba/source/include/rpcclient.h

  -rwxr-xr-x   1 root      users        2825 Jul 21  2000
/opt/samba_src/samba/source/codepages/codepage_def.852

  -rwxr-xr-x   1 root      users        2846 May 16  2001 /opt/samba/docs/textdocs/GOTCHAS.txt
  -rwxr-xr-x   1 root      users        2867 May 16  2001 /opt/samba/docs/textdocs/File-Cacheing.txt
  -rwxr-xr-x   1 root      users        2899 Jun 21  2001 /opt/samba/swat/help/welcome.html
  -rwxr-xr-x   1 root      users        2933 Jul 22  1999 /opt/samba_src/samba/source/smbwrapper/smbsh.c
  -rwxr-xr-x   1 root      users        2947 Jul 21  2000 /opt/samba/docs/htmldocs/smbspool.8.html
  -rwxr-xr-x   1 root      users        2947 Jun 21  2001 /opt/samba/swat/help/smbspool.8.html
  -rwxr-xr-x   1 root      users        2949 Jun 21  2001 /opt/samba/man/man1/testprns.1
  -rwxr-xr-x   1 root      users        2949 May 16  2001 /opt/samba/docs/manpages/testprns.1
  -rwxr-xr-x   1 root      users        2952 Jul 21  2000 /opt/samba/docs/yodldocs/lmhosts.5.yo
  -rwxr-xr-x   1 root      users        2955 Jul 21  2000 /opt/samba_src/samba/source/script/installswat.sh
  -rwxr-xr-x   1 root      users        3005 May 16  2001 /opt/samba/docs/textdocs/Win95.txt
  -rwxr-xr-x   1 root      users        3048 Jun 21  2001 /opt/samba/swat/help/samba_setup.1.html
  -rwxr-xr-x   1 root      users        3048 Mar 22  2000 /opt/samba/docs/htmldocs/samba_setup.1.html
  -rwxr-xr-x   1 root      users        3056 Jul 21  2000 /opt/samba/docs/textdocs/PROJECTS
  -rwxr-xr-x   1 root      users        3077 Jul 21  2000 /opt/samba_src/samba/source/profile/profile.c
  -rwxr-xr-x   1 root      users        3084 Jul 21  2000 /opt/samba/docs/htmldocs/smbrun.1.html
  -rwxr-xr-x   1 root      users        3084 Jun 21  2001 /opt/samba/swat/help/smbrun.1.html
  -rwxr-xr-x   1 root      users        3094 Jun 21  2001 /opt/samba/man/man1/make_unicodemap.1
  -rwxr-xr-x   1 root      users        3094 May 16  2001 /opt/samba/docs/manpages/make_unicodemap.1
```

```
  -rwxr-xr-x   1 root      users       3132 Jul 21  2000 /opt/samba/docs/htmldocs/smbsh.1.html
  -rwxr-xr-x   1 root      users       3132 Jun 21  2001 /opt/samba/swat/help/smbsh.1.html

  -rwxr-xr-x   1 root      users       3151 Jul  7  1999
/opt/samba_src/samba/source/codepages/codepage_def.437

  -rwxr-xr-x   1 root      users       3193 Jul 21  2000 /opt/samba/docs/yodldocs/testprns.1.yo
  -rwxr-xr-x   1 root      users       3221 Jul  7  1999 /opt/samba/docs/faq/Samba-meta-FAQ.html
  -rwxr-xr-x   1 root      users       3294 Jul  7  1999 /opt/samba_src/samba/source/lib/bitmap.c
  -rwxr-xr-x   1 root      users       3326 Jul 21  2000 /opt/samba_src/samba/source/libsmb/passchange.c
  -rwxr-xr-x   1 root      users       3330 Jul  7  1999
/opt/samba_src/samba/source/nmbd/nmbd_lmhosts.c
  -rwxr-xr-x   1 root      users       3331 Jul 21  2000 /opt/samba/docs/yodldocs/make_unicodemap.1.yo
  -rwxr-xr-x   1 root      users       3426 Jul  7  1999 /opt/samba/docs/faq/Samba-Server-FAQ.html
  -rwxr-xr-x   1 root      users       3432 Jul 21  2000 /opt/samba/docs/htmldocs/smbmount.8.html
  -rwxr-xr-x   1 root      users       3432 Jul 21  2000 /opt/samba/docs/htmldocs/smbstatus.1.html
  -rwxr-xr-x   1 root      users       3432 Jun 21  2001 /opt/samba/swat/help/smbmount.8.html
  -rwxr-xr-x   1 root      users       3432 Jun 21  2001 /opt/samba/swat/help/smbstatus.1.html
  -rwxr-xr-x   1 root      users       3441 Jul 22  1999 /opt/samba_src/samba/source/include/client.h
  -rwxr-xr-x   1 root      users       3448 Jul  7  1999
/opt/samba_src/samba/source/rpc_server/srv_wkssvc.c
  -rwxr-xr-x   1 root      users       3526 Jul  7  1999 /opt/samba_src/samba/source/lib/getsmbpass.c
  -rwxr-xr-x   1 root      users       3527 Jun 21  2001 /opt/samba/man/man1/testparm.1
  -rwxr-xr-x   1 root      users       3527 May 16  2001 /opt/samba/docs/manpages/testparm.1
  -rwxr-xr-x   1 root      users       3540 Jun 20  2000 /opt/samba_src/samba/source/include/acls.h
  -rwxr-xr-x   1 root      users       3559 Jul  7  1999 /opt/samba/examples/validchars/msdos70.out
  -rwxr-xr-x   1 root      users       3568 Jul 21  2000 /opt/samba/docs/htmldocs/lmhosts.5.html
  -rwxr-xr-x   1 root      users       3568 Jun 21  2001 /opt/samba/swat/help/lmhosts.5.html
  -rwxr-xr-x   1 root      users       3589 Oct 24  2000 /opt/samba_src/samba/source/printing/print_svid.c
  -rwxr-xr-x   1 root      users       3642 Jun 21  2001 /opt/samba/man/man1/smbtar.1
  -rwxr-xr-x   1 root      users       3642 May 16  2001 /opt/samba/docs/manpages/smbtar.1
  -rwxr-xr-x   1 root      users       3643 Jun 21  2001 /opt/samba/swat/images/samba.gif
  -rwxr-xr-x   1 root      users       3664 May 16  2001 /opt/samba/docs/textdocs/smbmount.txt

  -rwxr-xr-x   1 root      users       3671 Jul  7  1999
/opt/samba_src/samba/source/rpcclient/cmd_netlogon.c

  -rwxr-xr-x   1 root      users       3723 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0702.gif
  -rwxr-xr-x   1 root      users       3763 Jul  7  1999 /opt/samba_src/samba/source/lib/crc32.c
  -rwxr-xr-x   1 root      users       3800 May 16  2001 /opt/samba/docs/textdocs/CVS_ACCESS.txt
  -rwxr-xr-x   1 root      users       3801 Jul  7  1999 /opt/samba/examples/validchars/nwdos70.out
  -rwxr-xr-x   1 root      users       3806 Oct 26  1999 /opt/cifsclient/conf/master.d/cifs.master
  -rwxr-xr-x   1 root      users       3809 Jul  7  1999 /opt/samba/examples/thoralf/smb.conf

  -rwxr-xr-x   1 root      users       3867 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_nodestatus.c

  -rwxr-xr-x   1 root      users       3943 Jul 21  2000 /opt/samba/docs/htmldocs/testprns.1.html
  -rwxr-xr-x   1 root      users       3943 Jun 21  2001 /opt/samba/swat/help/testprns.1.html
  -rwxr-xr-x   1 root      users       4016 Jul 21  2000 /opt/samba_src/samba/source/include/rpc_secdes.h
  -rwxr-xr-x   1 root      users       4035 Jul  7  1999 /opt/samba/docs/faq/sambafaq.html
  -rwxr-xr-x   1 root      users       4036 Jul 21  2000 /opt/samba/docs/yodldocs/testparm.1.yo
  -rwxr-xr-x   1 root      users       4051 May 16  2001 /opt/samba/docs/textdocs/Tracing.txt
  -rwxr-xr-x   1 root      users       4068 Jul  7  1999 /opt/samba_src/samba/source/lib/signal.c
  -rwxr-xr-x   1 root      users       4105 Jul  7  1999 /opt/samba_src/samba/source/smbd/error.c
```

```
  -rwxr-xr-x  1 root     users       4107 Jul 21  2000
/opt/samba/docs/htmldocs/make_unicodemap.1.html
  -rwxr-xr-x  1 root     users       4107 Jun 21  2001 /opt/samba/swat/help/make_unicodemap.1.html
  -rwxr-xr-x  1 root     users       4121 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0303.gif
  -rwxr-xr-x  1 root     users       4122 Jul  7  1999 /opt/samba/examples/validchars/readme

  -rwxr-xr-x  1 root     users       4194 Jul  7  1999
/opt/samba_src/samba/source/codepages/codepage_def.866

  -rwxr-xr-x  1 root     users       4206 Jul  7  1999 /opt/samba_src/samba/source/lib/netatalk.c
  -rwxr-xr-x  1 root     users       4237 Jul 21  2000 /opt/samba/docs/yodldocs/smbtar.1.yo
  -rwxr-xr-x  1 root     users       4330 Jul  7  1999 /opt/samba_src/samba/source/lib/md4.c
  -rwxr-xr-x  1 root     users       4344 Jul  7  1999 /opt/samba_src/samba/source/smbd/predict.c

  -rwxr-xr-x  1 root     users       4527 Nov 12  1999
/opt/samba_src/samba/source/rpc_client/ntclienttrust.c

  -rwxr-xr-x  1 root     users       4558 Nov 12  1999 /opt/samba_src/samba/source/client/smbumount.c
  -rwxr-xr-x  1 root     users       4568 May 16  2001 /opt/samba/docs/textdocs/WinNT.txt
  -rwxr-xr-x  1 root     users       4571 Jun 21  2001 /opt/samba/swat/using_samba/ch01_08.html
  -rwxr-xr-x  1 root     users       4658 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0106.gif
  -rwxr-xr-x  1 root     users       4773 Jul  7  1999 /opt/samba_src/samba/source/install-sh
  -rwxr-xr-x  1 root     users       4779 Jul  7  1999 /opt/samba_src/samba/source/utils/smbfilter.c
  -rwxr-xr-x  1 root     users       4808 Jun 21  2001 /opt/samba/man/man8/swat.8
  -rwxr-xr-x  1 root     users       4808 May 16  2001 /opt/samba/docs/manpages/swat.8
  -rwxr-xr-x  1 root     users       4862 Jul 22  1999 /opt/samba_src/samba/source/script/smbtar
  -rwxr-xr-x  1 root     users       4862 Jun 21  2001 /opt/samba/bin/smbtar
  -rwxr-xr-x  1 root     users       4862 Jun 21  2001 /opt/samba/script/smbtar
  -rwxr-xr-x  1 root     users       4872 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0304.gif
  -rwxr-xr-x  1 root     users       4897 Jun 21  2001 /opt/samba/swat/using_samba/ch01_06.html
  -rwxr-xr-x  1 root     users       4917 Jul 22  1999 /opt/samba_src/samba/source/utils/nbio.c
  -rwxr-xr-x  1 root     users       4948 Nov 12  1999 /opt/samba_src/samba/source/printing/print_cups.c
  -rwxr-xr-x  1 root     users       4956 May  3  2001
/opt/samba_src/samba/source/smbwrapper/shared.c
  -rwxr-xr-x  1 root     users       4960 Nov 12  1999 /opt/samba_src/samba/source/lib/fnmatch.c
  -rwxr-xr-x  1 root     users       5011 Jul 21  2000 /opt/samba/docs/yodldocs/swat.8.yo
  -rwxr-xr-x  1 root     users       5028 Jul  7  1999 /opt/samba/docs/faq/Samba-meta-FAQ-3.html
  -rwxr-xr-x  1 root     users       5039 Jul 21  2000 /opt/samba_src/samba/source/smbd/conn.c
  -rwxr-xr-x  1 root     users       5108 Jul 21  2000 /opt/samba_src/samba/source/include/ntdomain.h
  -rwxr-xr-x  1 root     users       5184 May  3  2001 /opt/samba_src/samba/source/smbd/message.c
  -rwxr-xr-x  1 root     users       5190 Jun 21  2001 /opt/samba/man/man7/samba.7
  -rwxr-xr-x  1 root     users       5190 May 16  2001 /opt/samba/docs/manpages/samba.7
  -rwxr-xr-x  1 root     users       5197 Jul 21  2000 /opt/samba/docs/htmldocs/testparm.1.html
  -rwxr-xr-x  1 root     users       5197 Jun 21  2001 /opt/samba/swat/help/testparm.1.html
  -rwxr-xr-x  1 root     users       5199 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0314.gif
  -rwxr-xr-x  1 root     users       5209 Mar 28  2001 /opt/cifsclient/bin/cifsclient
  -rwxr-xr-x  1 root     users       5226 Jun 21  2001 /opt/samba/man/man1/make_smbcodepage.1
  -rwxr-xr-x  1 root     users       5226 May 16  2001
/opt/samba/docs/manpages/make_smbcodepage.1
  -rwxr-xr-x  1 root     users       5239 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0404.gif
  -rwxr-xr-x  1 root     users       5279 May 16  2001 /opt/samba/docs/textdocs/security_level.txt

  -rwxr-xr-x  1 root     users       5366 Jul 21  2000
/opt/samba_src/samba/source/codepages/codepage_def.775

  -rwxr-xr-x  1 root     users       5382 May 16  2001 /opt/samba_src/samba/source/lib/smbrun.c
```

```
  -rwxr-xr-x  1 root     users       5400 Jul  7  1999
/opt/samba_src/samba/source/rpc_parse/parse_wks.c
  -rwxr-xr-x  1 root     users       5401 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0201.gif
  -rwxr-xr-x  1 root     users       5421 Jul  7  1999
/opt/samba_src/samba/source/passdb/smbpassgroup.c
  -rwxr-xr-x  1 root     users       5423 Jun 21  2001 /opt/samba/swat/using_samba/appe_01.html
  -rwxr-xr-x  1 root     users       5435 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/debugparse.h
  -rwxr-xr-x  1 root     users       5436 Jul  7  1999 /opt/samba/examples/simple/smb.conf
  -rwxr-xr-x  1 root     users       5482 Jul 21  2000
/opt/samba/docs/yodldocs/make_smbcodepage.1.yo
  -rwxr-xr-x  1 root     users       5499 May 16  2001 /opt/samba/docs/textdocs/BUGS.txt
  -rwxr-xr-x  1 root     users       5550 Nov 12  1999
/opt/samba_src/samba/source/libsmb/smbencrypt.c
  -rwxr-xr-x  1 root     users       5572 Jul 21  2000 /opt/samba/docs/announce
  -rwxr-xr-x  1 root     users       5598 Jul 21  2000
/opt/samba_src/samba/source/rpcclient/cmd_lsarpc.c

  -rwxr-xr-x  1 root     users       5634 Jul  7  1999
/opt/samba_src/samba/source/smbwrapper/smbw_stat.c

  -rwxr-xr-x  1 root     users       5683 May 16  2001 /opt/samba/docs/textdocs/DOMAIN_MEMBER.txt
  -rwxr-xr-x  1 root     users       5702 Jul  7  1999 /opt/samba_src/samba/source/architecture.doc
  -rwxr-xr-x  1 root     users       5708 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0406.gif
  -rwxr-xr-x  1 root     users       5714 Jun 21  2001 /opt/samba/man/man1/nmblookup.1
  -rwxr-xr-x  1 root     users       5714 May 16  2001 /opt/samba/docs/manpages/nmblookup.1
  -rwxr-xr-x  1 root     users       5780 Jul  7  1999 /opt/samba/docs/THANKS
  -rwxr-xr-x  1 root     users       5788 Jun 21  2001 /opt/samba/swat/using_samba/appa_02.html
  -rwxr-xr-x  1 root     users       5823 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0103.gif
  -rwxr-xr-x  1 root     users       5846 Jul 21  2000 /opt/samba_src/samba/source/include/local.h
  -rwxr-xr-x  1 root     users       5874 May 16  2001 /opt/samba/docs/textdocs/DOMAIN_CONTROL.txt
  -rwxr-xr-x  1 root     users       5876 May 16  2001 /opt/samba/docs/textdocs/Printing.txt
  -rwxr-xr-x  1 root     users       5898 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0701.gif
  -rwxr-xr-x  1 root     users       5901 Jul 21  2000 /opt/samba/docs/yodldocs/samba.7.yo
  -rwxr-xr-x  1 root     users       5943 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/ubi_dLinkList.c
  -rwxr-xr-x  1 root     users       5952 Jul 21  2000 /opt/samba/docs/htmldocs/smbtar.1.html
  -rwxr-xr-x  1 root     users       5952 Jun 21  2001 /opt/samba/swat/help/smbtar.1.html
  -rwxr-xr-x  1 root     users       5959 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0327.gif
  -rwxr-xr-x  1 root     users       5962 Jun 21  2001 /opt/samba/swat/using_samba/ch02_06.html
  -rwxr-xr-x  1 root     users       5972 Jul  7  1999 /opt/samba_src/samba/source/include/kanji.h
  -rwxr-xr-x  1 root     users       5979 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0315.gif
  -rwxr-xr-x  1 root     users       6005 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0603.gif

  -rwxr-xr-x  1 root     users       6082 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_logonnames.c

  -rwxr-xr-x  1 root     users       6142 Jul  7  1999 /opt/samba/docs/faq/Samba-meta-FAQ-1.html
  -rwxr-xr-x  1 root     users       6142 Jul 21  2000 /opt/samba/docs/htmldocs/swat.8.html
  -rwxr-xr-x  1 root     users       6142 Jun 21  2001 /opt/samba/swat/help/swat.8.html
  -rwxr-xr-x  1 root     users       6147 Jul  7  1999 /opt/samba/docs/htmldocs/wfw_slip.htm
  -rwxr-xr-x  1 root     users       6180 Jul 21  2000 /opt/samba/docs/yodldocs/nmblookup.1.yo
  -rwxr-xr-x  1 root     users       6227 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0110.gif

  -rwxr-xr-x  1 root     users       6237 Jul 21  2000
/opt/samba_src/samba/source/passdb/smbpasschange.c

  -rwxr-xr-x  1 root     users       6268 Jul 21  2000 /opt/samba/docs/yodldocs/DOMAIN_MEMBER.yo
```

```
  -rwxr-xr-x  1 root     users       6277 Jul  7  1999
/opt/samba_src/samba/source/nmbd/nmbd_browserdb.c

  -rwxr-xr-x  1 root     users       6284 Jun 21  2001 /opt/samba/swat/using_samba/gifs/samba.s.gif
  -rwxr-xr-x  1 root     users       6427 May 16  2001 /opt/samba/docs/textdocs/Faxing.txt
  -rwxr-xr-x  1 root     users       6457 Jul  7  1999 /opt/samba_src/samba/source/rpc_client/cli_login.c
  -rwxr-xr-x  1 root     users       6507 Nov 12  1999 /opt/samba_src/samba/source/client/smbmnt.c
  -rwxr-xr-x  1 root     users       6511 Nov 12  1999 /opt/samba_src/samba/source/web/po/ja.po
  -rwxr-xr-x  1 root     users       6548 Jul 21  2000
/opt/samba/docs/htmldocs/make_smbcodepage.1.html
  -rwxr-xr-x  1 root     users       6548 Jun 21  2001 /opt/samba/swat/help/make_smbcodepage.1.html
  -rwxr-xr-x  1 root     users       6587 Jul  8  1999 /opt/samba_src/samba/source/passdb/passgrp.c
  -rwxr-xr-x  1 root     users       6631 Jul 22  1999 /opt/samba_src/samba/source/lib/genrand.c
  -rwxr-xr-x  1 root     users       6634 Dec  4  2000 /opt/samba_src/samba/source/smbd/close.c
  -rwxr-xr-x  1 root     users       6682 Jul  7  1999 /opt/samba_src/samba/source/libsmb/credentials.c

  -rwxr-xr-x  1 root     users       6752 Jul  7  1999
/opt/samba_src/samba/source/codepages/codepage_def.861

  -rwxr-xr-x  1 root     users       6754 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0405.gif
  -rwxr-xr-x  1 root     users       6799 Jul  7  1999 /opt/samba_src/samba/source/smbd/groupname.c
  -rwxr-xr-x  1 root     users       6820 Jul  7  1999 /opt/samba_src/samba/source/include/rpc_misc.h
  -rwxr-xr-x  1 root     users       7019 Nov 12  1999 /opt/samba_src/samba/source/libsmb/pwd_cache.c
  -rwxr-xr-x  1 root     users       7079 Jul 21  2000 /opt/samba/docs/htmldocs/DOMAIN_MEMBER.html
  -rwxr-xr-x  1 root     users       7079 Jun 21  2001 /opt/samba/swat/help/DOMAIN_MEMBER.html
  -rwxr-xr-x  1 root     users       7093 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0326.gif
  -rwxr-xr-x  1 root     users       7150 Jul 21  2000 /opt/samba/docs/htmldocs/samba.7.html
  -rwxr-xr-x  1 root     users       7150 Jun 21  2001 /opt/samba/swat/help/samba.7.html
  -rwxr-xr-x  1 root     users       7225 Jun 21  2001 /opt/samba/swat/using_samba/licenseinfo.html
  -rwxr-xr-x  1 root     users       7238 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0504.gif
  -rwxr-xr-x  1 root     users       7257 Jun 21  2001 /opt/samba/swat/using_samba/ch01_05.html
  -rwxr-xr-x  1 root     users       7260 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/ubi_sLinkList.c
  -rwxr-xr-x  1 root     users       7317 Jul 21  2000 /opt/samba_src/samba/source/utils/nmblookup.c
  -rwxr-xr-x  1 root     users       7328 May 16  2001 /opt/samba/docs/textdocs/NetBIOS.txt
  -rwxr-xr-x  1 root     users       7354 Jul  7  1999 /opt/samba_src/samba/source/groupdb/groupfile.c
  -rwxr-xr-x  1 root     users       7384 Nov 12  1999 /opt/samba_src/samba/source/web/statuspage.c
  -rwxr-xr-x  1 root     users       7493 Dec 22  2000 /opt/samba_src/samba/source/libsmb/validate.c
  -rwxr-xr-x  1 root     users       7515 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0704.gif
  -rwxr-xr-x  1 root     users       7540 Jul  7  1999 /opt/samba_src/samba/source/groupdb/aliasfile.c

  -rwxr-xr-x  1 root     users       7582 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_mynames.c

  -rwxr-xr-x  1 root     users       7604 Jul  7  1999 /opt/samba_src/samba/source/libsmb/smberr.c
  -rwxr-xr-x  1 root     users       7634 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0505.gif
  -rwxr-xr-x  1 root     users       7703 Jul 21  2000 /opt/samba_src/samba/source/smbd/pipes.c
  -rwxr-xr-x  1 root     users       7714 May 16  2001 /opt/samba/docs/textdocs/HINTS.txt
  -rwxr-xr-x  1 root     users       7757 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0502.gif
  -rwxr-xr-x  1 root     users       7773 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0708.gif
  -rwxr-xr-x  1 root     users       7816 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0328.gif
  -rwxr-xr-x  1 root     users       7832 Feb 16  2001 /opt/samba_src/samba/source/rpc_server/srv_reg.c
  -rwxr-xr-x  1 root     users       7839 Jul  8  1999 /opt/samba_src/samba/source/utils/debug2html.c
  -rwxr-xr-x  1 root     users       7863 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_synclists.c
  -rwxr-xr-x  1 root     users       7890 Jul  7  1999 /opt/samba_src/samba/source/lib/util_file.c
```

```
  -rwxr-xr-x   1 root      users       7943 Jul 21  2000
/opt/samba_src/samba/source/utils/make_unicodemap.c

  -rwxr-xr-x   1 root      users       7985 Jul 22  1999 /opt/samba_src/samba/source/lib/access.c
  -rwxr-xr-x   1 root      users       7999 May 16  2001 /opt/samba/docs/textdocs/PRINTER_DRIVER.txt
  -rwxr-xr-x   1 root      users       8003 Jul 21  2000 /opt/samba/docs/htmldocs/nmblookup.1.html
  -rwxr-xr-x   1 root      users       8003 Jun 21  2001 /opt/samba/swat/help/nmblookup.1.html
  -rwxr-xr-x   1 root      users       8045 Jul  7  1999
/opt/samba_src/samba/source/rpcclient/cmd_srvsvc.c
  -rwxr-xr-x   1 root      users       8055 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0306.gif
  -rwxr-xr-x   1 root      users       8062 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0905.gif
  -rwxr-xr-x   1 root      users       8081 Jun 21  2001 /opt/samba/man/man5/smbpasswd.5
  -rwxr-xr-x   1 root      users       8081 May 16  2001 /opt/samba/docs/manpages/smbpasswd.5
  -rwxr-xr-x   1 root      users       8088 Jun 21  2001 /opt/samba/swat/using_samba/appa_04.html
  -rwxr-xr-x   1 root      users       8100 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0503.gif
  -rwxr-xr-x   1 root      users       8142 Jul 21  2000 /opt/samba_src/samba/source/client/smbspool.c
  -rwxr-xr-x   1 root      users       8185 Jun 21  2001 /opt/samba/swat/using_samba/ch08_02.html

  -rwxr-xr-x   1 root      users       8187 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_responserecordsdb.c

  -rwxr-xr-x   1 root      users       8210 Jul 22  1999 /opt/samba/examples/autofs/mount.smb

  -rwxr-xr-x   1 root      users       8228 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_winsproxy.c

  -rwxr-xr-x   1 root      users       8247 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0111.gif

  -rwxr-xr-x   1 root      users       8274 Feb 16  2001
/opt/samba_src/samba/source/rpc_server/srv_lsa_hnd.c

  -rwxr-xr-x   1 root      users       8275 Jul 21  2000
/opt/samba_src/samba/source/codepages/CPISO8859-7.TXT

  -rwxr-xr-x   1 root      users       8307 Jul 21  2000
/opt/samba_src/samba/source/smbwrapper/realcalls.h
  -rwxr-xr-x   1 root      users       8326 Jul 21  2000 /opt/samba_src/samba/source/lib/util_sec.c
  -rwxr-xr-x   1 root      users       8351 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0401.gif

  -rwxr-xr-x   1 root      users       8362 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_namerelease.c

  -rwxr-xr-x   1 root      users       8378 Jul 21  2000 /opt/samba/docs/yodldocs/smbpasswd.5.yo
  -rwxr-xr-x   1 root      users       8409 May 16  2001 /opt/samba/docs/textdocs/DHCP-Server-
Configuration.txt

  -rwxr-xr-x   1 root      users       8422 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.ab02.gif
  -rwxr-xr-x   1 root      users       8445 May  3  2001 /opt/samba_src/samba/source/utils/testparm.c
  -rwxr-xr-x   1 root      users       8500 Jul  7  1999 /opt/samba_src/samba/source/internals.doc
  -rwxr-xr-x   1 root      users       8529 Jun 21  2001 /opt/samba/swat/using_samba/ch01_01.html

  -rwxr-xr-x   1 root      users       8531 Jul 21  2000
/opt/samba_src/samba/source/codepages/CPISO8859-5.TXT

  -rwxr-xr-x   1 root      users       8553 Jul 28  1999 /opt/samba_src/samba/source/lib/netmask.c
```

```
  -rwxr-xr-x   1 root      users       8570 Jun 21  2001 /opt/samba/swat/using_samba/ch04_07.html
  -rwxr-xr-x   1 root      users       8591 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0402.gif
  -rwxr-xr-x   1 root      users       8602 Jun 21  2001 /opt/samba/swat/using_samba/appa_01.html
  -rwxr-xr-x   1 root      users       8616 Jul  7  1999 /opt/samba/docs/textdocs/README.jis
  -rwxr-xr-x   1 root      users       8666 Jul 21  2000 /opt/samba_src/samba/source/smbd/dosmode.c

  -rwxr-xr-x   1 root      users       8687 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_namequery.c

  -rwxr-xr-x   1 root      users       8692 Jul 21  2000
/opt/samba_src/samba/source/codepages/CPISO8859-1.TXT

  -rwxr-xr-x   1 root      users       8707 Jul  7  1999 /opt/samba/examples/smb.conf.default

  -rwxr-xr-x   1 root      users       8734 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_processlogon.c

  -rwxr-xr-x   1 root      users       8800 Jul 21  2000 /opt/samba_src/samba/source/utils/status.c
  -rwxr-xr-x   1 root      users       8809 Jul  7  1999 /opt/samba/docs/faq/Samba-meta-FAQ-4.html
  -rwxr-xr-x   1 root      users       8815 Jul 21  2000 /opt/samba_src/samba/source/smbd/dfree.c
  -rwxr-xr-x   1 root      users       8824 Jul  7  1999 /opt/samba/examples/validchars/validchr.com

  -rwxr-xr-x   1 root      users       8920 Jul 21  2000
/opt/samba_src/samba/source/codepages/CPISO8859-2.TXT

  -rwxr-xr-x   1 root      users       8959 Jun 21  2001 /opt/samba/swat/using_samba/ch08_04.html
  -rwxr-xr-x   1 root      users       8965 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0507.gif
  -rwxr-xr-x   1 root      users       8977 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0904.gif
  -rwxr-xr-x   1 root      users       9023 Nov 12  1999
/opt/samba_src/samba/source/passdb/smbpassfile.c
  -rwxr-xr-x   1 root      users       9024 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0602.gif
  -rwxr-xr-x   1 root      users       9025 Mar 20  2001 /opt/samba_src/samba/source/include/rpc_lsa.h
  -rwxr-xr-x   1 root      users       9031 Jul  7  1999 /opt/samba_src/samba/source/smbd/ssl.c
  -rwxr-xr-x   1 root      users       9065 Jun 21  2001 /opt/samba/man/man8/nmbd.8
  -rwxr-xr-x   1 root      users       9065 May 16  2001 /opt/samba/docs/manpages/nmbd.8
  -rwxr-xr-x   1 root      users       9245 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/ubi_dLinkList.h
  -rwxr-xr-x   1 root      users       9261 Jul 21  2000 /opt/samba_src/samba/source/lib/replace.c
  -rwxr-xr-x   1 root      users       9284 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0403.gif
  -rwxr-xr-x   1 root      users       9371 Nov 12  1999
/opt/samba_src/samba/source/rpc_client/cli_lsarpc.c

  -rwxr-xr-x   1 root      users       9388 Jul  7  1999
/opt/samba_src/samba/source/include/MacExtensions.h

  -rwxr-xr-x   1 root      users       9403 Jul  7  1999 /opt/samba_src/samba/source/rpc_server/srv_util.c
  -rwxr-xr-x   1 root      users       9423 Jul 21  2000 /opt/samba_src/samba/source/lib/interfaces.c
  -rwxr-xr-x   1 root      users       9426 Nov 12  1999 /opt/samba_src/samba/source/utils/masktest.c
  -rwxr-xr-x   1 root      users       9495 Jul 21  2000 /opt/samba_src/samba/source/include/rpc_dce.h
  -rwxr-xr-x   1 root      users       9562 Jul 21  2000 /opt/samba/docs/yodldocs/nmbd.8.yo
  -rwxr-xr-x   1 root      users       9579 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0316.gif
  -rwxr-xr-x   1 root      users       9659 Jan  6  2000 /opt/samba_src/samba/source/lib/acl.c
  -rwxr-xr-x   1 root      users       9675 Jul 22  1999 /opt/samba_src/samba/source/nmbd/asyncdns.c
  -rwxr-xr-x   1 root      users       9690 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0803.gif
  -rwxr-xr-x   1 root      users       9694 Jul 21  2000
/opt/samba_src/samba/source/codepages/CP850.TXT
  -rwxr-xr-x   1 root      users       9694 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0312.gif
```

```
  -rwxr-xr-x  1 root     users       9812 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/ubi_sLinkList.h
  -rwxr-xr-x  1 root     users       9819 Jul 21  2000
/opt/samba_src/samba/source/codepages/CP866.TXT
  -rwxr-xr-x  1 root     users       9848 Jul 21  2000
/opt/samba_src/samba/source/codepages/CP437.TXT
  -rwxr-xr-x  1 root     users       9850 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0101.gif
  -rwxr-xr-x  1 root     users       9861 Jun 21  2001 /opt/samba/swat/using_samba/ch09_03.html
  -rwxr-xr-x  1 root     users       9873 May 16  2001 /opt/samba/docs/textdocs/BROWSING-Config.txt
  -rwxr-xr-x  1 root     users       9880 Jul 21  2000
/opt/samba_src/samba/source/codepages/CP861.TXT
  -rwxr-xr-x  1 root     users       9881 Jul 21  2000
/opt/samba_src/samba/source/codepages/CP737.TXT
  -rwxr-xr-x  1 root     users       9905 Jun 21  2001 /opt/samba/swat/using_samba/ch08_07.html
  -rwxr-xr-x  1 root     users       9913 Apr 10  2000 /opt/samba/HA/active_standby/samba.conf
  -rwxr-xr-x  1 root     users       9959 Jul 21  2000 /opt/samba/docs/htmldocs/smbpasswd.5.html
  -rwxr-xr-x  1 root     users       9959 Jun 21  2001 /opt/samba/swat/help/smbpasswd.5.html
  -rwxr-xr-x  1 root     users       9992 Apr 10  2000 /opt/samba/HA/active_active/samba.conf
  -rwxr-xr-x  1 root     users       9993 Jul 21  2000
/opt/samba_src/samba/source/codepages/CP852.TXT
  -rwxr-xr-x  1 root     users       9998 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0318.gif
  -rwxr-xr-x  1 root     users      10028 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.ab01.gif
  -rwxr-xr-x  1 root     users      10033 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0601.gif
  -rwxr-xr-x  1 root     users      10149 Nov 12  1999 /opt/samba_src/samba/source/lib/interface.c
  -rwxr-xr-x  1 root     users      10164 Jul 21  2000 /opt/samba/docs/faq/sambafaq-2.html
  -rwxr-xr-x  1 root     users      10212 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0407.gif
  -rwxr-xr-x  1 root     users      10215 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0313.gif
  -rwxr-xr-x  1 root     users      10244 Jun 21  2001 /opt/samba/swat/using_samba/ch02_05.html
  -rwxr-xr-x  1 root     users      10277 Jun 21  2001 /opt/samba/swat/using_samba/appb_01.html
  -rwxr-xr-x  1 root     users      10347 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0107.gif
  -rwxr-xr-x  1 root     users      10358 Jun 21  2001 /opt/samba/swat/using_samba/ch01_07.html
  -rwxr-xr-x  1 root     users      10366 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0705.gif
  -rwxr-xr-x  1 root     users      10423 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/debugparse.c
  -rwxr-xr-x  1 root     users      10508 Jun 21  2001 /opt/samba/swat/using_samba/ch04_03.html
  -rwxr-xr-x  1 root     users      10577 Jul  7  1999 /opt/samba_src/samba/source/groupdb/groupdb.c
  -rwxr-xr-x  1 root     users      10618 Jul  7  1999 /opt/samba_src/samba/source/groupdb/aliasdb.c
  -rwxr-xr-x  1 root     users      10618 May 16  2001 /opt/samba/docs/textdocs/UNIX-SMB.txt
  -rwxr-xr-x  1 root     users      10649 Jul  7  1999 /opt/samba/docs/history
  -rwxr-xr-x  1 root     users      10722 Jul 21  2000 /opt/samba_src/samba/source/lib/charcnv.c
  -rwxr-xr-x  1 root     users      10751 Nov 12  1999 /opt/samba_src/samba/source/printing/pcap.c
  -rwxr-xr-x  1 root     users      10805 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0321.gif
  -rwxr-xr-x  1 root     users      10813 Jul  7  1999 /opt/samba_src/samba/source/include/rpc_reg.h
  -rwxr-xr-x  1 root     users      10816 Jul 21  2000 /opt/samba_src/samba/source/lib/username.c
  -rwxr-xr-x  1 root     users      10874 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0319.gif
  -rwxr-xr-x  1 root     users      10904 Dec  4  2000 /opt/samba_src/samba/source/lib/hash.c
  -rwxr-xr-x  1 root     users      10919 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0320.gif
  -rwxr-xr-x  1 root     users      10933 Jul 21  2000 /opt/samba_src/samba/source/smbd/uid.c
  -rwxr-xr-x  1 root     users      10938 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0102.gif
  -rwxr-xr-x  1 root     users      10973 Jul 22  1999
/opt/samba_src/samba/source/rpc_client/cli_srvsvc.c
  -rwxr-xr-x  1 root     users      11038 Jun 21  2001 /opt/samba/swat/using_samba/index.html
  -rwxr-xr-x  1 root     users      11067 Jul  7  1999 /opt/samba_src/samba/source/libsmb/smbdes.c
  -rwxr-xr-x  1 root     users      11071 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0707.gif
  -rwxr-xr-x  1 root     users      11176 Jan  6  2000 /opt/samba_src/samba/source/include/trans2.h
  -rwxr-xr-x  1 root     users      11204 Jul 21  2000 /opt/samba_src/samba/source/codepages/CPKOI8-
R.TXT
```

```
  -rwxr-xr-x   1 root      users       11207 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_workgroupdb.c

  -rwxr-xr-x   1 root      users       11211 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0804.gif
  -rwxr-xr-x   1 root      users       11253 Jul 21  2000
/opt/samba_src/samba/source/smbwrapper/wrapped.c

  -rwxr-xr-x   1 root      users       11421 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_subnetdb.c

  -rwxr-xr-x   1 root      users       11432 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0105.gif
  -rwxr-xr-x   1 root      users       11604 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0301.gif
  -rwxr-xr-x   1 root      users       11689 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0309.gif
  -rwxr-xr-x   1 root      users       11715 Jul 21  2000 /opt/samba_src/samba/source/include/byteorder.h
  -rwxr-xr-x   1 root      users       11731 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0324.gif
  -rwxr-xr-x   1 root      users       11732 Jul 21  2000 /opt/samba/docs/htmldocs/nmbd.8.html
  -rwxr-xr-x   1 root      users       11732 Jun 21  2001 /opt/samba/swat/help/nmbd.8.html
  -rwxr-xr-x   1 root      users       11868 May 16  2001 /opt/samba/docs/textdocs/Recent-FAQs.txt
  -rwxr-xr-x   1 root      users       11927 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0805.gif
  -rwxr-xr-x   1 root      users       11960 Jun 21  2001 /opt/samba/swat/using_samba/appf_01.html
  -rwxr-xr-x   1 root      users       12108 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0113.gif
  -rwxr-xr-x   1 root      users       12132 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0801.gif
  -rwxr-xr-x   1 root      users       12145 Jul 21  2000 /opt/samba_src/samba/source/smbd/files.c
  -rwxr-xr-x   1 root      users       12184 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0302.gif
  -rwxr-xr-x   1 root      users       12210 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0604.gif

  -rwxr-xr-x   1 root      users       12337 Mar 20  2001
/opt/samba_src/samba/source/include/rpc_netlogon.h

  -rwxr-xr-x   1 root      users       12474 Jul 21  2000 /opt/samba_src/samba/source/utils/rpctorture.c
  -rwxr-xr-x   1 root      users       12529 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0307.gif

  -rwxr-xr-x   1 root      users       12532 Nov 12  1999
/opt/samba_src/samba/source/utils/make_smbcodepage.c

  -rwxr-xr-x   1 root      users       12535 Jul 21  2000 /opt/samba_src/samba/source/lib/util_sid.c
  -rwxr-xr-x   1 root      users       12597 May 16  2001 /opt/samba/docs/textdocs/UNIX_INSTALL.txt

  -rwxr-xr-x   1 root      users       12656 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_elections.c

  -rwxr-xr-x   1 root      users       12693 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0310.gif
  -rwxr-xr-x   1 root      users       12849 May 16  2001 /opt/samba/docs/textdocs/DIAGNOSIS.txt
  -rwxr-xr-x   1 root      users       12917 Jul  7  1999 /opt/samba_src/samba/source/parsing.doc
  -rwxr-xr-x   1 root      users       12958 May 16  2001 /opt/samba/docs/textdocs/NT_Security.txt
  -rwxr-xr-x   1 root      users       12962 May 16  2001 /opt/samba/docs/textdocs/Speed.txt
  -rwxr-xr-x   1 root      users       12974 Jun 21  2001 /opt/samba/swat/using_samba/ch02_04.html
  -rwxr-xr-x   1 root      users       12988 Jan  7  2000 /opt/samba_src/samba/source/script/samba_setup
  -rwxr-xr-x   1 root      users       12988 Jun 21  2001 /opt/samba/bin/samba_setup
  -rwxr-xr-x   1 root      users       12988 Jun 21  2001 /opt/samba/script/samba_setup
  -rwxr-xr-x   1 root      users       13012 Jul 21  2000 /opt/samba_src/samba/source/lib/charset.c
  -rwxr-xr-x   1 root      users       13014 Jun 21  2001 /opt/samba/man/man8/smbpasswd.8
  -rwxr-xr-x   1 root      users       13014 May 16  2001 /opt/samba/docs/manpages/smbpasswd.8
  -rwxr-xr-x   1 root      users       13047 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0703.gif
  -rwxr-xr-x   1 root      users       13095 Jun 21  2001 /opt/samba/swat/using_samba/ch04_02.html
  -rwxr-xr-x   1 root      users       13322 Jul 21  2000 /opt/samba_src/samba/source/smbd/negprot.c
```

```
  -rwxr-xr-x   1 root      users       13333 Jun 21  2001 /opt/samba/swat/using_samba/ch04_04.html
  -rwxr-xr-x   1 root      users       13347 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0311.gif
  -rwxr-xr-x   1 root      users       13412 May 16  2001 /opt/samba/docs/textdocs/ENCRYPTION.txt
  -rwxr-xr-x   1 root      users       13504 Jul 21  2000 /opt/samba/docs/faq/sambafaq-3.html
  -rwxr-xr-x   1 root      users       13525 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0605.gif
  -rwxr-xr-x   1 root      users       13549 Jun 18  2001 /opt/samba_src/samba/source/locking/locking.c
  -rwxr-xr-x   1 root      users       13586 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0506.gif
  -rwxr-xr-x   1 root      users       13656 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0323.gif
  -rwxr-xr-x   1 root      users       13719 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0204.gif

  -rwxr-xr-x   1 root      users       13825 Jul 22  1999
/opt/samba_src/samba/source/smbwrapper/smbw_dir.c

  -rwxr-xr-x   1 root      users       13913 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_nameregister.c

  -rwxr-xr-x   1 root      users       13955 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0112.gif
  -rwxr-xr-x   1 root      users       14012 Mar 19  2001 /opt/samba_src/samba/source/lib/acl_unix.c

  -rwxr-xr-x   1 root      users       14043 Nov 12  1999
/opt/samba_src/samba/source/nmbd/nmbd_serverlistdb.c

  -rwxr-xr-x   1 root      users       14078 Jul 21  2000 /opt/samba/docs/yodldocs/NT_Security.yo
  -rwxr-xr-x   1 root      users       14093 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0325.gif
  -rwxr-xr-x   1 root      users       14114 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0709.gif
  -rwxr-xr-x   1 root      users       14115 Jul 21  2000 /opt/samba/docs/yodldocs/smbpasswd.8.yo
  -rwxr-xr-x   1 root      users       14138 Apr  2  2001 /opt/samba_src/samba/source/lib/doscalls.c
  -rwxr-xr-x   1 root      users       14140 Jun 21  2001 /opt/samba/swat/using_samba/ch02_03.html
  -rwxr-xr-x   1 root      users       14146 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0305.gif
  -rwxr-xr-x   1 root      users       14439 Jul 21  2000
/opt/samba_src/samba/source/utils/make_printerdef.c

  -rwxr-xr-x   1 root      users       14463 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_become_dmb.c

  -rwxr-xr-x   1 root      users       14498 Jul 21  2000 /opt/samba_src/samba/source/utils/smbpasswd.c
  -rwxr-xr-x   1 root      users       14698 Jul 21  2000 /opt/samba_src/samba/source/smbd/connection.c
  -rwxr-xr-x   1 root      users       14760 Jul 22  1999
/opt/samba_src/samba/source/rpc_parse/parse_sec.c
  -rwxr-xr-x   1 root      users       14849 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0317.gif
  -rwxr-xr-x   1 root      users       14910 Jun 21  2001 /opt/samba/swat/using_samba/ch08_01.html
  -rwxr-xr-x   1 root      users       14940 Jul 21  2000 /opt/samba/docs/faq/Samba-meta-FAQ-2.html
  -rwxr-xr-x   1 root      users       15031 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0322.gif
  -rwxr-xr-x   1 root      users       15078 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.aa01.gif
  -rwxr-xr-x   1 root      users       15146 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0508.gif
  -rwxr-xr-x   1 root      users       15155 Jul 22  1999 /opt/samba_src/samba/source/include/rpc_srvsvc.h
  -rwxr-xr-x   1 root      users       15299 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0802.gif
  -rwxr-xr-x   1 root      users       15359 Jun 21  2001 /opt/samba/swat/using_samba/ch06_01.html
  -rwxr-xr-x   1 root      users       15642 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0501.gif
  -rwxr-xr-x   1 root      users       15672 May 16  2001 /opt/samba/docs/textdocs/PROFILES.txt
  -rwxr-xr-x   1 root      users       15701 Jul 21  2000 /opt/samba/docs/faq/sambafaq-1.html
  -rwxr-xr-x   1 root      users       15709 Jun 21  2001 /opt/samba/swat/using_samba/ch02_01.html
  -rwxr-xr-x   1 root      users       15715 Jul 21  2000 /opt/samba/docs/htmldocs/NT_Security.html
  -rwxr-xr-x   1 root      users       15715 Jun 21  2001 /opt/samba/swat/help/NT_Security.html
  -rwxr-xr-x   1 root      users       15989 Jul 21  2000 /opt/samba_src/samba/source/web/cgi.c
  -rwxr-xr-x   1 root      users       16162 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0308.gif
```

```
  -rwxr-xr-x  1 root     users      16182 Jul 21  2000 /opt/samba_src/samba/source/smbd/service.c
  -rwxr-xr-x  1 root     users      16309 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0901.gif
  -rwxr-xr-x  1 root     users      16825 Jul 21  2000 /opt/samba_src/samba/source/lib/time.c
  -rwxr-xr-x  1 root     users      16887 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0606.gif
  -rwxr-xr-x  1 root     users      17167 Jul 21  2000 /opt/samba_src/samba/source/client/smbmount.c
  -rwxr-xr-x  1 root     users      17386 Jul  7  1999
/opt/samba_src/samba/source/ubiqx/ubi_SplayTree.h
  -rwxr-xr-x  1 root     users      17406 Jul 21  2000 /opt/samba/docs/htmldocs/smbpasswd.8.html
  -rwxr-xr-x  1 root     users      17406 Jun 21  2001 /opt/samba/swat/help/smbpasswd.8.html
  -rwxr-xr-x  1 root     users      17411 Jun  4  2001 /opt/samba_src/samba/source/lib/nt_acl.c
  -rwxr-xr-x  1 root     users      17418 Jun 21  2001 /opt/samba/man/man8/smbd.8
  -rwxr-xr-x  1 root     users      17418 May 16  2001 /opt/samba/docs/manpages/smbd.8
  -rwxr-xr-x  1 root     users      17438 Jun 21  2001 /opt/samba/swat/using_samba/ch08_05.html
  -rwxr-xr-x  1 root     users      17540 Jun 21  2001 /opt/samba/swat/using_samba/ch01_02.html
  -rwxr-xr-x  1 root     users      17617 Dec  4  2000 /opt/samba_src/samba/source/smbd/server.c
  -rwxr-xr-x  1 root     users      17870 Jul 21  2000 /opt/samba_src/samba/source/smbd/fileio.c
  -rwxr-xr-x  1 root     users      17899 Jul 21  2000 /opt/samba/docs/yodldocs/smbd.8.yo
  -rwxr-xr-x  1 root     users      17902 Nov  7  2000 /opt/samba_src/samba/source/include/includes.h
  -rwxr-xr-x  1 root     users      17982 Jul  7  1999 /opt/samba/COPYING
  -rwxr-xr-x  1 root     users      17982 Jul  7  1999 /opt/samba_src/COPYING
  -rwxr-xr-x  1 root     users      17982 Jul  7  1999 /opt/samba_src/samba/COPYING
  -rwxr-xr-x  1 root     users      18052 Jul 21  2000
/opt/samba_src/samba/source/locking/shmem_sysv.c
  -rwxr-xr-x  1 root     users      18137 Jun 21  2001 /opt/samba/swat/using_samba/ch04_05.html
  -rwxr-xr-x  1 root     users      18147 Apr 27  2001
/opt/samba_src/samba/source/rpcclient/cmd_samr.c
  -rwxr-xr-x  1 root     users      18159 Jul 21  2000 /opt/samba_src/samba/source/lib/debug.c
  -rwxr-xr-x  1 root     users      18189 Jan  3  2001 /opt/samba/HA/active_standby/README.txt
  -rwxr-xr-x  1 root     users      18293 Jul  7  1999 /opt/samba_src/samba/source/config.guess
  -rwxr-xr-x  1 root     users      18414 Jul 21  2000 /opt/samba_src/samba/source/include/nameserv.h
  -rwxr-xr-x  1 root     users      18573 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0903.gif
  -rwxr-xr-x  1 root     users      18638 Jul 21  2000 /opt/samba/docs/faq/Samba-Server-FAQ-2.html
  -rwxr-xr-x  1 root     users      18667 Jul 21  2000 /opt/samba_src/samba/source/rpcclient/rpcclient.c
  -rwxr-xr-x  1 root     users      18832 Jul 21  2000 /opt/samba_src/samba/source/lsarpcd/srv_lsa.c
  -rwxr-xr-x  1 root     users      18852 Jul  7  1999
/opt/samba_src/samba/source/rpc_server/srv_lookup.c
  -rwxr-xr-x  1 root     users      19066 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0203.gif
  -rwxr-xr-x  1 root     users      19110 Jul 21  2000 /opt/samba_src/samba/source/rpc_server/srv_lsa.c
  -rwxr-xr-x  1 root     users      19203 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/ubi_Cache.h
  -rwxr-xr-x  1 root     users      19217 May 16  2001 /opt/samba/docs/textdocs/SSLeay.txt
  -rwxr-xr-x  1 root     users      19779 Jul 21  2000
/opt/samba_src/samba/source/rpc_parse/parse_prs.c
  -rwxr-xr-x  1 root     users      20065 Jul 21  2000 /opt/samba/docs/faq/Samba-Server-FAQ.sgml
  -rwxr-xr-x  1 root     users      20076 Jul 21  2000 /opt/samba_src/samba/source/smbd/blocking.c
  -rwxr-xr-x  1 root     users      20223 Jul 21  2000 /opt/samba/docs/htmldocs/smbd.8.html
  -rwxr-xr-x  1 root     users      20223 Jun 21  2001 /opt/samba/swat/help/smbd.8.html
  -rwxr-xr-x  1 root     users      20602 Apr 27  2001
/opt/samba_src/samba/source/rpc_client/cli_samr.c
  -rwxr-xr-x  1 root     users      20713 Jul 21  2000 /opt/samba_src/samba/source/lib/snprintf.c
  -rwxr-xr-x  1 root     users      20723 Jul 21  2000 /opt/samba_src/samba/source/param/params.c
  -rwxr-xr-x  1 root     users      20973 Jul 21  2000 /opt/samba_src/samba/source/smbd/quotas.c
  -rwxr-xr-x  1 root     users      20973 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0104.gif
  -rwxr-xr-x  1 root     users      21058 Jun 21  2001 /opt/samba/swat/using_samba/ch02_02.html
  -rwxr-xr-x  1 root     users      21163 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/ubi_Cache.c
  -rwxr-xr-x  1 root     users      21228 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0108.gif
  -rwxr-xr-x  1 root     users      21298 Dec  4  2000 /opt/samba_src/samba/source/smbd/filename.c
```

```
  -rwxr-xr-x   1 root      users       21353 Nov 12  1999
/opt/samba_src/samba/source/nmbd/nmbd_sendannounce.c

  -rwxr-xr-x   1 root      users       21396 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_namelistdb.c

  -rwxr-xr-x   1 root      users       21417 Jul  7  1999
/opt/samba_src/samba/source/ubiqx/ubi_SplayTree.c

  -rwxr-xr-x   1 root      users       21557 Jul  7  1999
/opt/samba_src/samba/source/nmbd/nmbd_incomingrequests.c

  -rwxr-xr-x   1 root      users       21627 May 16  2001 /opt/samba/docs/textdocs/DOMAIN.txt
  -rwxr-xr-x   1 root      users       21646 Jul  7  1999
/opt/samba_src/samba/source/mem_man/mem_man.c
  -rwxr-xr-x   1 root      users       21762 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0109.gif
  -rwxr-xr-x   1 root      users       21764 Jun 21  2001 /opt/samba/swat/using_samba/ch08_03.html
  -rwxr-xr-x   1 root      users       21785 Jul  7  1999 /opt/samba_src/samba/source/rpcclient/cmd_reg.c
  -rwxr-xr-x   1 root      users       21792 Apr 10  2000 /opt/samba/HA/active_standby/samba.cntl
  -rwxr-xr-x   1 root      users       21806 Jul 21  2000 /opt/samba_src/samba/source/smbd/chgpasswd.c
  -rwxr-xr-x   1 root      users       21864 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0202.gif

  -rwxr-xr-x   1 root      users       22133 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_become_lmb.c

  -rwxr-xr-x   1 root      users       22306 Jul  7  1999 /opt/samba_src/samba/source/lib/ufc.c
  -rwxr-xr-x   1 root      users       22417 May  3  2001 /opt/samba_src/samba/source/include/config.h.in
  -rwxr-xr-x   1 root      users       22437 Jul 22  1999
/opt/samba_src/samba/source/locking/locking_shm.c

  -rwxr-xr-x   1 root      users       22592 Dec  9  2000
/opt/samba_src/samba/source/rpc_client/cli_netlogon.c

  -rwxr-xr-x   1 root      users       22695 Apr 27  2001 /opt/samba_src/samba/source/include/nterr.h
  -rwxr-xr-x   1 root      users       22855 Jul 21  2000 /opt/samba_src/samba/source/nmbd/nmbd.c
  -rwxr-xr-x   1 root      users       22884 Jul 21  2000 /opt/samba_src/samba/source/config.sub
  -rwxr-xr-x   1 root      users       23219 Jun 21  2001 /opt/samba/swat/using_samba/appa_05.html
  -rwxr-xr-x   1 root      users       23343 Jan  3  2001 /opt/samba/HA/active_active/samba.cntl

  -rwxr-xr-x   1 root      users       23462 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_browsesync.c

  -rwxr-xr-x   1 root      users       23507 Jul 21  2000
/opt/samba_src/samba/source/rpc_server/srv_pipe_hnd.c

  -rwxr-xr-x   1 root      users       23597 Jun 21  2001 /opt/samba/swat/using_samba/appa_03.html
  -rwxr-xr-x   1 root      users       24015 Jun 21  2001 /opt/samba/swat/using_samba/ch03_02.html
  -rwxr-xr-x   1 root      users       24058 Jul 21  2000 /opt/samba_src/samba/source/smbd/dir.c
  -rwxr-xr-x   1 root      users       24226 May  4  2001 /opt/samba_src/samba/source/include/config.h
  -rwxr-xr-x   1 root      users       24272 Jul 21  2000 /opt/samba_src/samba/source/lib/util_unistr.c
  -rwxr-xr-x   1 root      users       24623 Jun 21  2001 /opt/samba/swat/using_samba/ch04_08.html
  -rwxr-xr-x   1 root      users       24643 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0114.gif
  -rwxr-xr-x   1 root      users       24793 Jun 21  2001 /opt/samba/swat/using_samba/ch07_03.html
  -rwxr-xr-x   1 root      users       25040 Nov 12  1999 /opt/samba_src/samba/source/rpc_client/cli_reg.c
  -rwxr-xr-x   1 root      users       25083 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0706.gif
```

```
  -rwxr-xr-x   1 root      users       25114 Apr 10  2001 /opt/samba_src/samba/source/Makefile
  -rwxr-xr-x   1 root      users       25116 Jun 21  2001 /opt/samba/swat/using_samba/ch09_01.html
  -rwxr-xr-x   1 root      users       25134 May 16  2001 /opt/samba/docs/textdocs/BROWSING.txt
  -rwxr-xr-x   1 root      users       25225 Apr 10  2001 /opt/samba_src/samba/source/Makefile.in
  -rwxr-xr-x   1 root      users       25237 Jul 22  1999
/opt/samba_src/samba/source/passdb/pass_check.c
  -rwxr-xr-x   1 root      users       25256 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/COPYING.LIB
  -rwxr-xr-x   1 root      users       25442 Jun 21  2001 /opt/samba/swat/using_samba/ch05_05.html
  -rwxr-xr-x   1 root      users       25597 Jun 21  2001 /opt/samba/swat/using_samba/ch06_02.html
  -rwxr-xr-x   1 root      users       25760 Jun 21  2001 /opt/samba/swat/using_samba/ch04_01.html
  -rwxr-xr-x   1 root      users       25935 Jun 21  2001 /opt/samba/swat/using_samba/ch06_05.html
  -rwxr-xr-x   1 root      users       26076 Jun 21  2001 /opt/samba/swat/using_samba/appb_02.html
  -rwxr-xr-x   1 root      users       26194 Apr  2  2001 /opt/samba/HA/active_active/README.txt
  -rwxr-xr-x   1 root      users       26201 Jun 21  2001 /opt/samba/swat/using_samba/ch04_06.html
  -rwxr-xr-x   1 root      users       26399 Jun 21  2001 /opt/samba/swat/using_samba/figs/sam.0902.gif
  -rwxr-xr-x   1 root      users       26441 Jul  7  1999
/opt/samba_src/samba/source/rpc_parse/parse_lsa.c
  -rwxr-xr-x   1 root      users       26595 Jul  7  1999 /opt/samba_src/samba/source/client/clientutil.c
  -rwxr-xr-x   1 root      users       26960 Jun 21  2001 /opt/samba/swat/using_samba/ch05_04.html
  -rwxr-xr-x   1 root      users       27182 Jun 21  2001 /opt/samba/swat/using_samba/ch08_06.html
  -rwxr-xr-x   1 root      users       27228 Jul 21  2000 /opt/samba_src/samba/source/libsmb/namequery.c
  -rwxr-xr-x   1 root      users       27477 Jul  7  1999 /opt/samba_src/samba/source/locking/shmem.c

  -rwxr-xr-x   1 root      users       27772 Nov 12  1999
/opt/samba_src/samba/source/nmbd/nmbd_incomingdgrams.c

  -rwxr-xr-x   1 root      users       27786 Jul 21  2000 /opt/samba_src/samba/source/lib/system.c
  -rwxr-xr-x   1 root      users       27954 Jul 21  2000 /opt/samba_src/samba/source/lib/util_sock.c
  -rwxr-xr-x   1 root      users       27984 Jun 21  2001 /opt/samba/swat/using_samba/ch05_02.html
  -rwxr-xr-x   1 root      users       28115 Jun 21  2001 /opt/samba/swat/using_samba/ch03_01.html
  -rwxr-xr-x   1 root      users       28283 Jul 21  2000 /opt/samba_src/samba/source/passdb/ldap.c
  -rwxr-xr-x   1 root      users       28339 Jun 21  2001 /opt/samba/swat/using_samba/ch06_03.html
  -rwxr-xr-x   1 root      users       28342 Jun 21  2001 /opt/samba/swat/using_samba/ch05_03.html
  -rwxr-xr-x   1 root      users       28576 Jun 21  2001 /opt/samba/swat/using_samba/ch01_04.html

  -rwxr-xr-x   1 root      users       28761 Nov 12  1999
/opt/samba_src/samba/source/rpc_server/srv_netlog.c

  -rwxr-xr-x   1 root      users       28840 Mar 19  2001
/opt/samba_src/samba/source/lib/acl_hpux_posix.c
  -rwxr-xr-x   1 root      users       28911 Jun  4  2001 /opt/samba_src/samba/source/include/rpc_samr.h
  -rwxr-xr-x   1 root      users       29732 Jul 21  2000 /opt/samba_src/samba/source/libsmb/nmblib.c
  -rwxr-xr-x   1 root      users       29932 Jul 21  2000 /opt/samba_src/samba/source/smbwrapper/smbw.c

  -rwxr-xr-x   1 root      users       30417 Nov 12  1999
/opt/samba_src/samba/source/rpc_server/srv_srvsvc.c

  -rwxr-xr-x   1 root      users       30423 Jun 21  2001 /opt/samba/man/man1/smbclient.1
  -rwxr-xr-x   1 root      users       30423 May 16  2001 /opt/samba/docs/manpages/smbclient.1
  -rwxr-xr-x   1 root      users       30474 Oct 31  2000 /opt/samba_src/samba/source/web/swat.c
  -rwxr-xr-x   1 root      users       30530 Jun 21  2001 /opt/samba/swat/using_samba/ch03_03.html
  -rwxr-xr-x   1 root      users       30974 Jul 21  2000 /opt/samba_src/samba/source/lib/util_str.c
  -rwxr-xr-x   1 root      users       31106 Jul 21  2000 /opt/samba/docs/yodldocs/smbclient.1.yo
  -rwxr-xr-x   1 root      users       31425 Jul 21  2000
/opt/samba_src/samba/source/locking/locking_slow.c
  -rwxr-xr-x   1 root      users       31735 Jul 21  2000 /opt/samba_src/samba/source/lib/kanji.c
```

```
  -rwxr-xr-x  1 root     users      31867 Jun 21  2001 /opt/samba/swat/using_samba/ch06_06.html
  -rwxr-xr-x  1 root     users      32234 Jul 21  2000 /opt/samba_src/samba/source/smbd/process.c
  -rwxr-xr-x  1 root     users      32369 Jun  4  2001
/opt/samba_src/samba/source/rpc_server/srv_pipe.c
  -rwxr-xr-x  1 root     users      32856 Jun 21  2001 /opt/samba/swat/using_samba/ch01_03.html
  -rwxr-xr-x  1 root     users      32989 Jul 21  2000 /opt/samba/docs/faq/Samba-meta-FAQ.sgml
  -rwxr-xr-x  1 root     users      33053 Jul 21  2000 /opt/samba_src/samba/source/smbd/mangle.c
  -rwxr-xr-x  1 root     users      33691 Jul 21  2000
/opt/samba_src/samba/source/rpc_parse/parse_rpc.c
  -rwxr-xr-x  1 root     users      33970 Jul 21  2000 /opt/samba_src/samba/source/passdb/passdb.c
  -rwxr-xr-x  1 root     users      34072 Jul 21  2000 /opt/samba_src/samba/source/passdb/nispass.c
  -rwxr-xr-x  1 root     users      34550 Jul  7  1999 /opt/samba_src/samba/source/libsmb/nterr.c
  -rwxr-xr-x  1 root     users      35174 Nov 12  1999 /opt/samba_src/samba/source/rpcclient/display.c
  -rwxr-xr-x  1 root     users      35539 May  3  2001 /opt/samba_src/samba/source/printing/printing.c
  -rwxr-xr-x  1 root     users      36137 Jul  7  1999 /opt/samba_src/samba/source/rpc_client/cli_pipe.c

  -rwxr-xr-x  1 root     users      36306 Nov 12  1999
/opt/samba_src/samba/source/rpc_parse/parse_misc.c

  -rwxr-xr-x  1 root     users      36599 Jul 21  2000 /opt/samba/docs/faq/Samba-meta-FAQ.txt
  -rwxr-xr-x  1 root     users      36780 Jul 21  2000 /opt/samba_src/samba/source/passdb/smbpass.c
  -rwxr-xr-x  1 root     users      37104 Jun  4  2001
/opt/samba_src/samba/source/rpc_parse/parse_reg.c
  -rwxr-xr-x  1 root     users      38454 Jul 21  2000 /opt/samba/docs/htmldocs/smbclient.1.html
  -rwxr-xr-x  1 root     users      38454 Jun 21  2001 /opt/samba/swat/help/smbclient.1.html
  -rwxr-xr-x  1 root     users      38856 Jul 21  2000 /opt/samba/docs/faq/sambafaq.sgml
  -rwxr-xr-x  1 root     users      39196 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/ubi_BinTree.h
  -rwxr-xr-x  1 root     users      39968 Mar 20  2001
/opt/samba_src/samba/source/rpc_parse/parse_net.c
  -rwxr-xr-x  1 root     users      40151 Jun 21  2001 /opt/samba/swat/using_samba/ch07_01.html
  -rwxr-xr-x  1 root     users      41592 Jul 21  2000 /opt/samba_src/samba/source/utils/torture.c
  -rwxr-xr-x  1 root     users      41839 Jul 21  2000 /opt/samba/docs/faq/sambafaq.txt
  -rwxr-xr-x  1 root     users      42020 Jun 21  2001 /opt/samba/swat/using_samba/ch07_02.html
  -rwxr-xr-x  1 root     users      42090 Jul 21  2000 /opt/samba_src/samba/source/smbd/password.c
  -rwxr-xr-x  1 root     users      43854 Jun 18  2001 /opt/samba_src/samba/source/smbd/open.c
  -rwxr-xr-x  1 root     users      43987 Jul 21  2000 /opt/samba_src/samba/source/smbd/oplock.c
  -rwxr-xr-x  1 root     users      45818 Jun 21  2001 /opt/samba/swat/using_samba/appb_03.html
  -rwxr-xr-x  1 root     users      45877 Jul  7  1999 /opt/samba_src/samba/source/ubiqx/ubi_BinTree.c
  -rwxr-xr-x  1 root     users      47987 May 16  2001 /opt/samba/docs/textdocs/cifsntdomain.txt
  -rwxr-xr-x  1 root     users      49039 Jul 21  2000 /opt/samba_src/samba/source/client/clitar.c
  -rwxr-xr-x  1 root     users      50638 Jun 21  2001 /opt/samba/swat/using_samba/ch06_04.html
  -rwxr-xr-x  1 root     users      50930 Jun 21  2001 /opt/samba/swat/using_samba/ch05_01.html
  -rwxr-xr-x  1 root     users      52538 Jul 22  1999
/opt/samba_src/samba/source/rpc_parse/parse_srv.c

  -rwxr-xr-x  1 root     users      53004 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_winsserver.c

  -rwxr-xr-x  1 root     users      53248 Mar 28  2001 /opt/cifsclient/bin/cifsumount
  -rwxr-xr-x  1 root     users      55710 May  4  2001 /opt/samba_src/samba/source/configure.in
  -rwxr-xr-x  1 root     users      56294 Jun 21  2001 /opt/samba/swat/using_samba/inx.html
  -rwxr-xr-x  1 root     users      57344 Mar 28  2001 /opt/cifsclient/bin/cifsmount
  -rwxr-xr-x  1 root     users      59074 Jun  4  2001
/opt/samba_src/samba/source/rpc_server/srv_samr.c
  -rwxr-xr-x  1 root     users      61039 Jul 21  2000 /opt/samba_src/samba/source/include/smb.h
  -rwxr-xr-x  1 root     users      61127 May  3  2001 /opt/samba_src/samba/source/client/client.c
```

```
  -rwxr-xr-x   1 root      users       62013 Jun 21  2001
/opt/samba/HP_docs/CIFS9k_Server_Rel_Notes.pdf
  -rwxr-xr-x   1 root      users       62880 Jul 21  2000
/opt/samba_src/samba/source/nmbd/nmbd_packets.c
  -rwxr-xr-x   1 root      users       68981 Sep 27  2000 /opt/samba_src/samba/source/smbd/nttrans.c
  -rwxr-xr-x   1 root      users       72853 Jun 21  2001 /opt/samba/swat/using_samba/appd_01.html
  -rwxr-xr-x   1 root      users       79269 Jul  7  1999 /opt/samba_src/samba/source/change-log
  -rwxr-xr-x   1 root      users       80218 May  3  2001 /opt/samba_src/samba/source/lib/util.c
  -rwxr-xr-x   1 root      users       85675 Apr  2  2001 /opt/samba_src/samba/source/smbd/trans2.c
  -rwxr-xr-x   1 root      users       86693 Jul 21  2000 /opt/samba_src/samba/source/libsmb/clientgen.c

  -rwxr-xr-x   1 root      users      102630 Jun  4  2001
/opt/samba_src/samba/source/rpc_parse/parse_samr.c

  -rwxr-xr-x   1 root      users      103412 Jul 21  2000 /opt/samba_src/samba/source/smbd/ipc.c
  -rwxr-xr-x   1 root      users      113692 Mar 28  2001 /opt/cifsclient/conf/lib/libcifs.a
  -rwxr-xr-x   1 root      users      114470 Jun 18  2001 /opt/samba_src/samba/source/param/loadparm.c
  -rwxr-xr-x   1 root      users      118740 Jun 21  2001 /opt/samba/swat/using_samba/appc_01.html
  -rwxr-xr-x   1 root      users      124175 Jun 21  2001 /opt/samba/swat/using_samba/ch09_02.html
  -rwxr-xr-x   1 root      users      129811 Mar 14  2001 /opt/samba_src/samba/source/smbd/reply.c
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.437
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.737
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.850
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.852
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.861
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.866
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001
/etc/opt/samba/codepages/unicode_map.ISO8859-1
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001
/etc/opt/samba/codepages/unicode_map.ISO8859-2
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001
/etc/opt/samba/codepages/unicode_map.ISO8859-5
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001
/etc/opt/samba/codepages/unicode_map.ISO8859-7
  -rwxr-xr-x   1 root      users      131614 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.KOI8-R
  -rwxr-xr-x   1 root      users      135489 Jun  4  2001 /opt/samba_src/samba/source/include/proto.h
  -rwxr-xr-x   1 root      users      234167 Jun 18  2001 /opt/samba/docs/manpages/smb.conf.5
  -rwxr-xr-x   1 root      users      234167 Jun 21  2001 /opt/samba/man/man5/smb.conf.5
  -rwxr-xr-x   1 root      users      235942 Jul 21  2000 /opt/samba/docs/yodldocs/smb.conf.5.yo
  -rwxr-xr-x   1 root      users      262174 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.932
  -rwxr-xr-x   1 root      users      262174 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.936
  -rwxr-xr-x   1 root      users      262174 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.949
  -rwxr-xr-x   1 root      users      262174 Jun 21  2001 /etc/opt/samba/codepages/unicode_map.950
  -rwxr-xr-x   1 root      users      299912 Jun 18  2001 /opt/samba/docs/htmldocs/smb.conf.5.html
  -rwxr-xr-x   1 root      users      299912 Jun 21  2001 /opt/samba/swat/help/smb.conf.5.html

  -rwxr-xr-x   1 root      users      303531 Jul 21  2000
/opt/samba_src/samba/source/codepages/CP932.TXT

  -rwxr-xr-x   1 root      users      307200 Jun 21  2001 /opt/samba/bin/make_unicodemap
  -rwxr-xr-x   1 root      users      307200 Jun 21  2001 /opt/samba/bin/testparm
  -rwxr-xr-x   1 root      users      309025 May  4  2001 /opt/samba_src/samba/source/configure
  -rwxr-xr-x   1 root      users      311296 Jun 21  2001 /opt/samba/bin/make_printerdef
  -rwxr-xr-x   1 root      users      311296 Jun 21  2001 /opt/samba/bin/make_smbcodepage
  -rwxr-xr-x   1 root      users      323584 Jun 21  2001 /opt/samba/bin/testprns
  -rwxr-xr-x   1 root      users      339968 Jun 21  2001 /opt/samba/bin/smbstatus
```

```
  -rwxr-xr-x   1 root      users      417792 Jun 21  2001 /opt/samba/bin/nmblookup
  -rwxr-xr-x   1 root      users      417792 Jun 21  2001 /opt/samba/bin/smbspool
  -rwxr-xr-x   1 root      users      499712 Jun 21  2001 /opt/samba/bin/smbclient

  -rwxr-xr-x   1 root      users      522724 Jul 21  2000
/opt/samba_src/samba/source/codepages/CP950.TXT

  -rwxr-xr-x   1 root      users      598016 Jun 21  2001 /opt/samba/bin/nmbd
  -rwxr-xr-x   1 root      users      618496 Mar 28  2001 /opt/cifsclient/sbin/cifsclientd
  -rwxr-xr-x   1 root      users      733184 Jun 21  2001 /opt/samba/bin/smbpasswd
  -rwxr-xr-x   1 root      users      778240 Jun 21  2001 /opt/samba/bin/rpcclient
  -rwxr-xr-x   1 root      users      784456 Mar 28  2001 /opt/samba/HP_docs/CIFS9k_Server_Manual.pdf

  -rwxr-xr-x   1 root      users      807995 Jul 21  2000
/opt/samba_src/samba/source/codepages/CP949.TXT

  -rwxr-xr-x   1 root      users      815104 Jun 21  2001 /opt/samba/bin/swat

  -rwxr-xr-x   1 root      users      839370 Jul 21  2000
 /opt/samba_src/samba/source/codepages/CP936.TXT

  -rwxr-xr-x   1 root      users     1355776 Jun 21  2001 /opt/samba/bin/smbd
  dr-x------   2 ids       ids          96 Jun 12 13:31 /opt/ids/bin/gui/License
  dr-x------   2 ids       ids          96 Jun 12 13:31 /opt/ids/lib
  dr-x------   2 ids       ids          96 Jun 12 13:31 /opt/ids/newconfig/etc/opt/ids
  dr-x------   2 ids       ids          96 Jun 12 13:31 /opt/ids/response/vpo
  dr-x------   2 ids       ids        1024 Jun 12 13:31 /opt/ids/bin/gui/javaHelp
  dr-x------   2 ids       ids        1024 Jun 12 13:31 /opt/ids/bin/gui/symlib
  dr-x------   2 ids       ids        1024 Jun 12 13:31 /opt/ids/lbin
  dr-x------   2 ids       ids        1024 Jun 12 13:31 /opt/ids/newconfig/var/opt/ids/gui/SurveillanceGroups
  dr-x------   2 ids       ids        1024 Jun 12 13:31
/opt/ids/newconfig/var/opt/ids/gui/SurveillanceSchedules
  dr-x------   2 ids       ids        1024 Jun 12 13:31 /opt/ids/newconfig/var/opt/ids/gui/Templates
  dr-x------   2 ids       ids        1024 Jun 12 13:31 /opt/ids/templates
  dr-x------   2 ids       ids        2048 Jun 12 13:31 /opt/ids/bin/gui/Images
  dr-x------   3 ids       ids          96 Jun 12 13:31 /opt/ids/newconfig/etc
  dr-x------   3 ids       ids          96 Jun 12 13:31 /opt/ids/newconfig/etc/opt
  dr-x------   3 ids       ids          96 Jun 12 13:31 /opt/ids/newconfig/var
  dr-x------   3 ids       ids          96 Jun 12 13:31 /opt/ids/newconfig/var/opt
  dr-x------   3 ids       ids          96 Jun 12 13:31 /opt/ids/newconfig/var/opt/ids
  dr-x------   3 ids       ids          96 Jun 12 13:31 /opt/ids/response
  dr-x------   3 ids       ids        1024 Jun 12 13:31 /opt/ids/bin
  dr-x------   4 ids       ids          96 Jun 12 13:31 /opt/ids/newconfig
  dr-x------   4 ids       ids          96 May 23 14:56 /etc/opt/ids/certs
  dr-x------   5 ids       ids          96 Jun 12 13:31 /opt/ids/newconfig/var/opt/ids/gui
  dr-x------   6 ids       ids        1024 Jun 12 13:40 /opt/ids/bin/gui
  dr-xr-xr-x   2 ids       ids          96 Jun 12 13:31 /opt/ids/share/doc
  dr-xr-xr-x   2 ids       ids          96 Jun 12 13:31 /opt/ids/share/man/man5
  dr-xr-xr-x   2 ids       ids        1024 Jun 12 13:31 /opt/ids/share/examples
  dr-xr-xr-x   2 ids       ids        1024 Jun 12 13:31 /opt/ids/share/man/man1m
  dr-xr-xr-x   4 ids       ids          96 Jun 12 13:31 /opt/ids/share/man
  dr-xr-xr-x   5 ids       ids          96 Jun 12 13:31 /opt/ids/share
  dr-xr-xr-x   9 ids       ids        1024 Jun 12 13:31 /opt/ids
  drwx------   2 ids       ids          96 Jul 19 09:17 /etc/opt/ids/certs/agent
  drwx------   2 ids       ids          96 Jun 12 13:31 /etc/opt/OV/share/conf/ecs/1
  drwx------   2 ids       ids        1024 Jun 13 07:16 /etc/opt/ids/certs/admin
```

```
drwx------  3 ids      ids          96 Jun 12 13:31 /etc/opt/ids/gui
drwx------  4 ids      ids          96 Jul  9 14:35 /etc/opt/ids
drwx------  6 ids      ids        1024 Aug  6 08:06 /var/opt/ids
drwxr-xr-x  2 ids      ids          96 Jul 29 14:37 /etc/opt/ids/gui/config
drwxr-xr-x  2 root     users        96 May 15 08:35 /opt/cifsclient/HP_Docs
drwxr-xr-x  2 root     users        96 May 15 08:35 /opt/cifsclient/conf/lib
drwxr-xr-x  2 root     users        96 May 15 08:35 /opt/cifsclient/conf/master.d
drwxr-xr-x  2 root     users        96 May 15 08:35 /opt/cifsclient/newconfig/etc/opt/cifsclient
drwxr-xr-x  2 root     users        96 May 15 08:35 /opt/cifsclient/sbin
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/HA/active_active
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/HA/active_standby
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/HP_docs
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/examples/autofs
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/examples/dce-dfs
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/examples/misc
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/examples/printing
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/examples/simple
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/examples/svr4-startup
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/examples/thoralf
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/examples/wins_hook
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/man/man5
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/man/man7
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/newconfig/etc/opt/samba
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/newconfig/etc/rc.config.d
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba/swat/include
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba_src/samba/source/bin
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba_src/samba/source/groupdb
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba_src/samba/source/lsarpcd
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba_src/samba/source/mem_man
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba_src/samba/source/param
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba_src/samba/source/profile
drwxr-xr-x  2 root     users        96 May 15 08:38 /opt/samba_src/samba/source/web/po
drwxr-xr-x  2 root     users        96 May 15 08:40 /opt/cifsclient/pam/newconfig/etc/opt/cifsclient/pam
drwxr-xr-x  2 root     users        96 May 15 08:51 /etc/opt/cifsclient/pam
drwxr-xr-x  2 root     users      1024 May 15 08:35 /opt/cifsclient/bin
drwxr-xr-x  2 root     users      1024 May 15 08:38 /etc/opt/samba/codepages
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/bin
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/docs/faq
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/docs/htmldocs
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/docs/manpages
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/docs/yodldocs
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/examples/printer-accounting
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/examples/tridge
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/examples/validchars
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/man/man1
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/man/man8
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/script
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/swat/help
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/swat/images
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba/swat/using_samba/gifs
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba_src/samba/source/client
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba_src/samba/source/codepages
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba_src/samba/source/include
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba_src/samba/source/lib
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba_src/samba/source/libsmb
drwxr-xr-x  2 root     users      1024 May 15 08:38 /opt/samba_src/samba/source/locking
```

```
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/nmbd
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/passdb
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/printing
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/rpc_client
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/rpc_parse
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/rpc_server
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/rpcclient
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/script
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/smbd
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/smbwrapper
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/tests
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/ubiqx
drwxr-xr-x  2 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/utils
drwxr-xr-x  2 root     users     2048 May 15 08:35 /etc/opt/cifsclient/unitables
drwxr-xr-x  2 root     users     2048 May 15 08:38 /opt/samba/docs/textdocs
drwxr-xr-x  2 root     users     3072 May 15 08:38 /opt/samba/swat/using_samba/figs
drwxr-xr-x  3 root     users       96 May 15 08:35 /opt/cifsclient/newconfig
drwxr-xr-x  3 root     users       96 May 15 08:35 /opt/cifsclient/newconfig/etc/opt
drwxr-xr-x  3 root     users       96 May 15 08:38 /etc/opt/samba
drwxr-xr-x  3 root     users       96 May 15 08:38 /opt/samba/newconfig
drwxr-xr-x  3 root     users       96 May 15 08:38 /opt/samba/newconfig/etc/opt
drwxr-xr-x  3 root     users       96 May 15 08:38 /opt/samba_src
drwxr-xr-x  3 root     users       96 May 15 08:38 /opt/samba_src/samba
drwxr-xr-x  3 root     users       96 May 15 08:38 /var/opt/samba
drwxr-xr-x  3 root     users       96 May 15 08:40 /opt/cifsclient/pam/newconfig
drwxr-xr-x  3 root     users       96 May 15 08:40 /opt/cifsclient/pam/newconfig/etc
drwxr-xr-x  3 root     users       96 May 15 08:40 /opt/cifsclient/pam/newconfig/etc/opt
drwxr-xr-x  3 root     users       96 May 15 08:40 /opt/cifsclient/pam/newconfig/etc/opt/cifsclient
drwxr-xr-x  3 root     users     1024 May 15 08:38 /opt/samba_src/samba/source/web
drwxr-xr-x  4 root     users       96 May 15 08:35 /opt/cifsclient/conf
drwxr-xr-x  4 root     users       96 May 15 08:35 /opt/cifsclient/newconfig/etc
drwxr-xr-x  4 root     users       96 May 15 08:38 /opt/samba/HA
drwxr-xr-x  4 root     users       96 May 15 08:38 /opt/samba/newconfig/etc
drwxr-xr-x  4 root     users       96 May 15 08:50 /etc/opt/cifsclient
drwxr-xr-x  4 root     users     2048 May 15 08:38 /opt/samba/swat/using_samba
drwxr-xr-x  6 root     users       96 May 15 08:38 /opt/samba/man
drwxr-xr-x  6 root     users       96 May 15 08:38 /opt/samba/swat
drwxr-xr-x  7 root     users     1024 May 15 08:38 /opt/samba/docs
drwxr-xr-x  8 root     users     1024 May 15 08:40 /opt/cifsclient
drwxr-xr-x 11 root     users     1024 May 15 08:38 /opt/samba
drwxr-xr-x 13 root     users     1024 May 15 08:38 /opt/samba/examples
drwxr-xr-x 28 root     users     1024 May 15 08:38 /opt/samba_src/samba/source

drwxrwxr-x  2 20000    12064       96 May 15 08:51
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/4

drwxrwxr-x  2 20000    12064     1024 May 15 08:51
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct/2

drwxrwxr-x  4 20000    12064       96 May 15 08:51
/opt/OV/newconfig/OpC/var/opt/OV/conf/OpC/hpux/instruct
```

Explanation

With a few exceptions (which are not reported) system files should be owned by an administrative user and group (administrative users are those logins with an UID below 100 and have an impossible password, except for the root login; administrative groups are those group names with GIDs below 10 with a impossible password [containing a "*" within the password field]). Ownerships other than an administrative user, increases the chance of accidental (or intentional) removal or alteration of system files. If an administrative user has a usable password, then files owned by it will be reported as a non-standard. Equally, system files should not be publicly writable.

Corrective Action

Change the owner of the indicated file(s) to an administrative user (root or bin are good examples). Acceptable group ownerships are other or bin. Take care NOT to change the owners of SUID or SGID files.

Execute the following for each indicated file:

chown bin <filename>
chgrp bin <filename>

- Improper ownerships/permissions with users' $HOME directory and/or files: [file/directory ownerships should be that of login; directory permissions should be at most 755 (SUID-0 logins' $HOME should be at most 740); file permissions should be at most 740.]

```
Login: root: (UID: 0)
  drwxr-xr-x  35 root      root        2048 Aug 23 14:14 /
  -r--r--r--   1 bin       bin         1157 May 16 09:28 /.profile

Login: bevb: (UID: 102)
  -rw-r--r--   1 bevb      adm          632 Jul 26 11:02 /home/bevb/.profile
  -rw-r--r--   1 bevb      adm          832 May 21 08:01 /home/bevb/.cshrc
  -rw-r--r--   1 bevb      adm          334 May 21 08:01 /home/bevb/.login
  -rw-r--r--   1 bevb      adm          347 May 21 08:01 /home/bevb/.exrc

Login: nanf: (UID: 103)
  -rw-r--r--   1 nanf      adm          540 Jun 19 09:02 /home/nanf/.profile
  -rw-r--r--   1 nanf      adm          832 May 21 08:04 /home/nanf/.cshrc
  -rw-r--r--   1 nanf      adm          334 May 21 08:04 /home/nanf/.login
  -rw-r--r--   1 nanf      adm          347 May 21 08:04 /home/nanf/.exrc

Login: scotth: (UID: 104)
  -rw-r--r--   1 scotth    adm          439 May 21 08:07 /home/scotth/.profile
  -rw-r--r--   1 scotth    adm          832 May 21 08:07 /home/scotth/.cshrc
  -rw-r--r--   1 scotth    adm          334 May 21 08:07 /home/scotth/.login
  -rw-r--r--   1 scotth    adm          347 May 21 08:07 /home/scotth/.exrc

Login: dianemcd: (UID: 106)
  -rw-r--r--   1 dianemc   dba         1272 Jul  8 15:19 /home/dianemc/.profile
  -rw-r--r--   1 dianemc   dba          832 May 21 08:19 /home/dianemc/.cshrc
  -rw-r--r--   1 dianemc   dba          334 May 21 08:19 /home/dianemc/.login
  -rw-r--r--   1 dianemc   dba          347 May 21 08:19 /home/dianemc/.exrc

Login: oracle: (UID: 107)
  -rw-r--r--   1 oracle    dba         1362 Jul  9 09:48 /home/oracle/.profile
```

```
-rw-r--r--  1 oracle    dba          832 May 21 08:21 /home/oracle/.cshrc
-rw-r--r--  1 oracle    dba          334 May 21 08:21 /home/oracle/.login
-rw-r--r--  1 oracle    dba          347 May 21 08:21 /home/oracle/.exrc

Login: monah: (UID: 108)
-rw-r--r--  1 monah     users        439 May 22 08:33 /home/monah/.profile
-rw-r--r--  1 monah     users        832 May 22 08:33 /home/monah/.cshrc
-rw-r--r--  1 monah     users        334 May 22 08:33 /home/monah/.login
-rw-r--r--  1 monah     users        347 May 22 08:33 /home/monah/.exrc

Login: bobm: (UID: 109)
-rw-r--r--  1 bobm      users        439 May 22 08:35 /home/bobm/.profile
-rw-r--r--  1 bobm      users        832 May 22 08:35 /home/bobm/.cshrc
-rw-r--r--  1 bobm      users        334 May 22 08:35 /home/bobm/.login
-rw-r--r--  1 bobm      users        347 May 22 08:35 /home/bobm/.exrc

Login: randys: (UID: 111)
-rw-r--r--  1 randys    adm          439 Jun 12 13:19 /home/randys/.profile
-rw-r--r--  1 randys    adm          832 Jun 12 13:19 /home/randys/.cshrc
-rw-r--r--  1 randys    adm          334 Jun 12 13:19 /home/randys/.login
-rw-r--r--  1 randys    adm          347 Jun 12 13:19 /home/randys/.exrc
```

Explanation

As a matter of good overall security, users' $HOME directories and their environment files,. profile, .kshrc, .login, .logout, .cshrc, .rhosts, .emacs, .forward, exrc, .netrc should be only writable by the owner (.netrc should be only writable AND readable by the owner since it contains un-encrypted passwords). It is critically important that these files are at minimum not publicly writable.

It is good system administration to ensure that individual login directories are not publicly readable/writable/executable and not group writable. A directory with the execute bit set containing files which are publicly readable, allows intruders the ability to copy files to another directory and read the contents. This generally violates the idea of an individual login account. This is especially true for users that can gain root privileges. This is for their own protection but also makes it more difficult for an intruder to gain wide access to the system.

Corrective Action

- Change the file/directory permissions to the permissions listed below:

 # Permissions for users' directory.
directory_mode=750

 # Permissions for users' login scripts (see sfiles_user file).
file_mode=740

then execute:

chmod 750 <users' $HOME directories>
chmod 740 <$HOME/login_files>

- Also ensure that ownerships of the <login_files> are correct by executing:

cd <users' $HOME directory>
find . -exec chown <user> {} \;

If the "/" directory was reported, it is not recommended to change the "/" permissions but it is advised to move root's $HOME directory out of the system root directory (e.g. to /roothome).

- Device files not located in /dev directory

crw------- 1 root root 203 0x043000 May 16 16:21
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1021580510700089

crw------- 1 root root 203 0x060000 May 16 16:21
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1021580514707122

crw------- 1 root root 203 0x050500 May 21 10:28
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1021991306505152

crw------- 1 root root 203 0x051100 May 21 12:43
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1021999399167609

crw------- 1 root root 203 0x072000 May 21 13:15
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1022001310127265

crw------- 1 root root 203 0x072000 May 21 13:15
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1022001310129539

crw------- 1 root root 203 0x051000 May 21 13:28
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1022002090104401

crw------- 1 root root 203 0x051000 May 21 13:28
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102200209098895

crw------- 1 root root 203 0x050500 May 30 11:03
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1022770989502467

crw------- 1 root root 203 0x050500 May 30 11:03
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1022770989508694

crw------- 1 root root 203 0x070000 May 31 10:55
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1022856933294557

crw------- 1 root root 203 0x080000 May 31 10:55
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1022856938179120

```
  crw-------  1 root     root     203 0x032000 Jun  3 15:49
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023133743549307

  crw-------  1 root     root     203 0x032000 Jun  3 15:49
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023133743566986

  crw-------  1 root     root     203 0x070000 Jun  3 15:49
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023133749470268

  crw-------  1 root     root     203 0x070000 Jun 11 09:32
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023802358852588

  crw-------  1 root     root     203 0x032000 Jun 12 09:59
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023890371441013

  crw-------  1 root     root     203 0x070000 Jun 12 09:59
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023890378677281

  crw-------  1 root     root     203 0x070000 Jun 12 10:05
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023890754694770

  crw-------  1 root     root     203 0x070000 Jun 12 13:42
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023903750246854

  crw-------  1 root     root     203 0x051000 Jun 13 12:45
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023986709231715

  crw-------  1 root     root     203 0x070000 Jun 13 12:45
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023986717188295

  crw-------  1 root     root     203 0x070000 Jun 13 12:51
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102398708534169

  crw-------  1 root     root     203 0x060000 Jun 13 13:26
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023989211511997

  crw-------  1 root     root     203 0x060000 Jun 13 13:26
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023989217852167

  crw-------  1 root     root     203 0x060000 Jun 13 13:33
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1023989586790345

  crw-------  1 root     root     203 0x051000 Jun 14 14:04
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024077878783332

  crw-------  1 root     root     203 0x060000 Jun 14 14:04
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102407788648051

  crw-------  1 root     root     203 0x060000 Jun 14 14:11
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024078263591850

  crw-------  1 root     root     203 0x022000 Jun 14 15:55
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102408455080540
```

crw------- 1 root root 203 0x060000 Jun 14 15:55
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024084558502144

crw------- 1 root root 203 0x060000 Jun 14 16:04
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024085055736861

crw------- 1 root root 203 0x060000 Jun 14 18:55
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024095359141698

crw------- 1 root root 203 0x060000 Jun 14 19:02
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102409572985856

crw------- 1 root root 203 0x050400 Jun 14 19:11
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024096263329526

crw------- 1 root root 203 0x050400 Jun 14 19:11
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024096263335363

crw------- 1 root root 203 0x060000 Jun 14 19:11
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024096270787001

crw------- 1 root root 203 0x060000 Jun 14 19:17
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024096642924638

crw------- 1 root root 203 0x060000 Jun 19 15:21
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024514470722365

crw------- 1 root root 203 0x060000 Jun 19 15:27
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024514850125382

crw------- 1 root root 203 0x060000 Jun 21 10:07
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024668437926206

crw------- 1 root root 203 0x070100 Jun 21 10:07
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024668439716138

crw------- 1 root root 203 0x060000 Jun 21 10:13
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024668813178992

crw------- 1 root root 203 0x060000 Jun 24 11:14
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1024931677780371

crw------- 1 root root 203 0x050000 Jun 26 07:49
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1025092170472847

crw------- 1 root root 203 0x050000 Jun 26 07:49
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1025092170475640

crw------- 1 root root 203 0x060000 Jun 26 07:49
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1025092176710843

crw------- 1 root root 203 0x043000 Jun 26 07:49
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1025092181558559

crw------- 1 root root 203 0x060000 Jun 26 07:55
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1025092548110682

```
  crw-------  1 root     root     203 0x060000 Jun 26 15:34
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1025120087507101

  crw-------  1 root     root     203 0x060000 Jun 26 15:41
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1025120473222573

  crw-------  1 root     root     203 0x060000 Jul  1 14:10
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102554701495260

  crw-------  1 root     root     203 0x060000 Jul  2 08:10
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1025611835753453

  crw-------  1 root     root     203 0x060000 Jul  2 12:30
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102562745159465

  crw-------  1 root     root     203 0x060000 Jul  8 08:13
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1026130390785042

  crw-------  1 root     root     203 0x060000 Jul  8 12:14
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1026144875154191

  crw-------  1 root     root     203 0x060000 Jul  8 12:29
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102614575626126

  crw-------  1 root     root     203 0x060000 Jul 19 08:36
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1027082198416719

  crw-------  1 root     root     203 0x051600 Jul 22 11:03
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1027350229512838

  crw-------  1 root     root     203 0x051600 Jul 22 11:03
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1027350229518591

  crw-------  1 root     root     203 0x060000 Jul 22 11:03
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102735023714491

  crw-------  1 root     root     203 0x070100 Jul 22 11:04
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1027350240249744

  crw-------  1 root     root     203 0x060000 Jul 22 11:10
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1027350604437461

  crw-------  1 root     root     203 0x060000 Jul 30 16:12
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102805995051017

  crw-------  1 root     root     203 0x060000 Jul 30 16:18
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.102806031928468

  crw-------  1 root     root     203 0x060000 Aug  1 06:24
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.10281974904279

  crw-------  1 root     root     203 0x043000 Aug  1 06:24
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028197495608767
```

crw------- 1 root root 203 0x043000 Aug 1 06:24
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028197495619553

crw------- 1 root root 203 0x060000 Aug 1 06:30
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028197858931954

crw------- 1 root root 203 0x060000 Aug 1 08:42
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028205755918042

crw------- 1 root root 203 0x060000 Aug 1 08:48
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028206124406986

crw------- 1 root root 203 0x050400 Aug 1 09:57
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028210220420317

crw------- 1 root root 203 0x060000 Aug 1 09:57
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028210226801085

crw------- 1 root root 203 0x072200 Aug 1 09:57
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028210232922013

crw------- 1 root root 203 0x060000 Aug 1 10:03
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028210597871721

crw------- 1 root root 203 0x060000 Aug 1 15:39
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028230749397498

crw------- 1 root root 203 0x070000 Aug 1 15:39
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028230753626976

crw------- 1 root root 203 0x060000 Aug 1 15:45
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028231117926827

crw------- 1 root root 203 0x060000 Aug 2 14:23
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028312607875886

crw------- 1 root root 203 0x043000 Aug 2 14:23
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028312612679274

crw------- 1 root root 203 0x060000 Aug 2 14:29
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028312976676986

crw------- 1 root root 203 0x060000 Aug 6 08:06
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028635589623399

crw------- 1 root root 203 0x060000 Aug 6 14:57
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028660265373800

crw------- 1 root root 203 0x072000 Aug 6 14:57
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028660269741796

crw------- 1 root root 203 0x060000 Aug 6 15:04
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028660649486199

crw------- 1 root root 203 0x032000 Aug 7 09:43
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028727800478465

```
  crw-------  1 root     root      203 0x032000 Aug  7 09:43
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028727800488867

  crw-------  1 root     root      203 0x060000 Aug  7 09:43
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028727809447305

  crw-------  1 root     root      203 0x060000 Aug  7 09:49
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028728190637599

  crw-------  1 root     root      203 0x060000 Aug  7 12:15
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028736928578846

  crw-------  1 root     root      203 0x060000 Aug  9 07:26
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1028892360231026

  crw-------  1 root     root      203 0x060000 Aug 22 09:53
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1030024423364270

  crw-------  1 root     root      203 0x060000 Aug 22 10:48
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.103002771816258

  crw-------  1 root     root      203 0x050600 Aug 22 10:48
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1030027720282783

  crw-------  1 root     root      203 0x060000 Aug 22 10:54
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1030028096384179

  crw-------  1 root     root      203 0x060000 Aug 22 11:09
/var/opt/sanmgr/hostagent/tmp/SG_DEV_FILE.1030028978977301

  crw-------  1 root     root      203 0x012000 Jun  3 10:41 /var/tmp/rdskULAa02693
```

Explanation

Devices, such as terminals, disks, tape drives, are accessed through special files known as device files. These files are located in the /dev directory. Device files outside of the /dev directory probably should be relocated to /dev. These files can easily go unnoticed potentially permitting logins to have direct access to the systems' devices (bypassing the UNIX file system security - file permissions).

Corrective Action

Determine why the file exists and why it isn't located in /dev (or one of its subdirectories). If the file is in use, and you deem its use appropriate, relocate it (and all references to it) to an appropriate entry in the /dev directory. Be aware that in a clustered environment /dev is context dependent.

- No umask set in /etc/profile, /etc/csh.login

Explanation

A good way to insure appropriate file permissions system-wide is to have an appropriate umask setting. The umask setting determines permissions for all newly created files. If the system umask is set to 000 or 001 or 004, then newly created files will be publicly writable for any users who do not set their own umask. This is generally undesirable, and is especially so in the case of root. A umask of 002 is considered minimally secure while 022 is preferred.

Corrective Action

Add the following line to /etc/profile and/or /etc/csh.login: umask 022

Note: It is also good policy to have root's. profile, .cshrc, .kshrc or login, set an appropriate umask.

Class B Problem

- System files/directories publicly writable

```
  -r-xr-xrwx   1 root      sys          107 Jun 19 09:49 /etc/banner.telnet
  -rw-rw-rw-   1 bevb       adm        1520 Jun 21 10:07 /usr/local/flexlm/bin/logfile
  -rw-rw-rw-   1 bin        bin        2012 Oct 25  2001
/usr/newconfig/var/stm/config/tools/exercise/hosts.cfg

  -rw-rw-rw-   1 lp         lp            0 Aug 23 10:04 /opt/hpnpl/tmp/lj5x6535
  -rw-rw-rw-   1 lp         lp            0 May 20 11:40 /opt/hpnpl/tmp/ljx0005520
  -rw-rw-rw-   1 root       root          0 Jun 24 11:04 /stand/.kmsystune_lock
  -rw-rw-rw-   1 root       root          0 May 15 09:02 /var/adm/automount.log
  -rw-rw-rw-   1 root       root          5 Aug 22 11:38 /var/adm/cmcluster/cmcld.pid
  -rw-rw-rw-   1 root       root        697 Jul 31 09:58 /etc/ORATAB
  -rw-rw-rw-   1 root       root        697 Jul 31 09:58 /etc/ORATAB.bckp
  -rw-rw-rw-   1 root       root      84734 Aug 22 11:09
/opt/sanmgr/hostagent/TraceFile.txt

  -rw-rw-rw-   1 root       sys           0 May 23 12:13 /etc/ftpd/ftpgroups
  -rw-rw-rw-   1 root       sys           6 May 20 10:41 /opt/hpnpl/admin/activefile
  -rw-rw-rw-   1 root       sys           6 May 30 08:31 /etc/ftpd/ftpd.pid
  -rw-rw-rw-   1 root       sys          28 May 21 11:10 /etc/cmcluster/cmclnodelist
  -rw-rw-rw-   1 root       sys          47 Jun 12 10:43 /etc/pfs_fstab
  -rw-rw-rw-   1 root       sys          52 Jun 19 12:33 /etc/default/security
```

```
  -rw-rw-rw-   1 root      sys           78 Jun 19 09:23 /etc/motd
  -rw-rw-rw-   1 root      sys         1085 May 15 12:09 /etc/bevout
  -rw-rw-rw-   1 root      sys         1168 May 16 12:08 /var/adm/cleanup.log
  -rw-rw-rw-   1 root      sys         1776 Aug 22 11:31 /etc/opt/ipf/ipf.conf
  -rw-rw-rw-   1 root      sys         4908 Aug 22 11:15
/etc/cmcluster/cmclconfig.ascii.old
  -rw-rw-rw-   1 root      sys        10814 Jun  3 16:18
/opt/sanmgr/commandview/client/sbin/cvuiTaskLog.log

  -rw-rw-rw-   1 root      sys        75963 Aug 25 11:19
/opt/sanmgr/commandview/client/sbin/TraceFile.txt

  -rw-rw-rw-   1 root      sys       363959 Aug 26 08:01
/etc/cmcluster/oracle_sid/oracle_sid.cntl.log

  -rw-rw-rw-   1 root      sys     24903680 Jul 31 08:41 /etc/cluster.tar
  drwxrwxrwt   2 bin       bin           96 May 15 08:21 /var/home
  drwxrwxrwx   2 bin       bin           96 Aug 26 09:59 /usr/local/bin
  drwxrwxrwx   2 bin       bin           96 May 15 08:22 /usr/local/man
  drwxrwxrwx   2 bin       bin           96 May 15 08:24 /usr/local/etc
  drwxrwxrwx   2 bin       bin           96 May 15 08:24 /usr/local/games
  drwxrwxrwx   2 bin       bin           96 May 15 08:38 /opt/tomcat/logs
  drwxrwxrwx   2 bin       bin           96 May 15 08:38 /opt/tomcat/work
  drwxrwxrwx   2 bin       bin           96 May 15 08:39 /opt/netscape/dynfonts
  drwxrwxrwx   2 bin       bin           96 May 15 08:40 /opt/netscape/plugins
  drwxrwxrwx   2 bin       bin           96 May 15 08:40 /opt/netscape/talkback
  drwxrwxrwx   2 bin       bin           96 May 15 08:48 /var/news
  drwxrwxrwx   2 bin       bin           96 May 23 14:56 /usr/local/lib
  drwxrwxrwx   2 bin       bin         1024 Aug 22 11:09 /opt/apache/logs
  drwxrwxrwx   2 bin       bin        10240 Aug 23 14:18 /var/rbootd
  drwxrwxrwx   2 root      other         96 May 15 08:42
/usr/newconfig/var/stm/tools/monitor

  drwxrwxrwx   2 root      other         96 May 15 08:42 /var/adm/diag
  drwxrwxrwx   2 root      sys           96 Jun 14 17:34 /var/opt/oracle
  drwxrwxrwx   2 root      sys           96 Jun 19 13:32 /usr/local/flexlm/daemons
  drwxrwxrwx   2 root      sys           96 Jun 20 15:30 /usr/local/flexlm/licenses
  drwxrwxrwx   2 root      sys           96 May 15 08:41 /opt/cmcluster/toolkit/db2
  drwxrwxrwx   2 root      sys           96 May 15 08:41 /opt/prm/newconfig/RelNotes
  drwxrwxrwx   2 root      sys           96 May 15 08:49 /var/adm/streams
  drwxrwxrwx   2 root      sys         1024 Aug 20 10:37 /etc/cmcluster/oracle_sid
  drwxrwxrwx   2 root      sys         1024 Jun 20 15:46 /usr/local/flexlm/bin
  drwxrwxrwx   2 root      sys         1024 May 15 08:41
/opt/prm/bin/jre/bin/PA_RISC2.0/native_threads

  drwxrwxrwx   3 root      other         96 May 15 08:42 /usr/newconfig/var/stm/tools
```

```
drwxrwxrwx  5 root     other        96 May 15 08:42 /var/stm
drwxrwxrwx  5 root     sys          96 Jun 19 13:32 /usr/local/flexlm
drwxrwxrwx  8 bin      bin        1024 Jun 19 13:31 /usr/local
```

Explanation

As a general rule, a file or directory should have public write permission turned on only if there is a need to do so. Nearly all system files should not be publicly writable, both as a matter of good practice and to prevent accidental (or intentional) unauthorized over-writing (unless there is a specific need for such permissions). The files and directories listed here should not have public write permissions and should only be writable by administrative UID/GIDs.

Corrective Action

Execute the following:

chmod o-w <file_or_dir> or chmod g-w <file_or_dir>

- Compromised fileset integrity in SD-installed software

Fileset "IDS.IDS-ADM-RUN,l=/opt/ids,r=B.02.01.32" issues
File "/opt/ids/bin/idsgui" should have mtime "1002751243" but the actual mtime is "1027598906"
File "/opt/ids/bin/idsgui" should have size "7099" bytes but the actual size is "7100" bytes
Fileset "IDS.IDS-ADM-RUN,l=/opt/ids,r=B.02.01.32" had file errors

Fileset "ASANMGRHA.SANMGRHA_TAR,l=/,r=C.0164.0" issues:
File "/opt/SanMgrHA.tar" missing.
Fileset "ASANMGRHA.SANMGRHA_TAR,l=/,r=C.0164.0" had file errors.

Fileset "CMDVIEWCLT.CLTCLASSES,l=/,r=A.1.04.00" issues:
File "/opt/sanmgr/commandview/client/classes/DOFactory.jar" should have mode "644" but the actual mode is "555".
File "/opt/sanmgr/commandview/client/classes/DOFactory.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".
File "/opt/sanmgr/commandview/client/classes/DeviceDB.jar" should have mode "644" but the actual mode is "555".
File "/opt/sanmgr/commandview/client/classes/DeviceDB.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/JBODMgrClui.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/JBODMgrClui.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/JBODMgrGui.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/JBODMgrGui.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/LogDB.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/LogDB.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/PerfDB.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/PerfDB.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/clui.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/clui.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/cvui.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/cvui.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/dev_obj/JBODObjSrv.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/dev_obj/JBODObjSrv.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/dev_obj/cassinidevobj.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/dev_obj/cassinidevobj.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/disc.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/disc.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/download.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/download.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/gui.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/gui.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/help/Cronus_Help_System.jar" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/help/Cronus_Help_System.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/help/JBODhelp.jar" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/help/JBODhelp.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/help/Launcherhelp.jar" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/help/Launcherhelp.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/hostcompsdk.jar" should have mode "544" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/hostcompsdk.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/jcchart.jar" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/jcchart.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/jcore.jar" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/jcore.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/jh.jar" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/jh.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/launcher.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/launcher.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/logclui.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/logclui.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/panutils.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/panutils.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/classes/sandevice.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/classes/sandevice.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

Fileset "CMDVIEWCLT.CLTCLASSES,l=/,r=A.1.04.00" had file errors.

Fileset "CMDVIEWCLT.CLTCOMMANDS,l=/,r=A.1.04.00" issues:

File "/opt/sanmgr/commandview/client/sbin/HA_Dial_Start" should have mode "544" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/sbin/HA_Dial_Start" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/HA_Dial_Stop" should have mode "544" but the actual mode is "555".

File "/opt/sanmgr/commandview/client/sbin/HA_Dial_Stop" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/JBODDdld" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/JBODDdsp" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/JBODDfmt" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/JBODDlog" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/JBODDmgr" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/PanScriptCommon.sh" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armcfg" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armcopy" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armdiscover" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armdownload" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armdsp" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armfeature" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armfmt" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armlog" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armmgr" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armperf" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armrbld" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armrecover" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armsecure" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armtopology" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/cmdviewDS" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/cmdviewVA" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/cvui" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/launcher" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/logdel" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/logprn" should have group,gid "bin,2" but the actual group,gid is "sys,3".

Fileset "CMDVIEWCLT.CLTCOMMANDS,l=/,r=A.1.04.00" had file errors.

Fileset "CMDVIEWCLT.CLTCONFIG,l=/,r=A.1.04.00" issues:

File "/opt/sanmgr/commandview/client/config/PanConfigParams.txt" should have mode "555" but the actual mode is "755".

File "/opt/sanmgr/commandview/client/config/PanConfigParams.txt" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/client/sbin/armhost" should have group,gid "bin,2" but the actual group,gid is "sys,3".

Fileset "CMDVIEWCLT.CLTCONFIG,l=/,r=A.1.04.00" had file errors.

Fileset "CMDVIEWCLT.CLTMANPAGES,l=/,r=A.1.04.00" issues:

File "/usr/man/man1m/armcfg.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armcfg.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armcopy.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armcopy.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armdiscover.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armdiscover.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armdownload.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armdsp.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armdsp.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armfeature.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armfeature.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armfmt.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armfmt.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armlog.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armlog.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armmgr.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armmgr.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armperf.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armperf.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armrbld.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armrbld.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armrecover.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armrecover.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/armsecure.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/armsecure.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/logdel.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/logdel.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

File "/usr/man/man1m/logprn.1m" should have mode "544" but the actual mode is "444".

File "/usr/man/man1m/logprn.1m" should have owner,uid "root,0" but the actual owner,uid is "bin,2".

Fileset "CMDVIEWCLT.CLTMANPAGES,l=/,r=A.1.04.00" had file errors.

Fileset "CMDVIEWSVR.SVRCLASSES,l=/,r=A.1.04.00" issues:

File "/opt/sanmgr/commandview/server/browser/Launcher.html" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/Launcher.html" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/DOFactory.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/DOFactory.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/DeviceDB.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/DeviceDB.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/JBODMgrGui.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/JBODMgrGui.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/JBODObjSrv.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/JBODObjSrv.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/PerfDB.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/PerfDB.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/cassinidevobj.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/cassinidevobj.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/gui.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/gui.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/help/Cassini_Help_System.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/help/Cassini_Help_System.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/help/Cronus_Help_System.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/help/Cronus_Help_System.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/help/JBODhelp.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/help/JBODhelp.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/help/Launcherhelp.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/help/Launcherhelp.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/hostcompsdk.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/hostcompsdk.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/jcchart.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/jcchart.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/jcore.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/jcore.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/jh.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/jh.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/launcher.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/launcher.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/panutils.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/panutils.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/classes/sandevice.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/classes/sandevice.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/cmdviewDS.html" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/cmdviewDS.html" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/browser/cmdviewVA.html" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/browser/cmdviewVA.html" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/DOFactory.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/DOFactory.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/DeviceDB.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/DeviceDB.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/LogDB.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/LogDB.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/PerfDB.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/PerfDB.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/Web.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/Web.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/dev_obj/JBODObjSrv.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/dev_obj/JBODObjSrv.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/dev_obj/cassinidevobj.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/dev_obj/cassinidevobj.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/disc.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/disc.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/discovery.jar" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/discovery.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/event.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/event.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/panutils.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/panutils.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/sandevice.jar" should have mode "644" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/sandevice.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/classes/xml.jar" should have mode "444" but the actual mode is "555".

File "/opt/sanmgr/commandview/server/classes/xml.jar" should have group,gid "bin,2" but the actual group,gid is "sys,3".

Fileset "CMDVIEWSVR.SVRCLASSES,l=/,r=A.1.04.00" had file errors.

Fileset "CMDVIEWSVR.SVRCONFIG,l=/,r=A.1.04.00" issues:

File "/etc/opt/sanmgr/commandview/server/config/ContactInfo.txt" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/etc/opt/sanmgr/commandview/server/config/PanConfigParams.txt" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/etc/opt/sanmgr/commandview/server/config/PanConfigParams.txt" should have mtime "1015880246" but the actual mtime is "1021571848".

File "/etc/opt/sanmgr/commandview/server/config/PanConfigParams.txt" should have size "327" bytes but the actual size is "345" bytes.

File "/var/tmp/pand_bucket/DOFactory.scp" missing.

File "/var/tmp/pand_bucket/EvConsumer.scp" missing.

File "/var/tmp/pand_bucket/EvProducer.scp" missing.

File "/var/tmp/pand_bucket/LogDB.scp" missing.

File "/var/tmp/pand_bucket/PanDB.scp" missing.

File "/var/tmp/pand_bucket/PanDisc.scp" missing.

File "/var/tmp/pand_bucket/PerfMetric.scp" missing.

File "/var/tmp/pand_bucket/SnmpCmdVw.configd" missing.

File "/var/tmp/pand_bucket/SnmpCmdVw.initd" missing.

File "/var/tmp/pand_bucket/Web.scp" missing.

File "/var/tmp/pand_bucket/cmdvwagt_11_00" missing.

Fileset "CMDVIEWSVR.SVRCONFIG,l=/,r=A.1.04.00" had file errors.

Fileset "CMDVIEWSVR.SVRDEVICES,l=/,r=A.1.04.00" issues:

File "/opt/sanmgr/commandview/server/devices/properties/HP_A5236A.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/devices/properties/HP_A6188A.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/devices/properties/HP_A6255A.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/devices/properties/HP_A6491A.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/devices/properties/HP_disk.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/devices/properties/SEAGATE_ST118202FC.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/devices/properties/SEAGATE_ST136403FC.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/devices/properties/SEAGATE_ST173404FC.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/devices/properties/SEAGATE_ST318203FC.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".

File "/opt/sanmgr/commandview/server/devices/properties/SEAGATE_ST318304FC.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".
File "/opt/sanmgr/commandview/server/devices/properties/SEAGATE_ST318451FC.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".
File "/opt/sanmgr/commandview/server/devices/properties/SEAGATE_ST336704FC.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".
File "/opt/sanmgr/commandview/server/devices/properties/SEAGATE_ST39102FC.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".
File "/opt/sanmgr/commandview/server/devices/properties/SEAGATE_ST39103FC.def" should have group,gid "bin,2" but the actual group,gid is "sys,3".
Fileset "CMDVIEWSVR.SVRDEVICES,l=/,r=A.1.04.00" had file errors.

Fileset "CMDVIEWSVR.SVREVENTLIB,l=/,r=A.1.04.00" issues:
File "/var/tmp/pand_bucket/libDMEvent.sl.hpux" missing.
Fileset "CMDVIEWSVR.SVREVENTLIB,l=/,r=A.1.04.00" had file errors.
Fileset "CMDVIEWSVR.SVRNEWCONFIG,l=/,r=A.1.04.00" issues:
File "/etc/opt/sanmgr/commandview/server/newconfig/PanConfigParams.txt" should have group,gid "bin,2" but the actual group,gid is "sys,3".
Fileset "CMDVIEWSVR.SVRNEWCONFIG,l=/,r=A.1.04.00" had file errors.

Fileset "LSM.nwr-cbin,l=/,r=5.5.lsm.Build.55" issues:
File "/usr/lib/nsr/C/nsr.help" should have mtime "913955584" but the actual mtime is "1023390315".
Fileset "LSM.nwr-cbin,l=/,r=5.5.lsm.Build.55" had file errors.

Fileset "LSM.nwr-man,l=/,r=5.5.lsm.Build.55" issues:
File "/opt/networker/man/ansrd.8" missing.
File "/opt/networker/man/mm_data.5" missing.
File "/opt/networker/man/mminfo.8" missing.
File "/opt/networker/man/mmlocate.8" missing.
File "/opt/networker/man/mmpool.8" missing.
File "/opt/networker/man/mmrecov.8" missing.
File "/opt/networker/man/networker.8" missing.
File "/opt/networker/man/newgems.1m" missing.
File "/opt/networker/man/nsr.5" missing.
File "/opt/networker/man/nsr.8" missing.
File "/opt/networker/man/nsr_archive_request.5" missing.
File "/opt/networker/man/nsr_client.5" missing.
File "/opt/networker/man/nsr_crash.8" missing.
File "/opt/networker/man/nsr_data.5" missing.
File "/opt/networker/man/nsr_device.5" missing.

File "/opt/networker/man/nsr_directive.5" missing.
File "/opt/networker/man/nsr_getdate.3" missing.
File "/opt/networker/man/nsr_group.5" missing.
File "/opt/networker/man/nsr_ize.8" missing.
File "/opt/networker/man/nsr_jukebox.5" missing.
File "/opt/networker/man/nsr_label.5" missing.
File "/opt/networker/man/nsr_layout.5" missing.
File "/opt/networker/man/nsr_license.5" missing.
File "/opt/networker/man/nsr_migration.5" missing.
File "/opt/networker/man/nsr_notification.5" missing.
File "/opt/networker/man/nsr_policy.5" missing.
File "/opt/networker/man/nsr_pool.5" missing.
File "/opt/networker/man/nsr_regexp.5" missing.
File "/opt/networker/man/nsr_resource.5" missing.
File "/opt/networker/man/nsr_schedule.5" missing.
File "/opt/networker/man/nsr_service.5" missing.
File "/opt/networker/man/nsr_shutdown.8" missing.
File "/opt/networker/man/nsr_stage.5" missing.
File "/opt/networker/man/nsr_storage_node.5" missing.
File "/opt/networker/man/nsradmin.8" missing.
File "/opt/networker/man/nsralist.8" missing.
File "/opt/networker/man/nsrarchive.8" missing.
File "/opt/networker/man/nsrcap.8" missing.
File "/opt/networker/man/nsrcat.8" missing.
File "/opt/networker/man/nsrck.8" missing.
File "/opt/networker/man/nsrclone.8" missing.
File "/opt/networker/man/nsrd.8" missing.
File "/opt/networker/man/nsrdmo.8" missing.
File "/opt/networker/man/nsrexec.8" missing.
File "/opt/networker/man/nsrexecd.8" missing.
File "/opt/networker/man/nsrhsmck.8" missing.
File "/opt/networker/man/nsrib.8" missing.
File "/opt/networker/man/nsriba.8" missing.
File "/opt/networker/man/nsrim.8" missing.
File "/opt/networker/man/nsrindexasm.8" missing.
File "/opt/networker/man/nsrindexd.8" missing.
File "/opt/networker/man/nsrinfo.8" missing.
File "/opt/networker/man/nsrlic.8" missing.
File "/opt/networker/man/nsrls.8" missing.
File "/opt/networker/man/nsrmig.8" missing.
File "/opt/networker/man/nsrmm.8" missing.
File "/opt/networker/man/nsrmmd.8" missing.
File "/opt/networker/man/nsrmmdbasm.8" missing.
File "/opt/networker/man/nsrmmdbd.8" missing.
File "/opt/networker/man/nsrmon.8" missing.
File "/opt/networker/man/nsrnotd.8" missing.

```
File "/opt/networker/man/nsrpmig.8" missing.
File "/opt/networker/man/nsrports.8" missing.
File "/opt/networker/man/nsrretrieve.8" missing.
File "/opt/networker/man/nsrssc.8" missing.
File "/opt/networker/man/nsrstage.8" missing.
File "/opt/networker/man/nsrsyb.8" missing.
File "/opt/networker/man/nsrsybcc.8" missing.
File "/opt/networker/man/nsrsybrc.8" missing.
File "/opt/networker/man/nsrsybsv.8" missing.
File "/opt/networker/man/nsrtrap.8" missing.
File "/opt/networker/man/nsrvault.8" missing.
File "/opt/networker/man/nsrwatch.8" missing.
File "/opt/networker/man/nwadmin.8" missing.
File "/opt/networker/man/nwarchive.8" missing.
File "/opt/networker/man/nwbackup.8" missing.
File "/opt/networker/man/nwrecover.8" missing.
File "/opt/networker/man/nwretrieve.8" missing.
File "/opt/networker/man/oraemcasm.8" missing.
File "/opt/networker/man/oraemcmap.8" missing.
File "/opt/networker/man/preclntsave.8" missing.
File "/opt/networker/man/pstclntsave.8" missing.
File "/opt/networker/man/rap.8" missing.
File "/opt/networker/man/rapcheck.8" missing.
File "/opt/networker/man/rapd.8" missing.
File "/opt/networker/man/rapgen.1" missing.
File "/opt/networker/man/rapxfer.8" missing.
File "/opt/networker/man/recgems.1m" missing.
File "/opt/networker/man/recover.8" missing.
File "/opt/networker/man/resource.5" missing.
File "/opt/networker/man/save.8" missing.
File "/opt/networker/man/savefs.8" missing.
File "/opt/networker/man/savegems.1m" missing.
File "/opt/networker/man/savegrp.8" missing.
File "/opt/networker/man/savepnpc.8" missing.
File "/opt/networker/man/scanner.8" missing.
File "/opt/networker/man/stli.8" missing.
File "/opt/networker/man/tapeexercise.8" missing.
File "/opt/networker/man/uasm.8" missing.
File "/opt/networker/man/vaultcnf.8" missing.
Fileset "LSM.nwr-man,l=/,r=5.5.lsm.Build.55" had file errors.
```

Explanation

Nearly all system files and binaries that are installed within products such as Os-Core, should not be modified after installation. File integrity of SD-installed software products is verified using the Software Distributor swverify command. Software verifications are

performed to ensure that all installed products have not been altered; non-volatile files have not been corrupted or lost after installation. Missing files, or files with different permissions, size, checksum, modification time, may compromise the software product integrity and the system operation.

Corrective Action

Although simple exceptions can be corrected by hand, you should consider re-installing the software filesets, which files have changed and the integrity has been compromised. See swinstall for further install instructions. If the problem cannot be solved by re-installing the product filesets, something is wrong within the package, so the problem should be escalated to the package provider.

However, if the reported exceptions were intentional changes, you should consider reflecting the changes in the SD Installed Product Database using swmodify as follows:

```
chmod u-s       /usr/contrib/bin/nettune
swmodify -xfiles=/usr/contrib/bin/nettune  Networking.NET-RUN
```

Class C Problem

- Login entries without password aging

```
root:P7u/8FbDAjOPo:0:3::/:/sbin/sh
bevb:AMhw9zUb4PEXE:102:4:Beverly Bond,,647-0828,231-
4895:/home/bevb:/usr/bin/sh

nanf:96bm7IlauRNh2:103:4:Nancy Finish,,615-1351,981-0344:/home/nanf:/usr/bin/sh
scotth:LRo8P5bOH5kPU:104:4:Scott Ham,,805-2219,:/home/scotth:/usr/bin/sh

dianemcd:2g99MMvBAHc/.:106:102:Diane Mac,,647-0823,:/home/dianemc:/usr/bin/sh

oracle:OJc3yBloaxhTc:107:102:oracle,,,:/home/oracle:/usr/bin/sh
ids:MMIctfwPWt/bE:110:104:IDS/9000 Administrator:/home/ids:/sbin/sh
randys:48EBgxKH1hf5Y:111:4:Randy Stall,,,:/home/randys:/usr/bin/sh
```

Explanation

HP-UX allows password aging to be implemented by adding a specific string to the end of the encrypted password in /etc/passwd. Opinions vary as to the desirability of implementing password aging, but logins that do not have password aging in place are reported so that potential corrective action can be taken. It is recommended to implement password aging since changing passwords regularly greatly improves the line of defense against break-ins.

Corrective Action

Corrective action is to append a valid password aging string to the password field. For example, the password aging string which will expire a password within one year and require a two week time period to elapse before the password may be changed again by the user (this is to keep users from changing their password to a new one and immediately back to the old one) is:

mrt:XUqrajULY9V9A,o0BH:26207:20:Mark Token:/home/mrt:/usr/bin/ksh
^^^^
password aging
string

The, o0 string after the encrypted password is the actually the password aging string which indicates the above mentioned time limits for changing the user password. The Bis used by passwd to know when the password was last changed.

- Group files not linked

Explanation

Group files include /etc/group and /etc/logingroup. /etc/group exists to supply names for each GID (used by commands such as /usr/bin/ls), and to support changing GIDs by means of the newgrp utility. /etc/logingroup is used by the operating system to allow users to acquire multiple GIDs at once. /etc/logingroup should be identical to /etc/group to compensate for the way /usr/sbin/sam (the System Administration Manager) manipulates the /etc/group file.

Corrective Action

Symlink /etc/logingroup to /etc/group via: ln -s /etc/group /etc/logingroup

- User root's (UID-0) $HOME is /

Explanation

By allowing root's $HOME to be the root directory, the file systems' integrity is compromised. Accidental mis-use of normal commands can result in disastrous effects to the complete file system. Finally, the "/" directory cannot be adequately protected against public read.

Corrective Action

It is recommended to move root's $HOME to either /roothome or put it under the /home directory.

- Root has no crontab

Explanation

This circumstance does not represent a specific security problem so much as an operational one. It is usually essential for proper system operation that there be a root crontab.

Corrective Action

See crontab(1) and the System Administration Tasks manual.

- Service bootps (/usr/lbin/bootpd) not found in /var/adm/inetd.sec
- Service chargen (internal) not found in /var/adm/inetd.sec
- Service cmsd (/usr/dt/bin/rpc.cmsd) not found in /var/adm/inetd.sec
- Service daytime (internal) not found in /var/adm/inetd.sec
- Service discard (internal) not found in /var/adm/inetd.sec
- Service echo (internal) not found in /var/adm/inetd.sec
- Service exec (/usr/lbin/rexecd) not found in /var/adm/inetd.sec
- Service ftp (/usr/lbin/ftpd) not found in /var/adm/inetd.sec
- Service hacl-cfg (/usr/lbin/cmclconfd) not found in /var/adm/inetd.sec
- Service hacl-probe (/opt/cmom/lbin/cmomd) not found in /var/adm/inetd.sec
- Service ident (/usr/lbin/identd) not found in /var/adm/inetd.sec
- Service instl_boots (/opt/ignite/lbin/instl_bootd) not found in /var/adm/inetd.sec
- Service klogin (/usr/lbin/rlogind) not found in /var/adm/inetd.sec
- Service kshell (/usr/lbin/remshd) not found in /var/adm/inetd.sec
- Service ntalk (/usr/lbin/ntalkd) not found in /var/adm/inetd.sec
- Service printer (/usr/sbin/rlpdaemon) not found in /var/adm/inetd.sec
- Service recserv (/usr/lbin/recserv) not found in /var/adm/inetd.sec
- Service registrar (/etc/opt/resmon/lbin/registrar) not found in /var/adm/inetd.sec
- Service shell (/usr/lbin/remshd) not found in /var/adm/inetd.sec
- Service swat (/opt/samba/bin/swat) not found in /var/adm/inetd.sec
- Service telnet (/usr/lbin/telnetd) not found in /var/adm/inetd.sec
- Service tftp (/usr/lbin/tftpd) not found in /var/adm/inetd.sec
- Service time (internal) not found in /var/adm/inetd.sec
- Service ttdbserver (/usr/dt/bin/rpc.ttdbserver) not found in /var/adm/inetd.sec

Explanation

This error refers to a network service offered in /etc/inetd.conf (or /export/private_roots/<node_name>/etc/inetd.conf) but not controlled in /var/adm/inetd.sec (or it's client's private configuration version). inetd.sec provides IP addresses/host names of machines that are allowed (or denied) network services on your system. If a service is not included in inetd.sec then no restrictions apply and all hosts, which have network access, can use the systems' network services. Network system access should be minimumly kept to internal HP use only (that is, "allow 15.*").

Corrective Action

Add an entry for the service in /var/adm/inetd.sec. Typically the following services are considered to be secure for all of HP:

ftp
telnet
ninstall

An acceptable inetd.sec entry would be:

ftp allow 15.*

Other services should be restricted to one or more specific subnets or hostnames. For example, a more restrictive inetd.sec entry would be:

mountd allow 15.xx.136-137.*

- Non-standard entries found in /var/adm/inetd.sec

  dtspc allow server1

Explanation

This indicates that some services are being offered too widely. Good practice indicates that most services should be offered only as widely as is necessary. At the very minimum, all services should be restricted to internal HP ("allow 15.*"). Some services may need more restrictions such as mountd, mserve, etc.

Corrective Action

Corrective action is to add subnet restrictions to the indicated services.

An acceptable inetd.sec entry would be:

ftp allow 15.*

Other services should be restricted to one or more specific subnets or hostnames. For example, a more restrictive inetd.sec entry would be:

```
mountd allow 15.xx.136-137.*
```

- Excessively open permissions on syslog file for ftpd logging

```
-rw-r--r--   1 root       root        121951 Aug 26 10:04 /var/adm/syslog/syslog.log
```

Explanation

The syslog file contains logging information from many subsystems such as inetd, ftpd as well as messages from the kernel. When ftpd logging is enabled ("-l" option specified in /etc/inetd.conf), the syslog file may contain ftp bad login information for each login attempt-using ftp. It is fertile ground for hunting for passwords, which are often mistakenly typed as logins inadvertently. The syslog file may be publicly readable if and only if the ftpd logging is disabled. If for some reason the ftpd logging has to be enabled, the syslog file should not be publicly readable.

Corrective Action

Evaluate the need for ftp logging and if not needed remove the "-l" option for ftpd in /etc/inetd.conf. See ftpd for more information. If ftpd logging cannot be disabled, remove the public read permissions and set the appropriate administrative ownership on the reported syslog file(s).

```
chmod o-r  /var/adm/syslog/syslog.log
chown root /var/adm/syslog/syslog.log
chgrp root /var/adm/syslog/syslog.log
```

- The following logins were considered administrative UIDs

Login	UID	Login	UID
root	0	daemon	1
bin	2	sys	3
adm	4	uucp	5
lp	9	nuucp	11
hpdb	27	nobody	-2
www	30	webadmin	40

- The following groups were considered administrative GIDs (Note any non-administrative group members.)

Group	GID	Members
nogroup	-2	No members
root	0	root
other	1	root,hpdb
bin	2	root,bin
sys	3	root,uucp
adm	4	root,adm
daemon	5	root,daemon
mail	6	root
lp	7	root,lp

Stale Login Accounts

- User accounts that show no recent login activity

User	$HOME directory	Period
bobm	/home/bobm	30 days
dsc	/home/dsc/./	30 days
monah	/home/monah	30 days
nanf	/home/nanf	30 days
opc_op	/home/opc_op	30 days
randys	/home/randys	30 days
scotth	/home/scotth	30 days

Explanation

As a general rule, user accounts that show no recent login activity should not stay on the systems forever. Account cleanup should be performed on a regular basis in order to eliminate the stale and unused logins.

Corrective Action

Contact the user or the owner of the account to determine whether the login is still used. If the account owner no longer needs the login, remove the account from the system. If the account owner does still need the login, remind them to periodically log into the account.

Policies, Procedures and Documentation

Finding: Sufficient	A1: Is security considered important in Your company? Do the policies and procedures reflect this? Does management consider security important?

Reason and Theory: Lip service is sometimes the only service done for security purposes. Security should be part of the day-to-day routine and it should be reflected in the policies and procedures of Your company as well as by support from senior management. Too often, bad security examples are punished and good security efforts are ignored. Examples of good security would be having security as part of the yearly employee performance evaluation or having a good security act rewarded by management. Actions such as these indicate to employees that management is serious about security and appreciates employees that "buy-in" to good security.

Recommendations: Create or update policies to enhance the importance of security within Your company. Obtain Senior Management backing for security and the implementation of security policies. Work with management to reward good security practices within Your company.

Comments: Yes. Findings showed that security is important to the University of Test Case, and that management reflects the same security objectives. HP was not able to review the Universities security policies and procedures document, but during discussions pieces were referred to verbally.

Finding: Sufficient	A2: Is the need for and advantages of good security practices clear to employees? Do employees treat security as a positive and desired condition?

Reason and Theory: It should be clearly understood by employees why security is important. Losses to Your company mean losses to the employees and a less open, more restrictive environment. The requirements of the law should be explained to employees. It would help them understand that a lapse in security could lead toward civil and criminal penalties for Your company, Your company management and possible the employees. A good security environment should not be a millstone around the employee's neck. The environment should be a positive and reward good security practice. This should include following established policies and procedures, reporting of possible security weaknesses when found, and keeping the workplace secure.

Recommendations: Review policies and procedures, if available, regarding security awareness training and security recognition. If none are available, discuss the issue with management; create policies to implement security awareness training and methods of rewarding good security practices. If current policies and procedures address this issue, review the security awareness training and if it is not being implemented, work with management to implement it. Work with management to include security in the employee performance evaluation.

Comments: Yes, employees are clear on why security procedures are in place and the advantages to them, along with the risks the company would have if they weren't in place. Employees, know the rules and consequences for any violations to the security polices.

Finding: Sufficient	A3: Is management holding regular security briefings with employees? Is there a feedback mechanism to management regarding security issues?
Reason and Theory: Management should stress the importance of system security to employees on a regular basis and should discuss the need for employees to be security conscious. Your company should consider having a security consultant explain to employees what are potential security breaches and on good security procedures. The security policy should also be reviewed regularly, maybe during employee's annual performance review. A method should be in place to allow employees to give feedback on issues such as security. Employees may be confused about the topic or need further information such as how to report problems confidentially. Communication is very important and the more that management takes employee input seriously about security, the better the security environment will be.	
Recommendations: Review policies and procedures, if available, regarding security awareness training. If none are available, discuss the issue with management, create a policy that management will brief employees on why security is important to Your company, publish the policy, and educate the user community. Review current security awareness training programs or create a security awareness-training program. Part the programs should be a once a year discussion with management on information and computer security.	
Comments: Yes, management holds security briefings with employees regularly throughout the year. Management is open to recommendations made by System Administrators on security practices. Additional briefings are held relating to security practices and procedures if employee turn-over happens.	

Finding: Sufficient	A4: Do the employees "buy into" security?
Reason and Theory: It is necessary but not sufficient for employees to understand the benefits of security and the consequences of its failure. Employees must "buy into the program" or they will do what they can to get the job done in spite of restrictions imposed by security measures. If employees truly appreciate security and believe it is an integral part of their responsibility, then it becomes easier to implement and even more strict security measures can be avoided.	
Recommendations: Managers at all levels and system personnel should be observant of employee attitudes toward security. Do they consider it important and are they willing to do what needs to be done. Alternatively, are they tolerant of security practices as another management imposed restriction on them? Attitudes should be gauged and if the latter is true, then work on getting the employees to understand the need for security by positive examples from management and communication methods such as employee newsletters.	

Comments: Yes, both employees and contractors are conscious of security practices, and buy into the program. They realize that non-conformity is not accepted within the Universities IT environment.

Finding: Sufficient	A5: Are the consequences for security violations clearly defined in the policies and procedures? Is the user community aware of the consequences of security violations?

Reason and Theory: The specific security rules must be clear and concise. They have to be taught to each employee. It is not only necessary for users to understand the general ideas, but they must know the specifics for selecting good passwords and the consequences their password to others. Employees must clearly know the potential (such as lost business) as well as actual consequences (such as loss of employment) for failing to practice security. The fact that the consequences are clearly spelled out also results in a more evenhanded enforcement of security. The consequences would be the same for a manager or an employee. This lets the employee know that security is important to management if the emphasis is applied to all. It also makes the enforcement easier for system administration and management. If an infraction occurs, the consequences are listed and then management via the human resources department can take care of applying the consequences.

Recommendations: Review policies and procedures, if available, for definition of consequences and security enforcement. If none are available, work with management to develop the policies that include consequences. Be sure to include a definition of an infraction versus a security breach. One is minor and the later puts Your company as a whole at risk. Use the Human Resources Department as a guide to determining how to handle the consequences of a security infraction.

Comments: Yes, the security violations are defined. Employees know the security rules and consequences for any violations.

Finding: Sufficient	A6: Does management take security violations seriously? Are all violators treated equally?

Reason and Theory: When a security violation occurs, managers must make it clear by their actions that security is important. Violators must be counseled or disciplined. All employees should be treated equally, and high-level violators not given wrist slaps while ordinary employees are severely disciplined. The consequences of a violation should be clearly spelled out in the policies and procedures. All violators, employee or management should be treated equally. A token punishment for a manager and severe punishment for an employee for the same violation will often do more to damage security than improve it.

Recommendations: Review policies and procedures, if available, for definition of consequences and security enforcement. If none are available, work with management to develop the policies that include consequences. Be sure to include a definition of an infraction versus a security breach. One is minor and the later puts Your company as a whole at risk. Use the Human Resources Department as a guide to determining how to handle the consequences of a security infraction.

Comments: Yes, management takes security violations seriously. Each episode relating to a security violation is treated in the same manner according to the published polices.

Finding: Sufficient	A7: Is the difference between a security lapse or infraction and a security breach clearly understood within Your company?
Reason and Theory: There is a difference between a security lapse and a security breach. A security infraction such as not having a good password and security breach such as giving away the Root user password must be clearly understood. Management must appreciate such differences and users must not feel that they will be so severely disciplined for minor violations that they will cover up failures. The result could be a more catastrophic security problem later. Those that commit violations that do not result in a loss of security must be counseled and reminded that security is for everyone. Those that cause loss or destruction of data should be held strictly accountable.	
Recommendations: Review policies and procedures, if available, for definition of consequences and security enforcement. If none are available, work with management to develop the policies that include definitions of breaches and infractions. One is minor and the later puts Your company as a whole at risk. Use the Human Resources Department as a guide to determining how to handle the consequences of a security infraction/lapse and a security breach with the appropriate level of response.	
Comments: Yes, management understands and has clearly defined security lapses as infractions that are dealt with immediately and don't necessarily require dismissal unless the offense is constantly repeated. Security breaches that cause loss of data or company property are dealt with harshly and chances to repeat the breach aren't tolerated.	

Finding: Sufficient	A8: Are employees (and contractors, if used) security conscious?
Reason and Theory: Employees should be encouraged by management to be security conscious and to report events out of the ordinary. Many break-ins have been thwarted by employees that noted unusually heavy activity on the system, activity at odd hours by those that normally do not do such things, etc. Management should not turn employees into police officers but should encourage not only good security procedures but also good security observance.	
Recommendations: Review policies and procedures, if available, for security awareness training and security problem reporting. If none are available, work with management to develop the appropriate policies for security awareness training and security problem reporting. Publish the policies and educate the user community. Review the current security training for the user community for appropriateness. Review current security issue reporting procedures to insure that they are working as planned. Encourage management and system personnel to encourage users to report any unusual occurrences to the appropriate department.	

Comments: Yes, both employees and contractors are conscious of security practices, and buy into the program. They realize that non-conformity is not accepted within the Universities IT environment.

Finding: Sufficient	A9: Does management include system administration personnel for security policy, procedure and issue suggestions? Is it done on a regular basis?

Reason and Theory: System personnel are key to any information and computer security issue. They are a valuable resource that should be tapped when ever possible during the development of security policy and procedures. A method should be available for communication of suggestions from the system personnel to management because system personnel will more than likely become aware of security issues during their normal and routine work. Scheduled meetings including key system administration personnel and management should be arranged. These meetings should be used to discuss security issues.

Recommendations: Review policy and procedures, if available, for requirements on security policy implementation and development. If none is available, discuss the issue with management to make them aware of this potential security resource. Develop a policy to require regular management and system personnel meetings to discuss security issues. If regular meetings are taking place, be sure to have documented meeting minutes so that issues need to be resolved are discussed and solutions documented. The solutions should become part of policy and procedure.

Comments: Yes, management includes and encourages the System Administrators to make suggestions where they may see deficiencies in the security policies and procedures. This can be done by submitting in writing or openly discussed during the scheduled meetings.

Finding: Sufficient	A10: Does management lead in setting an example for security?

Reason and Theory: Employees look to see what management is doing and how they are treating any subject within a company. If management displays the appropriate demeanor regarding security, employees are likely to follow the example. Good actions, like not writing down passwords and discussing sensitive customer information in open conversations, will help foster a good security environment.

Recommendations: Management should be aware of all computer and information security policies, if the policies are available. This includes all management and not just systems management. They should set a good example the employees and participate in security awareness training with the employees. If a manager does perpetrate a security infraction, the manager should take the counseling and advice just as an employee would. A manager should never be guilty of a security breach.

Comments: Yes, management participates in security awareness and practices of polices and procedures.

Finding: Needs Improvement	**A11: Does management seek legal counsel regarding security-related documents and other related issues? This could include the need to preserve evidence in case of a security incident?**
Reason and Theory: Management should consider legal advice regarding the necessity of requiring signing security documents upon initiation and termination of employment. Management should legal advice regarding evidence preservation should a security incident occur regarding unauthorized access or employee security violations. If policy dictates pursue and prosecute for security breaches, management should already be familiar with what constitutes legal evidence and what procedures should be followed. Corporate legal counsel that is familiar with information and computer security issues should review all policies.	
Recommendations: Review policies and procedures, if available, to determine when legal counsel should be involved. If none are available, discuss the issue with management. Be sure to indicate the need to involve legal counsel during any security incident to protect Your company from unnecessary exposure. Create the policy, publish it, and educate the system personnel and user community. Review the security incident plan to determine if the corporate legal counsel is part of the contact lists.	
Comments: Yes, customer management has met with legal counsel to understand how vulnerable management is personally, and the company for loss or public exposure of private data. It is also understood what needs to be done to minimize liability. The missing link – policies and procedures need to be in place and what actions need to be taken to ensure that coverage is not denied.	

Finding: Sufficient	**A12: Is security being treated as a continuing and ongoing process?**
Reason and Theory: Management and employees should treat security as something that is ever present and necessary. It should not be considered something needed when the auditors arrive or when something goes terribly wrong. If security is treated as haphazard or something to be done when it is thought then security will not be a pervasive and constant source of protection for the systems and the data stored on them.	
Recommendations: Review policies and procedures, if available, regarding security awareness training, new employee security introduction, and security reinforcement. If none are available, discuss the issue with management, develop the appropriate policies, and publish them. Institute security awareness training and employee security training programs. Review current awareness and training efforts to determine methods for improvement or an increase in frequency. Enlist management's help in fostering a continuing security atmosphere.	

Comments: Yes, Customer organization "BEFIT" responsibility is to review and update policies. These reviews address new hardware, software, and technology since last update. Also looks at new vulnerabilities or ones not previously addressed along with any deficiencies exposed by testing or real problems are also reviewed.

Finding: Sufficient	A13: Are Hewlett-Packard security resources being used?
Reason and Theory: Administrators with electronic mail should be on the Hewlett Packard security bulletin distribution. The security bulletins will notify administrators of known vulnerabilities. Similarly, administrators should get on the patch matrix distribution to be notified of any security patches applicable to the system. For those with World Wide Web (WWW) access, periodically checking Hewlett Packard's security page provides the latest information Administrators should have Hewlett Packard's electronic mail address for reporting any suspected security vulnerabilities. This address is security-alert@hp.com.	
Recommendations: Review Hewlett-Packard's security web service under support on the Hewlett-Packard web page under support.	
Comments: Yes, System Administrators subscribe to HP's security bulletins. Alerts are reviewed implemented if they pertain to services being utilized in the customer's environment. Customer also utilizes their assigned Account Support Engineer and the ITRC if they have questions relating to security.	

Finding: Sufficient	A14: Are security reference material such as books and security consultants used as necessary?
Reason and Theory: There are many good books on security available. "*Unix System Security*" by David Curry (Addison Wesley), "*Computer Security Basics*" by Russell and Gangemi (O'Reilly & Associates), and "*Practical Unix and Internet Security*" by Garfinkel and Spafford (O'Reilly & Associates) are three of more widely known and widely available. Management should consider having a security consultant come on site in order to observe procedures that cannot be seen by remote system evaluation. This should be done periodically as the use of the system expands and changes are made.	
Recommendations: Procure and use security reference material as needed to enhance security efforts. Review policy and procedures, if available, regarding security auditing and review procedures. If none are available discuss the issue with management, create a policy, publish it and work with management to procure security consultant services. Review any requirements that may be placed on Your company by customers or business partners to see if a security audit is required.	
Comments: Yes, customer has available to them several security books that were written by HP's Donald Pipkin and Chris Wong (HP's Security for 11i). Along with reference materials HP provides on the ITRC. The System Administrators utilize their ASE and administrators they have networked with at conferences such as Interex.	

Finding: Insufficient	A15: Are the Computer Emergency Response Team (CERT) advisories be used?
Reason and Theory: Administrators with internet access should regularly check for CERT advisories available from CERT. These advisories can be found at http://www.cert.org. Being forewarned is forearmed. A good security-aware system administrator must have knowledge regarding current attacks and other activities that might affect his/her systems. Other sources of information would be the BUGTRAQ mailing list, the SANS mailing lists and the Security Focus mailing list.	
Recommendations: Review policies and procedures, if available, regarding notification of security issues. If none are available, work with management to create a policy to requiring monitoring of computer security issues and notifications. Publish the policies and establish a procedure where system administration personnel subscribe to the appropriate email lists and check the appropriate web sites. The procedure should include the necessary notification protocol to alert other system administration personnel when a security alert is issued.	
Comments: No, customer hasn't utilized additional security resources other than those associated with Hewlett-Packard directly.	

Finding: Sufficient	A16: Are system personnel attending security training and conferences so that aware of current security trends, able to configure systems securely and activate processes that monitor security compliance?
Reason and Theory: Administrators should have had training on security and should regularly attend classes and seminars or read security information on a regular basis to keep up with the latest technology on potential attacks and countermeasures.	
Recommendations: Review policies and procedures, if available, regarding technical training for system personnel. If none is available, discuss the issue with management, create a policy on technical training, publish it, and inform the system personnel. If there is currently training policy, review it to see if security training is part of the recommended training. Work with management to include security-training attendance as part of the system personnel's yearly performance evaluation.	
Comments: Yes, System Administrators yearly attend HP Interex Conference where security practices are part of the conference curriculum. Recently customer has loaded and began testing of HP's IDS/9000 intrusion detection application.	

Finding: Sufficient	A17: Is security being overdone?
Reason and Theory: Security can be overdone and the reaction it may cause can make things worse. If users perceive that security is getting in the way of getting the job done, they will get around any security measures. Once an attitude is fostered that security is just a pain, it will become ineffective and create the type of resentment that will result in security breaches. Passwords shouldn't be changed too often or be too complicated or they will be written down. Employees will accept security measures they understand and believe in but will create obstacles to those that are too restrictive or seemingly ill advised. Employees and contractors must "buy in" to security. Managers must explain why security is in everyone's best interest and what the benefits are, not only, what the adverse consequences might be.	
Recommendations: Review policies and procedures, if available, regarding security awareness training and education. If none is available, work with management to establish the policies including a feedback mechanism to determine security acceptance levels. Publish the policy and educate the user community. After awareness training and education seminars, solicit feedback on the training and security environment to determine how well the training is being received. Also, solicit information from managers on how employees are reacting to a secure environment.	
Comments: No, the consensus is that security is being approached in a moderate but effective manner. The areas being addressed are password aging, ftp controls, monitoring of logging files, checking in and out of company equipment.	

Finding: Sufficient	A18: Is security compliance being monitored and effectiveness being gauged?
Reason and Theory: A method for monitoring security compliance is unavoidable. It is not acceptable to say, "we have not had a security incident so it must be working." Constant reviews at regularly scheduled meetings to determine if security incidents are being reported, are employees buying in to security are system personnel performing the specified checks? It may be necessary to create a dummy incident such as introducing an eicar virus on a PC to see how it is handled or something similar to see if the process work. Waiting for the "real thing" may be too late to discover something is not right.	
Recommendations: Use policies and procedures to develop monitoring procedures regarding security compliance. If there are no policies and procedures then there is no security environment. Work with management to develop the policies and procedures and be creative about testing the compliance of the procedures. When doing the testing be sure to have a "reward" structure in place for those employees that demonstrate good security awareness and adherence to procedures.	

Comments: Yes, the customer has periodic testing procedures in place. The use of public domain software is used to test the security of programs, log files are checked periodically, system and security patches are kept upto date, and log files and other critical files are backed up regularly.

Finding: Insufficient	A19: Has an independent security audit been performed or is it being considered?
Reason and Theory: No matter how good an administrator is, an outside security audit is as important as an outside financial audit. You need to bring in someone to look at your policy, your procedures and your system to see if they meet good security practice, your security policy and your requirements. An independent security audit, conducted regularly, is necessary. If you don't have a corporate team to provide such an audit, consider hiring an outside consultant. Make sure you know the credentials of the outsider both as to their ability to do the auditing as well as their honesty and integrity.	
Recommendations: Review policies and procedures, if available, to determine what the requirements are for auditing. If none are available, work with management to determine what auditing is required. This may be from legal requirements or demands from customers or business partners. Create a policy and publish it. Work with management to secure the appropriate auditing resources either inside Your company or from an external resource.	
Comments: At this time the University of Test Case hasn't engaged with any independent company to regularly perform security audits of their environment. This is the first time any third party has been invited to perform a security review.	

Finding: Insufficient	A20: Has a vulnerability assessment and a business impact analysis been conducted and the results acted upon?
Reason and Theory: A vulnerability assessment reviews the information systems to determine any hazards that might threaten them and the potential results of their occurrence. This may be a hacker attacking the system and from where or a risk to the files on a system from insecure passwords and file permissions. A business impact analysis determines how the business might be affected due to outages of the information systems based on the vulnerability analysis. This helps determine what has to get fixed first.	
Recommendations: Review policies and procedures, if available, to determine how a vulnerability assessment and business impact analysis fit into the security and disaster recovery schemes. If none are available, work with management to create policies and procedures for security disaster recovery and security incident planning. For the process to be complete urge management to consider the vulnerability analysis and the business impact analysis. Review policies and procedures, if available, to determine how a vulnerability assessment and business impact analysis fit into the security and disaster recovery schemes. If none are available, work with management to create policies and procedures for security disaster recovery and security incident planning. For the process to be complete urge management to consider the vulnerability analysis and the business impact analysis.	

Comments: Yes, a risk assessment identifying the assets and threats has been done, however a vulnerability assessment has not been done.

Finding: Sufficient	A21: Does Your company have a written security policy?
Reason and Theory: The first and foremost step in good information and computer security is having a written and communicated security policy. The policy serves as a guideline and checklist regarding usage, actions and performance. Without good written and well-communicated policies, security becomes difficult to administer, implement and enforce.	
Recommendations: Develop and publish security policies and procedures. After the policies have been written, publish them so that they are available to the user and I.T. community in an easily accessible manner. Establish a communications and education method to remind all in the user community how important security is and why it is necessary that they "buy in" to security.	
Comments: Yes, the University of Test Case has a written security policy that includes the following articles: Definition of Administrator's rights and responsibilities, configuration management procedures, handling of sensitive information, handling of changes once an administrator or end-user is no longer authorized access, confidentiality guidelines for individual employee rights as well as sensitive company information. These name the more visible ones but others are included in the security policy as well.	

Finding: Needs Improvement	A22: Does Your company have a written and tested security incident plan?
Reason and Theory: When a security incident occurs is the worse time to plan for it. A plan should be written that includes what constitutes a security incident. A list of who should be contacted and what steps should be taken to minimize possible harm to the assets of Your company. The plan should include things such as system shutdowns, control of network and communications, what steps should be taken to retain any legal evidence, etc.	
Recommendations: Develop a security incident plan and test it. Be sure to involve corporate legal counsel and management to be sure the incident plan fits into the security policies (so that procedures are taken coincide with the attitude of proceed and protect vs. pursue and prosecute.) The operations staff should be educated on how to access and implement the plan. This education should include how to recognize a possible security incident.	

Comments: Yes, the University of Test Case has parts of a company incident plan in place. Those pieces include: Who should be contacted, names of Managers and Administrators and the methods to be used to contact them if an incident did occur. If critical decision-making personnel can't be reached there are plans in place for what actions should be taken. And there is a plan to protect the system from further loss if a problem is discovered.

Where the plan needs to be improved to provide better benefits is in the following: Document immediate actions that should be taken by operators in case of a security incident. Create and document procedures for contacting law enforcement and corporate counsel in case of security incidents. Define when it is appropriate to report the incident to CERT. Put steps in place to protect information concerning an incident so it can be used to determine what occurred and use it as evidence if that becomes necessary.

Finding: Insufficient	A23: Does Your company have a written security incident recovery plan?

Reason and Theory: It is important from a security aspect to carefully plan for an event requiring the recovery or restoration of system. An unplanned restoration of files, especially system files could cause vital logs files, password files or other important data to be overwritten. This might result in old passwords being restored; log files that were needed to track the cause of the failure, or other system information being overwritten.

Recommendations: Develop a system recovery plan that follows the security policy guidelines (i.e. proceed and protect vs. pursue and prosecute) so that the restoration of files or systems does not impact secure operations. Balance the need for security with the requirements of business at all times during the development of the recovery plan. Use of well-written policies will provide a guide for the writing of this plan. Be sure to educate the operations staff on the plan's contents and also be sure to make it accessible in the event it is needed.

Comments: No, the University of Test Case doesn't currently have a written recovery plan. Some of the plans they have would be directly related to disaster recovery steps if they lose a server.

It would benefit the University if they would take the basics from their disaster recovery steps and add additional ones like file restorations. Combining those pieces would be a great beginning to an excellent security incident recovery plan.

Finding: Needs Improvement	A24: Are policies and plans reviewed and tested on a regular basis?

Reason and Theory: The changing of technology, business requirements, physical environment and other factors sometimes renders policies inappropriate and plans ineffectual. A periodic review and updating is as important as the initial writing of the policies and procedures. However, without a scheduled review, these policies and procedures are often allowed to go stale and not be in ready to use state.

Recommendations: Establish a semiannual review meeting that will review all plans and procedures regarding security issues. Be sure to involve management and corporate legal counsel where it is required. If environment changes force the issue, post an addendum to the current policies or procedures that will temporarily cover the discovered issue and acquire the appropriate managerial approval until the next scheduled review.

Comments: Yes, customer management has met with legal counsel to understand how vulnerable management is personally, and the company for loss or public exposure of private data. It is also understood what needs to be done to minimize liability. The missing link – policies and procedures need to be in place and what actions need to be taken to ensure that coverage is not denied.

Finding: Needs Improvement	A25: Is insurance coverage in place to cover data losses? Are the coverage requirements being met?
Reason and Theory: Many companies carry insurance to cover the loss of data due to physical destruction. If such insurance is carried it should be reviewed to see if it covers data loss due to a security incident. If it does then policy requirements should be checked to see if Your company is meeting the security requirements necessary for coverage.	
Recommendations: Review data insurance coverage. If coverage is supplied for a security incident be sure to review the requirements so that compliance is maintained.	
Comments: Yes, coverage is in place to cover data loss in case of break-ins. What is unknown is loss of time covered in case of break-ins, and what procedures need to be in place so that coverage is not denied if a claim is made. Those are the key points that should be reviewed and documented thoroughly so that the University would not be at risk if a claim would need to be filed.	

Physical System Security

Finding: Insufficient	B1: Is access to secure areas controlled and monitored?

Reason and Theory: Access to secure areas need to be rigorously controlled. A person accessing secure areas such as printing areas, console areas and CPU areas could have the opportunity to access or remove secure information or damage sensitive and vital equipment. While the person may have no malicious intent, they could view information such as payroll information, alter switch settings on equipment or even endanger themselves through exposure to computer equipment.

Recommendations: Provide controls for logging visitors to the secure area both in and out. All visitors should be given an identity badge that identifies them as a visitor and requiring escort at all times. System personnel should be vigilant as to where the visitor goes and what they do while inside the secure area. Vendor personnel should be identified and the reason for the visit documented. If any doubt as to why the vendor personnel is on site it, the reason for the visit should be confirmed with their company. Vendor personnel should be escorted at all times.

Comments: Yes, access is controlled to the point of an appointment needs to be made to visit management, system administrators for work being performed on any system. All vendors should be wearing their company's identification badge.

The procedure should be taken to the next level whereby visitors would need to login and out of the facility and identify the purpose of the visit in that log. Be escorted, and chaperoned during the time they are on the Universities premises.

Finding: **Needs Improvement**	**B2: Is the CPU and console in a secure area?**
Reason and Theory: The system console is the most powerful and most vulnerable peripheral attached to the system. It can be used to reboot the system into single user mode in an uncontrolled manner and provide access to an intruder that would allow the perpetration of a Denial of Service attack. It also displays system information that would be useful to an intruder. Access to the CPU would permit an intruder to power down the system in an uncontrolled manner.	
Recommendations: Only authorized, trained and trusted system personnel should be permitted access to the system console and CPU of a system. Access should be permitted only by a method of identification and authentication that is rigorous. Training should be implemented according to security policies that educate system personnel on how an intruder should be approached and what procedures should be activated to deal with the situation. All system consoles and CPUs should be in a locked and secured area.	
Comments: Yes, the CPU and console are considered in a secure area. The access door remains open most of the time and when it is closed during business hours it is unlocked, allowing anyone the ability to walk into the area. There are System Administrators that have work areas in that room so for the most part someone is there to ask questions of people they have no knowledge of needing to do work.	

Finding: Needs Improvement	B3: Is the computer room fully secured against unauthorized access?
Reason and Theory: Computer rooms may be accessed by more than the door. Do the walls go completely from the floor to the ceiling? Are there other accesses to the computer room such as storage closets, etc? Are there coded or other secure locks on all the doors? Is the computer room in a glass-enclosed area? Can any of these areas provide access to an intruder? If the computer is unattended, are there security devices that will detect the presence of an intruder?	
Recommendations: All doors to the computer area should have coded entry locks. The locks should be key-card access or encoded. Control of key cards should be reviewed on a semiannual basis to ensure that cards are in the possession of the correct individuals. Coded locks should be changed semiannually to insure the codes have not been revealed. All windows and doors should be checked to see if they are a security hazard. Conduct a risk analysis of the installation to determine what possible intrusion methods might be used.	

Comments: Yes, the computer room walls go from the floor to above the ceiling. Building is older and walls are solid concrete, and no drop floor is in this computer room.

Enhancements should be considered to provide higher security such as: Access door should always be closed and locked, entry should be allowed only if authorized by management or system administrators. If feasible card access should be implemented for the computer room door, or at least coded key pad entry lock that could be changed when personnel terminates.

Finding: Insufficient	B4: Is the Service Mode disabled on the CPU?
Reason and Theory: Some CPUs have a “service mode”, “test” or “TOC” key switch that enables reboot or direct hardware access without having login capability. Physical protection of the CPU and console should be sufficient to protect them from unauthorized access via the console. If remote dial in is permitted on the HP provided Service Modem, this capability is available remotely and, if the service mode is not turned off, the Disable Remote feature should be implemented.	
Recommendations: Unless specifically needed, disable service mode on all CPUs in production status. Review any server in test or development mode to see if service mode is required. If service mode is required, disable remote on the console until requested to enable it by a known person or HP support personnel. Be sure to log the request, the requestors’ name, and why it is needed for reference.	

Comments: No, service mode is not currently disabled on the CPU's.

University of Test Case should consider implementing this procedure to ensure one more step is in place to protect their systems environment.

Finding: Sufficient	B5: Are networking components protected and controlled?
Reason and Theory: Network components can be vulnerable to physical as well as electronic intrusion. Networks provide the links between the users and the systems and as such they can be an easy point of intrusion. If the network components are exposed they can be damaged due to deliberate and/or unintentional attacks. This could happen when cables are damaged by falling equipment or someone plugging an unauthorized network monitor (i.e. sniffer) into the network to gather information on user ids and passwords.	
Recommendations: Enclose all network components in a secure area or closet. Ensure that only authorized personnel have access to these areas with encode locks or key-card access. Be sure all network wiring is identified so that it can be reconnected if necessary.	
Comments: Yes, network components are secured in a locked closet. Only key personnel have access to this equipment.	

Finding: Sufficient	B6: Is equipment that is placed into or removed from the secure area controlled?
Reason and Theory: If a server is introduced to the data center that is not controlled, it could pose a security hazard. For example, a system that is new or on loan from a vendor may not have the appropriate security safeguards enabled. Individuals accessing this system could gain unauthorized access to other systems in the data center. If equipment is removed from the data center, for whatever reason, it should be protected if it contains sensitive data or "sanitized" to remove the sensitive data. Once it is outside the control of the data center, control of the information contained on it cannot be assured.	
Recommendations: Any server that is introduced into the data center should be subjected to the data center's policy and procedures regarding new systems to insure that it is secure. New system security procedures should be covered in the Security Policies and Procedures.	
Comments: Yes, equipment is logged in and out of the building if going for disposal or offsite repair. Disks and tape media are destroyed when they are rendered unusable.	

Finding: Needs Improvement	B7: Is the vendor supplied Installation and Update Media controlled? Is it stored safely and readily available if needed by the System Administration Staff?
Reason and Theory: The vendor supplied Installation/Update Media provides an insecure method that could be used to access the computer system that will bypass normal controls. It could also be used to replace configuration files, destroy disk configurations or access sensitive areas. The media also needs to be safely stored and accessible quickly by authorized system personnel in the event it is required for a recovery situation.	
Recommendations: Provide a locked, secure storage area for all vendors supplied media. The media should be labeled so that the possibility of an error in selection is reduced to a minimum. Provide access to the vendor-supplied media to key system personnel so that they can access it in the event it is required. Provide for usage of this media in the Security Policies and Recovery Plan.	

Comments: Yes, the media is in a controlled environment in the computer room during business hours. Once the workday is ended the media and documentation remain on the shelf above the servers in plan sight and accessible to anyone that has a key to the room.

To ensure that the media wouldn't fall into the wrongs hands it would be a good practice to have this media and documentation locked in a secure cabinet at the end of each business day.

Finding: Sufficient	B8: Is an offsite backup system being used? Are procedures in place to control backup media? Is the media moved in appropriate containers?
Reason and Theory: Backup media contains data, which is just as sensitive as the data on the systems. It should be controlled and treated with the same concerns as the data on the system. The backup media should be identified properly so that it can be used correctly and mistakes minimized. When it is moved offsite, it should be in protected carriers that will insure the backup media is safe. The media should have a receipt and check system so that it can be tracked.	
Recommendations: Provide a tape library system that labels and controls the backup media. A method of retrieving the backup media from the offsite location should be established and tested. Policies and Procedures should establish who could request the media from the offsite location. The service that delivers the media should have a list of authorized individuals who can request the media and who can accept the media when it is delivered.	

Comments: Yes, offsite storage is used for server backup media. Procedures are in place for when and how this is done and who has the authority to sign for the data if it is needed in case of a disaster.

Finding: Sufficient	B9: Are all disk and tape media destroyed when no longer usable?

Reason and Theory: The data on disk drives and tapes can be read even when all files are removed or overwritten. In the case of tapes, even if the physical transport no longer functions properly, the tape media can still be read. Physical destruction may be necessary. The most comprehensive solution is a 3rd party product that will "clean" disk drives to government standards. UniShred by Los Altos Technologies.

Recommendations: When upgrading disk media, arrange to have the file systems removed from the disks by overwriting the disks at least 26 times. A better solution would be to use a disk scrubber product that insures the disk is clean. If the media contains extremely sensitive data, check on a media retention clause for the support contract. In the event of a failed disk, check with the vendor to see how the old disk media will be handled and ask for a written assurance that the disks will be erased before reuse. Secure a bulk tape eraser and expose any tapes to it before they are discarded. Otherwise, destroy of the tapes through incineration.

Comments: Yes, procedures are in place to destroy disk and tape media when they are rendered no longer useable in the environment.

Finding: Sufficient	B10: Are computer printouts controlled?

Reason and Theory: Computer printouts can provide a wealth of information. This information may relate directly to the computer system such as configuration information or passwords. It may also relate to sensitive, private information such as payroll. The printouts, if not handled properly, could result in a security intrusion or possible legal issues for your company, its management or employees.

Recommendations: Provide appropriate receptacles for printouts that contain sensitive information. Arrangements should be made for authorized individuals to collect this output and properly destroy it by shredding or incineration.

Comments: Yes, the University of Test Case practices shredding of all computer printout data that is no longer needed or was printed in error. The same process is also in place for special forms.

Finding: Needs Improvement	B11: Is there a battery power system available with a generator backup. How long will these systems provide power?

Reason and Theory: In case of commercial power loss, there is a need to shutdown the systems in a controlled manner to prevent data loss. In addition, it may be necessary to continue to process for a period of time so that a controlled shutdown point can be reached.

Recommendations: Conduct a risk analysis to determine what the maximum length of time required to perform a controlled shutdown in case of a power loss. Provide suitable power systems that would protect the essential systems or the entire data center if required for at least that time. Remember to include a policy and procedure regarding what to do if the power outage will exceed your maximum down time as determined by a Business Impact Analysis such as initiating activation of a backup site.

Comments: Yes, the University of Test Case does have a power backup system available for their systems in case of emergencies. The system only has the ability to provide backup to the environment for 1 hour.

Alternative methods of providing power to the Universities environment should be looked into so that if outages exceed the 1 hour time frame they could continue to provide uptime to systems and there end-users until the power situation is fixed.

Finding: Sufficient	B12: Is the data center protected by a fire suppression system? Are there sufficient hand held fire extinguishers of the appropriate type for the data center? Have the system personnel received fire-fighting training?

Reason and Theory: Protection of the data center by an appropriate fire suppression system is important. It could minimize system outages and control damage in case of a fire. The use of fire extinguishers that are not approved for data centers could cause more damage than a small fire. In addition, fire fighting-training and prevention should be given to all employees for their protection. The purpose of the training should be to minimize damage and not to endanger their lives with unnecessary risk.

Recommendations: Install an approved computer room fire suppression system. The system should be tested regularly and all systems personnel trained on its usage. Deploy handheld fire extinguishers in the data center of the type approved for computer rooms and computer equipment. Fire Fighting personnel should train the systems staff in handling small computer room fires and how to best protect them in case of a fire.

Comments: Yes, the University of Test Case has implemented fire protection of one type or another for each of their facility locations. The types used are Fire Extinguishers in every location and in multiple areas for ease of accessibility. Haleon System and Sprinkler Systems where compliant to data-center regulations. All employees are knowledgeable in the use of these systems.

Security Of Normal User

Security of Root User

Finding: Sufficient	C1: Is the use of the Root user account restricted to only necessary usage?

Reason and Theory: The use of the Root user account should be restricted to only appropriate system functions. The system personnel should have their own normal user logins that permit functions such as reading email and other non-system-related functions. The Root user should not be logged on normally as a user since an intruder could "hijack" the device used by the Root user. The use of the Root user account for normal operations could result in accidental damage such as deletion of directories and files that would normally be protected by proper permissions.

Recommendations: Get administrators to do most of their work as themselves, thereby minimizing the chances of accidentally destroying the system or system security since root has unlimited privileges. Administrators should do normal work while logged in as regular users, becoming root only as needed, and doing so through the su command. The file /var/adm/sulog should be created to track su activity.

Comments: Yes, Only 2 System Administrators have the root password information and all root usage must be logged in as your own login with the su privileges exercised to the root profile.

Finding: Sufficient	C2: Are direct Root user logins prohibited from all terminals except the system console?

Reason and Theory: Administrators should implement a system capability to prohibit anyone directly logging on to the system as the Root user except at the system console. Permitting logins as the Root user outside of a secure environment could permit compromising the Root user password either via "social engineering", logging of the activities on the terminal, or possible network sniffing. While it necessary to use the Root user account outside of the secure console area, implementation of the secure tty file forces a user to login as a normal user and then switch to the Root user.

Recommendations: The /etc/securetty file should be created, and contain the single word, "console". If this is done, the only place that anyone can log in as root is on the system console. If it is desired that no one be able to log in as root on the console either, /etc/securetty should be created as an empty file. This will force even the console user to log in as a regular user and su to root, creating an audit trail for console logins. This is only recommended if the console is in an unsecured area.

Comments: Yes, the systems procedure is in place so that no root logins can be made directly into the systems unless you are directly logging in from the systems console.

Finding: Sufficient	C3: Are Root user logins logged and reviewed?
Reason and Theory: The Root user, being the user that has the authority to do anything, should be carefully monitored via logging. The Root user account should not be used for anything other than tasks that specifically require the authority of the Root user. All users who use the Root user account should be logged in as a normal user and then use the **su** command to switch to the Root user account. The only direct login for the Root user should be at the system console.	
Recommendations: Administrators should consider logging Root user (*root*) login attempts to the console and to an attached printer. Such logging can be done by executing "*tail -f /var/adm/sulog*" in the */etc/rc* or the */etc/inittab* file. All logs should be reviewed and any unknown activity by the Root user should be questioned and reviewed. Logging this information to hard copy will prevent the loss of this vital information in case of an action that results in data file destruction. Alternately, or in conjunction with paper logging, send this data via email to another secure system.	
Comments: Yes, root logins can only be exercised by using the su command. Logs are reviewed to determine if other users are gaining access they shouldn't have. Log files are included in the Universities backup practices. Since only the main two System Administrators have the root login information paper trail audits aren't necessary.	

Finding: Sufficient	C4: Is the Root user password changed on a regular basis?
Reason and Theory: The Root user password should be changed on a more frequent basis than normal user passwords. It should also be changed when a user who has Root user access leaves the employment of the Information Technology Department or no longer needs root access essentially to perform their daily duties. The period for changing the password should be between 25 and 35 days and the password should be a strong as possible.	
Recommendations: Establish a procedure for changing the Root user password according to the Security Policy guidelines. A list should be kept of all system personnel who have the Root user password and only the persons on the list should be given the new password. The time of change should vary between 25 and 35 days so that it will make it difficult for an intruder to guess how long the password will be in effect. The password should be stored on paper in a secure area or vault. The policy should specify whom and for what reason the password can be accessed.	
Comments: Yes, the System Administrators change the root password on a regular basis, and it is immediately changed anytime there are personnel changes in the environment.	

Finding: Needs Improvement	C5: Are "back door" accounts with Root user capability permitted on the system?

Reason and Theory: The use of alternate Root user logins is simply not a good idea. While sometimes it may be necessary to have an alternate *root* login, it is just bad security. Having multiple *Root user*s makes it more difficult to notice when an additional, unauthorized one is added. The alternate Root user account users generally have weaker passwords and form a habit of bypassing normal security.

Recommendations: Review the accounts on the system for any user that has a User Id (UID) of 0. Justify the existence of these accounts in light of the Security Policies. If they are not needed remove them and implement a security check to detect the existence of unauthorized Root user accounts. If the concern is password control of the Root user account then write the password on paper, place it in an envelope and secure it in a safe or a vault. Then establish a procedure on who can access this password and for what reasons.

Comments: Yes, the only "back door" access available is if the system is powered off and brought up into single-user mode. Otherwise all accounts have the correct UID's and none have additional one of UID 0.

Finding: Sufficient	C6: Are system capabilities that provide for temporary Root user access for system administration tasks being used?

Reason and Theory: System security should not be compromised by giving out the Root password to users who perform system administration tasks such as adding users or performing backups. Administrators should consider getting a public domain or 3rd party security package that will permit users who need to perform specific Root user functions temporarily or periodically but otherwise do not normally need such access. At HP-UX 10.X, the *SAM* program permits this capability.

Recommendations: Review who has Root user access to the system and why it is needed. Any user who needs system access to perform administrative functions such as adding or deleting users should be given access through System Administration Manager (SAM) or a public domain function such as SUDO. Any effort to limit the number of the individuals with Root user access will make the system more secure.

Comments: No, other persons have root capabilities other than the 2 main system administrators. University of Test Case has begun to test HP's product Service Control Manager, and if they fits into there daily operations even the 2 key admins would no longer need to access root privileges unless things real went astray.

Finding: Needs Improvement	C7: Is the home directory of *root* /.
Reason and Theory: The default directory of Root user is /. This should be changed to */root_home* or some other name. The home directory of the Root user (and any other user with a UID of 0) should have permissions that allow read/write/execute for the owner and no other permissions set. This cannot be done when root's home is the / directory as this would prevent any other users from accessing the system. It is critical that whatever directory is chosen it should be on the system boot disk and in a logical volume mounted at / to prevent problems with root's home directory not being available.	
Recommendations: Review the home directory of the Root user and if it is the / directory, create a new home directory for the Root user and move important files to it. Test this concept on a test system to insure that system personnel are comfortable with doing it.	
Comments: Yes, the current system configuration is set to roots home directory as the default /. The recommendation of moving roots homedir to /root_home should be considered as being implemented as part of the systems security practices.	

Finding: Needs Improvement	C8: Is the current directory in the Path variable of the Root user?
Reason and Theory: Often it is convenient not to have to specify the path of a program to execute it. Users want to be able to move to a directory and execute programs in that directory. This is accomplished by adding . (dot) to the PATH variable. A common attack is to have Root user unintentionally execute a command with the same name as a real command but which is in a local directory. The result is that the Root user executes the attacker's program. To prevent this, the Root user should have only known directories in the PATH variable and never have the dot. This will require that any program not in the default path be specified with the path name such as *./command* or */directory/command*. This will prevent the Root user from accidentally executing a "Trojan Horse" attack. All directories in the Root user's path should be secured (only writeable by the Root user).	
Recommendations: Review the Root user's PATH variable. Identify all directories in the PATH and make sure they are owned by root and only writeable by root. Remove the dot if it is present. The security policies should state that any user performing the Root user function should make every attempt to insure the programs being executed are the proper ones. The procedure would be to specify the path of the program desired every time a command is executed.	

Comments: Yes, the path variable for root does contain the . signifying current directory.

By reviewing and testing the removal of the . in roots path you would take another step closer in tightening up your security access points.

Finding: Sufficient	C9: Does a .rhost file exist for the Root user?
Reason and Theory: The existence of the .rhosts file can be a very real security issue. If the .rhosts file is not needed they should be removed from the entire system and automated procedures established to check for the creation of one. If there is a need for .rhosts file's then every user should have one including the Root user. The creation of .rhosts files, even if empty, with the proper permissions and ownership will prevent an intruder from giving a user a .rhosts file with inappropriate settings.	
Recommendations: Review the .rhosts found on the system. Review the need for the .rhosts file such as high availability products or system management tools. Once the appropriate use has been determined, check the content of the .rhosts files to insure that the systems listed in the files are fully qualified. In the procedures for adding and deleting users, add the appropriate verbiage to necessitate the creation of the .rhosts file for the user. Be sure to state ownership and permissions. As of HP-UX 11.0, scripts can be added to automatically perform this function.	
Comments: No, .rhosts is not used in the customers environment. It non-use is already part of there security practices.	

Finding: Sufficient	C10: Is the umask value of root set to avoid creation of world writeable, readable and executable files?
Reason and Theory: The easiest method of gaining Root user access to a system is by finding a file that is world writeable and executable and owned by the Root user. This file can be used to create a Set UID file that can be executed by a normal user to perform Root user tasks. This might be adding a new UID 0 account to the system or creating a Unix shell that executes with Root user privileges. The umask value of the Root user should be defaulted to read/write/execute for the owner and no other permissions set. This may result in extra work for system administrators but it will prevent the accidental creation of a file that can be used against the security of the system.	
Recommendations: Review policies and procedures, if available, regarding file creation and permissions on new files. If policies and procedures are not available, discuss the issue of file permissions with management and applications development, create a policy regarding the issue, and publish it. Change the umask settings to the appropriate value decided upon for the Root user and notify all system personnel with Root user access of the change. Remind them that it may require extra work to explicitly set permissions on some system files such as device files.	

Comments: Yes, the current security practice is to us the umask of 022

Finding: Sufficient	C11: Are the login script files for the Root user modifiable only by the Root user?
Reason and Theory: If the login script files such as the .profile file are modifiable by others, then the Root user could unknowingly execute a "Trojan Horse" type of attack. Placing malicious code in the files that are executed by the Root user when the login occurs would do this. This code could add an intruder's account to a group that has system administration privileges or create a new UID 0 account for the intruder, or create an SUID shell somewhere on the system.	
Recommendations: Review policies and procedures, if available, regarding file permissions of Root user owned files. If policy and procedures are not available, discuss the issue with management, create a policy regarding it, and publish it. Check the permissions of all files owned by the Root user and insure that they are only modifiable by Root. Institute an automated check of the files using the find command and cron. Be sure to place the output of these checks in a secure location where only System Administration personnel can view them.	
Comments: No, it is not in the Universities security practices to allow useage of login scripts for root, SUID or SGID scripts.	

Finding: Needs Improvement	C12: Is the Root user's password available to authorized personnel in case of an emergency?
Reason and Theory: Root passwords need to be protected, yet available in the event that the System Administrator(s) cannot be reached for whatever reason. A procedure should be in place so that certain personnel can retrieve the password from the safe in an emergency. This action needs to be authorized by an essential manager and the request validated to make sure it is necessary. The requester should sign for it, thus creating an audit trail. Policy should be developed that require the personnel who have the Root user password to practice safety procedures. This would be traveling in separate cars or airplanes so that in case of an accident no essential personnel are lost from your company.	
Recommendations: Review policies and procedures, if available, regarding safeguarding of the Root password. If none are available, discuss the issue with management, create a policy, publish it and educate system personnel as to when to use it. Establish a procedure to store the password in the appropriate location every time the password is changed. A procedure to retrieve the password should be established. This procedure should include who is authorized to retrieve it and the manager(s) who need to authorize the use of the retrieved password.	

Comments: No, currently only the 2 man System Administrators know the root password to the servers in the environment.

Investigation of a root password authorization method in case of an extreme emergency and neither of the main admins were available to handle the situation should be considered.

Finding: Needs Improvement	C13: Are periodic checks being performed to check for new UID 0 accounts in the /etc/passwd file?

Reason and Theory: An intruder will try to gain Root user access if they have penetrated your system as a normal user. Many attacks involve ways to append an entry to /etc/passwd with root access. Using startup or shutdown scripts or security weaknesses in the cron system can do this. These entries can be easily seen upon inspecting /etc/passwd for new accounts with a UID of 0. This is another reason that there should be one and only one user with the UID of 0.

Recommendations: Establish a procedure to detect the presence of a new user with a UID of 0. This procedure should be run automatically with cron but system personnel should also run it at irregular intervals. An attacker could be familiar with security checks on the system and have a way of removing the offending entry in the /etc/passwd file before the regular security check is run and then adding it again later. Any findings should be put somewhere that only system personnel know about. Entries in email or regular system logs could be found by the intruder and removed.

Comments: No, at this time the security practices don't include a procedure for checking for suid programs, or invalid entries in /etc/passwd that would allow user access with a UID of 0.

This practice should be added to the Universities security best practices procedures.

Security of Normal Users

Finding: Sufficient	D1: Is there a documented process, involving managerial approval that is required to grant new users access to the system?
Reason and Theory: Control of users on any computer system is one of the more critical tasks. System administration personnel usually perform the task of actually creating the entries that allow a new user to access system but they are not the ones who actually authorize a new user. This authorization has to come from management and the owners of the application. Without a proper authorization procedure, anyone could request user access to possibly sensitive data. Remember to document the differences between granting system access, which is required by system personnel, and granting access to applications. The owners of the applications should be responsible for granting access to the application.	
Recommendations: Review the Security Policies, if available, to determine how new users should be authorized. The procedures to be followed should be based on the Security Policies and require the proper authorizations and approvals for granting the user access to the system. Document the procedure, submit it for management approval and implement it.	
Comments: Yes, the University has a policy in place that documents what access end-users should receive and to what systems depending on the job description.	

Finding: Sufficient	D2: Are nondisclosure legal documents used for new users?
Reason and Theory: Company trade secrets, customer data, or other sensitive data such as medical records need to have legally enforceable agreements to protect them. A nondisclosure agreement provides the base for such protection. Remember, the protection is not only for your company but also for the individuals whose data resides on the system. Having such an agreements will help prevent possible enforcement problems later.	
Recommendations: Review the documents required to grant a new user access to the system. If a nondisclosure agreement is not included, check the security policies to see if one is required. If not stated in the security policies discuss the issue with management and corporate legal to see if one is necessary. If one is necessary, have corporate legal create it and added to the new user packet. The agreement should be signed and returned before system access is granted. Be sure to have the Human Resources department retain the nondisclosure agreement and any other documents that are signed by the user.	

Comments: No, the University currently doesn't use nondisclosure agreements for employees within this environment. They are used in other areas at the University but not here.

Finding: Not Applicable	D3: If there is a nondisclosure form used, does Your company require that it be reviewed and resigned on a yearly basis?
Reason and Theory: It is a good idea to have the nondisclosure form re-signed on a annual basis even though the employee agreed to it upon initial granting of access to the system or at the start of employment. This procedure not only reinforces the concept it also can be used to prevent the excuse of "it's been so long I forgot". This should also be part of information and computer security education to the user community.	
Recommendations: The Policies and Procedures, if they are available, should be reviewed to see what is required regarding the nondisclosure agreement. If it is not a requirement that it be re-signed, discuss it with management and corporate legal to see if it would be advisable to institute such a policy. The Policy does exist and it is not being followed then review the procedure with management to see if can be implemented on a stricter basis.	
Comments: Doesn't apply to this area of the University.	

Finding: Sufficient	D4: Are all users on the system required to have a password?
Reason and Theory: It is essential for system security that all users accessing the system be challenged by a password. The password is required so that authorization part of the security concept of identification can be satisfied. If a user exists on the system without a password then it is a gateway for an intruder to attack the system. Remember, only normal user access is required to "steal" the password files on a Unix system.	
Recommendations: Institute a procedure that regularly checks the /etc/passwd file for any user entry that contains a blank or null password. Remember; store the results of the check in a location that is known only to the system administration personnel so that an intruder cannot modify the results of the search.	
Comments: Yes, all users are required to have passwords.	

Finding: Sufficient	D5: Is there a policy that defines a strong password composition? Is it enforced?

Reason and Theory: Good passwords are at least 6 characters long contain at least one non-alphabetic character and are not any combination of the user's login name or other dictionary word with an appended digit. There are excellent public domain password generators that can generate easy to remember passwords. The password checker part of *C.O.P.S*. or a similar program, such as Crack, should be used to check for passwords that do not meet the password composition policy. The person doing this should get prior permission from management, in writing. Remember that there are other dictionaries beside English. If you have users native language is other than English to check for weak passwords in their languages too.

Recommendations: Institute a regular procedure that will check for weak passwords on the system. Check policies and procedures for the appropriate action to take if a weak password is found. If a procedure does not exist, review with management the appropriate action to be taken, document it in the procedures, and implement it.

Comments: Yes, the requirement for a password is at least 6 characters and it must be mixed of alpha and numeric format.

Finding: Sufficient	D6: Are new users on the system required to change their password during the initial login process?

Reason and Theory: If users change their passwords at initial login, even the System Administrator won't know their passwords. This is an important concept for security enforcement. If the new users assign their own passwords then they can be held responsible for actions under their user id. The policy should state that if a security infraction traced to a user id is the responsibility of the person assigned to that id. If only the user knows the password associated with that id then there can be no mistake regarding the identity of the user. The temporary password that system administration personnel assign for the new account should meet strong password composition guidelines.

Recommendations: Review the policies and procedures, if available, to see if new users are required to change their passwords during the initial login process. The System Administration Manager can be used to force a password change during initial login if it is required. If policies and procedures do not prescribe this requirement, discuss it with management, document the policy and implement it.

Comments: Yes, when new user accounts are setup the first login access of that user will require them to setup a new password.

Finding: Needs Improvement	D7: Do the security policies prohibit users from writing down their passwords? Is the policy enforced?
Reason and Theory: When users write passwords down (and place "yellow stickies" on monitors, under keyboards, etc.), anyone searching work areas can discover their passwords. This may permit an intruder to gain access to the system by using their user id and password. Remember, only normal user access is required to browse sensitive application information or to steal important system information.	
Recommendations: Review policies and procedures, if available, to determine if it is against policy to "write down" passwords and user ids. If the policies and procedures do not reference this, discuss this with management and develop a policy regarding it. Once the policy is developed, communicate it to the user community. Develop an associated procedure for department managers, supervisors, and any managerial personnel who visit the user's work areas to be aware of this policy and remind users who violate it that is a security infraction.	
Comments: Yes, it is expressed that passwords should be setup to something the user can remember without having to write it down. It however is not tracked so if a user is writing down his/her password it would go unknown by management.	

Finding: Needs Improvement	D8: Are users allowed to share their passwords with other users?
Reason and Theory: If users tell others their passwords, others will be able to log onto the users' accounts. If a system compromise occurs from those accounts (due to malicious acts, user error, etc.), there is no way to prove who caused the problem. Users should not share their passwords with others. It is in the user's interest not to do so. If the policy states the user id logged on owns the security infraction and passwords are not shared, then identifying the person owning the id is much easier.	
Recommendations: Review policies and procedures, if available, to determine if it is against policy to share their passwords and user ids. If the policies and procedures do not reference this, discuss this with management and develop a policy regarding it. Once the policy is developed, communicate it to the user community. Develop an associated procedure for department managers, supervisors, and any managerial personnel who visit the user's work areas to be aware of this policy and remind users who violate it that is a security infraction.	
Comments: No, users are not allowed to share their passwords. However, there is no formal process in place to determine if password sharing is happening.	

Finding: Needs Improvement	D9: Are users allowed to store their passwords in keyboard macros or other automated means of entry?
Reason and Theory: This password entry "convenience" can cause problems. If someone sees a user log on using the function key to enter his or her password, that person can return and log on to the user's account when the user is away from his or her work area. Only the login name, which is easily obtained, is needed. The password is already supplied in the macro. In addition, if an intruder can view the macro or other automated entry, the password can be stolen and used at another location.	
Recommendations: Review policies and procedures, if available, to determine if it is against policy to automate the entry of their passwords. If the policies and procedures do not reference this, discuss this with management and develop a policy regarding it. Once the policy is developed, communicate it to the user community. Develop an associated procedure for department managers, supervisors, and any managerial personnel who visit the user's work areas to be aware of this policy and remind users who violate it that is a security infraction.	
Comments: No, users are not allowed to store passwords in keyboard macros, or other automated means such as using the .netrc command. However, there is no procedure or practice in place to determine whether or not this happens today.	

Finding: Sufficient	D10: Are application users permitted to access the Unix shell or command line?
Reason and Theory: Application users sometimes have options in their application that execute a Unix shell and grant them access to the Unix system command line. This function, especially with an untrained user, can have serious security issues. Files can be accidentally deleted or other system-related incidents such as a system wide message sent can occur. If an intruder can access the Unix shell, then critical system information can be viewed and stolen.	
Recommendations: If this condition exists, work with application developers to see if it can be removed or changed. If it is a menu option, disable the menu option for only qualified application users who require a higher degree of system access than a normal user. A quality and security assurance team should review all programming that is being placed into production mode. This is to insure that such security holes are prevented.	
Comments: No, access for application users is directly setup into there profile and this can't be modified.	

Finding: Sufficient	D11: Do users share home directories on the system?
Reason and Theory: For security purposes, it is best that each user, if reasonably possible, has a separate home directory to prevent one user from affecting another in case the former manages to break basic security or accidentally removes files. While, in an application environment, it may be desirable for users to be in the same directory, this should not be their login directory. Their login script can be used to switch the user to the preferred application directory before starting the application software.	
Recommendations: Assign each user their own home directory with the appropriate files required to complete their login and start their application. The user should own their own home directory and the permissions should be set so that the user has read/write/execute access only. No permissions should be set for group or world access.	
Comments: Yes, all user accounts have homedir created upon creation of there login account. The permissions are dictated in there profile with the umask setting of 022	

Finding: Needs Improvement	D12: Is password aging implemented on the system?
Reason and Theory: Password aging allows the administrator to set a time limit on the life of the user's password. This reduces possible break-ins caused by local users who have given away their password to others or outside groups who may have had personnel changes. Minimum times should be set before a password can be changed to avoid having users change their password then change it right back. Password aging can be implemented by using SAM on HP/UX. As an alternative, users can be denied the right to change their own password and a password can be provided for them by using a password selection program.	
Recommendations: Review policies and procedures, if available, to determine if it is required for users to change their passwords after a certain period. If the policies and procedures do not reference this, discuss this with management and develop a policy regarding it. Once the policy is developed, communicate it to the user community. Use the available system utilities such as the System Administration Manager (SAM) to enforce the policy.	
Comments: No, automatic password aging is not established, however end-users are required to change there password once a year.	

Finding: Sufficient	D13: Are users permitted to "beat the system" or otherwise circumvent system security?

Reason and Theory: Users should not be encouraged to circumvent system security. This usually occurs when a user does not have the appropriate permissions to do something that is required to accomplish their job function. "Innovative" users find ways to get things done rather than go through the procedures of gaining higher security authorizations. The user, by doing this, may be creating a security issue that is not known to system personnel. This could lead to an intruder using the circumventing technique to damage the system or gain access to sensitive information. System personnel should strive to maintain a balance between usability of the system and security so that the users can accomplish their job functions.

Recommendations: Review policies and procedures, if available, to determine if it is appropriate for users to try to "beat the system." If the policies and procedures do not reference this, discuss this with management and develop a policy regarding it. Once the policy is developed, communicate it to the user community. Provide a method in the procedures that allow a user to request that a security issue that is impeding their job be reviewed and an accommodation made to help them.

Comments: No, currently the University has had no occurrence of any end-user trying to beat the system. It has been common practice that if they can't do something they are contacting the help desk or the system administrators for help and direction.

Finding: Sufficient	D14: Do users have "backdoors" into the system?

Reason and Theory: Users, like System Administrators, should not have alternate ways into the system that bypass normal security for the sake of convenience. This may be the existence of a generic user account. This account is enabled with higher authority than a normal user account so that if the user needs to do something "special" than can log on as this account and bypass their normal restrictions. It may also be programming code that permits a user to login automatically while in their application as a Root user. This may be to control a printer or other system device. The problem is that normal security is bypassed and an intruder can use the same methods to gain access to the system or a normal user may make a mistake while using the backdoor. This mistake could have a system wide effect.

Recommendations: Review policies and procedures, if available, to determine if it is appropriate for users to have "backdoors" into the system. If the policies and procedures do not reference this, discuss this with management and develop a policy regarding it. Once the policy is developed, communicate it to the user community. System personnel should monitor for illegal system access such as unusual Unix shells with applications as the parent. A procedure should be documented for handling the issue. System personnel should also work with applications development so that "backdoors" are not required.

Comments: No, if any user logging into the system doesn't have a home directory in the password file they won't be able to complete the login process.

Finding: Sufficient	D15: Are user files and data being provided with the maximum protection (i.e. minimum access by others) possible by the system?

Reason and Theory: File and directory permissions should be set so that only the users can access and modify their data. Review the Unix System Security Report for a report describing file permissions found on the system. Permissions on user files and directories can only be determined by the application developers and owners. They should be cautioned about having permissions that are too open. Allow system administration personnel to provide proper security safeguards.

Recommendations: User accounts should be checked to ensure that appropriate umasks are properly set. This will permit new files created by the user to have the proper permissions. If the umask is not set, it should be enabled with the proper settings. Previously existing files should be checked for proper permissions. Remember to perform this function in conjunction with Applications Development. System personnel should not perform blanket changes without investigating the ramifications. Failure to do this could result in an application failing.

Comments: Yes, this practice is in place and controlled by the global umask that is created for each user profile.

Finding: Sufficient	D16: Is the user data being safely stored in case of an incident requiring data restoration?

Reason and Theory: User data should be stored so that it can be safely restored in the event it is needed. Manual recovery of data could be a long, time consuming and expensive process. System wide backups may have the user data stored on them but recovering may also be a long involved process. A risk analysis should be done to see if the backup methods in use are adequate for the user data.

Recommendations: Review the backup methods. If it is advisable to have user data backed up separately from system and configuration data, implement a procedure to perform it.

Comments: Yes, the user data is backed up separately from the operating system files.

Finding: Sufficient	D17: Are users advised to watch for unusual occurrences such as a strange date of last login or strange data entries in their applications?

Reason and Theory: A break-in is first detected by a user who notices something that is not "quite right." Either files or data have changed while the user was not logged on or the date of the last login was while the user was on vacation. Any changes that are not directly attributable to a specific action by the user should be investigated.

Recommendations: Users should receive regular security awareness education. Review the policies and procedures, if available, to see if ongoing security awareness is mandated. If it is not, review the situation with management, document a policy regarding it, and publish it. Implement a security education program, on at least an annual basis, for the user community. This could be combined with other yearly training that is mandated by law such as fire or hazard training.

Comments: Yes, users have been made aware that they should be accountable for what's happening to there data, and if something doesn't look right they should be contacting the help desk to log the occurance for investigation and follow-up by the administrators.

Finding: Needs Improvement	D18: Are new users given computer and information security training?

Reason and Theory: In order to have and maintain good computer and information users should know what they are allowed to do and they are prohibited from doing. A new user will develop habits that may not lead to good security practices so introducing a new employee to security concepts as soon as possible is very important. A good introduction to security will not only prevent accidental security lapses but also help users understand what is expected from them and why it is important. This will lead to employee "buy-in" to security concepts.

Recommendations: Review policies and procedures, if they are available, regarding security training and education. If policies and procedures are not available discuss the issue with management, create a policy regarding it and publish it. Work with Human Resources or the department that is responsible for introducing new employees to Your company to develop a short presentation regarding computer and information security. Use the education period to have forms such as nondisclosure signed.

Comments: No, currently there is no mechanism in place to provide computer security training to new users.

This section should be looked into and considered for adding to the system security best practices.

Finding: Needs Improvement	**D19: Are security awareness techniques (i.e. bulletin boards, coffee talks, departmental meetings) being regularly used to educate users and reinforce computer security?**

Reason and Theory: Security is a constant and evolving subject. Users are concerned with doing their jobs and system administration personnel are concerned with keeping the systems operating. In order for security to keep in the forefront, constant reminders must be presented to all involved with computer systems and applications. Use of subtle reminders on bulletin boards and mentioning security in departmental meetings will help keep the employees aware of their responsibilities regarding security without over doing it. These reminders can also be used to alert employees to new security threats such as viruses.

Recommendations: Review policies and procedures, if available, to determine what is the appropriate company policy regarding computer security awareness. If there are no policies or procedures, discuss the issue with management, develop a policy and publish it. Work with management to arrange for security awareness reminders to be added to yearly performance evaluations, bulletin board notices and other employee communications vehicles such as newsletters. Remember to keep the reminders there but don't over do it so that security and the reminders become mundane and overlooked by their commonality.

Comments: No, users are made aware of best practices for virus passing and proper use of the system initially, but it is not taken to the point of meetings or bulletin boards etc…. as reinforcement of security practices.

Finding: Needs Improvement	D20: Is there an established procedure that users can use to report security infractions that will allow for confidentiality?

Reason and Theory: The users are out in the area where security infractions are most likely to concern. These infractions could be computer-printed material being left out or not deposited in the shredding area or terminals left logged on without a user present. Such infractions, while minor, could lead to other major security breaches that could leave Your company, its management, and employees open to legal actions. Providing a procedure to report the infractions that will allow a user to report the infraction in confidence will encourage a good security environment. This procedure should allow reporting of the infraction without the user's immediate management being involved. Remember, if the infraction is serious enough, outside agencies may be involved that requires the reporting individual's presence. Be sure to document this in the policies and procedures.

Recommendations: Review policies and procedures, if available, regarding security infractions and breaches to see if a method has been provided. If one has not, discuss it with management, establish a policy and publish it. Establish a procedure that will allow the employee to report the infraction to entity such as the help desk or system administration. Publish the procedure and be sure to educate the users during the introduction seminars and the other employee communication methods.

Comments: Users have a method in place of reporting infractions through the help desk but as far as having it be anonymous that is unknown.

Finding: Sufficient	D21: Are system administration personnel open and friendly with the user community?

Reason and Theory: Administrators who are open and friendly tend to run into fewer problems when they have to enforce rules or impose restrictions. Users will resent it if Administrators act as if the systems are their own personal property. The users will also tend to be more open about problems and issues they are the administrators will listen to them and at least acknowledge their concerns. It may be something that cannot be changed but a good explanation why may be better than ignoring them.

Recommendations: This is something that cannot be placed in the policies and procedures. A good system administrator should realize that they are there because the users need them to keep the systems up and running. A good system administrator will try to accommodate the user community where possible while maintaining a balance between security, performance and availability.

Comments: Yes, the system administrators are open and friendly to the user community. This practice establishes the open communication the end-users have and only reinforces that they can contact them if they have concerns relating to system security or just best practices.

Finding: Sufficient	D22: When a user is on an extended absence such as vacation or leave is the user's account disabled?

Reason and Theory: When a user is not going to be using their computer account for an extended period the account should be disabled. This will prevent an intruder from using the privileges granted to that user while they are away. Remember, if .rhosts files are set up incorrectly, a system can still be accessed from another system even though the account is disabled. Systems administration should be notified if a user account is not going to be used so that it can be disabled. Use of the system feature that disables the account after a period of no logins should also be investigated. This will automatically disable the account if a user leaves the employ of Your company and the system administration is not notified. Closing any avenue of attack by an intruder is always a good idea.

Recommendations: Review policies and procedures, if available, to determine what is recommended regarding disabling the accounts of users who will not be using their computer account for an extended time. If no policy exists, discuss the issue with management, create a policy and publish it. Create a procedure for management and the Human Resources Department to follow when they are aware of an employee who meets the extended absence requirements. If possible, use the System Administration Manager (SAM) to disable any unused accounts after a certain time.

Comments: Yes, all user accounts are disabled for extended leaves of absence from the University. This policy is set from Human Resources and they notify the system administrators of accounts that need to be disabled and when they can be reenabled.

Finding: Sufficient	D23: Is there a procedure in place to notify system administration of an employee leaving Your company?

Reason and Theory: Whenever an individual who had access to a computer system leaves, the system administration personnel should be notified immediately and the user's account should be disabled. This will prevent tampering with the account by an unauthorized person or prevent the employee that is leaving from doing any damage if the termination was on an unfriendly basis. This procedure should be part of the normal procedures exercised when an employee leaves. It should also be done in a timely manner. Waiting for a list of resigned employees to circulate once a month leaves the computer system open to unauthorized usage during that time period.

Recommendations: Review policy and procedures, if available, to determine if there is a policy and procedure in place regarding notification of system administration when an employee leaves. If there is none, discuss this with management, establish a policy for it, and publish it. Establish a procedure with the appropriate departments such as Human Resources to notify system administration of an employee's leaving on a timely basis. If there is a notification procedure and system administration is not part of the notification list, discuss the situation with management and have system administration added to the list.

Comments: Yes, Human Resources notifies system administrators anytime employees leave or are terminated from the University. It is policy that the account needs to be disabled and then removed from the system within 1 week of the employees leaving.

Finding: Sufficient	D24: Is there a procedure that requires the accounts of employees who have left Your company to be removed from the computer system?

Reason and Theory: The accounts, directories, files and other data that are owned by an employee who has left Your company should be either assigned to a new user or removed from the system. This may involve assigning or moving the files to the former employee's manager who will assign them to another employee or delete them. It is not a good practice to reuse the directories or login scripts from a previous account. Privileges or access capabilities may have been granted to that employee that should not be granted to another employee. The home directory and login scripts should be deleted and the ownership of all the files changed to new owners. There should be a time limit on this procedure so that old accounts are removed quickly.

Recommendations: Review policies and procedures, if available, for any requirements on removing accounts of former employees. If none is available, discuss the issue with management, create a policy for it, and publish it. Create a procedure that is to be followed by system personnel to move the files to the appropriate individual if necessary and then remove the account. Establish a time frame for how long to wait before doing this so that any legal issues can be resolved if necessary and what the maximum time is before the files will be archived and removed.

Comments: Yes, It is policy that the account needs to be disabled and then removed from the system within 1 week of the employees leaving.

Finding: Sufficient	D25: Do the users' displays automatically clear when a user logs off the system?
Reason and Theory: A potential attacker can gain information by looking at the display terminal of a user that logs off the system but leaves information on the screen. Since administrators may not be able to control the security access of outside users, the logoff from the system by default should cause the system to clear the user's screen. This will limit what might be left on the display, particularly for dial-in users, and prevent an intruder from reviewing the contents of the screen.	
Recommendations: Implement an automated process that clears the screen of any displayed information when the user logs off. This may have to done through the user application.	
Comments: Yes, the screens clear the display after logoff of the system.	

Finding: Sufficient	D26: Do users' terminals log off after a certain period of inactivity? Are users using GUI or PC terminal emulators required to use password protected screen savers?
Reason and Theory: A screen or terminal lock/logoff program should be utilized to lock or logoff idle terminals, particularly if the user's terminal or workstation is not in a secure area. Certain shell programs such as *csh* and *ksh* implement a very limited automatic logoff capability. A more extensive capability may require custom programming or third party software since logging off in an uncontrolled manner may not be acceptable to the application. If users are using Personal Computers or Workstations they should be required to implement a password protected screen saver. This capability will help prevent unauthorized use of the terminal.	
Recommendations: Review policies and procedures, if available, to determine what is required. If policies and procedures are not available or do not specify what action is required discuss the issue with management, create a policy, and publish it. Create a procedure in conjunction with the group responsible for supporting the end user to configure the terminals, Personal computers, or workstations to implement the automatic logoff or screen locking features.	
Comments: Yes, the screen terminal can be locked or after inactivity it will logoff the user.	

Finding: Needs Improvement	D27: Are users permitted use to extended network access files such as .netrc or .rhosts in their home directories?

Reason and Theory: Configuration files can facilitate network access. These files permit users to login to other machines as themselves or as certain specified users without supplying a password. Such programs can permit an unauthorized user an easy method to attack multiple machines once a single system has been breached. These files include *.rhosts* and *.netrc* files in the user's home directory, which an individual user can set up as well as the */etc/hosts.equiv* file, which the administrator can set up for all users. If these files are permitted the permissions on the files should be such as to prevent any other user from even reading them. The knowledge of which systems and/or users may connect without a password can assist an attacker in breaking security. In addition, the security of these files is based solely on system and user names and any system on the network can be set up to appear to be an authorized system. Any system specified in these files should contain a fully qualified domain name.

Recommendations: Review policies and procedures, if available, regarding intersystem access requirements (i.e. if a user is permitted access to one system are they automatically granted access to others) and permissions regarding use of files that grant intersystem access. If policies and procedures do not exist, discuss the issue with management, create a policy, and publish it. If the files are permitted be sure to create the files with the correct permissions for every user. These files should be created even if they are empty.

Comments: No, .netrc or .rhosts files are not permitted to be used in the University environment.

Finding: Sufficient	D28: Are user login scripts only modifiable by the owner?
Reason and Theory: As with the Root user, login script files of a normal user can be used to attack the system or application. An intruder with malicious intent can place code in the login files of the user that will execute when the user logins. This is called a "Trojan Horse" type of attack and does things such as delete data files or programs that the user is authorized to modify.	
Recommendations: Review policies and procedures, if available, regarding permissions and content of login files. If policies and procedures are not available discuss the issue with management, create a policy, and publish it. Review the file permissions of user login scripts. Insure that unauthorized individuals cannot modify them. Be sure that new user login scripts are created with the correct permissions and ownership. Use an automated checker such as C.O.P.S or TIGER or a commercial product to check for world writeable files.	
Comments: No, user login scripts can only be created by the System Adminstrators.	

Security of Files

Finding: Sufficient	E1: Is an umask value set for all users at login time?
Reason and Theory: By default, all users except the Root user create files and directories that are globally readable and writeable. Security principles state that the owners should be able to read and write to their own data, the group should be able to read the data and the world should not have any permission. This sometimes has to be modified for application reasons. Groups may require write permissions for application data and directories. Application and system administration personnel should work together to insure the tightest possible settings for the umask variable so that newly created user files are protected.	
Recommendations: Review policies and procedures, if available, regarding file permissions. If policies and procedures are not available, discuss the issue with management, create a policy and publish it. Work with applications development and system administration personnel to set the default umask value at restrictive value during initial login but allow application settings to modify the umask value to be more permissive during application usage. Programmatic methods are available to change a users group setting if necessary.	
Comments: Yes, a global umask value of 022 is created each time a user account is created.	

Finding: Needs Improvement	E2: Are system startup files readable and writeable only by the Root user?
Reason and Theory: System startup files are executed at time when the system is most vulnerable. Most system startup files are executed using the Root user account and do things that only the Root user should do. Users other than the Root user could plant malicious code in these files if they are modifiable. This is a way that an intruder could get the Root user to do something for the intruder such as increase his normal privileges to the Root user level or add the Intruder's account to a group with system administration privileges. See the Unix System Review Report.	
Recommendations: Review all system startup files and their directories to ensure that the proper permissions are set for these files. HP-UX ships with the correct permissions set on most system startup files but they may have been altered during program installations or other system configuration modifications. Review policies and procedures to see if a regular testing policy has been established regarding critical file permissions. If one has not been established discuss it with management and establish policy and procedure for it.	

Comments: Yes, the defaults are left in tack from the HP-UX system media loads. Whatever those defaults are they aren't changed.

Finding: Needs Improvement	E3: Are system wide or application wide login scripts protected from unauthorized modification?
Reason and Theory: System wide login files such as /etc/profile are executed by all users when they login. If these files are modifiable by anyone, other than authorized users, then malicious code could be introduced into them. This code would be executed when the user logs on to the system. The code could delete files, modifies user accounts or even displays an offensive message to the users. The results could be a Denial of Service, lost revenue or even legal issues for Your company. See the Unix System Review Report.	
Recommendations: Review policies and procedures, if available, regarding login scripts. If policy and procedures are not available, discuss the issue with management, establish policy regarding login scripts, and publish it. Review all system wide login scripts to insure that they are not modifiable by unauthorized individuals. Institute an automated checking routine that will validate the permissions and ownership of the login scripts and notify system administration if there is a change. Put the results of these checks in a place where only system administration personnel can view them.	
Comments: It is believed that application or login scripts are protected from unauthorized modification, however no verification method is currently in place. This should be reviewed and if necessary a policy and procedure should be written and added to the security best practices.	

Finding: Needs Improvement	E4: Are the HP-UX system directory permissions properly set?
Reason and Theory: The system directories contain programs, configuration information and other important system information that should not be accessible by the normal user. An untrained user or an intruder on the system using these files could result in a system outage or other disaster. Hewlett-Packard provides the proper protection on the system files when the system is installed and the permissions should not be changed. The ramifications of such changes should be carefully considered if they are made.	
Recommendations: Review policies and procedures, if available, regarding access to system programs or utilities and who may use them. If policies and procedures do not exist regarding this issue, discuss it with management, create a policy and publish it. Review the system directory permissions to ensure that unauthorized users cannot modify critical system files and that unauthorized users cannot execute sensitive system programs. Use a system-checking program such as C.O.P.S, a user written script or a commercial program to check for directories with improper permissions.	

Comments: Yes, believed to be so, but no verification method currently practiced.

Finding: Insufficient	E5: Do device files and the /dev directory have the proper permissions and ownership?
Reason and Theory: Device files, especially /dev/console, /dev/null, and /dev/tty, can be used to execute malicious programs or commands. An intruder can send commands to these files and have them executed just as if they were the users who are logged on at the devices. This is called "hijacking" and is a common way to get another user to do something for an intruder. A list of default permissions and ownership of device files is available on the "install special files" (insf) command manpage.	
Recommendations: Review the file permissions and ownership of all device files. Insure that they have not been modified from the original Hewlett-Packard setting without proper authorization. Review policies and procedures, if available, regarding the modification of system files ownership and permissions. If policy and procedure is not available, discuss the issue with management, create a policy, and publish it. Use a system checking program such as C.O.P.S, a user written script, or commercial program to check for directories with improper permissions.	
Comments: Unknown, believed to be setup with HP's defaults when a system is loaded for the first time.	

Finding: Sufficient	E6: Are program directories read only or on separate logical volumes mounted with read-only attributes?
Reason and Theory: Disk directories containing executable programs (such as *bin* directories) or files that are not normally modified can be placed on separate logical volumes and those volumes can be mounted read-only. This not only protects the files but if the system should crash, the *fsck* program will not have to repair any files on those volumes. Even *root* cannot write to a read-only file system. This does protect program files it does require special efforts when updating programs. Making the directories read-only requires only ownership of the directory to temporarily change permissions to update programs. It would be better to use separate logical volumes only in the case of extremely sensitive programs and protected directories for normal applications.	
Recommendations: Review the policies and procedures, if available, regarding software change control systems. If policies do not exist, work with management and applications development to create a policy to protect programming from unauthorized changes. Once the policy is created publish it and establish procedures for control software changes. Review all program directories for appropriate permissions. If protection through the above method is not feasible, consider instituting a change detection check such as Tripwire.	

Comments: No, however only root has the ability to mount these volumes.

Finding: **Needs Improvement**	**E7: Are "set user id" or "set group id" programs present on the system? Are adequate controls in place to prevent their abuse? Are protection methods in place to prevent unauthorized creation of such programs?**
Reason and Theory: Certain programs can be set to run "*suid*" (set user id) which makes them run as the owner of the program (which may be the Root user) rather than as the person who ran them (the normal user). Some programs require this capability. Any locally written commands that have been set up to allow *suid* capability should be protected with special access control lists (ACLs) that go beyond the standard UNIX ones. However, such commands can allow even those privileged users to break security in some circumstances. For example, if the programs are not properly tested to prevent it, a user may be able to break out of the program and obtain a Unix shell that still retains the attributes of the program owner (possibly the Root user). This will permit the user to execute commands at the command line as the Root user. See the Unix System Security Analysis for a list of detected suid and sgid programs.	
Recommendations: Review policies and procedures, if available, regarding programs with enhanced capabilities. If policies and procedures do not address this type of program, work with management and applications development to define policies that limit their use. Publish the policy. Implement automated procedures that detect the introduction of suid and sgid programs on the system. This can be done using the find command and cron. Be sure to place the output of such a check where only authorized system administrators can view it.	
Comments: No, set user id and set group id are avoided in this environment, however no mechanism is in place to verify.	

Finding: Sufficient	E8: Are file systems that should not normally contain suid files mounted without suid capability?
Reason and Theory: Certain suid programs are required but exist only on Hewlett Packard provided file systems. Such programs should not normally exist on user drives nor on non-essential file systems such as /tmp. When mounting a file system it is normal to mount it with suid programs allowed to execute. In order to protect the system from suid and sgid programs consider adding the option to prohibit suid programs from running on user and temporary file systems. Suid programs are a prime way for a break-in to be implemented. Any method that prevents execution of such programs enhances security. User disks and temporary directories are most vulnerable because of necessarily relaxed permissions; these disks should have the extra level of protection afforded by the file system.	
Recommendations: Review policy and procedure, if available, regarding creation of new file systems. If one is not available, work with management and applications development to create a policy stating that user and temporary file systems should be created with the no suid option. Publish the policy and educate the applications development group. Review all existing user and temporary file systems. If a file system does not contain a suid program, consider changing the mounting options to no suid so that it is in force during the next remount.	
Comments: No, Only root mounts these disks or filesystems.	

Finding: Needs Improvement	E9: Is protection of user files checked by automated or other means to insure that it is at the highest possible setting?
Reason and Theory: Any files that already exist will not be affected by changing the umask option to a stricter setting. If the umask variable has not been properly set all user files should be inspected to be certain the permissions and ownership is correct. Users are concerned with doing their job and information security some times drops to a lower position in their priority list. System administrators should conduct periodic review of users' files for any security anomalies and correct them. This should be done by an automated method and the results acted upon according to established policy. See the Unix System Security Review for a listing of weak file permissions or abnormal file permission settings.	
Recommendations: Review policy and procedures, if available, for file permission guidelines. If none exist, work with management to create a policy, publish it, and educate the user community. Use an automated method such as C.O.P.S., an internally written script, or a commercial product to periodically review file permission settings system wide. Review the reports with application development and the user community. Correct any deficiencies found and implement procedures to prevent reoccurrence.	

Comments: No, environment relies on the global umask 022, and no mechanism manual or automatic is in place to check that this isn't changing.

Finding: Insufficient	**E10: Are enhanced directory bit protection methods in use on the system?**
Reason and Theory: HP-UX supports two enhanced protection mechanisms for files. If a directory has the "sticky" bit set, then a user may not remove a file in that directory unless that user is the owner. This is particularly useful for shared work directories or directories like the temporary ones such as /tmp and /var/tmp. If a directory has the "*sgid*" bit set, then files in the directory have the group permission set to be the same as that of the directory itself rather than that of the user. This can be useful for trying to enforce specific group permissions.	
Recommendations: Review policies and procedures, if available, regarding creation of new directories on the system. If a policy is not available, work with management and applications development to create a policy regarding use of enhanced directory bits and publish it. Educate applications development and the user community regarding procedures to use when creating directories. If needed, create a script than will create directories for users that have the appropriate bits enabled automatically. Review existing directories to see if enhanced directory bit protection might safely be added.	
Comments: No, enhanced directory protection setting of bits is currently being used.	

Finding: Not Applicable	E11: Are NFS mounted file systems and exported file systems properly protected?
Reason and Theory: Because of the inherent weaknesses in NFS, disks exported or imported need to have special protection. If exported disks don't require remote systems to have write access, they should be exported as read-only. Restricted Root user accesses and exporting to specific hosts only should be the default by policy definition. Imported disks should always be mounted without "suid" access and executable programs on NFS mounted disks should be carefully scrutinized, particularly if the remote systems are not under the control of the local administrators. NFS network traffic should be restricted by network controls so that exported file systems that should not be accessible from user subnets are protected.	
Recommendations: Review policies and procedures, if available, regarding recommended controls on intersystem access and file system protection. If policy and procedures are not available, discuss this issue with management, create a policy for it, and publish it. Review all NFS usage on the system. Institute the proper mounting and export parameters to prevent abuse of the NFS file systems. Work with the network support group to insure NFS network traffic does not depart the local subnet. Investigate using Secure NFS available on HP-UX 11.X.	
Comments: NFS is not used in the Universities environment.	

Finding: Sufficient	E12: Is the system properly configured to protect from authorized ftp access? Is logging enabled on the ftpd?
Reason and Theory: Many security intrusions start via ftp. Improperly configured ftp access, especially if anonymous ftp is permitted, could result in an intruder gaining unauthorized access, destruction of sensitive data, or loss of system control resulting in a denial of service attack. Review the manpages on the ftpd, which has been highlighted to reflect security configuration issues.	
Recommendations: Review policies and procedures, if available, regarding recommended controls on intersystem access and file system protection. If policy and procedures are not available, discuss this issue with management, create a policy for it, and publish it. Review all ftp usage on the system. Institute the proper ftp configuration to prevent abuse of ftp access of the system. Insure that proper logging levels are set to allow logs to save ftp transfer information Investigate using secure ftp with Kerberos available on HP-UX 11.X. Use wu-ftpd which now available on HP-UX 11.X other solutions are not appropriate.	

Comments: Yes, ftpd logging is enabled as a security practice and policy.

Finding: Sufficient	E13: Is X windows access permitted to the system? Have appropriate steps been taken to insure its safety?

Reason and Theory: X Windows presents a unique security threat to the Unix systems. A part from bypassing the normal access controls such as /etc/securetty and /etc/profile there are many known and easily implemented “hacks” against it. “Hacks” can range from keystroke capture to session hijacking. X windows, unless needed for normal application work should be restricted to only trusted system administrators. In addition, network issues should be considered to restrict X windows to only trusted networks.

Recommendations: Review policies and procedures, if available, regarding recommended controls on intersystem access and system access protection. If policy and procedures are not available, discuss this issue with management, create a policy for it, and publish it. Review all X usage on the system. Review the xhost command and ensure that only trusted systems operated by trusted administrators are allowed to use X. If possible, work with the network group responsible for routing control and have X restricted within a trusted network. If not possible, use inetd.sec to restrict X network traffic. Establish procedures to restrict installation of X capable software on workstations that do not need it.

Comments: Yes, the only X Windows access is via the System Administrators PC’s.

Security of Modems

Finding: Not Applicable	F1: Are modems attached to the system turned off, disconnected from the system or telephone line or in some other way disabled until needed?
Reason and Theory: Modems present a convenient way for an intruder to attack the system without being present. The best way to protect the system from attack by modem is to turn the modems off or otherwise disable them. If the systems or modems are not close enough to the system console or other modems ring in the data center the systems personnel may not even detect the incoming calls until it is too late.	
Recommendations: Review policies and procedures, if available, regarding modem security. If policies and procedures are not available, discuss the issue with management, create a policy, and publish it. Institute a procedure that modems, especially the support modem, is turned off or disconnected until needed. The procedure should include specific procedures required to permit dial in access to the system especially for the Hewlett-Packard Support modem if service mode is enabled on the system.	
Comments: Modems, are not used in the customer's environment at all.	

Finding: Not Applicable	F2: Are procedures in place to automatically disable modems attached to the system?
Reason and Theory: For many reasons, modems should be automatically disabled on the system until the system is running in a normal mode. Modems could allow database servers to be started or file systems to be mounted. Control of modems could be done by using the inittab file and the run states. Run State 2 is the normal multi-user system state. It may be advisable to have the modems disabled at this state. Modems could be enabled by moving to Run State 3 and have the gettys for the modems activated at that state. System startup scripts could also accomplish by enabling or disabling modems at the correct time. Operators should be trained to enable and disable modems quickly in case of an attack on the system. When a system is being attacked is not the appropriate time to have operators trying to find the modems to disable them.	
Recommendations: Review policies and procedures, if available, regarding modem security. If policies and procedures are not available, discuss the issue with management, create a policy, and publish it. If applicable, create procedures or modify the inittab file to start modem connections at the appropriate time. Train operators on methods of disabling modem connections quickly if needed. Document the procedure and place it in the Security Incident Plan for quick reference.	

Comments:	Modems, are not used in the customer's environment at all.

Finding: Not Applicable	F3: Are dial-in passwords in use for modems attached to the system? If dial-in passwords are in use, do they meet the password composition policy?

Reason and Theory: The Hewlett-Packard HP9000 has the ability to require a second password for ports defined as "dial-in". This password is not unique to the user login but is based upon the user's login shell. The files /etc/dialups and /etc/d_passwd are used to implement this feature. However, dial-in password security must meet the strict guidelines as recommended for user passwords. Consideration should be made to implementing a different shell (or a different name for the same shell program) for different groups of users. This is so only users authorized for remote login can do so and administrators who may be using the same shell as users can have a different dial-in password.

Recommendations: Review policies and procedures, if available, regarding modem security. If policies and procedures are not available, discuss the issue with management, create a policy, and publish it. Create the appropriate files (/etc/dialups and /etc/d_passwd) to protect the modems attached to the system. See manpages or the HP Instant Information CD-ROM for information on creating these files. Remember to use passwords that meet the password composition policy.

Comments: Modems, are not used in the customer's environment at all.

Finding: Not Applicable	F4: Do modems attached to the system drop the connection to the system when the logs off or the user disconnects?

Reason and Theory: Modem ports, if configured correctly, will drop a connection after three-failed login attempts, after logging off or after abnormally disconnecting. The user will be logged off in the last case (abnormal disconnect) if still logged on. In addition, a modem time-out can be set such that a user can be given only a limited number of seconds (60 seconds or less is recommended) in which to successfully login without being dropped. These features insure that hackers must redial after failures thus slowing attempted attacks. In addition, it insures that the system will clean up after abnormal disconnects. Any modem connection that fails to hang-up properly upon logoff or abnormal disconnect should be disabled until proper operation is restored.

Recommendations: Review policies and procedures, if available, regarding modem security. If policies and procedures are not available, discuss the issue with management, create a policy, and publish it. Institute a modem installation procedure that includes testing for all possible disconnect situations. After an abnormal disconnect while logged on, dial back in to insure that the previous terminal session terminated. Conduct a test of all modem connections on a monthly basis to make sure unauthorized persons have not modified the modem configurations.

Comments:	Modems, are not used in the customer's environment at all.

Finding: Not Applicable	F5: Are secure modems or secure modem servers in use for user dial-ins?

Reason and Theory: Security modems should be considered for user dial-in if the modems are directly attached to the system. These are modems that will challenge the user with a one-time password, disconnect and then dial the user back at a preset telephone number or interact with software on the user's computer to identify the user. This should not be applied to the Hewlett-Packard supplied support modem, as it will seriously inhibit the Hewlett-Packard Response Center's ability to support the system. A better solution for user dial-in would be to have a modem server (a system dedicated to modem users only) that filters the incoming calls, uses strong authentication techniques and isolates the modems from critical systems. This technique is sometimes called a "sandbox" system.

Recommendations: Review policies and procedures, if available, regarding modem security. If policies and procedures are not available, discuss the issue with management, create a policy, and publish it. Conduct a risk analysis to determine if the use of secure modems or a secure modem server is feasible and appropriate for the environment.

Comments: Modems, are not used in the customer's environment at all.

Finding: Not Applicable	F6: Are modem telephone numbers changed periodically?

Reason and Theory: Administrators should consider changing the phone numbers of their modems periodically (once every year or two). Knowing the telephone numbers of systems is an important first step for anyone considering attempting to externally access it. Changing telephone numbers is not going to stop a serious hacker. Programs called War Dialers can be used to dial all numbers until a modem is found. Changing telephone numbers will limit attacks from former employees, customers, vendors or contractors who remember past logins and may wish to try to see if the information is still accurate. It is also a good practice to have modem telephone numbers that do not use the same prefix as the main telephone number as Your company.

Recommendations: Review policies and procedures, if available, regarding modem security. If policies and procedures are not available, discuss the issue with management, create a policy, and publish it. Review the advisability of changing modem telephone numbers. Consider the impact to the user community and balance it with the security considerations. Consider the use of dial-in passwords that are strong in place of this procedure.

Comments:	Modems, are not used in the customer's environment at all.

Finding: Not Applicable	F7: Are dial-in telephone lines separate from dial-out telephone lines?

Reason and Theory: If a dial-out line is used for dial-in, it is possible for a "spoof" attack to occur. A logged on user could connect to the modem and wait for another user to dial in. then "spoof" the incoming caller by putting a fake login/password prompt. This would display a fake login screen that would dupe the user into entering their login information for the attacker. For best security, separate modem ports should be used for calling out and calling in.

Recommendations: Review policies and procedures, if available, regarding modem security. If policies and procedures are not available, discuss the issue with management, create a policy, and publish it. Review the use of the modems on the system and, if possible, separate their functions into dial-in and dial-out. Have telephone services enable dial-out capability on the dial-out modems so that incoming calls are rejected. Be sure the permissions on the modem device files are correct to so a normal user cannot use it to create an attack scenario.

Comments: Modems, are not used in the customer's environment at all.

Finding: Not Applicable	F8: Is the use of the Remote Support Modem strictly controlled and only used for Hewlett-Packard Support purposes?

Reason and Theory: Because the Remote Support modem can have special access and may be left on or left enabled inadvertently, this modem should be more strictly controlled. It should not be on a "rotary" with other telephone lines such that if another modem or line were busy, the connection would be rolled over to this line. Remote Support modems are best left for remote access by authorized Hewlett-Packard personnel. The Remote Support Modem should not be used for normal user access.

Recommendations: Review policies and procedures, if available, regarding modem security. If policies and procedures are not available, discuss the issue with management, create a policy, and publish it. Restrict the use of the Hewlett-Packard Supplied Support Modem to support purposes only! Require manual intervention to activate it after system personnel confirm the identity of the remote user. If service mode is enabled on the system, use the DR command to disable remote access until it is needed.

Comments: Modems, are not used in the customer's environment at all.

Security Of Normal User

Overall Security of the Systems

Finding: Insufficient	G1: Are the system accounts (sys, bin, lp, etc.) disabled to prevent logins using these accounts?
Reason and Theory: All Unix systems have accounts that are used to control various special functions such as printing and logging. HP-UX ships with these accounts disabled. Access to these accounts would provide an intruder access to many system functions that if misused could lead to denial of service or theft of information. These account should have an * in the password field to indicate that they are disabled or if a trusted configuration is used, the account should so disabled under the System Administration Manager (SAM).	
Recommendations: Review policy and procedures regarding system accounts. If policies and procedures are not available discuss the issue with management, create a policy, and publish it. Review all supplied with the system to insure that they are disabled with the exception of the Root user. If any of the accounts are not disabled, be sure to have a very strong password on the account. Establish a procedure to review the system accounts at least once per month to make sure that they are still disabled and secure. If possible automate this procedure. Place the output of this check in a location where only trusted system administrators can view it.	
Comments: No, whatever the HP-UX load defaults for sys, bin, lp, uucp in /etc/passwd are what they are today.	

Finding: Insufficient	G2: Is the mail of system users (bin, adm, sys, lp, etc.) being read regularly?
Reason and Theory: The “system” users like bin, adm, sys, lp, etc and others automatically execute certain programs on the system. At times, like when periodic jobs are run by the cron daemon, mail is sent automatically to themselves. Unlike root’s mail, which is likely read by administrators, the mail of these “users” may never be seen but may contain critical information, especially if a message indicates that something that used to work no longer does. This could indicate the presence of an intruder on the system, a configuration error that may be opening the system up to attack or other precarious situation? It also conserves space of the system. On some systems, the size of the mail files has been as much as 50 megabytes of disk space.	
Recommendations: Review policy and procedures regarding system accounts. If policies and procedures are not available discuss the issue with management, create a policy, and publish it. Review the mail of the user accounts currently on the system. If possible, forward the mail to the Root user account of the system or to another system where the mail can be read and kept under control. Create a procedure for any new system being installed to set the mail up properly before the system is put into production.	

Comments: No, only root mail is currently read according to practices in place today.

Finding: **Needs Improvement**	**G3: Does the file "btmp" exist, are the permissions correct, and it is monitored and controlled?**
Reason and Theory: The file "btmp" is used to log bad login attempts to the system. It should exist on the system, in the directory /var/adm/btmp, and have the permissions such that the Root user can read and write to it but no one else can. The reason is that this file could possible contain passwords as the result of failed logins. For example, a failed login would occur if a user types his password in the user id field. If an intruder were to have access to this file and the wtmp he could compare logins and, possibly, find passwords for users. This file can be monitored for successive bad logins for to see if an intruder is trying to gain access by trying multiple passwords. If you see this you should disable the account and investigate. Watch for bad logins for the Root user and other system accounts.	
Recommendations: Review policy and procedures regarding logs and intruder detection. If policies and procedures are not available discuss the issue with management, create a policy, and publish it. Immediately check to see if the btmp file exists and a possible link to it in the /etc directory. Make sure that the files have the correct ownership (Root user) and permissions (rw-------). If this file is not to be used, delete it to prevent its contents from being used against your system. If is to be used, monitor it and trim it periodically. Automate checking this file for permissions and ownership.	
Comments: Yes, the btmp file exists and the log files are read regularly, however monitoring of the file permissions aren't being done.	

Finding: Insufficient	G4: Does the /etc/shutdown log exist and are the permissions correct?

Reason and Theory: The /etc/shutdown file logs all system shutdowns and startups including system panics. It does not exist by default. It should be created and write access prohibited to normal users. It is important to have the correct permissions and ownership on this file, and all logging files. If logging files do not have the correct permissions, a hacker can erase evidence of his activities on your system. In case of problems, this file can provide valuable evidence of the system uptime and downtime.

Recommendations: Review policy and procedures regarding logs and intruder detection. If policies and procedures are not available discuss the issue with management, create a policy, and publish it. Immediately check to see if the shutdown log file exists. Make sure that the file has the correct ownership (Root user) and permissions (rw-------). If this file is not to be used, delete it to prevent its contents from being used against your system. If is to be used, monitor it and trim it periodically. Automate checking this file for permissions and ownership. Also check it daily for evidence of an unauthorized shutdown.

Comments: No, the /etc/shutdown log file hasn't been created on the system, therefore it's not one of the log files regularly being monitored.

Finding: **Needs Improvement**	**G5: Are security related logs reviewed on an adequate basis? Do the log files have the correct permissions?**
Reason and Theory: Log files are kept for one reason. To be read by system administration personnel. For most systems, this is only done when there a problem is discovered. By doing it more often, problems can be prevented. Logs should be read daily by system personnel or an automated means of review such as ITO and ITA or other security programs. It may be more convenient to send the syslog (found in the /var/adm/syslog directory) to a central system where it can be reviewed by an automated means. Most logs are owned by the Root user (root). The group for logs is usually sys or root. This may not be true in all cases and each log file should be reviewed for the appropriate. The permissions for logs are usually read/write for the owner and either read for the group and world or no other permissions.	
Recommendations: Review policies and procedures, if available, for system logging requirements. If policies and procedures are not available, discuss the issue with management to determine the appropriate level of logging and log review requirements, publish it, and educate system personnel. Institute a procedure of regular log review including the syslog, mail log, and the logs of any other services offered by the system. Investigate the use of the logger command with applications to concentrate log information in one spot for easy review.	
Comments: Yes, the following log files are reviewed daily – sulog, wtmp, btmp, syslog and ftpd logging, however reviewing of file permissions isn't monitored currently.	

Finding: Sufficient	G6: Do system administrators and personnel investigate unusual occurrences or log entries on the system? Do they file incident reports with the appropriate security group?

Reason and Theory: System personnel should always take time to investigate any thing unusual that occurs with a system. A modem dialing when it should not be, an entry in the shutdown log when there should not have been a shutdown, multiple logon attempts detected in the btmp file, or sudden unusual system activity could be indications of a hacker at work. It may be nothing but even if it isn't, an incident report should be filed. A series of occurrences that individually mean nothing could when put together indicate a pattern of attack.

Recommendations: Review policies and procedures, if available, for incident review requirements. If policies and procedures are not available, discuss the issue with management to determine the appropriate policy regarding unusual incidents, create a policy, publish it, and educate system personnel. Establish a procedure to log the incidents for later review. Be sure to store the logged information where only trusted system administrators can review it. If an intruder can view this data, the intruder will modify his attack methodology once aware that he/she is being monitored.

Comments: Yes, system administrators practice security in there daily activities. If something looks to be out of the ordinary they take the time to investigate and notify the proper channels if that is what is needed.

Finding: Sufficient	G7: Are system administrators and personnel security conscience? Do they practice good security techniques and adhere to policy and procedures regarding security?

Reason and Theory: Users will typically follow the example of System Administrators, so the Administrators need to practice good security. This includes not having "Back Doors," not having weak passwords, not dialing in from home when it is against policy just because it is easier, etc. System administrators and personnel should also be aware of what is contained in the policies and procedures and be able to act on their contents. System administrators and personnel should be included in the user education process so that they are aware of what the users are being taught regarding security.

Recommendations: Review policies and procedures, if available, for system personnel and requirements regarding security awareness. If policies and procedures are not available, discuss the issue with management to determine the appropriate security education of system personnel, create a policy, publish it, and educate system personnel.

Comments: Yes, system administrators practice security in there daily activities. If something looks to be out of the ordinary they take the time to investigate and notify the proper channels if that is what is needed.

Finding: Sufficient	G8: If system personnel discover a security weakness on the system, do they report it and take steps to minimize the exposure until it is corrected?

Reason and Theory: System personnel are the first line of defense for system security. They will usually discover weaknesses in security (incorrect file permissions, etc.) during their normal and routine activities. It is important that they are encouraged to report the weakness and take steps, if possible, to minimize the exposure of the weakness. The reporting of the weakness is most important since it may take a higher knowledge level of the operating system or interaction with applications development to correct the issue. Awareness of the weakness begins with the documentation process and all reports should be investigated. Results of the investigation should be shared with the reporting individual so that the individual knows management takes these reports seriously.

Recommendations: Review policies and procedures, if available, for system personnel and requirements regarding security awareness. If policies and procedures are not available, discuss the issue with management to determine the appropriate security education of system personnel, create a policy, publish it, and educate system personnel. Establish a procedure for reporting discovered weaknesses, investigation of the report, and a method for reporting on the disposition of the report. Include a method that will affect the reporting individual's performance evaluation in a positive manner for being security aware.

Comments: Yes, If something looks to be out of the ordinary they take the time to investigate and notify the proper channels if that is what is needed.

Finding: Sufficient	G9: Are security procedures well documented and available for new system personnel?
Reason and Theory: Security procedures should be documented and available for all system personnel to review. It is much more important in the case of a new system administrator. If the policies and procedures are not documented then the procedures will have to be "handed down" by word-of-mouth to a new system administrator. This leads to inconsistencies and mistakes resulting in security deficiencies that will leave the systems vulnerable to attack.	
Recommendations: Review policies and procedures, if available, for documentation standards and publishing methods. These methods should include an easily obtainable copy for system personnel to review quickly such as an internal web site. If policies and procedures are not available, discuss this issue with management, create a documentation policy, and publish it. Review the current documentation to see if it is adequate and available to system personnel. If not, institute a procedure to create the necessary security documentation and make it available.	
Comments: Yes, security procedures are documented and reviewed with new system administration personnel.	

Finding: Needs Improvement	G10: Is the additional security of the inetd.sec file being used?
Reason and Theory: Any attempt to limit access to a system improves system security. The inetd.sec file (at HP-UX 11.X found in the /var/adm directory) provides a means to limit what subnets can access the system and what protocols can be used. Evaluating the networks that need to access the system and what protocols are needed can identify what is needed. Implementing the inetd.sec will limit access to only valid and authorized users on the appropriate network and using the correct protocols. In the case of client-server environments, it is a good idea to implement this technique to isolate the servers from the user population if possible. The inetd.sec file would permit only the application servers to "talk" to the database servers.	
Recommendations: Review policies and procedures, if available, for network access provisions. If not available, discuss the issue with management and network support, create a policy for limiting network access, publish it, and educate the system personnel regarding it. Conduct an analysis of the networks and user requirements and implement inetd.sec as appropriate. Institute a procedure for new applications and servers that require identification of networks and protocols to insure that new servers are correctly installed.	

Comments: No, not used within this environment.

Finding: Sufficient	G11: Have network services on the system been reviewed and unnecessary services disabled?

Reason and Theory: Most servers are installed with all network services active. This includes services such as chargen, tod (time of day), discard and qotd (quote of the day). These services are not necessary for many applications or system requirements. While having these services active is usually not a hazard, a hacker can make use of them for a network denial of service attack. If the system is not protected by properly configured routers or firewalls, minimizing the number of services offered to only those needed removes many opportunities for attack.

Recommendations: Review policies and procedures, if available, for network access requirements and new system installation policies and procedures. If none are available, discuss with management and network support, create a policy that requires minimizing unneeded network services, publish it, and educate system and network personnel. Create a procedure for new system that disables unneeded network services via the System Administration Manager (SAM) or inetd.conf. Review current systems with the purpose of minimizing unneeded services. Have network support use a commercial network port scanner or shareware scanner such as NMAP (www.insecure.org) to determine how your systems respond from the network.

Comments: Yes, /etc/services file has been modified to remove services not used in this environment.

Finding: Sufficient	G12: Has changing to a "Trusted System" configuration been considered?

Reason and Theory: Trusted Systems implement a trusted computing base that limits the ability to view the encrypted user passwords. This prevents a common hacker attack where the password file is stolen by using an ordinary user account. The password file is then subjected to a password-cracking program in an effort to acquire the passwords of accounts with more privileges. Trusted systems also allow extensive auditing of user actions. It also allows for checking of minimum password length, variable time between failed logins and control of password composition. However, use of a trusted system should be carefully considered when working with some third party programs such as databases.

Recommendations: Review Trusted System configuration and its implications. If appropriate, discuss the issue including manageability issues with management. If appropriate, test the configuration on a test server by activating it with the System Administration Manager (SAM). If tests prove successful, implement it on the production servers.

Comments: Yes, but the decision was made not to implement.

Finding: Insufficient	G13: Is a software source control system in use?
Reason and Theory: Source Code Control Systems (SCCS) help insure the integrity of scripts or programs. It documents who created or modified a program and what was changed. It will also enable administrators to go back to previous versions if a possibly compromised program is found. Both the standard UNIX SCCS and Berkeley UNIX RCS are available on HP-UX systems. If a standard UNIX SCCS/RCS utility is not used, all scripts and program sources should contain documentation at the beginning of the file of who is making the changes, when the change was made, and a reason for the change. A procedure should be implemented to review the modification date with the date of the file the system. Any radical difference should be reported.	
Recommendations: Review policies and procedures, if available, regarding source code controls. If none exist, discuss the issue with management and applications development, create a policy, and publish it. Implement a procedure using SCCS/RCS to control scripts, programs and other files that are modified on the system that could contain harmful code. Establish a testing procedure to periodically review dates on source code and on production code to make sure unauthorized revisions have not occurred.	
Comments: No, source code control in not implemented.	

Finding: Insufficient	G14: Are software vendors or developers required to explain the security of their programs? Is 3rd party software reviewed to make sure it works with in security policies and procedures?
Reason and Theory: Software vendors should be asked to explain the security of their products, including whether security is integrated into the product or added on, how vulnerable the product is to a break-in, and what security standards the product meets. Software products should be review with security policies and procedures in mind. If a product requires violation of policies and procedures, it should be considered a security hazard.	
Recommendations: Always evaluate any new product with security in mind. If a product does not meet security policies, discuss the issue with management. Be sure to have the requirements of what will be needed to secure the product. This may mean added cost. This may include installing the product on a separate server and isolating it to protect your environment. Discuss the issue with the vendor to see if changes can be made to secure the product.	

Comments: No, the University doesn't require this.

Finding: Sufficient	G15: Is an appropriate warning banner displayed at login to the system?
Reason and Theory: While administrators may wish to discuss the exact wording with legal counsel, every login should display a message that unauthorized access is prohibited. It is recommended that any messages issued prior to login NOT displays anything that would give an unauthorized user a clue as to the nature or type of system being accessed. The login process should notify the user that your company owns the system and that everything can be monitored. It should also state their activities might be monitored in the normal course of system administration. The last line should state that by proceeding they are explicitly agreeing to this.	
Recommendations: Review policies and procedures, if available, regarding the login process and login banner contents. If none is available, discuss the issue with management and corporate legal, create a policy, publish it, and educate the user community. Review current login banners and modify them to the one agreed upon by Your company. Establish a procedure for new systems so that all new systems will have the appropriate login banner. Work with the network group to insure that the login banner is displayed at the earliest possible time such as a network login.	
Comments: Yes, a warning banner is display stating unauthorized access to this system is strictly prohibited and is subject to legal prosecution.	

Finding: Sufficient	G16: Are guest accounts in use on the system?
Reason and Theory: These low-use, seldom monitored accounts are an ideal target for potential intruders. Many attackers will check for accounts called “guest” with a password of “guest.” Remember that a guest account is still a normal user and has access to some system files such as the password file. Illicit use of the guest account could be the initial start of an attack to gain access to the system as a user with higher privileges.	
Recommendations: Review policy and procedures, if available, regarding the use of guest accounts, account sharing, user identification and password ownership. If none are available, discuss the issue with management, create a policy severely limiting the use of guest accounts, publish it, and educate the user community. Review the current use of guest accounts, determine why they are in use, and work out procedures to replace them with normal user accounts. Work with the department that assigns new user accounts to expedite the procedure so new employees will not require “guest” accounts.	

Comments: No, guest accounts are not used; every user has a login account.

Periodic Testing

Finding: Insufficient	H1: Are system personnel using swverify or other public domain program to check for modifications in Hewlett-Packard supplied programs?
Reason and Theory: An intruder may modify Hewlett-Packard supplied programs to gain access or to maintain access to the system. Many known attacks use modified system files to reactivate a weakness after system personnel have closed it. Other attacks, sometimes called a root kit attack, replace operating system programs with modified programs. These programs, when run, allow access to the system as the Root user or mask the presence of other files used to attack the system. In many cases, these programs are common programs such as the ls command. The only way to detect the presence of these attacks is to have a method that checks the integrity of the operating system programs. Using the swverify command or a public domain program such as tripwire can do this.	
Recommendations: Review policies and procedures, if available, for system testing and intrusion detecting policy. If none are available, discuss the issue with management, create a policy, publish it, and educate system personnel. Create a procedure that will run the **swverify** command or public domain program to check the integrity of the system files. This procedure should be run on an automated basis using cron and at random times by system personnel. Be sure to put the output of this check in a location where only trusted system personnel can view it.	
Comments: No, customer doesn't have this procedure as part of security practices currently.	

Finding: Insufficient	**H2: Is a public domain or commercial security-checking program being used? Is testing being done to insure the integrity of files and compliance to policies being done?**

Reason and Theory: The public domain program C.O.P.S. provides an extensive report and is an excellent security checker. If commercial programs are not purchased, this program should be used. There are other public domain programs available such as "Crack" which is designed to test password files, "SATAN" which tests network security and "Tripwire" which checks for any changes in files. Such public domain programs are available on the Internet. This testing is important especially when policies and procedures have been established. In many instances, a legal challenge to a policy may be lost if there is no method available to enforce compliance. **Note: The Tripwire license has been purchased and is now a commercial product.**

Recommendations: Review policies and procedures, if available, regarding system security testing and policy compliance such as password composition. If none is available, discuss the issue with management, create a policy regarding testing, publish it, and educate system personnel and user community. Establish procedures to run periodic tests on the system using the appropriate system checking software. In the procedure, document appropriate notification and action requirements when a deficiency is found such as the notification of management.

Comments: No, customer doesn't have this procedure as part of security practices currently.

Finding: Insufficient	H3: Is there an automated check for new "set user id" (suid) programs that might appear on the system? As a minimum, is it run at least once every 24 hours?

Reason and Theory: Any file that has suid or set sgid (set group id) capability can be a potential problem. However, certain programs MUST run suid but these programs have other protection that prevents unauthorized use. For example, the suid /usr/bin/passwd program allows users to change their own password though the passwd file is not writeable by ordinary users. Programs such as these should check the users' authorization and limit them appropriately. There should not be any unrecognized suid or sgid programs on the system. Detecting their presence should be a warning that something is potentially wrong. A list of suid/sgid programs that are authorized should be kept in a secure location and this list compared to those actually found. Detection of suid/sgid programs can be done by Unix security checking program such as C.O.P.S or by the find command. Use of the find command in a cron script will allow for daily checking for new suid/sgid programs which may be better than waiting for a once per week or monthly run of the Unix security checking program.

Recommendations: Review policies and procedures, if available, for security testing requirements and the approved presence of programs that assume the ID of another user when run. If none is available, discuss the issue with management, create a policy for security testing and suid/sgid programs, publish it, and educate system personnel, applications development and the user community. Use a testing method to identify suid/sgid programs currently on the system. Identify any which pose a security risk and work on removing them. Institute a procedure that will automatically detect the presence of new suid/sgid programs.

Comments: No, customer doesn't have this procedure as part of security practices currently.

Finding: Insufficient	H4: If cron jobs are being used to check the system, are the checks also run at intermittent intervals by system personnel and are the check scripts being audited for accuracy?
Reason and Theory: The cron program can be used to check the system integrity on a regular basis by running the aforementioned swverify, checks for new UID 0 accounts, and using the find command to look for suid programs. The results of these checks could be mailed to system personnel for review or stored in a protected location. Information from the log files could also be sent. However, automated checking must be accompanied by periodic manual testing, as relying solely on automated procedures that can be attacked is dangerous.	
Recommendations: Review policy and procedures, if available, regarding system security testing. If none is available, discuss the issue with management, create a policy requiring automated and manual testing, publish it, and educate system personnel about it. Review current automated testing procedures, if available, and create a series of test programs to be run on an intermittent basis. If not available, create a series of test programs to be automated via cron and a set to run manually. Instruct system personnel on procedures for running and interpreting this test.	
Comments: No, customer doesn't have this procedure as part of security practices currently.	

Finding: Sufficient	H5: Are system administrators keeping up to date with system patches? Is at least one system administrator subscribed to the Hewlett-Packard Security Bulletin electronic mailing list?
Reason and Theory: While not strictly a security issue, it is important that the administrator keep up to date with their patches as some of them may affect security on the system. Hewlett-Packard provides a higher level of support that, among other things, includes periodic analysis and custom patch selection. As an alternative, the administrator can get on an electronic mailing list to be notified of new patches, can browse patches for their applicability on the Internet and can download patches via Internet access. Listings of security patches are available and these should be reviewed immediately, and if applicable, implemented immediately. Customers can subscribe to these patches at the Hewlett-Packard web site under support.	
Recommendations: Review policies and procedures, if available, regarding system patching. If not available, discuss with management, create a policy regarding system patching, publish it, and educate system administration personnel. Subscribe to the Hewlett-Packard security bulletin service, if not already done. Create a procedure to review all announced patches with respect to system environment to determine the need for the patch, methods of testing the impact of the patch on systems and applications, and method of patch application.	

Comments: Yes, system patches and security patches are kept up to date with contract deliverables, and as security notification are sent they are implemented outside of the regularly scheduled patch analysis's .

Finding: Sufficient	**H6: Are critical system configuration files and log files being stored offline safely and protected from unauthorized access?**
Reason and Theory: It is important, particularly when a security incident occurs, that there be good backups of files that could determine what changes might have been made. This could be to the password and other files. These files may also be used to determine who may have been on the system improperly. A separate backup of security and logging files is important. Of course, this should be done prior to truncating them. The permissions need to be set strictly on these files. If a change detection system such as tripwire is not in place, a backup copy of a directory may be the only means of detecting what the original files looked like.	
Recommendations: Review policies and procedures, if available, regarding system backups. If none are available, discuss the issue with management, create a policy for the backup of critical system files such as /etc/passwd and log files. Publish the policy, and educate system personnel about it. Create procedures that will regularly backup the critical files, identify the secondary storage media, and securely store it to prevent unauthorized access. Develop additional procedures for restoring the files in case they are needed for a security incident resolution.	
Comments: Yes, these files are backed up according to customers backup schedule and sent offsite with the regular schedule of rotation of tapes.	

Finding: **Needs Improvement**	**H7: Do "alarm" or host based intrusion detection programs exist on the system?**
Reason and Theory: Just as a business installs burglar alarms, systems should have programs that detect unauthorized usage. These programs should monitor log files, check critical directories for unauthorized alterations, and review general system status for unusual events. These programs should be designed to filter out spurious events that are not critical but alert system administration if a serious problem is detected. This could be done via a pager or electronic mail according the level of the event.	
Recommendations: Review policy and procedure, if available, regarding security testing and system monitoring. If none is available, discuss the issue with management; create a policy listing testing and notification methods. Publish the policy and educate system personnel. Create a procedure for monitoring systems with scripts or with commercial intrusion detection software. Determine appropriate notification levels and actions to be taken in accordance with the security incident plan, if it is available.	
Comments: Yes, University of Test Case has installed HP's IDS/9000 product. It's not production implemented to date, still working out some bugs with the response center.	