**UNCLASSIFIED**

**Solaris 10 X86 Security Technical Implementation Guide**

**Version: 1**

**Release: 1**

**2 Aug 2012**

**XSL Release 6/19/2012     Sort by:   STIGID**  
**Description:** The Solaris 10 (X86) Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. Comments or proposed revisions to this document should be sent via e-mail to the following address: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
**Group ID (Vulid):** V-12031  
**Group Title:** GEN000000-SOL00020  
**Rule ID:** SV-12532r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00020  
**Rule Title:**The nosuid option must be configured in the /etc/rmmount.conf file.  
  
  
**Vulnerability Discussion:**  The rmmount.conf file controls the mounting of removable media on a Solaris system. Removable media is not to be trusted with privileged access, and therefore the filesystems must be mounted with the nosuid option, which prevents any executables with the setuid bit set on this filesystem from running with owner privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
# grep mount /etc/rmmount.conf  
  
Confirm the nosuid option is configured.  
  
mount \* hsgs udgs ufs -o nosuid  
  
If the nosuid option is not configured in the /etc/rmmount.conf file, this is a finding.  
  
  
  
**Fix Text:**Edit /etc/rmmount.conf and add the nosuid mount option to the configuration.     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4353  
**Group Title:** GEN000000-SOL00040  
**Rule ID:** SV-4353r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00040  
**Rule Title:**The /etc/security/audit\_user file must not define a different auditing level for specific users.  
  
  
**Vulnerability Discussion:**  The audit\_user file may be used to selectively audit more, or fewer, auditing features for specific individuals. If used this way it could subject the activity to a lawsuit and could cause the loss of valuable auditing data in the case of a system compromise. If an item is audited for one individual (other than for root and administrative users - who have more auditing features) it must be audited for all.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Perform:  
  
      #       more /etc/security/audit\_user  
  
If /etc/security/audit\_user has entries other than root, ensure the users defined are audited with the same flags as all users as defined in /etc/security/audit\_control file.   
  
  
**Fix Text:**Edit the audit\_user file and remove specific user configurations differing from the global audit settings.     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4352  
**Group Title:** GEN000000-SOL00060  
**Rule ID:** SV-4352r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00060  
**Rule Title:**The /etc/security/audit\_user file must be owned by root.  
  
  
**Vulnerability Discussion:**  The /etc/security/audit\_user is a sensitive file and must be owned by root to prevent possible system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/security/audit\_user ownership.  
  
# ls -lL /etc/security/audit\_user  
  
If /etc/security/audit\_user is not owned by root, this is a finding.  
  
  
**Fix Text:**Change the owner of the /etc/security/audit\_user file to root.  
# chown root /etc/security/audit\_user     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4351  
**Group Title:** GEN000000-SOL00080  
**Rule ID:** SV-4351r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00080  
**Rule Title:**The /etc/security/audit\_user file must be group-owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  The Solaris audit\_user file allows for selective auditing or non-auditing of features for certain users. If it is not protected, it could be compromised and used to mask audit events. This could cause the loss of valuable forensics data in the case of a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/security/audit\_user group ownership.  
  
# ls -lL /etc/security/audit\_user  
  
If /etc/security/audit\_user is not group owned by root, sys, or bin, this is a finding.  
  
  
**Fix Text:**Change the group owner of the audit\_user file to root, bin, or sys.  
Example:  
# chgrp root /etc/security/audit\_user     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4245  
**Group Title:** GEN000000-SOL00100  
**Rule ID:** SV-4245r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00100  
**Rule Title:**The /etc/security/audit\_user file must have mode 0640 or less permissive.  
  
  
**Vulnerability Discussion:**  Audit\_user is a sensitive file that, if compromised, would allow a malicious user to select auditing parameters to ignore his sessions. This would allow malicious operations the auditing subsystem would not log for that user.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/security/audit\_user permissions.  
  
# ls -lL /etc/security/audit\_user  
  
If /etc/security/audit\_user is more permissive than 0640, this is a finding.  
  
  
**Fix Text:**Change the mode of the audit\_user file to 0640.  
# chmod 0640 /etc/security/audit\_user     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22599  
**Group Title:** GEN000000-SOL00110  
**Rule ID:** SV-27004r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00110  
**Rule Title:**The /etc/security/audit\_user file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Audit\_user is a sensitive file that, if compromised, would allow a malicious user to select auditing parameters to ignore their sessions. This would allow malicious operations the auditing subsystem would not detect for that user. It could also result in long-term system compromise possibly leading to the compromise of other systems and networks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/security/audit\_user  
If the permissions of the file contain a "+", an extended ACL is present, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/security/audit\_user     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4313  
**Group Title:** GEN000000-SOL00120  
**Rule ID:** SV-36751r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00120  
**Rule Title:**The ASET master files must be located in the /usr/aset/masters directory.  
  
  
**Vulnerability Discussion:**  If ASET is used and the master files (tune.high, tune.med, tune.low, and uid\_aliases) are not located in the proper place, ASET cannot operate correctly and valuable security findings could be lost.   
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify ASET is being used.  
  
# crontab -l |grep aset   
  
If there is an output, then check to make sure the files in question are in the /usr/aset/masters directory.  
  
      #       ls -l /usr/aset/masters  
  
The following files should be in the listing: tune.high, tune.low, tune.med, and uid\_aliases. If any of the files are not in the directory listing, this is a finding.  
  
**Fix Text:**Install the default ASET configuration files.     
  
**CCI:**CCI-000032  
  
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4312  
**Group Title:** GEN000000-SOL00140  
**Rule ID:** SV-4312r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00140  
**Rule Title:**The /usr/aset/masters/uid\_aliases must be empty.  
  
  
**Vulnerability Discussion:**  If uid\_aliases has entries, users may not be properly identified in ASET records.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# more /usr/aset/masters/uid\_aliases  
  
If the /usr/aset/masters/uid\_aliases file is not empty or all contents are not commented out, this is a finding.  
  
**Fix Text:**Empty or comment out the entries in the uid\_aliases file.     
  
**CCI:**CCI-000032  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4309  
**Group Title:** GEN000000-SOL00160  
**Rule ID:** SV-4309r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00160  
**Rule Title:**If the system is a firewall, ASET must be used on the system, and the firewall parameters must be set in /usr/aset/asetenv.  
  
  
**Vulnerability Discussion:**  ASET will not perform firewall tasks if it is not listed as a parameter in /usr/aset/asetenv.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Perform the following to determine if ASET is being used.  
  
      # crontab -l |grep aset  
  
A returned entry would indicate ASET is being utilized. Determine if ASET is configured to check firewall settings.  
  
      # grep TASKS /usr/aset/asetenv | grep firewall  
  
If an entry is not returned, this is a finding.  
  
**Fix Text:**If the system is used as a firewall and ASET is used, ensure the firewall parameter is configured in /usr/aset/asetenv.     
  
**CCI:**CCI-000032  
  
  
**CCI:**CCI-000366  
  
  
**CCI:**CCI-001298  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-953  
**Group Title:** GEN000000-SOL00180  
**Rule ID:** SV-953r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00180  
**Rule Title:**The Solaris system Automated Security Enhancement Tool (ASET) configurable parameters in the asetenv file must be correct.  
  
  
**Vulnerability Discussion:**  If settings in the asetenv file have been modified, then system vulnerabilities may not be detected.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if ASET is being used.  
      #       crontab -l | grep aset  
  
Check the configuration of ASET.  
      #       more /usr/aset/asetenv  
  
OR  
  
Check that asetenv has not been modified since installation.  
# pkgchk SUNWast  
  
If there are any changes below the following two lines that are not comments, this is a finding.  
  
# Don't change from here on down ... #  
# there shouldn't be any reason to. #  
  
In addition, if any of the following lines do not match, this is a finding.  
  
TASKS="firewall env sysconf usrgrp tune cklist eeprom"  
CKLISTPATH\_LOW=${ASETDIR}/tasks:#${ASETDIR} \  
/util:${ASETDIR}/masters:/etc  
CKLISTPATH\_MED=${CKLISTPATH\_LOW}:/usr/bin:/usr/ucb  
CKLISTPATH\_HIGH=${CKLISTPATH\_MED}:/usr/lib:/sbin: \  
                  /usr/sbin:/usr/ucblib  
YPCHECK=false  
PERIODIC\_SCHEDULE="0 0 \* \* \*"  
UID\_ALIASES=${ASETDIR}/masters/uid\_aliases  
  
(The default asetenv file can be found on the Solaris installation media.)  
  
**Fix Text:**Restore the ASET configuration to vendor default and only modify the portions of the configuration designated as customizable.     
  
**CCI:**CCI-000032  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-954  
**Group Title:** GEN000000-SOL00200  
**Rule ID:** SV-36750r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00200  
**Rule Title:**The asetenv file YPCHECK variable must be set to true when NIS+ is configured.  
  
  
**Vulnerability Discussion:**  If YPCHECK is not set to true in asetenv, then ypfiles may not be checked.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Perform the following to determine if ASET is configured to check NIS+.  
  
      #       grep YPCHECK /usr/aset/asetenv  
  
If NIS+ is running and the YPCHECK variable is set to false, then this is a finding.  
  
  
**Fix Text:**Edit the ASET configuration and set YPCHECK to true on systems running NIS. (If NIS+ is configured, YPCHECK must only be set to false to avoid going into NIS compatibility mode.) Configure NIS to use YPCHECK.     
  
**CCI:**CCI-000032  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-955  
**Group Title:** GEN000000-SOL00220  
**Rule ID:** SV-955r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00220  
**Rule Title:**The /usr/aset/userlist file must exist.  
  
  
**Vulnerability Discussion:**  If the userlist file does not exist, then an unauthorized user may exist in the /etc/passwd file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if ASET is being used.  
# crontab -l | grep aset  
If ASET is not used on the system, this is not applicable.  
If ASET is being used, but is not invoked with the "-u /usr/aset/userlist" option, this is a finding.  
  
Check the /usr/aset/userlist file.  
# ls -lL /usr/aset/userlist  
If /usr/aset/userlist file does not exist, this is a finding. An empty /usr/aset/userlist file, while not optimal, is not a finding.  
  
**Fix Text:**Create the /usr/aset/userlist file and populate it with a list of authorized users.     
  
**CCI:**CCI-000032  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-956  
**Group Title:** GEN000000-SOL00240  
**Rule ID:** SV-956r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00240  
**Rule Title:**The /usr/aset/userlist file must be owned by root.  
  
  
**Vulnerability Discussion:**  If the userlist file is not owned by root, then an unauthorized user can modify the file and enter an unauthorized user.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
If ASET is not used on the system, this is not applicable.  
  
Check the ownership of the /usr/aset/userlist file.  
# ls -lL /usr/aset/userlist  
If the owner of the file is not root, this is a finding.  
  
**Fix Text:**Use the chmod command to change the owner of the /usr/aset/userlist file.   
  
# chown root /usr/aset/userlist     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22600  
**Group Title:** GEN000000-SOL00250  
**Rule ID:** SV-27013r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00250  
**Rule Title:**The /usr/aset/userlist file must be group-owned by root.  
  
  
**Vulnerability Discussion:**  The /usr/aset/userlist file is critical to system security and must be protected from unauthorized access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the file.  
# ls -lLd /usr/aset/userlist  
If the group owner of the file is not root, this is a finding.  
  
**Fix Text:**Change the group ownership of the file.  
# chgrp root /usr/aset/userlist     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-957  
**Group Title:** GEN000000-SOL00260  
**Rule ID:** SV-957r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00260  
**Rule Title:**The /usr/aset/userlist file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  A permission mask not set to the required level could allow unauthorized access to sensitive system files and resources.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /usr/aset/userlist  
  
If /usr/aset/userlist has a mode more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the /usr/aset/userlist file to 0600.  
# chmod 0600 /usr/aset/userlist     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22601  
**Group Title:** GEN000000-SOL00270  
**Rule ID:** SV-27015r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00270  
**Rule Title:**The /usr/aset/userlist file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  File system ACLs can provide access to files beyond what is allowed by the mode numbers of the files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lLd /usr/aset/userlist  
If the permissions of the file or directory contains a "+", an extended ACL is present, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.   
# chmod A- /usr/aset/userlist     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4300  
**Group Title:** GEN000000-SOL00400  
**Rule ID:** SV-40041r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00400  
**Rule Title:**The NFS server must have logging implemented.  
  
  
**Vulnerability Discussion:**  Filesystem logging, especially for NFS exported file systems, can be critical to detecting data misuse and possible hardware/system errors that may, otherwise, go unnoticed.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
To enable NFS server logging the log option must be applied to all exported file systems in the /etc/dfs/dfstab. Perform the following to verify NFS is enabled.  
  
# share  
  
The preceding command will display all exported filesystems. Each line should contain a log entry to indicate logging is enabled. If the log entry is not present, this is a finding. If the share command does not return anything, then this is not an NFS server and this is considered not applicable.  
  
NFS version 4 does not support server logging. Verify NFS\_SERVER\_VERSMAX in /etc/default/nfs.  
  
# grep NFS\_SERVER\_VERSMAX /etc/default/nfs  
  
If NFS\_SERVER\_VERSMAX is commented out or set to any value but 2 or 3, this is a finding.  
  
**Fix Text:**Edit /etc/dfs/dfstab and add the log option to all exported filesystems. Run the shareall command for the changes to take effect.  
  
NFS version 2 or 3 must be forced by updating the NFS\_SERVER\_VERSMAX variable appropriately in /etc/default/nfs and restarting the NFS daemon.     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12032  
**Group Title:** GEN000000-SOL00420  
**Rule ID:** SV-12533r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00420  
**Rule Title:**Hidden extended file attributes must not exist on the system.  
  
  
**Vulnerability Discussion:**  Solaris extended attributes are essentially files themselves that are of an arbitrary size and content. They could be used to hide files from ordinary system file scans.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Search for all files with hidden extended attributes.  
  
# find / -xattr -print -exec runat {} ls -al \;  
  
If hidden extended file attributes exist, this is a finding.  
  
  
**Fix Text:**Remove the hidden extended file attributes.  
# runat <file name> rm <attribute name>  
    
  
**CCI:**CCI-000032  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12033  
**Group Title:** GEN000000-SOL00440  
**Rule ID:** SV-12534r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN000000-SOL00440  
**Rule Title:**The root account must be the only account with GID of 0.  
  
  
**Vulnerability Discussion:**  Accounts with a GID of 0 have root group privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check passwd and group files for non-root user ids and group ids with a GID of 0.  
  
# more /etc/passwd   
# more /etc/group  
  
OR  
  
# awk -F: '$4 == 0' /etc/passwd  
# awk -F: '$3 == 0' /etc/group  
  
Confirm the only account with a group id of 0 is root.  
  
If the root account is not the only account with GID of 0, this is a finding.  
  
  
**Fix Text:**Change the default GID of non-root accounts to a valid GID other than 0.  
    
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000764  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22603  
**Group Title:** GEN000000-SOL00540  
**Rule ID:** SV-27016r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00540  
**Rule Title:**The /etc/zones directory, and its contents, must be owned by root.  
  
  
**Vulnerability Discussion:**  Solaris zones configuration files must be protected against illicit creation, modification, and deletion.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the files and directories.  
  
# ls -lLdR /etc/zones  
  
If the owner of the file is not root, this is a finding.  
  
**Fix Text:**Change the ownership of the files and directories.  
# chown -R root /etc/zones     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22604  
**Group Title:** GEN000000-SOL00560  
**Rule ID:** SV-27018r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00560  
**Rule Title:**The /etc/zones directory, and its contents, must be group-owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  Solaris zones configuration files must be protected against illicit creation, modification, and deletion.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the files and directories.  
  
# ls -lLRa /etc/zones  
  
If the group owner of the directory and all files is not root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the group ownership of the files and directories.  
# chgrp -R sys /etc/zones  
# chgrp root /etc/zones/\*.xml  
# chgrp bin /etc/zones/SUN\*.xml     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22605  
**Group Title:** GEN000000-SOL00580  
**Rule ID:** SV-27019r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00580  
**Rule Title:**The /etc/zones directory, and its contents, must not be group- or world-writable.  
  
  
**Vulnerability Discussion:**  Solaris zones configuration files must be protected against illicit creation, modification, and deletion.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the files and directories.  
  
# ls -lLdR /etc/zones  
  
If the mode of a directory is more permissive than 0755, or the mode of a file more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the file or directory.  
  
# chmod 0644 <file>  
For directories:  
# chmod 0755 <directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22606  
**Group Title:** GEN000000-SOL00600  
**Rule ID:** SV-27020r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00600  
**Rule Title:**The /etc/zones directory, and its contents, must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Solaris zones configuration files must be protected against illicit creation, modification, and deletion.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lLd /etc/zones  
# ls -lLR /etc/zones  
If the permissions of the file or directory contains a "+", an extended ACL is present, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- <file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22607  
**Group Title:** GEN000000-SOL00620  
**Rule ID:** SV-27022r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00620  
**Rule Title:**The inherit-pkg-dir zone option must be set to none or the system default list defined for sparse root zones.  
  
  
**Vulnerability Discussion:**  Solaris zones have the capability to inherit elements of the global zone's filesystem, which reduces the amount storage required for a zone, but also limits the flexibility of the zone. The inherit-pkg-dir option defines which paths are shared between the zones. If set incorrectly, private information from the global zone could be made available to the non-global zone. This option must be set to none (for a whole-root non-global zone), the vendor-specified list of paths for sparse-root non-global zones, or a list specified by the SA for operational reasons which has been justified and documented with the IAO.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
If the system is not a global zone, this vulnerability is not applicable.  
List the non-global zones on the system.  
# zoneadm list -vi  
List the configuration for each zone.  
# zonecfg -z <zone> info  
Check the inherit-pkg-dir lines. If no such lines exist, this is not a finding. If the lines contain only those defined for sparse root zones (/lib, /platform, /sbin, /usr), this is not a finding. Otherwise, this is a finding.  
  
**Fix Text:**Remove the inherit-pkg-dir lines or the directories not defined for sparse root zones.  
# zonecfg -z <zone> remove inherit-pkg-dir=<somedir>     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22608  
**Group Title:** GEN000000-SOL00640  
**Rule ID:** SV-27023r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00640  
**Rule Title:**The limitpriv zone option must be set to the vendor default or less permissive.  
  
  
**Vulnerability Discussion:**  Solaris zones can be assigned privileges generally reserved for the global zone using the limitpriv zone option. Any privilege assignments in excess of the vendor defaults may provide the ability for a non-global zone to compromise the global zone.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
If the system is not a global zone, this vulnerability is not applicable.  
List the non-global zones on the system.  
# zoneadm list -vi  
List the configuration for each zone.  
# zonecfg -z <zone> info  
Check the limitpriv lines. If a line set other than default, this is a finding. If limitpriv is not set, this is not a finding.  
  
**Fix Text:**Change the limitpriv setting to default.  
# zonecfg -z <zone> set limitpriv=default     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22609  
**Group Title:** GEN000000-SOL00660  
**Rule ID:** SV-27024r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-SOL00660  
**Rule Title:**The physical devices must not be assigned to non-global zones.  
  
  
**Vulnerability Discussion:**  Solaris non-global zones can be assigned physical hardware devices. This increases the risk of such a non-global zone having the capability to compromise the global zone.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
If the system is not a global zone, this vulnerability is not applicable.  
List the non-global zones on the system.  
# zoneadm list -vi  
List the configuration for each zone.  
# zonecfg -z <zone> info  
Check for device lines. If such a line exists, this is a finding.  
  
**Fix Text:**Remove all device assignments from the non-global zone.  
# zonecfg -z <zone> delete device <device>     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-756  
**Group Title:** GEN000020  
**Rule ID:** SV-36752r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000020  
**Rule Title:**The system must require authentication upon booting into single-user and maintenance modes.  
  
  
**Vulnerability Discussion:**  If the system does not require valid root authentication before it boots into single-user or maintenance mode, anyone who invokes single-user or maintenance mode is granted privileged access to all files on the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
This can be checked in the /etc/default/sulogin file (on Solaris 5.X systems) to check if the system runs sulogin, or an equivalent, when booting into single-user mode.  
  
**Fix Text:**Edit /etc/default/sulogin and set PASSREQ=YES or remove /etc/default/sulogin entirely.   
  
NOTE: This is a default on Solaris 5.5.1 and later.     
  
**CCI:**CCI-000213  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11940  
**Group Title:** GEN000100  
**Rule ID:** SV-27051r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN000100  
**Rule Title:**The operating system must be a supported release.  
  
  
**Vulnerability Discussion:**  An operating system release is considered supported if the vendor continues to provide security patches for the product. With an unsupported release, it will not be possible to resolve security issues discovered in the system software.  
  
**Severity Override Guidance:**   
If an extended support agreement provides security patches for the unsupported product is procured from the vendor, this finding may be downgraded to a CAT III.  
  
**Responsibility:**  System Administrator  
**IAControls:**  VIVM-1  
  
**Check Content:**    
# uname -a  
  
Oracle has committed to indefinite "sustaining support" for recent Solaris operating system releases. Verify proof of purchase of support from Oracle.  
  
If the release is not supported, this is a finding.  
  
**Fix Text:**Upgrade to a supported version of the operating system.     
  
**CCI:**CCI-001230  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-783  
**Group Title:** GEN000120  
**Rule ID:** SV-40813r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000120  
**Rule Title:**Vendor-recommended software patches and updates, and system security patches and updates, must be installed and up-to-date.  
  
  
**Vulnerability Discussion:**  Timely patching is critical for maintaining the operational availability, confidentiality, and integrity of Information Technology (IT) systems. However, failure to keep operating system and application software patched is a common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches. When new weaknesses in an operating system exist, patches are usually made available by the vendor to resolve the problems. If the most recent recommended updates and security patches are not installed, unauthorized users may take advantage of weaknesses present in the unpatched software. The lack of prompt attention to patching could result in a system compromise.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  VIVM-1  
  
**Check Content:**    
Use the smpatch(1m) utility to check for available updates from Oracle.  
# smpatch analyze  
If there are updates available, this is a finding.  
  
**Fix Text:**Apply available updates from Oracle.  
# smpatch update     
  
**CCI:**CCI-001227  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11941  
**Group Title:** GEN000140  
**Rule ID:** SV-12442r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000140  
**Rule Title:**A file integrity baseline must be created and maintained.  
  
  
**Vulnerability Discussion:**  A file integrity baseline is a collection of file metadata which is to evaluate the integrity of the system. A minimal baseline must contain metadata for all device files, setuid files, setgid files, system libraries, system binaries, and system configuration files. The minimal metadata must consist of the mode, owner, group owner, and modification times. For regular files, metadata must also include file size and a cryptographic hash of the file’s contents.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSW-1  
  
**Check Content:**    
Determine if a file integrity baseline, which includes cryptographic hashes, has been created and maintained for the system. If no file integrity baseline exists for the system, this is a finding. If the file integrity baseline contains no cryptographic hashes, this is a finding. If the file integrity baseline is not maintained (has not been updated to be consistent with the latest approved system configuration changes), this is a finding.  
  
**Fix Text:**Create a file integrity baseline, including cryptographic hashes, for the system.     
  
**CCI:**CCI-000293  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11945  
**Group Title:** GEN000220  
**Rule ID:** SV-28610r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000220  
**Rule Title:**A file integrity tool must be used at least weekly to check for unauthorized file changes, particularly the addition of unauthorized system libraries or binaries, or for unauthorized modification to authorized system libraries or binaries.  
  
  
**Vulnerability Discussion:**  Changes in system libraries and binaries can indicate compromise or significant system events, such as patching needing to be checked by automated processes and the results reviewed by the SA.  
  
NOTE: For MAC I systems, increase the frequency to daily.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Determine if there is a cron job, scheduled to run weekly or more frequently, to run the file integrity tool to check for unauthorized system libraries or binaries, or unauthorized modification to authorized system libraries or binaries.   
  
Procedure:  
# crontab -l  
  
If there is no cron job meeting these requirements, this is a finding.  
  
NOTE: For MAC I systems, increase the frequency to daily.  
  
**Fix Text:**Create a cron job, scheduled to run weekly or more frequently, to run the file integrity tool to check for unauthorized system libraries or binaries, or unauthorized modification to authorized system libraries or binaries.  
  
NOTE: For MAC I systems, increase the frequency to daily.     
  
**CCI:**CCI-001069  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4301  
**Group Title:** GEN000240  
**Rule ID:** SV-40040r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000240  
**Rule Title:**The system clock must be synchronized to an authoritative DoD time source.  
  
  
**Vulnerability Discussion:**  To assure the accuracy of the system clock, it must be synchronized with an authoritative time source within DoD. Many system functions, including time-based login and activity restrictions, automated reports, system logs, and audit records depend on an accurate system clock. If there is no confidence in the correctness of the system clock, time-based functions may not operate as intended and records may be of diminished value.  
  
Authoritative time sources include authorized time servers within the enclave that synchronize with upstream authoritative sources. Specific requirements for the upstream synchronization of Network Time Protocol (NTP) servers are covered in the Network Other Devices STIG.  
  
For systems located on isolated or closed networks, it is not necessary to synchronize with a global authoritative time source. If a global authoritative time source is not available to systems on an isolated network, a local authoritative time source must be established on this network and used by the systems connected to this network. This is necessary to provide the ability to correlate events and allow for the correct operation of time-dependent protocols between systems on the isolated network.  
  
If the system is completely isolated (no connections to networks or other systems), time synchronization is not required as no correlation of events between systems will be necessary. If the system is completely isolated, this requirement is not applicable.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for a running NTP daemon or the root crontab for an ntpdate entry.  
# svcs ntp | grep online  
or  
# crontab -l | grep -v "^#" | grep ntpdate  
  
If NTP is not running, this is a finding.  
  
If NTP is running confirm the servers and peers or multicast client (as applicable) are local or an authoritative U.S. DoD source.  
  
For the NTP daemon  
# more /etc/inet/ntp.conf  
  
For the ntpdate command:  
# crontab -l | grep -v "^#" | grep ntpdate  
  
If a non-local/non-authoritative (U.S. DoD source) time-server is used, this is a finding.  
  
**Fix Text:**Use a local authoritative time server synchronizing to an authorized DoD time source. Ensure all systems in the facility feed from one or more local time servers that feed from the authoritative time server.     
  
**CCI:**CCI-001492  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22290  
**Group Title:** GEN000241  
**Rule ID:** SV-26291r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000241  
**Rule Title:**The system clock must be synchronized continuously, or at least daily.   
  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. Internal system clocks tend to drift and require periodic resynchronization to ensure their accuracy. Software, such as NTPD, can be used to continuously synchronize the system clock with authoritative sources. Alternatively, the system may be synchronized periodically, with a maximum of one day between synchronizations.  
  
If the system is completely isolated (no connections to networks or other systems), time synchronization is not required as no correlation of events or operation of time-dependent protocols between systems will be necessary. If the system is completely isolated, this requirement is not applicable.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for a running NTP daemon.  
# svcs ntp | grep online  
If ntp is running as a daemon, this is not a finding.  
  
If ntp is not running as a daemon, check the root crontab for ntpdate jobs running at least daily.  
# crontab -l | grep ntpdate  
Columns 3, 4, and 5 must be an asterisk (\*) for the job to be run daily.  
If this job exists, this is not a finding. Otherwise, this is a finding.  
  
**Fix Text:**Enable the NTP daemon for continuous synchronization.  
svcadm enable ntp  
  
OR  
  
Add a daily or more frequent cronjob to perform synchronization using ntpdate.  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22291  
**Group Title:** GEN000242  
**Rule ID:** SV-26303r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000242  
**Rule Title:**The system must use at least two time sources for clock synchronization.  
  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. For redundancy, two time sources are required so synchronization continues to function if one source fails.   
  
If the system is completely isolated (no connections to networks or other systems), time synchronization is not required as no correlation of events or operation of time-dependent protocols between systems will be necessary. If the system is completely isolated, this requirement is not applicable.  
  
NOTE: For the Network Time Protocol (NTP), the requirement is two servers, but it is recommended to configure at least four distinct time servers which allow NTP to effectively exclude a time source not consistent with the others. The system's local clock must be excluded from the count of time sources.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the root crontab for ntpdate entries.  
# crontab -l | grep ntpdate  
If the ntpdate command is not invoked with at least two external NTP servers listed, this is a finding.  
  
Check the NTP daemon configuration for at least two external servers.  
# grep '^server' /etc/inet/ntp.conf | egrep -v '(127.127.1.1|127.127.1.0)'  
If less than two servers or external reference clocks (127.127.x.x other than 127.127.1.0 or 127.127.1.1) are listed, this is a finding.  
  
  
**Fix Text:**If using ntpdate, add additional NTP servers to the cron job running ntpdate.  
  
If using the NTP daemon, add an additional server line to /etc/inet/ntp.conf for each additional NTP server.     
  
**CCI:**CCI-000160  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22292  
**Group Title:** GEN000244  
**Rule ID:** SV-26305r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000244  
**Rule Title:**The system must use time sources local to the enclave.  
  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. The network architecture should provide multiple time servers within an enclave that provide local service to the enclave and synchronize with time sources outside of the enclave.  
  
If this server is an enclave time server, this requirement is not applicable.  
  
If the system is completely isolated (no connections to networks or other systems), time synchronization is not required as no correlation of events or operation of time-dependent protocols between systems will be necessary. If the system is completely isolated, this requirement is not applicable.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the root crontab for ntpdate entries.   
# crontab -l | grep ntpdate   
If the ntpdate command is invoked with NTP servers outside of the enclave, this is a finding.  
  
Check the NTP daemon configuration.   
# grep '^server' /etc/inet/ntp.conf  
If an NTP server is listed outside of the enclave, this is a finding.  
  
**Fix Text:**If using ntpdate, remove NTP servers that are external to the enclave from the cron job running ntpdate.   
  
If using the NTP daemon, remove the server line from /etc/inet/ntp.conf for each NTP server that is external to the enclave.     
  
**CCI:**CCI-000160  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22294  
**Group Title:** GEN000250  
**Rule ID:** SV-26293r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000250  
**Rule Title:**The time synchronization configuration file (such as /etc/ntp.conf) must be owned by root.  
  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. If an illicit time source is used for synchronization, the integrity of system logs and the security of the system could be compromised. If the configuration files controlling time synchronization are not owned by a system account, unauthorized modifications could result in the failure of time synchronization.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Run ls -l /etc/inet/ntp.conf to display the owner of the NTP configuration file. If the owner is not root, this is a finding.  
  
**Fix Text:**Change the owner of the NTP configuration file to root.  
# chown root /etc/inet/ntp.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22295  
**Group Title:** GEN000251  
**Rule ID:** SV-26296r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000251  
**Rule Title:**The time synchronization configuration file (such as /etc/ntp.conf) must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. If an illicit time source is used for synchronization, the integrity of system logs and the security of the system could be compromised. If the configuration files controlling time synchronization are not owned by a system group, unauthorized modifications could result in the failure of time synchronization.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the NTP configuration file.  
  
Procedure:  
# ls -l /etc/inet/ntp.conf  
  
If the group owner is not root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the NTP configuration file.  
  
Procedure:  
# chgrp root /etc/inet/ntp.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22296  
**Group Title:** GEN000252  
**Rule ID:** SV-26298r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000252  
**Rule Title:**The time synchronization configuration file (such as /etc/ntp.conf) must have mode 0640 or less permissive.  
  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. If an illicit time source is used for synchronization, the integrity of system logs and the security of the system could be compromised. If the configuration files controlling time synchronization are not protected, unauthorized modifications could result in the failure of time synchronization.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the mode for the NTP configuration file is not more permissive than 0640.  
# ls -l /etc/inet/ntp.conf  
  
If the mode is more permissive than 0640, this is a finding.  
  
**Fix Text:**Change the mode of the NTP configuration file to 0640 or less permissive.  
# chmod 0640 /etc/inet/ntp.conf  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22297  
**Group Title:** GEN000253  
**Rule ID:** SV-26301r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000253  
**Rule Title:**The time synchronization configuration file (such as /etc/ntp.conf) must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. If an illicit time source is used for synchronization, the integrity of system logs and the security of the system could be compromised. If the configuration files controlling time synchronization are not protected, unauthorized modifications could result in the failure of time synchronization.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check for an extended ACL on the NTP configuration file.  
# ls -l /etc/inet/ntp.conf  
If the permissions contain a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/inet/ntp.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-760  
**Group Title:** GEN000280  
**Rule ID:** SV-41504r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000280  
**Rule Title:**Direct logins must not be permitted to shared, default, application, or utility accounts.  
  
  
**Vulnerability Discussion:**  Shared accounts (accounts where two or more people log in with the same user identification) do not provide identification and authentication. There is no way to provide for non-repudiation or individual accountability.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1, IAIA-1  
  
**Check Content:**    
Use the last command to check for multiple accesses to an account from different workstations/IP addresses. If users log directly onto accounts, rather than using the su command from their own named account to access them, this is a finding (such as logging directly on to Oracle). Also, ask the SA or the IAO if shared accounts are logged into directly or if users log on to an individual account and switch user to the shared account.  
  
  
  
**Fix Text:**Use the switch user (su) command from a named account login to access shared accounts. Maintain audit trails that identify the actual user of the account name. Document requirements and procedures for users/administrators to log into their own accounts first and then switch user (su) to the shared account.     
  
**CCI:**CCI-000770  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4269  
**Group Title:** GEN000290  
**Rule ID:** SV-4269r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000290  
**Rule Title:**The system must not have unnecessary accounts.  
  
  
**Vulnerability Discussion:**  Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAAC-1  
  
**Check Content:**    
Check the system for unnecessary user accounts.  
  
Procedure:  
# more /etc/passwd  
  
Some examples of unnecessary accounts include games, news, gopher, ftp, and lp. If any unnecessary accounts are found, this is a finding.  
  
**Fix Text:** Remove all unnecessary accounts, such as games, from the /etc/passwd file before connecting a system to the network. Other accounts, such as news and gopher, associated with a service not in use should also be removed.     
  
**CCI:**CCI-000012  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-761  
**Group Title:** GEN000300  
**Rule ID:** SV-27061r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000300  
**Rule Title:**All accounts on the system must have unique user or account names.  
  
  
**Vulnerability Discussion:**  A unique user name is the first part of the identification and authentication process. If user names are not unique, there can be no accountability on the system for auditing purposes. Multiple accounts sharing the same name could result in the Denial of Service to one or both of the accounts or unauthorized access to files or privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the system for duplicate account names.  
  
Example:  
# logins -u | sort | uniq -c | awk '$1 > 1 {print $2}'  
  
If any duplicate account names are found, this is a finding.  
  
**Fix Text:**Change user account names, or delete accounts, so each account has a unique name.     
  
**CCI:**CCI-000764  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-762  
**Group Title:** GEN000320  
**Rule ID:** SV-27065r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000320  
**Rule Title:**All accounts must be assigned unique User Identification Numbers (UIDs).  
  
  
**Vulnerability Discussion:**  Accounts sharing a UID have full access to each others' files. This has the same effect as sharing a login. There is no way to assure identification, authentication, and accountability because the system sees them as the same user. If the duplicate UID is 0, this gives potential intruders another privileged account to attack.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Perform the following to ensure there are no duplicate UIDs.  
# logins -d  
If any duplicate UIDs are found, this is a finding.  
  
**Fix Text:**Edit user accounts to provide unique UIDs for each account.     
  
**CCI:**CCI-000764  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11946  
**Group Title:** GEN000340  
**Rule ID:** SV-12447r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000340  
**Rule Title:**UIDs reserved for system accounts must not be assigned to non-system accounts.  
  
  
**Vulnerability Discussion:**  Reserved UIDs are typically used by system software packages. If non-system accounts have UIDs in this range, they may conflict with system software, possibly leading to the user having permissions to modify system files.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the UID assignments of all accounts.  
# more /etc/passwd  
  
Confirm all accounts with a UID of 99 and below are used by a system account. If a UID reserved for system accounts (0 - 99) is used by a non-system account, this is a finding.   
  
**Fix Text:**Change the UID numbers for non-system accounts with reserved UIDs (those less or equal to 99).     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-780  
**Group Title:** GEN000360  
**Rule ID:** SV-28658r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000360  
**Rule Title:**GIDs reserved for system accounts must not be assigned to non-system groups.  
  
  
**Vulnerability Discussion:**  Reserved GIDs are typically used by system software packages. If non-system groups have GIDs in this range, they may conflict with system software, possibly leading to the group having permissions to modify system files.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# more /etc/passwd   
Confirm all accounts with a GID of 99 and below are used by a system account. If a GID reserved for system accounts (0 - 99) is used by a non-system account, this is a finding.   
  
**Fix Text:**Change the primary group GID numbers for non-system accounts with reserved primary group GIDs (those less or equal to 99).  
  
# usermod -g <new\_group> <user>     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-781  
**Group Title:** GEN000380  
**Rule ID:** SV-27069r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000380  
**Rule Title:**All GIDs referenced in the /etc/passwd file must be defined in the /etc/group file.  
  
  
**Vulnerability Discussion:**  If a user is assigned the GID of a group not existing on the system, and a group with the same GID is subsequently created, the user may have unintended rights to the group.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Perform the following to ensure there are no GIDs referenced in /etc/passwd not defined in /etc/group.  
# logins -o | awk -F: '$3 == ""'  
If any lines are returned, there are GIDs referenced in /etc/passwd that are not defined in /etc/group, this is a finding.  
  
**Fix Text:**Add a group to the system for each GID referenced that does not have a corresponding group.   
  
#/usr/sbin/groupadd < group >     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-763  
**Group Title:** GEN000400  
**Rule ID:** SV-28596r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000400  
**Rule Title:**The Department of Defense (DoD) login banner must be displayed immediately prior to, or as part of, console login prompts.  
  
  
**Vulnerability Discussion:**  Failure to display the login banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECWM-1  
  
**Check Content:**    
Access the system console and make a logon attempt. Check for either of the following login banners based on the character limitations imposed by the system. An exact match is required. If one of these banners is not displayed, this is a finding.  
  
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. "  
  
OR  
  
"I've read & consent to terms in IS user agreem't."  
  
**Fix Text:**Edit /etc/issue and add one of the DoD login banners (based on the character limitations imposed by the system).  
  
DoD Login Banners:  
  
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."  
  
OR  
  
"I've read & consent to terms in IS user agreem't."     
  
**CCI:**CCI-000048  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24331  
**Group Title:** GEN000402  
**Rule ID:** SV-39880r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000402  
**Rule Title:**The Department of Defense (DoD) login banner must be displayed immediately prior to, or as part of, graphical desktop environment login prompts.  
  
  
**Vulnerability Discussion:**  Failure to display the login banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.  
  
This requirement applies to graphical desktop environments provided by the system to locally attached displays and input devices as well as to graphical desktop environments provided to remote systems, including thin clients.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECWM-1  
  
**Check Content:**    
If the system does not use XWindows, this is not applicable.  
  
Check the "Dtlogin\*greeting.labelString" parameter in /etc/dt/config/C/Xresources for either of the following login banners based on the character limitations imposed by the system. An exact match is required. If one of these banners is not displayed, this is a finding. If the file does not exist, this is a finding.  
  
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. "  
  
OR  
  
"I've read & consent to terms in IS user agreem't."  
  
**Fix Text:**Create/update /etc/dt/config/C/Xresources with Dtlogin\*greeting.labelString: [DoD login banner text].  
  
DoD Login Banners:  
  
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."  
  
OR  
  
"I've read & consent to terms in IS user agreem't."     
  
**CCI:**CCI-000048  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23732  
**Group Title:** GEN000410  
**Rule ID:** SV-39879r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000410  
**Rule Title:**The FTPS/FTP service on the system must be configured with the Department of Defense (DoD) login banner.  
  
  
**Vulnerability Discussion:**  Failure to display the logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.  
  
NOTE: SFTP and FTPS are encrypted alternatives to FTP that should be used in place of FTP. SFTP is implemented by the SSH service and uses its banner configuration.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECWM-1  
  
**Check Content:**    
FTP to the system.  
# ftp localhost  
Check for either of the following login banners based on the character limitations imposed by the system. An exact match is required. If one of these banners is not displayed, this is a finding. If the system does not run the FTP service, this is not applicable.  
  
DoD Login Banners:  
  
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."  
  
OR  
  
"I've read & consent to terms in IS user agreem't."  
  
**Fix Text:**Edit /etc/ftpd/ftpaccess and add or edit the BANNER parameter ("banner /etc/ftpd/banner.msg").  
# vi /etc/ftpd/ftpaccess  
  
Add one of the DoD Login Banners (based on the character limitations imposed by the system) to the /etc/ftpd/banner.msg file.  
# vi /etc/ftpd/banner.msg  
  
DoD Login Banners:  
  
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."  
  
OR  
  
"I've read & consent to terms in IS user agreem't."     
  
**CCI:**CCI-000048  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-765  
**Group Title:** GEN000440  
**Rule ID:** SV-27080r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000440  
**Rule Title:**Successful and unsuccessful logins and logouts must be logged.  
  
  
**Vulnerability Discussion:**  Monitoring and recording successful and unsuccessful logins assist in tracking unauthorized access to the system. Without this logging, the ability to track unauthorized activity to specific user accounts may be diminished.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Determine if successful logons are being logged.  
# last | more  
  
Determine if unsuccessful logons are being logged.  
# more /var/adm/loginlog  
  
If the commands do not return successful and unsuccessful logins, this is a finding.  
  
Check the syslog daemon configuration for authentication logging.  
# egrep "auth\.(info|debug)" /etc/syslog.conf  
If there are no entries in syslog for the auth service, this is a finding.  
  
**Fix Text:**Verify that login logs are handled correctly in the /etc/syslog.conf file. Edit the /etc/syslog.conf file and add one of the entries below.  
  
auth.debug /var/log/authlog  
OR   
auth.\* /var/log/authlog  
  
Verify that service startup scripts for syslog and utmp (if present) are enabled.   
    
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22299  
**Group Title:** GEN000452  
**Rule ID:** SV-26310r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000452  
**Rule Title:**The system must display the date and time of the last successful account login upon login.  
  
  
**Vulnerability Discussion:**  Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system displays the date and time of the last successful login upon logging in. This can be accomplished by logging into the system and verifying whether or not the necessary information is displayed. If the system does not provide this information upon login, this is a finding.  
  
Last login information is provided automatically by the login(1) program for telnet and console login sessions.  
  
Verify the SSH daemon is configured to display last login information.  
  
# grep -i PrintLastLog /etc/ssh/sshd\_config  
If PrintLastLog is present in the configuration and not disabled, this is not a finding. Otherwise, this is a finding.  
  
**Fix Text:**Configure the system to display the date and time of the last successful login upon logging in.  
  
Enable PrintLastLog in the SSH daemon.  
  
To enable PrintLastLog in the SSH daemon, remove any lines disabling this option from /etc/ssh/sshd\_config.     
  
**CCI:**CCI-000052  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-766  
**Group Title:** GEN000460  
**Rule ID:** SV-39815r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000460  
**Rule Title:**The system must disable accounts after three consecutive unsuccessful login attempts.  
  
  
**Vulnerability Discussion:**  Disabling accounts after a limited number of unsuccessful login attempts improves protection against password guessing attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLO-1, ECLO-2  
  
**Check Content:**    
Verify RETRIES is set in the login file.  
  
# grep RETRIES /etc/default/login   
If RETRIES is not set or is more than 3, this is a finding.  
  
Verify the account locks after invalid login attempts.  
# grep LOCK\_AFTER\_RETRIES /etc/security/policy.conf   
If LOCK\_AFTER\_RETRIES is not set to YES, this is a finding.  
  
**Fix Text:**Set RETRIES to 3 in the /etc/default/login file.  
#vi /etc/default/login  
  
Set LOCK\_AFTER\_RETRIES to YES in the /etc/security/policy.conf file.  
#vi /etc/security/policy.conf     
  
**CCI:**CCI-000044  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-768  
**Group Title:** GEN000480  
**Rule ID:** SV-27094r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000480  
**Rule Title:**The delay between login prompts following a failed login attempt must be at least 4 seconds.  
  
  
**Vulnerability Discussion:**  Enforcing a delay between successive failed login attempts increases protection against automated password guessing attacks.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLO-1, ECLO-2  
  
**Check Content:**    
Check the SLEEPTIME parameter in the /etc/default/login file.  
  
# grep SLEEPTIME /etc/default/login  
  
If SLEEPTIME is not listed, commented out, or less than 4, this is a finding.  
  
**Fix Text:**Edit the /etc/default/login file and set SLEEPTIME to 4.     
  
**CCI:**CCI-000043  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4083  
**Group Title:** GEN000500  
**Rule ID:** SV-39814r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000500  
**Rule Title:**Graphical desktop environments provided by the system must automatically lock after 15 minutes of inactivity and the system must require users to re-authenticate to unlock the environment.  
  
  
**Vulnerability Discussion:**  If graphical desktop sessions do not lock the session after 15 minutes of inactivity, requiring re-authentication to resume operations, the system or individual data could be compromised by an alert intruder who could exploit the oversight. This requirement applies to graphical desktop environments provided by the system to locally attached displays and input devices as well as to graphical desktop environments provided to remote systems, including thin clients.  
  
**Responsibility:**  System Administrator  
**IAControls:**  PESL-1  
  
**Check Content:**    
Examine the dtsession timeout variable setting:  
  
# cat /etc/dt/config/C/sys.resources | grep -i dtsession | grep -i lockTimeout  
If the dtsession timeout is greater than 15, commented or does not exist, this is a finding.  
  
Examine the Open Windows timeout settings, both global and for every user.  
  
# cat /usr/openwin/lib/app-defaults/XScreenSaver | egrep -i '\\*(lock|timeout):'  
If the global Open Windows timeout is greater than 15 minutes, commented or does not exist, this is a finding. If the global lock setting is not true, this is a finding.  
  
# cut -d: -f6 /etc/passwd | xargs -iX egrep -i '^(lock|timeout):' X/.xscreensaver  
If the Open Windows timeout is greater than 15 minutes for any user, this is a finding. If the lock setting is not true for any user, this is a finding.  
  
**Fix Text:**Configure the CDE lock manager to lock your screen after a certain amount of inactive time. To configure the CDE lock manager to lock the screen after 15 minutes of inactive time, enter the following commands (be sure NOT to overwrite an existing file).  
# cp /usr/dt/config/C/sys.resources /etc/dt/config/C/sys.resources  
# vi /etc/dt/config/C/sys.resources  
  
Locate and add/uncomment/change the line to N=15.  
dtsession\*lockTimeout: <N>  
dtsession\*lockTimeout: 15  
  
Log out of CDE and log back in to verify that the timeout is in effect.   
  
The timeout parameter in /usr/openwin/lib/app-defaults/XScreenSaver and all users' .xscreensaver files should also be confirmed to be uncommented and set to 0:15:00.     
  
**CCI:**CCI-000057  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22301  
**Group Title:** GEN000510  
**Rule ID:** SV-39865r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000510  
**Rule Title:**The system must display a publicly-viewable pattern during a graphical desktop environment session lock.  
  
  
**Vulnerability Discussion:**  To protect the on-screen content of a session, it must be replaced with a publicly-viewable pattern upon session lock. Examples of publicly viewable patterns include screen saver patterns, photographic images, solid colors, or a blank screen, so long as none of those patterns convey sensitive information.  
  
This requirement applies to graphical desktop environments provided by the system to locally attached displays and input devices, as well as, to graphical desktop environments provided to remote systems using remote access protocols.  
  
**Responsibility:**  System Administrator  
**IAControls:**  PESL-1  
  
**Check Content:**    
Determine if a publicly-viewable pattern is displayed during a session lock. If the session lock pattern is not publicly-viewable, this is a finding.  
  
Acceptable checks for settings.  
  
# grep -i dtsession /etc/dt/config/C/sys.resources | egrep -i "saverList|saverTimeout"  
  
The saverTimeout value should be 15 (see GEN000500).  
The saverList value of StartDtscreenBlank is an acceptable screensaver.  
  
**Fix Text:**Edit the /etc/dt/config/C/sys.resources file and add/edit the following lines, using 15 for the saverTimeout, and using StartDtscreenBlank for the saverList.  
  
dtsession\*saverTimeout: 15  
dtsession\*saverList: StartDtscreenBlank     
  
**CCI:**CCI-000061  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-769  
**Group Title:** GEN000520  
**Rule ID:** SV-769r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000520  
**Rule Title:**The root user must not own the logon session for an application requiring a continuous display.  
  
  
**Vulnerability Discussion:**  If an application is providing a continuous display and is running with root privileges, unauthorized users could interrupt the process and gain root access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  PESL-1  
  
**Check Content:**    
If there is an application running on the system continuously in use (such as a network monitoring application), ask the SA what the name of the application is. Execute the following to determine which user owns the process(es) associated with the application. If the owner is root, this is a finding.  
  
# ps -ef | more  
  
**Fix Text:**Configure the system so the owner of a session requiring a continuous screen display, such as a network management display, is not root. Ensure the display is also located in a secure, controlled access area. Document and justify this requirement. Ensure the terminal and keyboard for the display (or workstation) are secure from all but authorized personnel by maintaining them in a secure area, in a locked cabinet where a swipe card, or other positive forms of identification, must be used to gain entry.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1032  
**Group Title:** GEN000540  
**Rule ID:** SV-39809r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000540  
**Rule Title:**Users must not be able to change passwords more than once every 24 hours.  
  
  
**Vulnerability Discussion:**  The ability to change passwords frequently facilitates users reusing the same password. This can result in users effectively never changing their passwords. This would be accomplished by users changing their passwords when required and then immediately changing it to the original value.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the minimum time period between password changes for each user account is 1 day or greater.  
# awk -F: '$4 < 1 {print $1}' /etc/shadow  
If any results are returned that are not associated with a system account, this is a finding.  
  
**Fix Text:**Edit the /etc/default/passwd file and set the variable "MINWEEKS" to 1 or greater.   
Set the per-user minimum password change times by using the following command on each user account.  
# passwd -n <number of days> <accountname>     
  
**CCI:**CCI-000198  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-770  
**Group Title:** GEN000560  
**Rule ID:** SV-27105r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN000560  
**Rule Title:**The system must not have accounts configured with blank or null passwords.  
  
  
**Vulnerability Discussion:**  If an account is configured for password authentication but does not have an assigned password, it may be possible to log into the account without authentication. If the root user is configured without a password, the entire system may be compromised. For user accounts not using password authentication, the account must be configured with a password lock value instead of a blank or null value.   
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Verify no accounts have blank passwords.  
  
# logins -p  
  
If any account with a blank password is found, this is a finding.  
  
**Fix Text:**Remove, lock, or configure a password for any account with a blank password.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11947  
**Group Title:** GEN000580  
**Rule ID:** SV-27110r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000580  
**Rule Title:**The system must require passwords contain a minimum of 14 characters.  
  
  
**Vulnerability Discussion:**  The use of longer passwords reduces the ability of attackers to successfully obtain valid passwords using guessing or exhaustive search techniques by increasing the password search space.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the system password length setting.  
# grep PASSLENGTH /etc/default/passwd  
If PASSLENGTH is not set to 14 or more, this is a finding.  
  
**Fix Text:**Edit /etc/default/passwd and set the PASSLENGTH variable to 14 or greater.     
  
**CCI:**CCI-000205  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22302  
**Group Title:** GEN000585  
**Rule ID:** SV-26318r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000585  
**Rule Title:**The system must enforce compliance of the entire password during authentication.  
  
  
**Vulnerability Discussion:**  Some common password hashing schemes only process the first eight characters of a user's password, which reduces the effective strength of the password.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Verify no password hash in /etc/passwd or /etc/shadow begins with a character other than an underscore (\_) or dollar sign ($).  
  
# cut -d ':' -f2 /etc/passwd | egrep -v '^[\*!$\_]'  
# cut -d ':' -f2 /etc/shadow | egrep -v '^[\*!$\_]'  
  
If any unlocked password hash is present without an initial underscore (\_) or dollar sign ($) character, this is a finding.  
  
**Fix Text:**Edit /etc/security/policy.conf and add or change the CRYPT\_DEFAULT setting to something other than \_\_unix\_\_, such as 6. Allowable values for CRYPT\_DEFAULT may be found in the /etc/security/crypt.conf file.  
  
Change any passwords using non-compliant hashes.     
  
**CCI:**CCI-000205  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22303  
**Group Title:** GEN000590  
**Rule ID:** SV-40776r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000590  
**Rule Title:**The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes.  
  
  
**Vulnerability Discussion:**  Systems must employ cryptographic hashes for passwords using the SHA-2 family of algorithms or FIPS 140-2 approved successors. The use of unapproved algorithms may result in weak password hashes more vulnerable to compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1, IAIA-1, IAIA-2  
  
**Check Content:**    
Verify the traditional UNIX crypt algorithm is deprecated.  
# egrep CRYPT\_ALGORITHMS\_DEPRECATE /etc/security/policy.conf  
If CRYPT\_ALGORITHMS\_DEPRECATE is not set or does not include "\_\_unix\_\_", this is a finding.  
  
Verify new password hashes are generated using either the SHA-256 or SHA-512 cryptographic hashing algorithm.  
# egrep CRYPT\_DEFAULT /etc/security/policy.conf  
If CRYPT\_DEFAULT is not set or is not equal to 5 or 6, this is a finding.  
  
**Fix Text:**Edit the /etc/security/policy.conf file.  
# vi /etc/security/policy.conf  
Uncomment the CRYPT\_ALGORITHMS\_DEPRECATE line and set it to "\_\_unix\_\_". Update the CRYPT\_DEFAULT default line to be equal to 5 or 6. The following lines are acceptable.  
  
CRYPT\_ALGORITHMS\_DEPRECATE=\_\_unix\_\_  
CRYPT\_DEFAULT=6     
  
**CCI:**CCI-000803  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22304  
**Group Title:** GEN000595  
**Rule ID:** SV-40790r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000595  
**Rule Title:**The password hashes stored on the system must have been generated using a FIPS 140-2 approved cryptographic hashing algorithm.  
  
  
**Vulnerability Discussion:**  Systems must employ cryptographic hashes for passwords using the SHA-2 family of algorithms or FIPS 140-2 approved successors. The use of unapproved algorithms may result in weak password hashes more vulnerable to compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1, IAIA-1, IAIA-2  
  
**Check Content:**    
Determine if any password hashes stored on the system were not generated using a FIPS 140-2 approved cryptographic hashing algorithm.  
  
Procedure:  
# cut -d ':' -f2 /etc/passwd  
# cut -d ':' -f2 /etc/shadow  
  
If any password hashes are present not beginning with $5$ or $6$, this is a finding.  
  
Verify that FIPS 140-2 approved cryptographic hashing algorithms are available.  
# egrep '^[56]' /etc/security/crypt.conf  
If no lines are returned, this is a finding.  
  
**Fix Text:**If the /etc/security/crypt.conf file does not support FIPS 140-2 approved cryptographic hashing algorithms, upgrade to at least the Solaris 10 8/07 release.  
  
Edit the /etc/security/policy.conf file.  
# vi /etc/security/policy.conf  
Uncomment the CRYPT\_ALGORITHMS\_DEPRECATE line and set it to "\_\_unix\_\_". Update the CRYPT\_DEFAULT default line to be equal to 5 or 6. The following lines are acceptable.  
  
CRYPT\_ALGORITHMS\_DEPRECATE=\_\_unix\_\_  
CRYPT\_DEFAULT=6  
  
Update passwords for all accounts with non-compliant password hashes.     
  
**CCI:**CCI-000196  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11948  
**Group Title:** GEN000600  
**Rule ID:** SV-27115r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000600  
**Rule Title:**The system must require passwords to contain at least one uppercase alphabetic character.  
  
  
**Vulnerability Discussion:**  To enforce the use of complex passwords, minimum numbers of characters of different classes are mandated. The use of complex passwords reduces the ability of attackers to successfully obtain valid passwords using guessing or exhaustive search techniques. Complexity requirements increase the password search space by requiring users to construct passwords from a larger character set than they may otherwise use.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the MINUPPER setting.  
# egrep MINUPPER /etc/default/passwd  
If MINUPPER is not set to 1 or more, this is a finding.  
  
**Fix Text:**Edit /etc/default/passwd and set the MINUPPER setting to at least 1.     
  
**CCI:**CCI-000192  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11972  
**Group Title:** GEN000620  
**Rule ID:** SV-27119r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000620  
**Rule Title:**The system must require passwords to contain at least one numeric character.  
  
  
**Vulnerability Discussion:**  To enforce the use of complex passwords, minimum numbers of characters of different classes are mandated. The use of complex passwords reduces the ability of attackers to successfully obtain valid passwords using guessing or exhaustive search techniques. Complexity requirements increase the password search space by requiring users to construct passwords from a larger character set than they may otherwise use.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the MINDIGIT setting.  
# grep MINDIGIT /etc/default/passwd  
If the MINDIGIT setting is less than 1, this is a finding.  
  
**Fix Text:**Edit /etc/default/passwd and set the MINDIGIT setting to 1.     
  
**CCI:**CCI-000194  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11973  
**Group Title:** GEN000640  
**Rule ID:** SV-27123r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000640  
**Rule Title:**The system must require passwords to contain at least one special character.  
  
  
**Vulnerability Discussion:**  To enforce the use of complex passwords, minimum numbers of characters of different classes are mandated. The use of complex passwords reduces the ability of attackers to successfully obtain valid passwords using guessing or exhaustive search techniques. Complexity requirements increase the password search space by requiring users to construct passwords from a larger character set than they may otherwise use.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the MINSPECIAL setting.  
# grep MINSPECIAL /etc/default/passwd  
If the MINSPECIAL setting is less than 1, this is a finding.  
  
**Fix Text:**Edit /etc/default/passwd and set MINSPECIAL to 1.     
  
**CCI:**CCI-001619  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11975  
**Group Title:** GEN000680  
**Rule ID:** SV-27126r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000680  
**Rule Title:**The system must require passwords to contain no more than three consecutive repeating characters.  
  
  
**Vulnerability Discussion:**  To enforce the use of complex passwords, the number of consecutive repeating characters is limited. Passwords with excessive repeated characters may be more vulnerable to password-guessing attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the MAXREPEATS setting.  
# grep MAXREPEATS /etc/default/passwd  
If the MAXREPEATS setting is greater than 3, this is a finding.  
  
**Fix Text:**Edit /etc/default/passwd and set MAXREPEATS to 3.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11976  
**Group Title:** GEN000700  
**Rule ID:** SV-39845r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000700  
**Rule Title:**User passwords must be changed at least every 60 days.  
  
  
**Vulnerability Discussion:**  Limiting the lifespan of authenticators limits the period of time an unauthorized user has access to the system while using compromised credentials and reduces the period of time available for password-guessing attacks to run against a single password.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the max days field (the 5th field) of /etc/shadow.  
# awk -F: '{print $1 ":" $5;}' /etc/shadow  
If the max days field is equal to 0 or greater than 60 for any human user or shared account that is not password-locked, this is a finding.  
  
**Fix Text:**Set the max days field to 60 for all user accounts.  
# passwd -x 60 <user>   
Set the MAXWEEKS parameter in /etc/default/passwd to a positive, non-zero value of 60 or less.     
  
**CCI:**CCI-000180  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11977  
**Group Title:** GEN000740  
**Rule ID:** SV-12478r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000740  
**Rule Title:**All non-interactive/automated processing account passwords must be changed at least once per year or be locked.  
  
  
**Vulnerability Discussion:**  Limiting the lifespan of authenticators limits the period of time an unauthorized user has access to the system while using compromised credentials and reduces the period of time available for password-guessing attacks to run against a single password. Locking the password for non-interactive and automated processing accounts is preferred as it removes the possibility of accessing the account by a password. On some systems, locking the passwords of these accounts may prevent the account from functioning properly. Passwords for non-interactive/automated processing accounts must not be used for direct logon to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Ask the SA if there are any automated processing accounts on the system. If there are automated processing accounts on the system, ask the SA if the passwords for those automated accounts are changed at least once a year. If SA indicates passwords for automated processing accounts are not changed once per year, this is a finding.  
  
  
**Fix Text:**Implement or establish procedures to change the passwords of automated processing accounts at least once per year.     
  
**CCI:**CCI-000199  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22306  
**Group Title:** GEN000750  
**Rule ID:** SV-26324r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000750  
**Rule Title:**The system must require at least four characters be changed between the old and new passwords during a password change.  
  
  
**Vulnerability Discussion:**  To ensure password changes are effective in their goals, the system must ensure old and new passwords have significant differences. Without significant changes, new passwords may be easily guessed based on the value of a previously compromised password.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check /etc/default/passwd to verify the MINDIFF setting.   
  
# grep MINDIFF /etc/default/passwd  
  
If the setting is not present, or is less than 4, this is a finding.  
  
**Fix Text:**Edit /etc/default/passwd and set or add a MINDIFF setting equal to or greater than 4.     
  
**CCI:**CCI-000195  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-918  
**Group Title:** GEN000760  
**Rule ID:** SV-39824r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000760  
**Rule Title:**Accounts must be locked upon 35 days of inactivity.  
  
  
**Vulnerability Discussion:**  On some systems, accounts with disabled passwords still allow access using rcp, remsh, or rlogin through equivalent remote hosts. All that is required is the remote host name and the user name match an entry in a hosts.equiv file and have a .rhosts file in the user directory. Using a shell called /bin/false or /dev/null (or an equivalent) will add a layered defense.  
  
Non-interactive accounts on the system, such as application accounts, may be documented exceptions.  
  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  IAAC-1  
  
**Check Content:**    
Indications of inactive accounts are those without entries in the last log. Check the date in the last log to verify it is within the last 35 days.  
  
Obtain a listing of user accounts.  
#cat /etc/passwd | cut -f1 -d ":"  
  
Run the last command for each user account.  
# last < user account >  
  
If any user's account has not been accessed in the last 35 days and the account is not disabled via an entry in the password field in the /etc/passwd or /etc/shadow (or equivalent), check the /etc/passwd file to check if the account has a valid shell. If an inactive account is found that is not disabled, this is a finding.  
  
**Fix Text:**All inactive accounts will have /bin/false, /usr/bin/false, or /dev/null as the default shell in the /etc/passwd file and have the password disabled. Disable the inactive accounts. Examine the inactive accounts using the last command. Note the date of last login for each account. If any (other than system and application accounts) exceed 35 days, then disable them by placing a shell of /bin/false or /dev/null in the shell field of the passwd file entry for that account. An alternative, and preferable method, is to disable the account using smc or the passwd command.  
  
# passwd -l < account to lock >     
  
**CCI:**CCI-000017  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22307  
**Group Title:** GEN000790  
**Rule ID:** SV-26345r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000790  
**Rule Title:**The system must prevent the use of dictionary words for passwords.  
  
  
**Vulnerability Discussion:**  An easily guessable password provides an open door to any external or internal malicious intruder. Many computer compromises occur as the result of account name and password guessing. This is generally done by someone with an automated script using repeated logon attempts until the correct account and password pair is guessed. Utilities, such as cracklib, can be used to validate passwords are not dictionary words and meet other criteria during password changes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check /etc/default/passwd for dictionary check configuration.  
  
# grep DICTION /etc/default/passwd  
  
If the DICTIONLIST or DICTIONDBDIR settings are not present, or are set to non-existent files or directories, this is a finding.  
  
**Fix Text:**Edit /etc/default/passwd; add or set DICTIONLIST to the dictionary file and DICTIONDBDIR to a database directory such as /var/passwd. Generate the password dictionary by running the mkpwdict command.     
  
**CCI:**CCI-000189  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4084  
**Group Title:** GEN000800  
**Rule ID:** SV-27132r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000800  
**Rule Title:**The system must prohibit the reuse of passwords within five iterations.  
  
  
**Vulnerability Discussion:**  If a user, or root, used the same password continuously or was allowed to change it back shortly after being forced to change it to something else, it would provide a potential intruder with the opportunity to keep guessing at one user's password until it was guessed correctly.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the HISTORY setting.  
# grep HISTORY /etc/default/passwd  
If HISTORY is not set to 5 or more, this is a finding.  
  
**Fix Text:**Edit /etc/default/passwd and set HISTORY to 5.     
  
**CCI:**CCI-000200  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22308  
**Group Title:** GEN000850  
**Rule ID:** SV-39876r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000850  
**Rule Title:**The system must restrict the ability to switch to the root user to members of a defined group.  
  
  
**Vulnerability Discussion:**  Configuring a supplemental group for users permitted to switch to the root user prevents unauthorized users from accessing the root account, even with knowledge of the root credentials.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the root user is configured as a role, rather than a normal user.  
# egrep '^root:' /etc/user\_attr  
If the returned line does not include "type=role", this is a finding.  
  
Verify at least one local user has been assigned the root role.  
# egrep '[:;]roles=[^;]\*,?root([,;]|$)' /etc/user\_attr  
If no lines are returned, no users are permitted to assume the root role, this is a finding.  
  
**Fix Text:**Convert the root user into a role.  
# usermod -K type=role root  
  
Add the root role to authorized users' logins.  
# usermod -R root <userid>     
  
**CCI:**CCI-000009  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-773  
**Group Title:** GEN000880  
**Rule ID:** SV-39820r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000880  
**Rule Title:**The root account must be the only account having an UID of 0.  
  
  
**Vulnerability Discussion:**  If an account has an UID of 0, it has root authority. Multiple accounts with an UID of 0 afford more opportunity for potential intruders to guess a password for a privileged account.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1, IAIA-1, IAIA-2  
  
**Check Content:**    
Check the system for duplicate UID 0 assignments by listing all accounts assigned UID 0.  
  
Procedure:  
# awk -F: '$3 == 0' /etc/passwd  
  
If any accounts other than root are assigned UID 0, this is a finding.  
  
**Fix Text:**Remove or change the UID of accounts other than root that have UID 0.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-774  
**Group Title:** GEN000900  
**Rule ID:** SV-774r2\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000900  
**Rule Title:**The root user's home directory must not be the root directory (/).  
  
  
**Vulnerability Discussion:**  Changing the root home directory to something other than / and assigning it a 0700 protection makes it more difficult for intruders to manipulate the system by reading the files that root places in its default directory. It also gives root the same discretionary access control for root's home directory as for the other plain user home directories.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Determine if root is assigned a home directory other than / by listing its home directory.  
  
Procedure:  
# grep "^root" /etc/passwd | awk -F":" '{print $6}'  
  
If the root user home directory is /, this is a finding.  
  
**Fix Text:**The root home directory should be something other than / (such as /rootdir).  
  
Procedure:  
# mkdir /rootdir  
# chown root /rootdir  
# chgrp root /rootdir  
# chmod 700 /rootdir  
# cp -r /.??\* /rootdir  
  
Edit the passwd file and change the root home directory to /rootdir. The cp -r /.??\* command copies all files and subdirectories of file names beginning with "." into the new root directory, which preserves the previous root environment. The cp command must be executed from the / directory.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-775  
**Group Title:** GEN000920  
**Rule ID:** SV-775r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000920  
**Rule Title:**The root account's home directory (other than /) must have mode 0700.  
  
  
**Vulnerability Discussion:**  Permissions greater than 0700 could allow unauthorized users access to the root home directory.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the mode of the root home directory.  
  
Procedure:  
# grep "^root" /etc/passwd | awk -F":" '{print $6}'  
# ls -ld <root home directory>  
  
If the mode of the directory is not equal to 0700, this is a finding. If the home directory is /, this is not applicable.  
  
**Fix Text:**The root home directory will have permissions of 0700. Do not change the protections of the / directory. Use the following command to change protections for the root home directory.  
# chmod 0700 /rootdir.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22309  
**Group Title:** GEN000930  
**Rule ID:** SV-26353r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000930  
**Rule Title:**The root account's home directory must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the root account's home directory has no extended ACL.  
# ls -ld ~root  
If the permissions include a "+", the directory has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the directory.  
# chmod A- ~root     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-776  
**Group Title:** GEN000940  
**Rule ID:** SV-776r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000940  
**Rule Title:**The root account's executable search path must be the vendor default and must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory or other relative paths, executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. Entries starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2, ECSC-1  
  
**Check Content:**    
To view the root user's PATH, log in as the root user, and execute the following.  
# env | grep PATH  
  
This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is a finding. If an entry starts with a character other than a slash (/), this is a finding. If directories beyond those in the vendor's default root path are present, this is a finding.  
  
**Fix Text:**Edit the root user's local initialization files. Change any found PATH variable settings to the vendor's default path for the root user. Remove any empty path entries or references to relative paths.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22310  
**Group Title:** GEN000945  
**Rule ID:** SV-26355r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000945  
**Rule Title:**The root account's library search path must be the system default and must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The library search path environment variable(s) contain a list of directories for the dynamic linker to search to find libraries. If this path includes the current working directory or other relative paths, libraries in these directories may be loaded instead of system libraries. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. Entries starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the LD\_LIBRARY\_PATH environment variable is empty or not defined for the root user.  
# echo $LD\_LIBRARY\_PATH  
If a path list is returned, this is a finding.  
  
**Fix Text:**Edit the root user initialization files and remove any definition of LD\_LIBRARY\_PATH.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22311  
**Group Title:** GEN000950  
**Rule ID:** SV-26357r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000950  
**Rule Title:**The root account's list of preloaded libraries must be empty.  
  
  
**Vulnerability Discussion:**  The library preload list environment variable contains a list of libraries for the dynamic linker to load before loading the libraries required by the binary. If this list contains paths to libraries relative to the current working directory, unintended libraries may be preloaded. This variable is formatted as a space-separated list of libraries. Paths starting with (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the LD\_PRELOAD environment variable is empty or not defined for the root user.  
# echo $LD\_PRELOAD  
If a path list is returned, this is a finding.  
  
**Fix Text:**Edit the root user initialization files and remove any definition of LD\_PRELOAD.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-777  
**Group Title:** GEN000960  
**Rule ID:** SV-37075r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000960  
**Rule Title:**The root account must not have world-writable directories in its executable search path.  
  
  
**Vulnerability Discussion:**  If the root search path contains a world-writable directory, malicious software could be placed in the path by intruders and/or malicious users and inadvertently run by root with all of root's privileges.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check for world-writable permissions on all directories in the root user's executable search path. Procedure (on multiple lines):   
  
# echo $PATH | sed 's/ /\\ /g; s/:/  
/g' | xargs ls -ld  
  
If any of the directories in the PATH variable are world-writable, this is a finding.  
  
**Fix Text:**For each world-writable path in root's executable search path, perform one of the following.  
  
1. Remove the world-writable permission on the directory.  
Procedure:  
# chmod o-w <path>  
  
2. Remove the world-writable directory from the executable search path.  
  
Procedure:  
Identify and edit the initialization file referencing the world-writable directory and remove it from the PATH variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-778  
**Group Title:** GEN000980  
**Rule ID:** SV-27143r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000980  
**Rule Title:**The system must prevent the root account from directly logging in except from the system console.  
  
  
**Vulnerability Discussion:**  Limiting the root account direct logins to only system consoles protects the root account from direct unauthorized access from a non-console device.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1, ECSD-2  
  
**Check Content:**    
Check the CONSOLE setting in /etc/default/login  
# grep CONSOLE /etc/default/login  
If CONSOLE is set to a value other than /dev/console, this is a finding.  
  
**Fix Text:**Edit the /etc/default/login file and uncomment the line containing /dev/console if it is commented out.     
  
**CCI:**CCI-000770  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4298  
**Group Title:** GEN001000  
**Rule ID:** SV-27147r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001000  
**Rule Title:**Remote consoles must be disabled or protected from unauthorized access.  
  
  
**Vulnerability Discussion:**  The remote console feature provides an additional means of access to the system which could allow unauthorized access if not disabled or properly secured. With virtualization technologies, remote console access is essential as there is no physical console for virtual machines. Remote console access must be protected in the same manner as any other remote privileged access method.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify no auxiliary consoles are defined.  
# consadm -p  
If any output is generated, this is a finding.  
  
**Fix Text:**Remove each auxiliary console.  
# consadm -d <console device>     
  
**CCI:**CCI-000070  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11979  
**Group Title:** GEN001020  
**Rule ID:** SV-39848r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001020  
**Rule Title:**The root account must not be used for direct logins.  
  
  
**Vulnerability Discussion:**  Direct login with the root account prevents individual user accountability. Acceptable non-routine uses of the root account for direct login are limited to emergency maintenance, the use of single-user mode for maintenance, and situations where individual administrator accounts are not available.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Check if the root is used for direct logins.  
  
Procedure:  
# last root | grep -v reboot  
  
If any direct login records for root exist, this is a finding.  
  
Verify the root user is configured as a role, rather than a normal user.  
  
Procedure:  
# egrep '^root:' /etc/user\_attr  
  
If the returned line does not include "type=role", this is a finding.  
  
  
**Fix Text:**Convert the root user into a role.  
# usermod -K type=role root  
  
Add the root role to authorized users' logins.  
# usermod -R root <userid>     
  
**CCI:**CCI-000770  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11980  
**Group Title:** GEN001060  
**Rule ID:** SV-39850r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001060  
**Rule Title:**The system must log successful and unsuccessful access to the root account.  
  
  
**Vulnerability Discussion:**  If successful and unsuccessful logins and logouts are not monitored or recorded, access attempts cannot be tracked. Without this logging, it may be impossible to track unauthorized access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the following log files to determine if access to the root account is being logged. Try to su - and enter an incorrect password.  
# more /var/adm/sulog  
If root login accounts are not being logged, this is a finding.  
  
**Fix Text:**Update /etc/default/su and set SYSLOG=YES.  
  
Ensure /etc/syslog.conf is configured to log auth.crit messages to capture all failed su attempts.     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1062  
**Group Title:** GEN001080  
**Rule ID:** SV-27157r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001080  
**Rule Title:**The root shell must be located in the / file system.  
  
  
**Vulnerability Discussion:**  To ensure the root shell is available in repair and administrative modes, the root shell must be located in the / file system.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Perform the following to determine if /usr is partitioned.  
# grep /usr /etc/vfstab   
  
If /usr is partitioned, check the location of root's default shell.   
# awk -F: '$1 == "root" {print $7}' /etc/passwd  
If the root shell is found to be on a partitioned /usr filesystem or is in a directory symlinked to a partitioned /usr filesystem, even if the actual root shell is a symlink back to the root filesystem, this is a finding.  
  
**Fix Text:**Change the root account's shell to one present on the / filesystem. Example:   
  
# usermod -s /sbin/sh root     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1046  
**Group Title:** GEN001100  
**Rule ID:** SV-1046r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN001100  
**Rule Title:**Root passwords must never be passed over a network in clear text form.  
  
  
**Vulnerability Discussion:**  If a user accesses the root account (or any account) using an unencrypted connection, the password is passed over the network in clear text form and is subject to interception and misuse. This is true even if recommended procedures are followed by logging on to a named account and using the su command to access root.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECNK-1, ECNK-2, IAIA-1, IAIA-2  
  
**Check Content:**    
Determine if root has logged in over an unencrypted network connection.  
  
First, determine if root has logged in over a network.  
Procedure:  
# last | grep "^root " | egrep -v "reboot|console" | more  
  
Next, determine if the SSH daemon is running.  
Procedure:  
# ps -ef |grep sshd  
  
If root has logged in over the network and SSHD is not running, this is a finding.  
  
  
**Fix Text:**Enable SSH on the system and use it for all remote connections used to attain root access.     
  
**CCI:**CCI-000197  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1047  
**Group Title:** GEN001120  
**Rule ID:** SV-39811r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001120  
**Rule Title:**The system must not permit root logins using remote access programs such as SSH.   
  
  
**Vulnerability Discussion:**  Even though communications are encrypted, an additional layer of security may be gained by extending the policy of not logging directly on as root. In addition, logging in with a user-specific account preserves the audit trail.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Determine if the SSH daemon is configured to permit root logins.  
  
Procedure:  
# grep -v "^#" /etc/ssh/sshd\_config | grep -i permitrootlogin  
  
If the PermitRootLogin entry is not found or is not set to "no", this is a finding.  
  
**Fix Text:**Edit the configuration file and set the PermitRootLogin option to no.     
  
**CCI:**CCI-000770  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-784  
**Group Title:** GEN001140  
**Rule ID:** SV-39833r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001140  
**Rule Title:**System files and directories must not have uneven access permissions.  
  
  
**Vulnerability Discussion:**  Discretionary access control is undermined if users, other than a file owner, have greater access permissions to system files and directories than the owner.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check system directories for uneven file permissions.   
Procedure:  
# ls -lL /etc /bin /usr/bin /usr/ucb /sbin /usr/sbin   
  
Uneven file permissions exist if the file owner has less permissions than the group or other user classes. If any of the files in the above listed directories contain uneven file permissions, this is a finding.   
  
**Fix Text:**Change the mode of files with uneven permissions so owners do not have less permission than group or world users.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-785  
**Group Title:** GEN001160  
**Rule ID:** SV-785r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001160  
**Rule Title:**All files and directories must have a valid owner.  
  
  
**Vulnerability Discussion:**  Unowned files and directories may be unintentionally inherited if a user is assigned the same UID as the UID of the unowned files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the system for files with no assigned owner.  
  
Procedure:  
# find / -nouser -print  
  
If any files have no assigned owner, this is a finding.  
  
**Fix Text:**All directories and files (executable and data) will have an identifiable owner and group name. Either trace files to an authorized user, change the file's owner to root, or delete them. Determine the legitimate owner of the files and use the chown command to set the owner and group to the correct value. If the legitimate owner cannot be determined, change the owner to root (but make sure none of the changed files remain executable because they could be Trojan horses or other malicious code). Examine the files to determine their origin and the reason for their lack of an owner/group.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22312  
**Group Title:** GEN001170  
**Rule ID:** SV-26358r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001170  
**Rule Title:**All files and directories must have a valid group-owner.  
  
  
**Vulnerability Discussion:**  Files without a valid group-owner may be unintentionally inherited if a group is assigned the same GID as the GID of the files without a valid group-owner.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Search the system for files without a valid group-owner.  
# find / -nogroup -print  
If any files are found, this is a finding.  
  
**Fix Text:**Change the group owner for each file without a valid group owner.  
# chgrp <a-valid-group> /tmp/a-file-without-a-valid-group-owner     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-786  
**Group Title:** GEN001180  
**Rule ID:** SV-27161r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001180  
**Rule Title:**All network services daemon files must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  Restricting permission on daemons will protect them from unauthorized modification and possible system compromise.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of network services daemons.  
# ls -la /usr/bin /usr/sbin  
If the mode of a network services daemon is more permissive than 0755, this is a finding.  
NOTE: Network daemons not residing in these directories (such as httpd or sshd) must also be checked for the correct permissions.  
  
A way to locate network daemons, such as httpd and sshd, is with the ps command.  
# ps -ef | egrep '(sshd|httpd)'  
  
**Fix Text:**Change the mode of the network services daemon.  
# chmod 0755 <path>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22313  
**Group Title:** GEN001190  
**Rule ID:** SV-26361r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001190  
**Rule Title:**All network services daemon files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Restricting permission on daemons will protect them from unauthorized modification and possible system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify network services daemon files have no extended ACLs.  
# ls -la /usr/sbin  
# ls -la /usr/bin  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
NOTE: Network daemons not residing in these directories (such as httpd or sshd) must also be checked for the correct permissions.  
  
A way to locate network daemons, such as httpd and sshd, is with the ps command.  
# ps -ef | egrep '(sshd|httpd)'  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [file with extended ACL]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-794  
**Group Title:** GEN001200  
**Rule ID:** SV-794r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001200  
**Rule Title:**All system command files must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  Restricting permissions will protect system command files from unauthorized modification. System command files include files present in directories used by the operating system for storing default system executables and files present in directories included in the system's default executable search paths.  
  
**Severity Override Guidance:**   
Elevate to Severity Code I if any file listed is world-writable.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/ucb, /sbin, and /usr/sbin.  
  
Procedure:  
# ls -lL /etc /bin /usr/bin /usr/lbin /usr/ucb /sbin /usr/sbin  
  
If any file listed has a mode more permissive than 0755, this is a finding.  
  
NOTE: Elevate to Severity Code I if any file listed is world-writable.  
  
**Fix Text:**Change the mode for system command files to 0755 or less permissive.  
  
Procedure:  
# chmod 0755 <filename>     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22314  
**Group Title:** GEN001210  
**Rule ID:** SV-26365r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001210  
**Rule Title:**All system command files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Restricting permissions will protect system command files from unauthorized modification. System command files include files present in directories used by the operating system for storing default system executables and files present in directories included in the system's default executable search paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify all system command files have no extended ACLs.  
# ls -lL /etc /bin /usr/bin /usr/lbin /usr/ucb /sbin /usr/sbin  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.   
# chmod A- [file with extended ACL]     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-795  
**Group Title:** GEN001220  
**Rule ID:** SV-795r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001220  
**Rule Title:**All system files, programs, and directories must be owned by a system account.  
  
  
**Vulnerability Discussion:**  Restricting permissions will protect the files from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of system files, programs, and directories.  
  
Procedure:  
# ls -lLa /etc /bin /usr/bin /usr/lbin /usr/ucb /sbin /usr/sbin  
  
If any of the system files, programs, or directories are not owned by a system account, this is a finding.  
  
**Fix Text:**Change the owner of system files, programs, and directories to a system account.  
  
Procedure:  
# chown root /some/system/file  
  
(A different system user may be used in place of root.)     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-796  
**Group Title:** GEN001240  
**Rule ID:** SV-796r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001240  
**Rule Title:**System files, programs, and directories must be group-owned by a system group.  
  
  
**Vulnerability Discussion:**  Restricting permissions will protect the files from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of system files, programs, and directories.  
  
Procedure:  
# ls -lLa /etc /bin /usr/bin /usr/lbin /usr/ucb /sbin /usr/sbin  
  
If any system file, program, or directory is not group-owned by a system group, this is a finding.  
  
**Fix Text:**Change the group owner of system files to a system group.  
  
Procedure:  
# chgrp root /path/to/system/file  
  
(System groups other than root may be used.)     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-787  
**Group Title:** GEN001260  
**Rule ID:** SV-39832r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001260  
**Rule Title:**System log files must have mode 0640 or less permissive.  
  
  
**Vulnerability Discussion:**  If the system log files are not protected, unauthorized users could change the logged data, eliminating its forensic value.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECTP-1  
  
**Check Content:**    
Check the mode of log file hierarchies.  
  
Procedure:  
# ls -lLRa /var/log /var/adm  
  
If any of the log files or their directories have modes more permissive than 0640, this is a finding.  
  
**Fix Text:**Change the mode of the system log file(s) to 0640 or less permissive.  
  
Procedure:  
# chmod 0640 /path/to/system-log-file  
  
NOTE: Do not confuse system log files with audit logs. Any subsystems that require less stringent permissions must be documented.     
  
**CCI:**CCI-001314  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22315  
**Group Title:** GEN001270  
**Rule ID:** SV-26369r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001270  
**Rule Title:**System log files must not have extended ACLs, except as needed to support authorized software.  
  
  
**Vulnerability Discussion:**  If the system log files are not protected, unauthorized users could change the logged data, eliminating its forensic value. Authorized software may be given log file access through the use of extended ACLs when needed and configured to provide the least privileges required.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1, ECTP-1  
  
**Check Content:**    
Verify all system log files have no extended ACLs.  
  
Procedure:   
# ls -lL /var/adm   
If the permissions include a "+", the file has an extended ACL. If an extended ACL exists, verify with the SA if the ACL is required to support authorized software and provides the minimum necessary permissions. If an extended ACL exists that provides access beyond the needs of authorized software, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [file with extended ACL]     
  
**CCI:**CCI-001314  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-792  
**Group Title:** GEN001280  
**Rule ID:** SV-39835r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001280  
**Rule Title:**Manual page files must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  If manual pages are compromised, misleading information could be inserted, causing actions that may compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the mode of the manual page files.  
Procedure:   
# ls -lLR /usr/share/man /usr/sfw/share/man /usr/sfw/man  
  
If any of the manual page files have a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of manual page files to 0644 or less permissive.  
  
Procedure (example):  
# chmod 0644 <path>/<manpage>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22316  
**Group Title:** GEN001290  
**Rule ID:** SV-26373r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001290  
**Rule Title:**All manual page files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  If manual pages are compromised, misleading information could be inserted, causing actions that may compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify all manual page files have no extended ACLs. Check environment variable $MANPATH for full list of manpage locations.   
# echo $MANPATH   
Check for ACLs, note only a partial list is presented below.   
# ls -lLR /usr/share/man /usr/sfw/man /usr/sfw/share/man  
  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [file with extended ACL]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-793  
**Group Title:** GEN001300  
**Rule ID:** SV-39821r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001300  
**Rule Title:**Library files must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  Unauthorized access could destroy the integrity of the library files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Check the mode of library files.  
  
Procedure:  
# ls -lLR /usr/lib /lib /usr/sfw/lib  
  
If any of the library files have a mode more permissive than 0755, this is a finding.  
  
  
**Fix Text:**Change the mode of library files to 0755 or less permissive.  
  
Procedure (example):  
# chmod 0755 /path/to/library-file  
  
NOTE: Library files should have an extension of .a or .so, possibly followed by a version number.     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22317  
**Group Title:** GEN001310  
**Rule ID:** SV-26377r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001310  
**Rule Title:**All library files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Unauthorized access could destroy the integrity of the library files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify system libraries have no extended ACLs.   
  
# ls -lL /usr/lib/\* /lib/\* /usr/sfw/lib  
  
If the permissions include a "+", the file has an extended ACL and this is a finding.   
  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [file with extended ACL]     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-789  
**Group Title:** GEN001320  
**Rule ID:** SV-27166r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001320  
**Rule Title:**NIS/NIS+/yp files must be owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  NIS/NIS+/yp files are part of the system's identification and authentication processes and are, therefore, critical to system security. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Perform the following to check NIS file ownership.  
# ls -lRa /usr/lib/netsvc/yp /var/yp  
If the file ownership is not root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the ownership of NIS/NIS+/yp files to root, bin, or sys.  
  
Procedure:  
# chown -R root /usr/lib/netsvc/yp /var/yp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-790  
**Group Title:** GEN001340  
**Rule ID:** SV-27171r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001340  
**Rule Title:**NIS/NIS+/yp files must be group-owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  NIS/NIS+/yp files are part of the system's identification and authentication processes and are, therefore, critical to system security. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Perform the following to check NIS file ownership.  
# ls -lRa /usr/lib/netsvc/yp /var/yp  
If the file group owner is not root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the group owner of the NIS files to root, bin, or sys.  
  
Procedure:  
# chgrp -R root /usr/lib/netsvc/yp /var/yp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-791  
**Group Title:** GEN001360  
**Rule ID:** SV-27175r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001360  
**Rule Title:**The NIS/NIS+/yp command files must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  NIS/NIS+/yp files are part of the system's identification and authentication processes and are, therefore, critical to system security. Unauthorized modification of these files could compromise these processes and the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Perform the following to check NIS file mode.  
# ls -lRa /usr/lib/netsvc/yp /var/yp  
If the file's mode is more permissive than 0755, this is a finding.  
  
**Fix Text:**Change the mode of NIS/NIS+/yp command files to 0755 or less permissive.  
  
Procedure:  
# chmod -R 0755 /usr/lib/netsvc/yp /var/yp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22318  
**Group Title:** GEN001361  
**Rule ID:** SV-26388r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001361  
**Rule Title:**NIS/NIS+/yp command files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  NIS/NIS+/yp files are part of the system's identification and authentication processes and are, therefore, critical to system security. ACLs on these files could result in unauthorized modification, which could compromise these processes and the system.   
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify NIS/NIS+/yp files have no extended ACLs.  
# ls -lLRa /usr/lib/netsvc/yp /var/yp  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the directory and files.  
# chmod -R A- /usr/lib/netsvc/yp /var/yp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22319  
**Group Title:** GEN001362  
**Rule ID:** SV-26395r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001362  
**Rule Title:**The /etc/resolv.conf file must be owned by root.  
  
  
**Vulnerability Discussion:**  The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions, such as time synchronization, centralized authentication, and remote system logging.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the /etc/resolv.conf file is owned by root.  
  
Procedure:  
# ls -l /etc/resolv.conf  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/resolv.conf file to root.  
# chown root /etc/resolv.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22320  
**Group Title:** GEN001363  
**Rule ID:** SV-39894r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001363  
**Rule Title:**The /etc/resolv.conf file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions such as time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the resolv.conf file.  
  
Procedure:  
# ls -lL /etc/resolv.conf  
  
If the file is not group owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/resolv.conf file to root, bin, or sys.  
  
Procedure:  
# chgrp root /etc/resolv.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22321  
**Group Title:** GEN001364  
**Rule ID:** SV-26397r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001364  
**Rule Title:**The /etc/resolv.conf file must have mode 0644 or less permissive.   
  
  
**Vulnerability Discussion:**  The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions, such as time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/resolv.conf file.  
  
Procedure:  
# ls -l /etc/resolv.conf  
If the file mode is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/resolv.conf file to 0644 or less permissive.  
  
# chmod 0644 /etc/resolv.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22322  
**Group Title:** GEN001365  
**Rule ID:** SV-26402r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001365  
**Rule Title:**The /etc/resolv.conf file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions such as time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify /etc/resolv.conf has no extended ACL.  
# ls -l /etc/resolv.conf  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/resolv.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22323  
**Group Title:** GEN001366  
**Rule ID:** SV-26410r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001366  
**Rule Title:**The /etc/hosts file must be owned by root.  
  
  
**Vulnerability Discussion:**  The /etc/hosts file (or equivalent) configures local host name to IP address mappings that typically take precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the /etc/hosts file is owned by root.  
  
Procedure:  
# ls -l /etc/hosts  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/hosts file to root.  
  
# chown root /etc/hosts     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22324  
**Group Title:** GEN001367  
**Rule ID:** SV-39896r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001367  
**Rule Title:**The /etc/hosts file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  The /etc/hosts file (or equivalent) configures local host name to IP address mappings that typically take precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the /etc/hosts file's group ownership.  
  
Procedure:  
# ls -lL /etc/hosts  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/hosts file to root, sys, or bin.  
  
Procedure:  
# chgrp root /etc/hosts     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22325  
**Group Title:** GEN001368  
**Rule ID:** SV-26412r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001368  
**Rule Title:**The /etc/hosts file must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  The /etc/hosts file (or equivalent) configures local host name to IP address mappings that typically take precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/hosts file.  
  
Procedure:  
# ls -l /etc/hosts  
If the file mode is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/hosts file to 0644 or less permissive.  
  
# chmod 0644 /etc/hosts     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22326  
**Group Title:** GEN001369  
**Rule ID:** SV-26415r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001369  
**Rule Title:**The /etc/hosts file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  The /etc/hosts file (or equivalent) configures local host name to IP address mappings that typically take precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify /etc/hosts has no extended ACL.  
# ls -lL /etc/hosts  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/hosts     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22327  
**Group Title:** GEN001371  
**Rule ID:** SV-26417r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001371  
**Rule Title:**The /etc/nsswitch.conf file must be owned by root.  
  
  
**Vulnerability Discussion:**  The nsswitch.conf file (or equivalent) configures the source of a variety of system security information including account, group, and host lookups. Malicious changes could prevent the system from functioning or compromise system security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the /etc/nsswitch.conf file is owned by root.  
  
Procedure:  
# ls -l /etc/nsswitch.conf  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/nsswitch.conf file to root.  
  
# chown root /etc/nsswitch.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22328  
**Group Title:** GEN001372  
**Rule ID:** SV-39897r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001372  
**Rule Title:**The /etc/nsswitch.conf file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  The nsswitch.conf file (or equivalent) configures the source of a variety of system security information including account, group, and host lookups. Malicious changes could prevent the system from functioning or compromise system security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the nsswitch.conf file.  
  
Procedure:  
# ls -lL /etc/nsswitch.conf  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/nsswitch.conf file to root, bin, or sys.  
  
Procedure:  
# chgrp root /etc/nsswitch.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22329  
**Group Title:** GEN001373  
**Rule ID:** SV-26419r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001373  
**Rule Title:**The /etc/nsswitch.conf file must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  The nsswitch.conf file (or equivalent) configures the source of a variety of system security information including account, group, and host lookups. Malicious changes could prevent the system from functioning or compromise system security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/nsswitch.conf file.  
  
Procedure:  
# ls -l /etc/nsswitch.conf  
If the file mode is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/nsswitch.conf file to 0644 or less permissive.  
  
Procedure:  
# chmod 0644 /etc/nsswitch.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22330  
**Group Title:** GEN001374  
**Rule ID:** SV-26422r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001374  
**Rule Title:**The /etc/nsswitch.conf file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  The nsswitch.conf file (or equivalent) configures the source of a variety of system security information including account, group, and host lookups. Malicious changes could prevent the system from functioning or compromise system security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify /etc/nsswitch.conf has no extended ACL.  
  
Procedure:  
# ls -l /etc/nsswitch.conf  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/nsswitch.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22332  
**Group Title:** GEN001378  
**Rule ID:** SV-26425r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001378  
**Rule Title:**The /etc/passwd file must be owned by root.  
  
  
**Vulnerability Discussion:**  The /etc/passwd file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the /etc/passwd file is owned by root.  
  
Procedure:  
# ls -l /etc/passwd  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/passwd file to root.  
  
# chown root /etc/passwd     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22333  
**Group Title:** GEN001379  
**Rule ID:** SV-39898r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001379  
**Rule Title:**The /etc/passwd file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  The /etc/passwd file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the passwd file.  
  
Procedure:  
# ls -lL /etc/passwd  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/passwd file to root, bin, or sys.  
  
Procedure:  
# chgrp root /etc/passwd     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-798  
**Group Title:** GEN001380  
**Rule ID:** SV-798r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001380  
**Rule Title:**The /etc/passwd file must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  If the password file is writable by a group owner or the world, the risk of password file compromise is increased. The password file contains the list of accounts on the system and associated information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/passwd file.  
  
Procedure:  
# ls -lL /etc/passwd  
  
If /etc/passwd has a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the passwd file to 0644.  
  
Procedure:  
# chmod 0644 /etc/passwd  
  
Document all changes.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22334  
**Group Title:** GEN001390  
**Rule ID:** SV-26429r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001390  
**Rule Title:**The /etc/passwd file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  File system ACLs can provide access to files beyond what is allowed by the mode numbers of the files. The /etc/passwd file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify /etc/passwd has no extended ACL.  
# ls -l /etc/passwd  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/passwd  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22335  
**Group Title:** GEN001391  
**Rule ID:** SV-26431r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001391  
**Rule Title:**The /etc/group file must be owned by root.  
  
  
**Vulnerability Discussion:**  The /etc/group file is critical to system security and must be owned by a privileged user. The group file contains a list of system groups and associated information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the /etc/group file is owned by root.  
  
Procedure:  
# ls -l /etc/group  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/group file to root.  
  
# chown root /etc/group     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22336  
**Group Title:** GEN001392  
**Rule ID:** SV-39899r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001392  
**Rule Title:**The /etc/group file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  The /etc/group file is critical to system security and must be protected from unauthorized modification. The group file contains a list of system groups and associated information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the /etc/group file.  
  
Procedure:  
# ls -lL /etc/group  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/group file.  
  
Procedure:  
# chgrp root /etc/group     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22337  
**Group Title:** GEN001393  
**Rule ID:** SV-26433r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001393  
**Rule Title:**The /etc/group file must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  The /etc/group file is critical to system security and must be protected from unauthorized modification. The group file contains a list of system groups and associated information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/group file.  
  
Procedure:  
# ls -l /etc/group  
If the file mode is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/group file to 0644 or less permissive.  
# chmod 0644 /etc/group     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22338  
**Group Title:** GEN001394  
**Rule ID:** SV-26436r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001394  
**Rule Title:**The /etc/group file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  The /etc/group file is critical to system security and must be protected from unauthorized modification. The group file contains a list of system groups and associated information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify /etc/group has no extended ACL.  
# ls -l /etc/group  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/group     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-797  
**Group Title:** GEN001400  
**Rule ID:** SV-39826r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001400  
**Rule Title:**The /etc/shadow (or equivalent) file must be owned by root.  
  
  
**Vulnerability Discussion:**  The /etc/shadow file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification. Failure to give ownership of sensitive files or utilities to root provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the /etc/shadow file.  
# ls -lL /etc/shadow  
If the /etc/shadow file is not owned by root, this is a finding.  
  
  
**Fix Text:**Change the ownership of the /etc/shadow file.  
# chown root /etc/shadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22339  
**Group Title:** GEN001410  
**Rule ID:** SV-39900r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001410  
**Rule Title:**The /etc/shadow file (or equivalent) must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  The /etc/shadow file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification. The file also contains password hashes which must not be accessible to users other than root.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the /etc/shadow file.  
  
Procedure:  
# ls -lL /etc/shadow  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/shadow file.  
  
Procedure:  
# chgrp root /etc/shadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-800  
**Group Title:** GEN001420  
**Rule ID:** SV-800r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001420  
**Rule Title:**The /etc/shadow (or equivalent) file must have mode 0400.  
  
  
**Vulnerability Discussion:**  The /etc/shadow file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification. The file also contains password hashes which must not be accessible to users other than root.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/shadow file.  
# ls -lL /etc/shadow  
If the /etc/shadow file has a mode more permissive than 0400, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/shadow (or equivalent) file.  
# chmod <mode> <file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22340  
**Group Title:** GEN001430  
**Rule ID:** SV-26440r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001430  
**Rule Title:**The /etc/shadow file must not have an extended ACL.   
  
  
**Vulnerability Discussion:**  The /etc/shadow file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification. The file also contains password hashes which must not be accessible to users other than root.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify /etc/shadow has no extended ACL.  
# ls -lL /etc/shadow  
  
If the permissions include a '+', the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/shadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-899  
**Group Title:** GEN001440  
**Rule ID:** SV-27184r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001440  
**Rule Title:**All interactive users must be assigned a home directory in the /etc/passwd file.  
  
  
**Vulnerability Discussion:**  If users do not have a valid home directory, there is no place for the storage and control of files they own.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Use pwck to verify home directory assignments are present.  
# pwck  
If any user is not assigned a home directory, this is a finding.  
  
**Fix Text:**Assign a home directory to any user without one.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-900  
**Group Title:** GEN001460  
**Rule ID:** SV-27192r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001460  
**Rule Title:**All interactive user home directories defined in the /etc/passwd file must exist.  
  
  
**Vulnerability Discussion:**  If a user has a home directory defined that does not exist, the user may be given the / directory, by default, as the current working directory upon logon. This could create a Denial of Service because the user would not be able to perform useful tasks in this location.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Use pwck to verify assigned home directories exist.  
# pwck  
If any user's assigned home directory does not exist, this is a finding.  
  
  
**Fix Text:**If a user has no home directory, determine why. If possible, delete accounts that have no home directory. If the account is valid, then create the home directory using the appropriate system administration utility or manually.  
  
For instance: mkdir directoryname; copy the skeleton files into the directory; chown accountname for the new directory and the skeleton files. Document all changes.   
  
Update the sixth field in the /etc/passwd file to reflect the user's home directory.   
# usermod -d  
OR  
# vi /etc/passwd     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22347  
**Group Title:** GEN001470  
**Rule ID:** SV-26467r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001470  
**Rule Title:**The /etc/passwd file must not contain password hashes.  
  
  
**Vulnerability Discussion:**  If password hashes are readable by non-administrators, the passwords are subject to attack through lookup tables or cryptographic weaknesses in the hashes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify no password hashes are present in /etc/passwd.  
# cut -d : -f 2 /etc/passwd | grep -v '^x$'  
If any password hashes are returned, this is a finding.  
  
**Fix Text:**Migrate /etc/passwd password hashes to /etc/shadow.  
# pwconv     
  
**CCI:**CCI-000201  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22348  
**Group Title:** GEN001475  
**Rule ID:** SV-26447r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001475  
**Rule Title:**The /etc/group file must not contain any group password hashes.  
  
  
**Vulnerability Discussion:**  Group passwords are typically shared and should not be used. Additionally, if password hashes are readable by non-administrators, the passwords are subject to attack through lookup tables or cryptographic weaknesses in the hashes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the /etc/group file for password hashes.  
Procedure:  
# cut -d : -f 2 /etc/group | egrep -v '^(x|!)$'  
If any password hashes are returned, this is a finding.  
If no password hashes are returned, there is no finding.  
  
**Fix Text:**Edit /etc/group and change the password field to an exclamation point (!) to lock the group password.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-901  
**Group Title:** GEN001480  
**Rule ID:** SV-901r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001480  
**Rule Title:**All users' home directories must have mode 0750 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on home directories allow unauthorized access to user's files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the home directory mode of each user in /etc/passwd.  
  
Procedure:  
# cut -d : -f 6 /etc/passwd | xargs -n1 ls -ld | more  
  
If a user's home directory's mode is more permissive than 0750, this is a finding.  
  
NOTE: Application directories are allowed and may need 0755 permissions (or greater) for correct operation.  
  
**Fix Text:**Change the mode of users' home directories to 0750 or less permissive.  
  
Procedure (example):  
# chmod 0750 <home directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22350  
**Group Title:** GEN001490  
**Rule ID:** SV-26451r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001490  
**Rule Title:**User's home directories must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Excessive permissions on home directories allow unauthorized access to user's files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify user's home directories have no extended ACLs.  
  
# cut -d : -f 6 /etc/passwd | xargs -n1 ls -ld   
  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [user home directory with extended ACL]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-902  
**Group Title:** GEN001500  
**Rule ID:** SV-39822r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001500  
**Rule Title:**All interactive user's home directories must be owned by their respective users.  
  
  
**Vulnerability Discussion:**  If users do not own their home directories, unauthorized users could access user files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of each user's home directory listed in the /etc/passwd file.  
  
Procedure:   
# cut -d : -f 6 /etc/passwd | xargs -n1 ls -ld | more  
  
If any user's home directory is not owned by the assigned user, this is a finding.  
  
**Fix Text:**Change the owner of a user's home directory to its assigned user.  
  
Procedure:  
# chown <user> <home directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-903  
**Group Title:** GEN001520  
**Rule ID:** SV-39823r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001520  
**Rule Title:**All interactive user's home directories must be group-owned by the home directory owner's primary group.  
  
  
**Vulnerability Discussion:**  If the GID of the home directory is not the same as the GID of the user, this would allow unauthorized access to files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership for each user in the /etc/passwd file.   
  
Procedure:   
# cut -d : -f 6 /etc/passwd | xargs -n1 ls -ld | more  
  
If any user's home directory is not group-owned by the assigned user's primary group, this is a finding. Home directories for application accounts requiring different group ownership must be documented using site-defined procedures.  
  
**Fix Text:**Change the group owner for user's home directories to the primary group of the assigned user.  
  
Procedure:  
# chgrp groupname directoryname  
  
(Replace examples with appropriate group and home directory.)  
  
Document all changes.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-914  
**Group Title:** GEN001540  
**Rule ID:** SV-39836r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001540  
**Rule Title:**All files and directories contained in interactive user's home directories must be owned by the home directory's owner.  
  
  
**Vulnerability Discussion:**  If users do not own the files in their directories, unauthorized users may be able to access them. Additionally, if files are not owned by the user, this could be an indication of system compromise.  
  
**Documentable:** YES   
**Responsibility:**  Information Assurance Officer  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
For each user in the /etc/passwd file, check for the presence of files and directories within the user's home directory not owned by the home directory owner or root.  
  
Procedure:  
# cut -d : -f 6 /etc/passwd | xargs -n1 -IDIR ls -alLR DIR | more  
  
OR  
  
# find /<usershomedirectory> ! -fstype nfs ! -user <username> -exec ls -ld {} \; | more  
  
If user's home directories contain files or directories not owned by the home directory owner or root, this is a finding.  
  
**Fix Text:**Change the ownership of files and directories in user's home directories to the owner of the home directory.   
Procedure:   
# chown accountowner filename   
OR  
# find /<usershomedirectory> ! -fstype nfs ! -user <username> ! /( -name .login -o -name .cshrc -o -name .logout -o -name .profile -o -name .bash\_profile -o -name .bashrc -o -name .env -o -name .dtprofile -o -name .dispatch -o -name .emacs -o -name .exrc \) -exec chown <username> {} \;     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22351  
**Group Title:** GEN001550  
**Rule ID:** SV-39877r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001550  
**Rule Title:**All files and directories contained in user home directories must be group-owned by a group of which the home directory's owner is a member.  
  
  
**Vulnerability Discussion:**  If a user's files are group-owned by a group of which the user is not a member, unintended users may be able to access them.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the contents of user home directories for files group-owned by a group of which the home directory's owner is not a member.  
  
1. List the user accounts.  
# cut -d : -f 1/etc/passwd  
2. For each user account, get a list of GIDs for files in the user's home directory.  
# find < users home directory > -exec ls -lLd \;  
3. Obtain the list of GIDs associated with the user's account.  
# id < user name >  
4. Check the GID lists. If there are GIDs in the file list not present in the user list, this is a finding.  
  
**Fix Text:**Change the group of a file not group-owned by a group where the home directory's owner is a member.  
# chgrp < user's primary group > <file with bad group ownership >     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-915  
**Group Title:** GEN001560  
**Rule ID:** SV-39840r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001560  
**Rule Title:**All files and directories contained in user's home directories must have mode 0750 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions allow unauthorized access to user's files.  
  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
For each user in the /etc/passwd file, check for files and directories with a mode more permissive than 0750.  
  
Procedure:   
# find /<usershomedirectory> ! -fstype nfs \( -perm -0001 -o -perm -0002 -o -perm -0004 -o -perm -0020 -o -perm -2000 -o -perm -4000 \) -exec ls -ld {} \;   
If user's home directories contain files or directories more permissive than 0750, this is a finding.  
  
**Fix Text:**Change the mode of files and directories within user's home directories to 0750.  
  
Procedure:  
# chmod 0750 filename  
  
Document all changes.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22352  
**Group Title:** GEN001570  
**Rule ID:** SV-26456r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001570  
**Rule Title:**All files and directories contained in user home directories must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Excessive permissions allow unauthorized access to user files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the contents of interactive user's home directories (99 < UID < 60000) for files with extended ACLs.   
  
# ls -alLR < users home dir >  
  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [user file with extended ACL]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-906  
**Group Title:** GEN001580  
**Rule ID:** SV-27199r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001580  
**Rule Title:**All run control scripts must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  If the startup files are writable by other users, they could modify the startup files to insert malicious commands into the startup files.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check run control script modes.  
  
# ls -lL /etc/rc\* /etc/init.d  
  
If any run control script has a mode more permissive than 0755, this is a finding.  
  
**Fix Text:**Ensure all system startup files have mode 0755 or less permissive. Examine the rc files, and all files in the rc1.d (rc2.d, and so on) directories, and in the /etc/init.d directory to ensure they are not world-writable. If they are world-writable, use the chmod command to correct the vulnerability and to research why.  
  
Procedure:   
# chmod 755 startupfile     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22353  
**Group Title:** GEN001590  
**Rule ID:** SV-26460r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001590  
**Rule Title:**All run control scripts must have no extended ACLs.  
  
  
**Vulnerability Discussion:**  If the startup files are writable by other users, they could modify the startup files to insert malicious commands into the startup files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify run control scripts have no extended ACLs.  
# ls -lL /etc/rc\* /etc/init.d  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [run control script with extended ACL]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-907  
**Group Title:** GEN001600  
**Rule ID:** SV-39837r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001600  
**Rule Title:**Run control scripts' executable search paths must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory or other relative paths, executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Verify run control scripts' executable search paths.   
Procedure:   
# find /etc/rc\* /etc/init.d -type f -print | xargs grep -i PATH  
  
This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/), this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the run control script and remove the relative path entry from the executable search path variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22354  
**Group Title:** GEN001605  
**Rule ID:** SV-26462r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001605  
**Rule Title:**Run control scripts' library search paths must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The library search path environment variable(s) contain a list of directories for the dynamic linker to search to find libraries. If this path includes the current working directory or other relative paths, libraries in these directories may be loaded instead of system libraries. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify run control scripts' library search paths.   
# find /etc/rc\* /etc/init.d -type f -print | xargs grep LD\_LIBRARY\_PATH  
This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/) this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the run control script and remove the relative path entry from the library search path variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22355  
**Group Title:** GEN001610  
**Rule ID:** SV-26464r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001610  
**Rule Title:**Run control scripts' lists of preloaded libraries must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The library preload list environment variable contains a list of libraries for the dynamic linker to load before loading the libraries required by the binary. If this list contains paths to libraries relative to the current working directory, unintended libraries may be preloaded. This variable is formatted as a space-separated list of libraries. Paths starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify run control scripts' library preload list.   
Procedure:  
# find /etc/rc\* /etc/init.d -type f -print | xargs grep LD\_PRELOAD  
  
  
This variable is formatted as a colon-separated list of paths. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/) this is a relative path, and this is a finding.  
  
  
**Fix Text:**Edit the run control script and remove the relative path entry from the library preload variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-910  
**Group Title:** GEN001640  
**Rule ID:** SV-39810r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN001640  
**Rule Title:**Run control scripts must not execute world-writable programs or scripts.   
  
  
**Vulnerability Discussion:**  World-writable files could be modified accidentally or maliciously to compromise system integrity.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the permissions on the files or scripts executed from system startup scripts to see if they are world-writable.  
Create a list of all potential run command level scripts.  
ls -l /sbin/init.d/\* | tr '\011' ' ' | tr -s ' ' | cut -f 9,9 -d " "  
  
Create a list of world writeable files.  
# find / -perm -002 -type f >> worldWriteableFileList  
  
Determine if any of the world writeable files in worldWriteableFileList are called from the run command level scripts. Note: Depending upon the number of scripts vs world writeable files, it may be easier to inspect the scripts manually.  
# more `ls -l /sbin/init.d/\* | tr '\011' ' ' | tr -s ' ' | cut -f 9,9 -d "`   
  
If any system startup script executes any file or script that is world-writable, this is a finding.  
  
  
**Fix Text:**Remove the world-writable permission from programs or scripts executed by run control scripts.  
  
Procedure:  
# chmod o-w <program or script executed from run control script>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4089  
**Group Title:** GEN001660  
**Rule ID:** SV-27207r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001660  
**Rule Title:**All system start-up files must be owned by root.  
  
  
**Vulnerability Discussion:**  System start-up files not owned by root could lead to system compromise by allowing malicious users or applications to modify them for unauthorized purposes. This could lead to system and network compromise.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check run control scripts' ownership.  
# ls -lL /etc/rc\* /etc/init.d  
If any run control script is not owned by root, this is a finding.  
  
**Fix Text:**Change the ownership of the run control script(s) with incorrect ownership.  
# chown root <run control script>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4090  
**Group Title:** GEN001680  
**Rule ID:** SV-27213r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001680  
**Rule Title:**All system start-up files must be group-owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  If system start-up files do not have a group owner of root or a system group, the files may be modified by malicious users or intruders.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check run control scripts' group ownership.  
  
Procedure:  
# ls -lL /etc/rc\* /etc/init.d  
  
If any run control script is not group-owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the group ownership of the run control script(s) with incorrect group ownership.  
  
Procedure:  
# chgrp root <run control script>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4091  
**Group Title:** GEN001700  
**Rule ID:** SV-27219r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001700  
**Rule Title:**System start-up files must only execute programs owned by a privileged UID or an application.  
  
  
**Vulnerability Discussion:**  System start-up files executing programs owned by other than root (or another privileged user) or an application indicates the system may have been compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Determine the programs executed by system start-up files. Determine the ownership of the executed programs.   
# cat /etc/rc\* /etc/init.d/\* | more  
Check the ownership of every program executed by the system start-up files.  
# ls -l <executed program>  
If any executed program is not owned by root, sys, bin, or in rare cases, an application account, this is a finding.  
  
**Fix Text:**Change the ownership of the file executed from system startup scripts to root, bin, or sys.  
# chown root <executed file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11981  
**Group Title:** GEN001720  
**Rule ID:** SV-39829r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001720  
**Rule Title:**All global initialization files must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  Global initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check global initialization files permissions.  
  
# ls -l /etc/.login  
# ls -l /etc/profile  
# ls -l /etc/bashrc  
# ls -l /etc/environment  
# ls -l /etc/security/environ  
# ls -l /etc/csh.login   
# ls -l /etc/csh.cshrc  
  
If global initialization files exist and are more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the global initialization file(s) to 0644.  
# chmod 0644 <global initialization file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22356  
**Group Title:** GEN001730  
**Rule ID:** SV-26471r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001730  
**Rule Title:**All global initialization files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Global initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check global initialization files for extended ACLs.  
# ls -lL /etc/profile /etc/bashrc /etc/csh.login /etc/csh.cshrc /etc/environment /etc/.login /etc/security/environ  
If the permissions on an existing file include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [global initialization file with extended ACL]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11982  
**Group Title:** GEN001740  
**Rule ID:** SV-39830r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001740  
**Rule Title:**All global initialization files must be owned by root.  
  
  
**Vulnerability Discussion:**  Global initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of global initialization files.   
Procedure:   
# ls -lL /etc/.login /etc/profile /etc/bashrc /etc/environment /etc/security/environ /etc/csh.login /etc/csh.cshrc  
  
If any global initialization file exists and is not owned by root, this is a finding.   
  
**Fix Text:**Change the ownership of global initialization files with incorrect ownership.  
  
Procedure:  
# chown bin <global initialization files>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11983  
**Group Title:** GEN001760  
**Rule ID:** SV-39831r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001760  
**Rule Title:**All global initialization files must be group-owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  Global initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of global initialization files.  
  
Procedure:  
# ls -lL /etc/.login /etc/profile /etc/bashrc /etc/environment /etc/security/environ /etc/csh.login /etc/csh.cshrc  
  
If any global initialization file exists and is not group-owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the group ownership of the global initialization file(s) with incorrect group ownership.  
  
Procedure:  
# chgrp root <global initialization file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-825  
**Group Title:** GEN001780  
**Rule ID:** SV-39828r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001780  
**Rule Title:**Global initialization files must contain the mesg -n or mesg n commands.  
  
  
**Vulnerability Discussion:**  If the mesg -n or mesg n command is not placed into the system profile, messaging can be used to cause a Denial of Service attack.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check global initialization files for the presence of "mesg -n" or "mesg n".  
  
Procedure:  
# grep mesg /etc/.login /etc/profile /etc/bashrc /etc/environment /etc/security/environ /etc/csh.login /etc/csh.cshrc  
  
If no existing global initialization files contain "mesg -n" or "mesg n", this is a finding.  
  
**Fix Text:**Edit /etc/profile or another global initialization script and add the mesg -n command.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-788  
**Group Title:** GEN001800  
**Rule ID:** SV-788r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001800  
**Rule Title:**All skeleton files (typically those in /etc/skel) must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  If the skeleton files are not protected, unauthorized personnel could change user startup parameters and possibly jeopardize user files.  
  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check skeleton files permissions.  
# ls -alL /etc/skel  
If a skeleton file has a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of skeleton files with incorrect mode.  
# chmod 0644 <skeleton file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22357  
**Group Title:** GEN001810  
**Rule ID:** SV-26475r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001810  
**Rule Title:**Skeleton files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  If the skeleton files are not protected, unauthorized personnel could change user's startup parameters and possibly jeopardize user's files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check skeleton files for extended ACLs.  
# ls -alL /etc/skel  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [skeleton file with extended ACL]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11984  
**Group Title:** GEN001820  
**Rule ID:** SV-12485r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001820  
**Rule Title:**All skeleton files and directories (typically in /etc/skel) must be owned by bin.  
  
  
**Vulnerability Discussion:**  If the skeleton files are not protected, unauthorized personnel could change user startup parameters and possibly jeopardize user files. Failure to give ownership of sensitive files or utilities to bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check skeleton files ownership.  
# ls -alL /etc/skel  
If a skeleton file is not owned by bin, this is a finding.  
  
**Fix Text:**Change the ownership of skeleton files with incorrect mode.  
# chown bin <skeleton file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22358  
**Group Title:** GEN001830  
**Rule ID:** SV-39901r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001830  
**Rule Title:**All skeleton files (typically in /etc/skel) must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the skeleton files are not protected, unauthorized personnel could change user startup parameters and possibly jeopardize user files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the skeleton files are group-owned by root.  
  
Procedure:  
# ls -alL /etc/skel  
  
If a skeleton file is not group-owned by root, this is a finding.  
  
**Fix Text:**Change the group owner of the skeleton file to root.  
  
Procedure:  
# chgrp <group> /etc/skel/[skeleton file]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11985  
**Group Title:** GEN001840  
**Rule ID:** SV-12486r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001840  
**Rule Title:**All global initialization files' executable search paths must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory or other relative paths, executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the global initialization files' executable search paths.  
  
Procedure:  
# grep -i PATH /etc/profile /etc/bashrc /etc/csh.login /etc/csh.cshrc /etc/environment /etc/.login /etc/security/environ  
  
This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/), this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the global initialization file(s) with PATH variables containing relative paths. Edit the file and remove the relative path from the PATH variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22359  
**Group Title:** GEN001845  
**Rule ID:** SV-26478r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001845  
**Rule Title:**Global initialization files' library search paths must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The library search path environment variable(s) contain a list of directories for the dynamic linker to search to find libraries. If this path includes the current working directory or other relative paths, libraries in these directories may be loaded instead of system libraries. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the global initialization files' library search paths.  
# grep LD\_LIBRARY\_PATH /etc/profile /etc/bashrc /etc/csh.login /etc/csh.cshrc /etc/environment /etc/.login /etc/security/environ  
This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/) this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the global initialization file and remove the relative path entry from the library search path variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22360  
**Group Title:** GEN001850  
**Rule ID:** SV-39839r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001850  
**Rule Title:**Global initialization files' lists of preloaded libraries must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The library preload list environment variable contains a list of libraries for the dynamic linker to load before loading the libraries required by the binary. If this list contains paths to libraries relative to the current working directory, unintended libraries may be preloaded. This variable is formatted as a space-separated list of libraries. Paths starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the global initialization files' library preload list.   
Procedure:  
# grep LD\_PRELOAD /etc/profile /etc/bashrc /etc/csh.login /etc/csh.cshrc /etc/environment /etc/.login /etc/security/environ   
This variable is formatted as a colon-separated list of paths. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/) this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the global initialization file(s) and remove the relative path entry from the library preload list variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-904  
**Group Title:** GEN001860  
**Rule ID:** SV-904r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001860  
**Rule Title:**All local initialization files must be owned by the user or root.  
  
  
**Vulnerability Discussion:**  Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of local initialization files.  
  
Procedure (using a shell that supports ~USER as USER's home directory):  
# cut -d : -f 1 /etc/passwd | xargs -n1 -IUSER sh -c "ls -l ~USER/.[a-z]\*"  
# cut -d : -f 1 /etc/passwd | xargs -n1 -IUSER find ~USER/.dt ! -fstype nfs ! -user USER -exec ls -ld {} \;  
  
If local initialization files are not owned by the home directory's user, this is a finding.  
  
**Fix Text:**Change the ownership of the startup and login files in the user's directory to the user or root, as appropriate. Examine each user's home directory and verify all file names beginning with "." are owned by the owner of the directory or root. If they are not, use the chown command to change the owner to the user and research the reasons why the owners were not assigned as required.   
  
Procedure:  
# chown username .filename  
Document all changes.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22361  
**Group Title:** GEN001870  
**Rule ID:** SV-37101r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001870  
**Rule Title:**Local initialization files must be group-owned by the user's primary group or root.  
  
  
**Vulnerability Discussion:**  Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check user home directories for local initialization files group-owned by a group other than the user's primary group or root.  
1. List user accounts and their primary GID.  
# cut -d : -f 1,4 /etc/passwd  
  
2. Check local initialization files for each user.  
# ls -al /<usershomedirectory>/.login  
# ls -al /<usershomedirectory>/.cshrc  
# ls -al /<usershomedirectory>/.logout  
# ls -al /<usershomedirectory>/.profile  
# ls -al /<usershomedirectory>/.bash\_profile  
# ls -al /<usershomedirectory>/.bashrc  
# ls -al /<usershomedirectory>/.bash\_logout  
# ls -al /<usershomedirectory>/.env  
# ls -al /<usershomedirectory>/.dtprofile  
# ls -al /<usershomedirectory>/.dispatch  
# ls -al /<usershomedirectory>/.emacs  
# ls -al /<usershomedirectory>/.exrc  
# find /<usershomedirectory>/.dt ! -fstype nfs ! -group <primary\_group> -exec ls -ld {} \;  
  
3. If any file is not group-owned by root or the user's primary GID, this is a finding.  
  
  
  
**Fix Text:**Change the group-owner of the local initialization file to the user's primary group, or root.  
# chgrp [USER's primary GID] ~USER/[local initialization file]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-905  
**Group Title:** GEN001880  
**Rule ID:** SV-905r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001880  
**Rule Title:**All local initialization files must have mode 0740 or less permissive.  
  
  
**Vulnerability Discussion:**  Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the modes of local initialization files.  
  
Procedure:  
# ls -al /<usershomedirectory>/.login  
# ls -al /<usershomedirectory>/.cshrc  
# ls -al /<usershomedirectory>/.logout  
# ls -al /<usershomedirectory>/.profile  
# ls -al /<usershomedirectory>/.bash\_profile  
# ls -al /<usershomedirectory>/.bashrc  
# ls -al /<usershomedirectory>/.bash\_logout  
# ls -al /<usershomedirectory>/.env  
# ls -al /<usershomedirectory>/.dtprofile (permissions should be 0755)  
# ls -al /<usershomedirectory>/.dispatch  
# ls -al /<usershomedirectory>/.emacs  
# ls -al /<usershomedirectory>/.exrc  
# find /<usershomedirectory>/.dt ! -fstype nfs \( -perm -0002 -o -perm -0020 \) -exec ls -ld {} \; (permissions not to be more   
permissive than 0755)  
  
If local initialization files are more permissive than 0740, the .dt directory or the .dtprofile file is more permissive than 0755, this is a finding.  
  
**Fix Text:**Ensure user startup files have permissions of 0740 or more restrictive. Examine each user's home directory and verify all file names beginning with "." have access permissions of 0740 or more restrictive. If they do not, use the chmod command to correct the vulnerability.   
  
Procedure:   
# chmod 0740 .filename   
  
NOTE: The period is part of the file name and is required.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22362  
**Group Title:** GEN001890  
**Rule ID:** SV-26484r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001890  
**Rule Title:**Local initialization files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check user home directories for local initialization files with extended ACLs.  
# cut -d : -f 6 /etc/passwd | xargs -n1 -IDIR ls -alL DIR/.login DIR/.cshrc DIR/.logout DIR/.profile DIR/.bash\_profile DIR/.bashrc DIR/.bash\_logout DIR/.env DIR/.dtprofile DIR/.dispatch DIR/.emacs DIR/.exrc  
  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [local initialization file with extended ACL]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11986  
**Group Title:** GEN001900  
**Rule ID:** SV-12487r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001900  
**Rule Title:**All local initialization files' executable search paths must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The executable search path (typically the PATH environment variable) contains a list of directories for the shell to search to find executables. If this path includes the current working directory or other relative paths, executables in these directories may be executed instead of system commands. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Examine the PATH variable contained in any user's local initialization files to ensure the use of only absolute paths, using a command shell that supports the use of ~USER as USER's home directory.  
  
# cat /etc/passwd | cut -f 1,1 -d ":" | xargs -n1 -IUSER sh -c 'grep -i PATH ~USER/.\*'  
  
The PATH variable is a colon-delimited directory list.   
  
An empty entry is defined by a leading/trailing colon or two consecutive colons.   
  
A relative path is defined as an entry beginning with a character other than a slash (/).  
  
If an empty or relative path is defined in the PATH variable, this is a finding.  
  
**Fix Text:**Edit the local initialization file(s) and remove the relative path entry from the PATH variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22363  
**Group Title:** GEN001901  
**Rule ID:** SV-26486r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001901  
**Rule Title:**Local initialization files' library search paths must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The library search path environment variable(s) contain a list of directories for the dynamic linker to search to find libraries. If this path includes the current working directory or other relative paths, libraries in these directories may be loaded instead of system libraries. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify local initialization files have library search path containing only absolute paths.  
# cut -d : -f 1 /etc/passwd | xargs -n1 -IUSER sh -c 'grep -l LD\_LIBRARY\_PATH ~USER/.\*'  
This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/) this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the local initialization file and remove the relative path entry from the library search path variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22364  
**Group Title:** GEN001902  
**Rule ID:** SV-26488r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001902  
**Rule Title:**Local initialization files' lists of preloaded libraries must contain only absolute paths.  
  
  
**Vulnerability Discussion:**  The library preload list environment variable contains a list of libraries for the dynamic linker to load before loading the libraries required by the binary. If this list contains paths to libraries relative to the current working directory, unintended libraries may be preloaded. This variable is formatted as a space-separated list of libraries. Paths starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify local initialization files have library preload list containing only absolute paths.  
# cut -d : -f 1 /etc/passwd | xargs -n1 -IUSER sh -c 'grep -l LD\_PRELOAD ~USER/.\*'  
This variable is formatted as a colon-separated list of paths. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/) this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the local initialization file and remove the relative path entry from the library preload variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4087  
**Group Title:** GEN001940  
**Rule ID:** SV-39812r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001940  
**Rule Title:**User start-up files must not execute world-writable programs.  
  
  
**Vulnerability Discussion:**  If start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to become Trojans destroying user files or otherwise compromising the system at the user, or higher, level. If the system is compromised at the user level, it is much easier to eventually compromise the system at the root and network level.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSW-1  
  
**Check Content:**    
Check local initialization files for any executed world-writable programs or scripts.  
  
Procedure:  
# find / -perm -002 -type f | egrep -v '^(/proc|/system/contract)' > wwlist  
# fgrep -f wwlist /<usershomedirectory>/.\*  
  
If any local initialization file executes a world-writable program or script, this is a finding.  
  
**Fix Text:**Remove the world-writable permission of files referenced by local initialization scripts, or remove the references to these files in the local initialization scripts.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11987  
**Group Title:** GEN001980  
**Rule ID:** SV-12488r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001980  
**Rule Title:**The .rhosts, .shosts, hosts.equiv, shosts.equiv, /etc/passwd, /etc/shadow, and/or /etc/group files must not contain a plus (+) without defining entries for NIS+ netgroups.  
  
  
**Vulnerability Discussion:**  A plus (+) in system accounts' files causes the system to lookup the specified entry using NIS. If the system is not using NIS, no such entries should exist.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check system configuration files for plus (+) entries.  
  
Procedure:  
# find / -name .rhosts -exec grep + {} \;  
  
# find / -name .shosts -exec grep + {} \;  
  
# find / -name hosts.equiv -exec grep + {} \;  
  
# find / -name shosts.equiv -exec grep + {} \;  
  
  
# grep + /etc/passwd  
# grep + /etc/shadow  
# grep + /etc/group  
  
If the .rhosts, .shosts, hosts.equiv, shosts.equiv, /etc/passwd, /etc/shadow, and/or /etc/group files contain a plus (+) and do not define entries for NIS+ netgroups, this is a finding.  
  
  
  
**Fix Text:**Edit the .rhosts, .shosts, hosts.equiv, shosts.equiv, /etc/passwd, /etc/shadow, and/or /etc/group files and remove entries containing a plus (+).  
  
  
  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-913  
**Group Title:** GEN002000  
**Rule ID:** SV-913r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002000  
**Rule Title:**There must be no .netrc files on the system.   
  
  
**Vulnerability Discussion:**  Unencrypted passwords for remote FTP servers may be stored in .netrc files. Policy requires passwords be encrypted in storage and not used in access scripts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2, IAIA-1, IAIA-2  
  
**Check Content:**    
Check the system for the existence of any .netrc files.  
  
Procedure:  
# find / -name .netrc   
  
If any .netrc file exists, this is a finding.  
  
**Fix Text:**Remove the .netrc file(s).  
  
Procedure:  
# rm .netrc     
  
**CCI:**CCI-000196  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4427  
**Group Title:** GEN002020  
**Rule ID:** SV-40331r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002020  
**Rule Title:**All .rhosts, .shosts, or host.equiv files must only contain trusted host-user pairs.  
  
  
**Vulnerability Discussion:**  If these files are not properly configured, they could allow malicious access by unknown malicious users from untrusted hosts who could compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Locate and examine all .rhosts, .shosts, hosts.equiv, and shosts.equiv files. The .rhosts and .shosts files are stored in home directories. (If a user does not have a home directory assigned in /etc/passwd, the root directory (/) is assigned as a default home directory.)  
  
Procedure:  
# for i in `cut -d: -f6 /etc/passwd | awk '$1 == "" {$1 = "/"} {print $1}'`; do more $i/.rhosts; more $i/.shosts; done  
# more /etc/hosts.equiv  
# more /etc/ssh/shosts.equiv  
  
If any .rhosts, .shosts, hosts.equiv, or shosts.equiv file contains other than host-user pairs, this is a finding.  
  
**Fix Text:**If possible, remove the .rhosts, .shosts, hosts.equiv, and shosts.equiv files. If the files are required, remove any content from the files except for necessary host-user pairs.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11988  
**Group Title:** GEN002040  
**Rule ID:** SV-40332r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN002040  
**Rule Title:**There must be no .rhosts, .shosts, hosts.equiv, or shosts.equiv files on the system.  
  
  
**Vulnerability Discussion:**  The .rhosts, .shosts, hosts.equiv, and shosts.equiv files are used to configure host-based authentication for individual users or the system. Host-based authentication is not sufficient for preventing unauthorized access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check for the existence of the files. The .rhosts and .shosts files are stored in home directories. (If a user does not have a home directory assigned in /etc/passwd, the root directory (/) is assigned as a default home directory.)  
  
Procedure (the first command is five lines long):  
# for homedir in `cut -d: -f6 /etc/passwd | awk '$1 == "" {$1 = "/"} {print $1}'`;  
do  
ls -l $homedir/.rhosts;  
ls -l $homedir/.shosts;  
done  
# ls -l /etc/hosts.equiv  
# ls -l /etc/ssh/shosts.equiv  
  
If .rhosts, .shosts, hosts.equiv, or shosts.equiv are found, this is a finding.  
  
**Fix Text:**Remove the .rhosts, .shosts, hosts.equiv, and/or shosts.equiv files.  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4428  
**Group Title:** GEN002060  
**Rule ID:** SV-40341r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002060  
**Rule Title:**All .rhosts, .shosts, .netrc, or hosts.equiv files must be accessible by only root or the owner.  
  
  
**Vulnerability Discussion:**  If these files are accessible by users other than root or the owner, they could be used by a malicious user to set up a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# for i in `cut -d: -f6 /etc/passwd | awk '$1 == "" {$1 = "/"} {print $1}'`; do ls -l $i/.rhosts $i/.shosts $i/.netrc; done  
# ls -l /etc/hosts.equiv  
# ls -l /etc/ssh/shosts.equiv  
  
If the .netrc, .rhosts, .shosts, hosts.equiv, or shosts.equiv files have permissions greater than 600, then this is a finding. (If a password entry has no home directory assigned, the root directory (/) is used as a default.)  
  
**Fix Text:**Ensure the permission for these files is set at 600 or less and the owner is the owner of the home directory that it is in. These files, outside of home directories (other than hosts.equiv in /etc and shosts.equiv in /etc/ssh; both are owned by root), have no meaning.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11989  
**Group Title:** GEN002100  
**Rule ID:** SV-40334r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002100  
**Rule Title:**The .rhosts file must not be supported in PAM.  
  
  
**Vulnerability Discussion:**  The .rhosts files are used to specify a list of hosts that are permitted remote access to a particular account without authenticating. The use of such a mechanism defeats strong identification and authentication requirements.  
  
**Responsibility:**  Information Assurance Officer  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the PAM configuration for rhosts\_auth.  
  
Procedure:  
# grep rhosts\_auth /etc/pam.conf  
  
If a rhosts\_auth entry is found that is not commented out, this is a finding.  
  
**Fix Text:**Edit /etc/pam.conf and remove the reference(s) to the rhosts\_auth module.  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-916  
**Group Title:** GEN002120  
**Rule ID:** SV-40806r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002120  
**Rule Title:**The /etc/shells (or equivalent) file must exist.  
  
  
**Vulnerability Discussion:**  The shells file (or equivalent) lists approved default shells. It helps provide layered defense to the security approach by ensuring users cannot change their default shell to an unauthorized shell that may not be secure.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify /etc/shells exists.  
# ls -l /etc/shells  
If the file does not exist, this is a finding.  
  
**Fix Text:**Create a /etc/shells file containing a list of valid system shells. The list below contains the default shells from the shells(4) man page.  
  
Procedure (the command is 24 lines long):  
cat >/etc/shells <<EOF  
/bin/bash  
/bin/csh  
/bin/jsh  
/bin/ksh  
/bin/pfcsh  
/bin/pfksh  
/bin/pfsh  
/bin/sh  
/bin/tcsh  
/bin/zsh  
/sbin/jsh  
/sbin/sh  
/usr/bin/bash  
/usr/bin/csh  
/usr/bin/jsh  
/usr/bin/ksh  
/usr/bin/pfcsh  
/usr/bin/pfksh  
/usr/bin/pfsh  
/usr/bin/sh  
/usr/bin/tcsh  
/usr/bin/zsh  
EOF     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-917  
**Group Title:** GEN002140  
**Rule ID:** SV-917r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002140  
**Rule Title:**All shells referenced in /etc/passwd must be listed in the /etc/shells file, except any shells specified for the purpose of preventing logins.  
  
  
**Vulnerability Discussion:**  The shells file lists approved default shells. It helps provide layered defense to the security approach by ensuring users cannot change their default shell to an unauthorized shell that may not be secure.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Confirm the login shells referenced in the /etc/passwd file are listed in the /etc/shells file.   
  
Procedure:  
# more /etc/passwd  
# more /etc/shells  
  
The /usr/bin/false, /bin/false, /dev/null, /sbin/nologin, (and equivalents), and sdshell will be considered valid shells for use in the /etc/passwd file, but will not be listed in the /etc/shells file.  
  
If a shell referenced in /etc/passwd is not listed in the shells file, excluding the above mentioned shells, this is a finding.  
  
**Fix Text:**Use the chsh utility or edit the /etc/passwd file and correct the error by changing the default shell of the account in error to an acceptable shell name contained in the /etc/shells file.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-921  
**Group Title:** GEN002200  
**Rule ID:** SV-921r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002200  
**Rule Title:**All shell files must be owned by root or bin.  
  
  
**Vulnerability Discussion:**  If shell files are owned by users other than root or bin, they could be modified by intruders or malicious users to perform unauthorized actions.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the system shells.  
# cat /etc/shells | xargs -n1 ls -lL  
If any shell is not owned by root or bin, this is a finding.  
  
**Fix Text:**Change the ownership of the shell with incorrect ownership.  
# chown root <shell>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22365  
**Group Title:** GEN002210  
**Rule ID:** SV-39902r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002210  
**Rule Title:**All shell files must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If shell files are group-owned by users other than root or a system group, they could be modified by intruders or malicious users to perform unauthorized actions.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
If /etc/shells exists, check the group ownership of each shell referenced.  
  
Procedure:  
# cat /etc/shells | xargs -n1 ls -lL  
  
Otherwise, check any shells found on the system.  
Procedure:  
# find / -name "\*sh" | xargs -n1 ls -lL  
  
If a shell is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group-owner of the shell to root, bin, or sys.  
  
Procedure:  
# chgrp root <shell>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-922  
**Group Title:** GEN002220  
**Rule ID:** SV-922r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN002220  
**Rule Title:**All shell files must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  Shells with world/group-write permissions give the ability to maliciously modify the shell to obtain unauthorized access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
If /etc/shells exists, check the group ownership of each shell referenced.  
# cat /etc/shells | xargs -n1 ls -lL  
  
Otherwise, check any shells found on the system.  
# find / -name "\*sh" | xargs -n1 ls -lL  
  
If a shell has a mode more permissive than 0755, this is a finding.  
  
**Fix Text:**Change the mode of the shell.  
# chmod 0755 <shell>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22366  
**Group Title:** GEN002230  
**Rule ID:** SV-26492r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002230  
**Rule Title:**All shell files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Shells with world/group write permissions give the ability to maliciously modify the shell to obtain unauthorized access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
If /etc/shells exists, check the permissions of each shell referenced.  
# cat /etc/shells | xargs -n1 ls -lL  
  
Otherwise, check any shells found on the system.  
# find / -name "\*sh" | xargs -n1 ls -lL  
  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [shell]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-923  
**Group Title:** GEN002260  
**Rule ID:** SV-923r2\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002260  
**Rule Title:**The system must be checked for extraneous device files at least weekly.  
  
  
**Vulnerability Discussion:**  If an unauthorized device is allowed to exist on the system, there is the possibility the system may perform unauthorized operations.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSW-1, ECSC-1  
  
**Check Content:**    
Check the system for an automated job, or check with the SA, to determine if the system is checked for extraneous device files on a weekly basis. If no automated or manual process is in place, this is a finding.  
  
  
  
**Fix Text:**Establish a weekly automated or manual process to create a list of device files on the system and determine if any files have been added, moved, or deleted since the last list was generated.   
  
Generate a list of device files.  
# find / -type b -o -type c > device-file-list     
  
**CCI:**CCI-000318  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-924  
**Group Title:** GEN002280  
**Rule ID:** SV-924r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002280  
**Rule Title:**Device files and directories must only be writable by users with a system account or as configured by the vendor.  
  
  
**Vulnerability Discussion:**  System device files in writable directories could be modified, removed, or used by an unprivileged user to control system hardware.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2, ECLP-1  
  
**Check Content:**    
Find all device files existing anywhere on the system.  
  
Procedure:  
# find / -type b -print > devicelist  
# find / -type c -print >> devicelist  
  
Check the permissions on the directories above subdirectories containing device files. If any of the device files or their parent directories is world-writable, excepting device files specifically intended to be world-writable, such as /dev/null, this is a finding.  
  
**Fix Text:**Remove the world-writable permission from the device file(s).  
  
Procedure:  
# chmod o-w <device file>  
  
Document all changes.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-925  
**Group Title:** GEN002300  
**Rule ID:** SV-925r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002300  
**Rule Title:**Device files used for backup must only be readable and/or writable by root or the backup user.  
  
  
**Vulnerability Discussion:**  System backups could be accidentally or maliciously overwritten and destroy the ability to recover the system if a compromise should occur. Unauthorized users could also copy system files.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the system for world-writable device files.  
  
Procedure:  
# find / -perm -2 -a \( -type b -o -type c \) -exec ls -ld {} \;  
  
If any device file(s) used for backup are writable by users other than root, this is a finding.  
  
**Fix Text:**Use the chmod command to remove the world-writable bit from the backup device files.   
  
Procedure:  
# chmod o-w backdevicefilename  
  
Document all changes.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1048  
**Group Title:** GEN002320  
**Rule ID:** SV-27241r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002320  
**Rule Title:**Audio devices must have mode 0660 or less permissive.  
  
  
**Vulnerability Discussion:**  Globally accessible audio and video devices have proven to be security hazards. There is software that can activate system microphones and video devices connected to user workstations and/or X terminals. Once the microphone has been activated, it is possible to eavesdrop on otherwise private conversations without the victim being aware of it. This action effectively changes the user's microphone to a bugging device.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of audio devices.  
# ls -lL /dev/audio  
If the mode of audio devices are more permissive than 0660, this is a finding.  
  
**Fix Text:**Change the mode of the audio device.  
# chmod -R 0660 /dev/audio     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22367  
**Group Title:** GEN002330  
**Rule ID:** SV-26496r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002330  
**Rule Title:**Audio devices must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  File system ACLs can provide access to files beyond what is allowed by the mode numbers of the files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of audio devices.  
# ls -lL /dev/audio  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /dev/audio     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1049  
**Group Title:** GEN002340  
**Rule ID:** SV-27246r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002340  
**Rule Title:**Audio devices must be owned by root.  
  
  
**Vulnerability Discussion:**  Globally Accessible audio and video devices have proven to be security hazards. There is software that can activate system microphones and video devices connected to user workstations and/or X terminals. Once the microphone has been activated, it is possible to eavesdrop on otherwise private conversations without the victim being aware of it. This action effectively changes the user's microphone to a bugging device.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the owner of audio devices.  
# ls -lL /dev/audio  
If the owner of any audio device file is not root, this is a finding.  
  
**Fix Text:**Change the owner of the audio device.  
# chown root <audio device>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1061  
**Group Title:** GEN002360  
**Rule ID:** SV-27251r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002360  
**Rule Title:**Audio devices must be group-owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  Without privileged group owners, audio devices will be vulnerable to being used as eaves-dropping devices by malicious users or intruders to possibly listen to conversations containing sensitive information.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group-owner of audio devices.  
  
Procedure:  
# ls -lL /dev/audio  
  
If the group-owner of an audio device is not root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the group owner of the audio device.  
  
Procedure:  
# chgrp system <audio device>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-801  
**Group Title:** GEN002380  
**Rule ID:** SV-801r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002380  
**Rule Title:**The owner, group owner, mode, ACL, and location of files with the setuid bit set must be documented using site-defined procedures.  
  
  
**Vulnerability Discussion:**  All files with the setuid bit set will allow anyone running these files to be temporarily assigned the UID of the file. While many system files depend on these attributes for proper operation, security problems can result if setuid is assigned to programs that allow reading and writing of files, or shell escapes. Only default vendor-supplied executables should have the setuid bit set.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Files with the setuid bit set will allow anyone running these files to be temporarily assigned the user or group ID of the file. If an executable with setuid allows shell escapes, the user can operate on the system with the effective permission rights of the user or group owner.  
  
List all setuid files on the system.  
Procedure:  
# find / -perm -4000 -exec ls -l {} \; | more   
  
NOTE: Executing these commands may result in large listings of files; the output may be redirected to a file for easier analysis.  
  
Ask the SA or IAO if files with the setuid bit set have been documented. If any undocumented file has its setuid bit set, this is a finding.  
  
**Fix Text:**Document the files with the setuid bit set or unset the setuid bit on the executable.     
  
**CCI:**CCI-000368  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-803  
**Group Title:** GEN002400  
**Rule ID:** SV-803r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002400  
**Rule Title:**The system must be checked weekly for unauthorized setuid files, as well as, unauthorized modification to authorized setuid files.  
  
  
**Vulnerability Discussion:**  Files with the setuid bit set will allow anyone running these files to be temporarily assigned the UID of the file. While many system files depend on these attributes for proper operation, security problems can result if setuid is assigned to programs that allow reading and writing of files, or shell escapes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Determine if a weekly automated or manual process is used to generate a list of setuid files on the system and compare it with the prior list. If no such process is in place, this is a finding.  
  
**Fix Text:**Establish a weekly automated or manual process to generate a list of setuid files on the system and compare it with the prior list. To create a list of setuid files use the following command.  
# find / -perm -4000 > setuid-file-list     
  
**CCI:**CCI-000318  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-805  
**Group Title:** GEN002420  
**Rule ID:** SV-39813r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002420  
**Rule Title:**Removable media, remote file systems, and any file system that does not contain approved setuid files must be mounted with the "nosuid" option.  
  
  
**Vulnerability Discussion:**  The "nosuid" mount option causes the system to not execute setuid files with owner privileges. This option must be used for mounting any file system that does not contain approved setuid files. Executing setuid files from untrusted file systems, or file systems that do not contain approved setuid files, increases the opportunity for unprivileged users to attain unauthorized administrative access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/vfstab and verify the "nosuid" mount option is used on any user filesystem (such as /export/home) or filesystems mounted from removable media or network shares.  
# cat /etc/vfstab  
  
Check zfs filesystems for setuid mounts.  
#zfs get suid  
  
**Fix Text:**Use the following procedure for UFS filesystems.  
Edit /etc/vfstab and add the "nosuid" mount option to any user filesystem (such as /export/home) or filesystems mounted from removable media or network shares.   
  
Use the following procedure for ZFS filesystems.  
# zfs setuid = off < file system >     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-802  
**Group Title:** GEN002440  
**Rule ID:** SV-802r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002440  
**Rule Title:**The owner, group-owner, mode, ACL, and location of files with the setgid bit set must be documented using site-defined procedures.  
  
  
**Vulnerability Discussion:**  All files with the setgid bit set will allow anyone running these files to be temporarily assigned the GID of the file. While many system files depend on these attributes for proper operation, security problems can result if setgid is assigned to programs that allow reading and writing of files, or shell escapes.  
  
**Documentable:** YES   
**Responsibility:**  Information Assurance Officer  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Locate all setgid files on the system.  
  
Procedure:  
# find / -perm -2000  
  
If the ownership, permissions, location, and ACLs of all files with the setgid bit set are not documented, this is a finding.  
  
**Fix Text:**All files with the setgid bit set will be documented in the system baseline and authorized by the Information Systems Security Officer. Locate all setgid files with the following command.  
  
find / -perm -2000 -exec ls -lLd {} \;  
  
Ensure setgid files are part of the operating system software, documented application software, documented utility software, or documented locally developed software. Ensure none are text files or shell programs.     
  
**CCI:**CCI-000368  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-804  
**Group Title:** GEN002460  
**Rule ID:** SV-804r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002460  
**Rule Title:**The system must be checked weekly for unauthorized setgid files, as well as, unauthorized modification to authorized setgid files.  
  
  
**Vulnerability Discussion:**  Files with the setgid bit set will allow anyone running these files to be temporarily assigned the group id of the file. While many system files depend on these attributes for proper operation, security problems can result if setgid is assigned to programs that allow reading and writing of files, or shell escapes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Determine if a weekly automated or manual process is used to generate a list of setgid files on the system and compare it with the prior list. If no such process is in place, this is a finding.  
  
**Fix Text:**Establish a weekly automated or manual process to generate a list of setgid files on the system and compare it with the prior list. To create a list of setgid files use the following command.  
# find / -perm -2000 > setgid-file-list     
  
**CCI:**CCI-000318  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1010  
**Group Title:** GEN002480  
**Rule ID:** SV-1010r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002480  
**Rule Title:**Public directories must be the only world-writable directories and world-writable files must be located only in public directories.  
  
  
**Vulnerability Discussion:**  World-writable files and directories make it easy for a malicious user to place potentially compromising files on the system.  
  
The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage (e.g., /tmp) and for directories requiring global read/write access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for world-writable files and directories.  
  
Procedure:  
# find / -perm -2 -a \( -type d -o -type f \) -exec ls -ld {} \;  
  
If any world-writable files or directories are located, except those required for system operation, such as /tmp and /dev/null, this is a finding.  
  
**Fix Text:**Remove or change the mode for any world-writable file or directory on the system that is not required to be world-writable.  
  
Procedure:  
# chmod o-w <file/directory>  
  
Document all changes.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-806  
**Group Title:** GEN002500  
**Rule ID:** SV-806r2\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002500  
**Rule Title:**The sticky bit must be set on all public directories.  
  
  
**Vulnerability Discussion:**  Failing to set the sticky bit on the public directories allows unauthorized users to delete files in the directory structure.  
  
The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage (e.g., /tmp) and for directories requiring global read/write access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Verify all world-writable directories have the sticky bit set.  
  
Procedure:  
# find / -type d -perm -002 ! -perm -1000 > wwlist  
  
If the sticky bit is not set on a world-writable directory, this is a finding.  
  
**Fix Text:**Set the sticky bit on all public directories.   
  
Procedure:  
# chmod 1777 /tmp  
  
(Replace /tmp with the public directory missing the sticky bit, if necessary.)     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-807  
**Group Title:** GEN002520  
**Rule ID:** SV-807r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002520  
**Rule Title:**All public directories must be owned by root or an application account.  
  
  
**Vulnerability Discussion:**  If a public directory has the sticky bit set and is not owned by a privileged UID, unauthorized users may be able to modify files created by others.  
  
The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage (e.g., /tmp) and for directories requiring global read/write access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of all public directories.  
  
Procedure:  
# find / -type d -perm -1002 -exec ls -ld {} \;  
  
If any public directory is not owned by root or an application user, this is a finding.  
  
**Fix Text:**Change the owner of public directories to root or an application account.  
  
Procedure:  
# chown root /tmp  
  
(Replace root with an application user and/or /tmp with another public directory as necessary.)     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11990  
**Group Title:** GEN002540  
**Rule ID:** SV-12491r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002540  
**Rule Title:**All public directories must be group-owned by root or an application group.  
  
  
**Vulnerability Discussion:**  If a public directory has the sticky bit set and is not group-owned by a system GID, unauthorized users may be able to modify files created by others.  
  
The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage (e.g., /tmp) and for directories requiring global read/write access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of public directories.  
  
Procedure:  
# find / -type d -perm -1002 -exec ls -ld {} \;  
  
If any public directory is not group-owned by root, sys, bin, or an application group (such as mail), this is a finding.  
  
**Fix Text:**Change the group ownership of the public directory.  
  
Procedure:  
# chgrp root /tmp  
  
(Replace root with a different system group and/or /tmp with a different public directory as necessary.)     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-808  
**Group Title:** GEN002560  
**Rule ID:** SV-28641r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002560  
**Rule Title:**The system and user default umask must be 077.  
  
  
**Vulnerability Discussion:**  The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a 4-digit number, the first digit representing special access modes is typically ignored or required to be 0. This requirement applies to the globally configured system defaults and the user defaults for each account on the system.  
  
**Documentable:** YES   
**Severity Override Guidance:**   
If the default umask is 000 or does not restrict the world-writable permission, this becomes a CAT I finding.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check global configuration:  
# find /etc -type f | xargs grep -i umask               
  
Check local initialization files:  
# cut -d: -f1 /etc/passwd | xargs -n1 -iUSER sh -c "grep umask ~USER/.\*"  
  
If the system and user default umask is not 077, this a finding.  
  
Note: If the default umask is 000 or allows for the creation of world writable files this becomes a CAT I finding..  
  
**Fix Text:**Edit the /etc/default/login file for Solaris. Set the variable UMASK=077  
Edit local and global initialization files containing "umask" and change them to use 077 instead of the correct value.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-810  
**Group Title:** GEN002640  
**Rule ID:** SV-39834r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002640  
**Rule Title:**Default system accounts must be disabled or removed.  
  
  
**Vulnerability Discussion:**  Vendor accounts and software may contain backdoors allowing unauthorized access to the system. These backdoors are common knowledge and present a threat to system security if the account is not disabled.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAAC-1  
  
**Check Content:**    
Determine if default system accounts (such as, those for sys, bin, uucp, nuucp, daemon, smtp, gdm, lp, nobody) have been disabled.   
# cat /etc/shadow   
If an account's password field is "\*", "\*LK\*", "NP", or is prefixed with a "!", the account is locked or disabled. If there are any default system accounts not locked, this is a finding.  
  
**Fix Text:**Lock the default system account(s).  
# passwd -l <user>  
    
  
**CCI:**CCI-000178  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-811  
**Group Title:** GEN002660  
**Rule ID:** SV-27266r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002660  
**Rule Title:**Auditing must be implemented.  
  
  
**Vulnerability Discussion:**  Without auditing, individual system accesses cannot be tracked and malicious activity cannot be detected and traced back to an individual account.   
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Determine if auditing is enabled.  
# ps -ef |grep auditd  
If the auditd process is not found, this is a finding.  
  
**Fix Text:**Use /etc/security/bsmconv to enable auditing on the system.     
  
**CCI:**CCI-000169  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-812  
**Group Title:** GEN002680  
**Rule ID:** SV-27271r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002680  
**Rule Title:**System audit logs must be owned by root.  
  
  
**Vulnerability Discussion:**  Failure to give ownership of system audit log files to root provides the designated owner and unauthorized users with the potential to access sensitive information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECTP-1  
  
**Check Content:**    
Perform the following to determine the location of audit logs and then check the ownership.  
# more /etc/security/audit\_control  
# ls -lLa <audit log dir>  
If any audit log file is not owned by root, this is a finding.  
  
**Fix Text:**Change the ownership of the audit log file(s).  
  
Procedure:  
# chown root <audit log file>     
  
**CCI:**CCI-000162  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22702  
**Group Title:** GEN002690  
**Rule ID:** SV-27277r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002690  
**Rule Title:**System audit logs must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  Sensitive system and user information could provide a malicious user with enough information to penetrate further into the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1, ECTP-1  
  
**Check Content:**    
Determine the location of audit logs and then check the group-ownership.  
  
Procedure:  
# more /etc/security/audit\_control  
# ls -lLd <audit log dir>  
  
If any audit log file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the audit log file(s).  
  
Procedure:  
# chgrp root <audit log file>     
  
**CCI:**CCI-000162  
  
  
**CCI:**CCI-000163  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-813  
**Group Title:** GEN002700  
**Rule ID:** SV-27282r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002700  
**Rule Title:**System audit logs must have mode 0640 or less permissive.  
  
  
**Vulnerability Discussion:**  If a user can write to the audit logs, audit trails can be modified or destroyed and system intrusion may not be detected. System audit logs are those files generated from the audit system and do not include activity, error, or other log files created by application software.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECTP-1  
  
**Check Content:**    
Perform the following to determine the location of audit logs and then check the mode of the files.  
# more /etc/security/audit\_control  
# ls -lLa <audit log dir>  
If the audit log directory has a mode more permissive than 0750 or any audit log file has a mode more permissive than 0640, this is a finding.  
  
**Fix Text:**Change the mode of the audit log directories/files.  
# chmod 0750 <audit directory>  
# chmod 0640 <audit file>  
    
  
**CCI:**CCI-000163  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22369  
**Group Title:** GEN002710  
**Rule ID:** SV-26502r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002710  
**Rule Title:**All system audit files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  If a user can write to the audit logs, then audit trails can be modified or destroyed and system intrusion may not be detected.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECTP-1  
  
**Check Content:**    
Check the audit configuration to determine the location of the system audit log files.  
# more /etc/security/audit\_control  
Check the system audit log files for extended ACLs.  
# ls -la [audit log dir]  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.   
# chmod A- [audit file]     
  
**CCI:**CCI-000163  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22370  
**Group Title:** GEN002715  
**Rule ID:** SV-26505r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002715  
**Rule Title:**System audit tool executables must be owned by root.  
  
  
**Vulnerability Discussion:**  To prevent unauthorized access or manipulation of system audit logs, the tools for manipulating those logs must be protected.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the audit tool executables are owned by root.  
# ls -l /usr/sbin/auditd /usr/sbin/audit /usr/sbin/bsmrecord /usr/sbin/auditreduce /usr/sbin/praudit /usr/sbin/auditconfig  
If any listed file is not owned by root, this is a finding.  
  
  
**Fix Text:**Change the owner of the audit tool executable to root.  
# chown root [audit tool executable]     
  
**CCI:**CCI-001493  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22371  
**Group Title:** GEN002716  
**Rule ID:** SV-26508r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002716  
**Rule Title:**System audit tool executables must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  To prevent unauthorized access or manipulation of system audit logs, the tools for manipulating those logs must be protected.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the audit tool executables are group-owned by root, bin, or sys.  
  
Procedure:  
# ls -lL /usr/sbin/auditd /usr/sbin/audit /usr/sbin/bsmrecord /usr/sbin/auditreduce /usr/sbin/praudit /usr/sbin/auditconfig  
  
If any listed file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group-owner of the audit tool executable to root, bin, or sys.  
  
Procedure:  
# chgrp root <audit tool executable>     
  
**CCI:**CCI-001493  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22372  
**Group Title:** GEN002717  
**Rule ID:** SV-26511r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002717  
**Rule Title:**System audit tool executables must have mode 0750 or less permissive.  
  
  
**Vulnerability Discussion:**  To prevent unauthorized access or manipulation of system audit logs, the tools for manipulating those logs must be protected.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of audit tool executables.  
# ls -l /usr/sbin/auditd /usr/sbin/audit /usr/sbin/bsmrecord /usr/sbin/auditreduce /usr/sbin/praudit /usr/sbin/auditconfig  
If any listed file has a mode more permissive than 0750, this is a finding.  
  
**Fix Text:**Change the mode of the audit tool executable to 0750, or less permissive.  
# chmod 0750 [audit tool executable]     
  
**CCI:**CCI-001493  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22373  
**Group Title:** GEN002718  
**Rule ID:** SV-26515r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002718  
**Rule Title:**System audit tool executables must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  To prevent unauthorized access or manipulation of system audit logs, the tools for manipulating those logs must be protected.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of audit tool executables.  
# ls -l /usr/sbin/auditd /usr/sbin/audit /usr/sbin/bsmrecord /usr/sbin/auditreduce /usr/sbin/praudit /usr/sbin/auditconfig  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [audit file]     
  
**CCI:**CCI-001493  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22374  
**Group Title:** GEN002719  
**Rule ID:** SV-40562r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002719  
**Rule Title:**The audit system must alert the SA in the event of an audit processing failure.  
  
  
**Vulnerability Discussion:**  An accurate and current audit trail is essential for maintaining   
a record of system activity. If the system fails, the SA must be notified and must take prompt   
action to correct the problem.  
  
Minimally, the system must log this event and the SA will receive this notification during the   
daily system log review. If feasible, active alerting (such as email or paging) should be   
employed consistent with the site’s established operations management systems and procedures.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Verify the presence of an audit\_warn entry in /etc/mail/aliases.  
  
# grep audit\_warn /etc/mail/aliases  
  
If there is no audit\_warn entry in /etc/mail/aliases, this is a finding.  
  
**Fix Text:**Add an audit\_warn alias to /etc/mail/aliases that will forward to designated system administrator(s).  
  
# vi /etc/mail/aliases  
  
Put the updated aliases file into service.  
  
# newaliases     
  
**CCI:**CCI-000139  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-814  
**Group Title:** GEN002720  
**Rule ID:** SV-27287r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002720  
**Rule Title:**The audit system must be configured to audit failed attempts to access files and programs.  
  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the system audit configuration to determine if failed attempts to access files and programs are audited.  
# more /etc/security/audit\_control  
If flags -fr or fr are not configured, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit\_control and add the fr or -fr flags to the flags list.  
Load the new audit configuration.  
# auditconfig -conf     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22375  
**Group Title:** GEN002730  
**Rule ID:** SV-40564r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002730  
**Rule Title:**The audit system must alert the SA when the audit storage volume approaches its capacity.  
  
  
**Vulnerability Discussion:**  An accurate and current audit trail is essential for maintaining a record of system activity. If the system fails, the SA must be notified and must take prompt action to correct the problem.  
  
Minimally, the system must log this event and the SA will receive this notification during the daily system log review. If feasible, active alerting (such as email or paging) should be employed consistent with the site’s established operations management systems and procedures.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the presence of an audit\_warn entry in /etc/mail/aliases.  
  
# grep audit\_warn /etc/mail/aliases  
  
If there is no audit\_warn entry in /etc/mail/aliases, this is a finding.  
  
Verify the minfree parameter in /etc/security/audit\_control.  
  
# egrep '^minfree:' /etc/security/audit\_control  
  
If the minfree parameter is set to zero or not set at all, this is a finding.  
  
**Fix Text:**If necessary, add an audit\_warn alias to /etc/mail/aliases that will forward to designated system administrator(s).  
  
# vi /etc/mail/aliases  
  
Put the updated aliases file into service.  
  
# newaliases  
  
If necessary, add or update the minfree: parameter in /etc/security/audit\_control.   
  
# vi /etc/security/audit\_control  
  
Ensure the minfree value is greater than zero and less than 100.     
  
**CCI:**CCI-000143  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-815  
**Group Title:** GEN002740  
**Rule ID:** SV-27292r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002740  
**Rule Title:**The audit system must be configured to audit file deletions.  
  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
# grep flags /etc/security/audit\_control   
Confirm flags fd or +fd and -fd are configured.  
  
**Fix Text:**Edit /etc/security/audit\_control and add the fd to the flags list.  
Load the new audit configuration.  
# auditconfig -conf     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22376  
**Group Title:** GEN002750  
**Rule ID:** SV-40605r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002750  
**Rule Title:**The audit system must be configured to audit account creation.  
  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises, and damages incurred during a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Check the system's audit configuration.  
  
# grep ua /etc/security/audit\_control  
  
If the ua flag is not set, and both the +ua and -ua flags are not set, this is a finding.  
If the ua naflag is not set, and both the +ua and -ua naflags are not set, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit\_control and add ua to the flags list and naflags list.  
Refresh auditd.  
# svcadm refresh auditd     
  
**CCI:**CCI-000018  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22377  
**Group Title:** GEN002751  
**Rule ID:** SV-40607r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002751  
**Rule Title:**The audit system must be configured to audit account modification.  
  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Check the system's audit configuration.  
  
# grep ua /etc/security/audit\_control  
  
If the ua flag is not set, and both the +ua and -ua flags are not set, this is a finding.  
If the ua naflag is not set, and both the +ua and -ua naflags are not set, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit\_control and add ua to the flags list and naflags list.  
Refresh auditd.  
# svcadm refresh auditd     
  
**CCI:**CCI-001403  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22378  
**Group Title:** GEN002752  
**Rule ID:** SV-40610r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002752  
**Rule Title:**The audit system must be configured to audit account disabling.  
  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Check the system's audit configuration.  
  
# grep ua /etc/security/audit\_control  
  
If the ua flag is not set, and both the +ua and -ua flags are not set, this is a finding.  
If the ua naflag is not set, and both the +ua and -ua naflags are not set, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit\_control and add ua to the flags list and naflags list.  
Refresh auditd.  
# svcadm refresh auditd     
  
**CCI:**CCI-001404  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22382  
**Group Title:** GEN002753  
**Rule ID:** SV-40611r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002753  
**Rule Title:**The audit system must be configured to audit account termination.  
  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Check the system's audit configuration.  
  
# grep ua /etc/security/audit\_control  
  
If the ua flag is not set, and both the +ua and -ua flags are not set, this is a finding.  
If the ua naflag is not set, and both the +ua and -ua naflags are not set, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit\_control and add ua to the flags list and naflags list.  
Refresh auditd.  
# svcadm refresh auditd     
  
**CCI:**CCI-001405  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-816  
**Group Title:** GEN002760  
**Rule ID:** SV-27298r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760  
**Rule Title:**The audit system must be configured to audit all administrative, privileged, and security actions.  
  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the auditing configuration of the system.  
# grep flags /etc/security/audit\_control  
If the am flag is not present, and either of the -am or +am flags is not present, this is a finding.  
  
  
**Fix Text:**Edit /etc/security/audit\_control and add am to the flags list.  
Load the new audit configuration.  
# auditconfig -conf     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-818  
**Group Title:** GEN002800  
**Rule ID:** SV-27303r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002800  
**Rule Title:**The audit system must be configured to audit login, logout, and session initiation.  
  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the system's audit configuration.  
  
# grep lo /etc/security/audit\_control  
  
If the lo flag is not set, and both the +lo and -lo flags are not set, this is a finding.  
If the lo naflag is not set, and both the +lo and -lo naflags are not set, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit\_control and add lo to the flags list and naflags list.  
Load the new audit configuration.  
# auditconfig -conf     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-819  
**Group Title:** GEN002820  
**Rule ID:** SV-27309r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820  
**Rule Title:**The audit system must be configured to audit all discretionary access control permission modifications.  
  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the system's audit configuration.  
# grep flags /etc/security/audit\_control  
Confirm flags fm or +fm and -fm are configured.  
  
  
**Fix Text:**Edit /etc/security/audit\_control and add fm to the flags list.  
Load the new audit configuration.  
# auditconfig -conf     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22383  
**Group Title:** GEN002825  
**Rule ID:** SV-26524r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002825  
**Rule Title:**The audit system must be configured to audit the loading and unloading of dynamic kernel modules.  
  
  
**Vulnerability Discussion:**  Actions concerning dynamic kernel modules must be recorded as they are substantial events. Dynamic kernel modules can increase the attack surface of a system. A malicious kernel module can be used to substantially alter the functioning of a system, often with the purpose of hiding a compromise from the SA.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1  
  
**Check Content:**    
Check /etc/security/audit\_control file.   
# grep flags /etc/security/audit\_control  
If the as element is missing from the flags line, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit\_control and add the as flag to the flag parameter.     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4357  
**Group Title:** GEN002860  
**Rule ID:** SV-4357r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002860  
**Rule Title:**Audit logs must be rotated daily.  
  
  
**Vulnerability Discussion:**  Rotate audit logs daily to preserve audit file system space and to conform to the DoD/DISA requirement. If it is not rotated daily and moved to another location, then there is more of a chance for the compromise of audit data by malicious users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for any crontab entries that rotate audit logs.  
Procedure:  
# crontab -l  
If such a cron job is found, this is not a finding.  
  
Otherwise, query the SA. If there is a process automatically rotating audit logs, this is not a finding. If the SA manually rotates audit logs, this is still a finding, because if the SA is not there, it will not be accomplished. If the audit output is not archived daily, to tape or disk, this is a finding. This can be ascertained by looking at the audit log directory and, if more than one file is there, or if the file does not have today's date, this is a finding.  
  
**Fix Text:**Configure a cron job or other automated process to rotate the audit logs on a daily basis.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24357  
**Group Title:** GEN002870  
**Rule ID:** SV-39881r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002870  
**Rule Title:**The system must be configured to send audit records to a remote audit server.  
  
  
**Vulnerability Discussion:**  Audit records contain evidence that can be used in the investigation of compromised systems. To prevent this evidence from compromise, it must be sent to a separate system continuously. Methods for sending audit records include, but are not limited to, system audit tools used to send logs directly to another host or through the system's syslog service to another host.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECTB-1  
  
**Check Content:**    
Audit records may be sent to a remote server in two ways, via an NFS mount of the audit directory, or via the audit\_syslog plugin (if available).  
  
NFS:  
Check the "dir" parameter in /etc/security/audit\_control. If the directory is on an NFS mount to a remote server, there is no finding.  
  
SYSLOG:  
Check the "plugin" parameter in /etc/security/audit\_control. Confirm that the audit\_syslog.so\* plugin is listed with "p\_flags=all".  
# grep audit\_syslog.so /etc/security/audit\_control  
Check that syslogd is sending messages to a remote server (GEN005450):  
# grep '@' /etc/syslog.conf | grep -v '^#'  
If both auditd is configured to send audit records to syslog, and syslogd is configured to send messages to a remote server, there is no finding.  
  
If auditd is saving audit records on a local directory, and audit records are not being sent to a remote server via syslog, this is a finding.   
  
**Fix Text:**Update the /etc/security/audit\_control file to save audit records to a remote NFS mount.  
  
dir:<remote NFS directory>  
  
OR  
  
If the /usr/lib/security/audit\_syslog.so\* exists, update the /etc/security/audit\_control file to send all audit records to syslog and update /etc/syslog.conf to send all audit messages to a remote server.  
  
/etc/security/audit\_control:  
plugin:name=audit\_syslog.so.1: p\_flags=all  
  
/etc/syslog.conf:  
audit.\* @<remote syslog server>     
  
**CCI:**CCI-000136  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-974  
**Group Title:** GEN002960  
**Rule ID:** SV-27317r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002960  
**Rule Title:**Access to the cron utility must be controlled using the cron.allow and/or cron.deny file(s).  
  
  
**Vulnerability Discussion:**  The cron facility allows users to execute recurring jobs on a regular and unattended basis. The cron.allow file designates accounts allowed to enter and execute jobs using the cron facility. If neither cron.allow nor cron.deny exists, then any account may use the cron facility. This may open the facility up for abuse by system intruders and malicious users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check for the existence of the cron.allow and cron.deny files.  
# ls -lL /etc/cron.d/cron.allow  
# ls -lL /etc/cron.d/cron.deny  
If neither file exists, this is a finding.  
  
**Fix Text:**Create /etc/cron.d/cron.allow and/or /etc/cron.d/cron.deny with appropriate content.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-975  
**Group Title:** GEN002980  
**Rule ID:** SV-27323r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002980  
**Rule Title:**The cron.allow file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  A cron.allow file that is readable and/or writable by other than root could allow potential intruders and malicious users to use the file contents to help discern information, such as who is allowed to execute cron programs, which could be harmful to overall system and network security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check mode of the cron.allow file.  
  
Procedure:  
# ls -lL /etc/cron.d/cron.allow  
  
If either file has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the cron.allow file to 0600.  
  
Procedure:  
# chmod 0600 /etc/cron.d/cron.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22384  
**Group Title:** GEN002990  
**Rule ID:** SV-26528r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002990  
**Rule Title:**The cron.allow file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  A cron.allow file that is readable and/or writable by other than root could allow potential intruders and malicious users to use the file contents to help discern information, such as who is allowed to execute cron programs, which could be harmful to overall system and network security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the cron.allow file.  
# ls -l /etc/cron.allow  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/cron.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-976  
**Group Title:** GEN003000  
**Rule ID:** SV-27329r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003000  
**Rule Title:**Cron must not execute group-writable or world-writable programs.  
  
  
**Vulnerability Discussion:**  If cron executes group-writable or world-writable programs, there is a possibility that unauthorized users could manipulate the programs with malicious intent. This could compromise system and network security.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List all cronjobs on the system.   
Procedure:   
# ls /var/spool/cron/crontabs/  
  
If cron jobs exist under any of the above directories search for programs executed by cron.  
Procedure:  
# more <cron job file>  
  
Determine if the file is group-writable or world-writable.  
Procedure:  
# ls -la <cron program file>  
  
If cron executes group-writable or world-writable files, this is a finding.  
  
**Fix Text:**Remove the world-writable and group-writable permissions from the cron program file(s) identified.  
# chmod go-w <cron program file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-977  
**Group Title:** GEN003020  
**Rule ID:** SV-27331r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003020  
**Rule Title:**Cron must not execute programs in, or subordinate to, world-writable directories.  
  
  
**Vulnerability Discussion:**  If cron programs are located in or subordinate to world-writable directories, they become vulnerable to removal and replacement by malicious users or system intruders.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List all cronjobs on the system.  
Procedure:  
# ls /var/spool/cron/crontabs/  
  
If cron jobs exist under any of the above directories search for programs executed by cron.  
Procedure:  
# more <cron job file>  
  
Determine if the directory containing programs executed from cron is world-writable.  
Procedure:  
# ls -ld <cron program directory>  
  
If cron executes programs in world-writable directories, this is a finding.  
  
**Fix Text:**Remove the world-writable permission from the cron program directories identified.  
  
Procedure:  
# chmod o-w <cron program directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11994  
**Group Title:** GEN003040  
**Rule ID:** SV-27333r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003040  
**Rule Title:**Crontabs must be owned by root or the crontab creator.  
  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and prevent malicious modification to these jobs, crontab files must be secured.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List all crontabs on the system.   
# ls -lL /var/spool/cron/crontabs/  
  
If any crontab is not owned by root or the creating user, this is a finding.  
  
**Fix Text:**Change the crontab owner to root or the crontab creator.  
# chown root <crontab file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22385  
**Group Title:** GEN003050  
**Rule ID:** SV-41044r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003050  
**Rule Title:**Crontab files must be group-owned by root, sys, or the crontab creator's primary group.  
  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and prevent malicious modification to these jobs, crontab files must be secured.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the crontab files.  
# ls -lL /var/spool/cron/crontabs/  
If the group owner is not root, sys, or the crontab owner's primary group, this is a finding.  
  
**Fix Text:**Change the group owner of the crontab file to root, sys, or the crontab's primary group.  
Procedure:  
# chgrp root [crontab file]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11995  
**Group Title:** GEN003060  
**Rule ID:** SV-27335r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003060  
**Rule Title:**Default system accounts (with the exception of root) must not be listed in the cron.allow file or must be included in the cron.deny file, if cron.allow does not exist.  
  
  
**Vulnerability Discussion:**  To centralize the management of privileged account crontabs, of the default system accounts, only root may have a crontab.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Check the cron.allow and cron.deny files for the system.  
# more /etc/cron.d/cron.allow  
# more /etc/cron.d/cron.deny  
If a default system account (such as bin, sys, adm, or others) is listed in the cron.allow file, or not listed in the cron.deny file if no cron.allow file exists, this is a finding.  
  
**Fix Text:**Remove default system accounts (such as bin, sys, adm, or others) from the cron.allow file if it exists, or add those accounts to the cron.deny file.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-978  
**Group Title:** GEN003080  
**Rule ID:** SV-27340r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003080  
**Rule Title:**Crontab files must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and prevent malicious modification to these jobs, crontab files must be secured.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the crontab files.  
# ls -lL /var/spool/cron/crontabs/  
If any crontab file has a mode more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the crontab files.  
# chmod 0600 /var/spool/cron/crontabs/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22386  
**Group Title:** GEN003090  
**Rule ID:** SV-26534r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003090  
**Rule Title:**Crontab files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and to prevent malicious modification to these jobs, crontab files must be secured. ACLs on crontab files may provide unauthorized access to the files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the crontab files.  
# ls -lL /var/spool/cron/crontabs/  
  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [crontab file]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-979  
**Group Title:** GEN003100  
**Rule ID:** SV-27342r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003100  
**Rule Title:**Cron and crontab directories must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and to prevent malicious modification to these jobs, crontab files must be secured.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the crontab directory.  
# ls -ld /var/spool/cron/crontabs  
If the mode of the crontab directory is more permissive than 0755, this is a finding.  
  
  
**Fix Text:**Change the mode of the crontab directory.  
# chmod 0755 /var/spool/cron/crontabs     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22387  
**Group Title:** GEN003110  
**Rule ID:** SV-26538r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003110  
**Rule Title:**Cron and crontab directories must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and to prevent malicious modification to these jobs, crontab files must be secured. ACLs on cron and crontab directories may provide unauthorized access to these directories. Unauthorized modifications to these directories or their contents may result in the addition of unauthorized cron jobs or deny service to authorized cron jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the crontab directories.  
# ls -ld /var/spool/cron/crontabs/  
  
If the permissions include a "+", the directory has an extended ACL and this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the directory.  
# chmod A- /var/spool/cron/crontabs/     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-980  
**Group Title:** GEN003120  
**Rule ID:** SV-27345r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003120  
**Rule Title:**Cron and crontab directories must be owned by root or bin.  
  
  
**Vulnerability Discussion:**  Incorrect ownership of the cron or crontab directories could permit unauthorized users the ability to alter cron jobs and run automated jobs as privileged users. Failure to give ownership of cron or crontab directories to root or to bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the owner of the crontab directory.  
# ls -ld /var/spool/cron/crontabs  
If the owner of the crontab directory is not root or bin, this is a finding.  
  
  
**Fix Text:**Change the owner of the crontab directory.  
# chown root /var/spool/cron/crontabs     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-981  
**Group Title:** GEN003140  
**Rule ID:** SV-27347r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003140  
**Rule Title:**Cron and crontab directories must be group-owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and to prevent malicious modification to these jobs, crontab files must be secured. Failure to give group-ownership of cron or crontab directories to a system group provides the designated group and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group owner of the crontab directories.  
  
Procedure:  
# ls -ld /var/spool/cron/crontabs  
  
If the directory is not group-owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the group owner of the crontab directories to root, sys, or bin.  
  
Procedure:  
# chgrp root /var/spool/cron/crontabs     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-982  
**Group Title:** GEN003160  
**Rule ID:** SV-27349r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003160  
**Rule Title:**Cron logging must be implemented.  
  
  
**Vulnerability Discussion:**  Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
# ls -lL /var/cron/log  
If this file does not exist, or is older than the last cron job, this is a finding.  
# more /etc/default/cron  
If a CRONLOG=YES line does not exist, this is a finding.  
  
**Fix Text:**Edit /etc/default/cron and set CRONLOG=YES.     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-983  
**Group Title:** GEN003180  
**Rule ID:** SV-27354r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003180  
**Rule Title:**The cronlog file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  Cron logs contain reports of scheduled system activities and must be protected from unauthorized access or manipulation.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1, ECTP-1  
  
**Check Content:**    
Check the mode of the cron log file.  
# ls -lL /var/cron/log  
If the mode is more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the cron log file.  
# chmod 0600 /var/cron/log  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22388  
**Group Title:** GEN003190  
**Rule ID:** SV-26542r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003190  
**Rule Title:**The cron log files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Cron logs contain reports of scheduled system activities and must be protected from unauthorized access or manipulation.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1, ECTP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /var/cron/log  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /var/cron/log     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4358  
**Group Title:** GEN003200  
**Rule ID:** SV-27359r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003200  
**Rule Title:**The cron.deny file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  If file permissions for cron.deny are more permissive than 0600, sensitive information could be viewed or edited by unauthorized users.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the cron.deny file.  
# ls -lL /etc/cron.d/cron.deny  
If the cron.deny file is more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the cron.deny file.  
# chmod 0600 /etc/cron.d/cron.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22389  
**Group Title:** GEN003210  
**Rule ID:** SV-26546r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003210  
**Rule Title:**The cron.deny file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  If file permissions for cron.deny are more permissive than 0700, sensitive information could be viewed or edited by unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/cron.d/cron.deny  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/cron.d/cron.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4360  
**Group Title:** GEN003220  
**Rule ID:** SV-27364r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003220  
**Rule Title:**Cron programs must not set the umask to a value less restrictive than 077.  
  
  
**Vulnerability Discussion:**  The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask is often represented as a 4-digit octal number, the first digit representing special access modes is typically ignored or required to be 0.  
  
**Documentable:** YES   
**Severity Override Guidance:**   
If a cron program sets the umask to 000 or does not restrict the world-writable permission, this becomes a CAT I finding.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Determine if there are any crontabs by viewing a long listing of the directory. If there are crontabs, examine them to determine what cron jobs exist. Check for any programs specifying an umask.  
  
# ls -lL /var/spool/cron/crontabs  
# cat <crontab file>  
# grep umask <cron program>  
  
If there are no cron jobs present, this vulnerability is not applicable. If any cron job contains an umask value more permissive than 077, this is a finding.  
  
**Fix Text:**Edit cron script files and modify the umask to 077.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4361  
**Group Title:** GEN003240  
**Rule ID:** SV-27366r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003240  
**Rule Title:**The cron.allow file must be owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the owner of the cron.allow file is not set to root, bin, or sys, the possibility exists for an unauthorized user to view or to edit sensitive information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /etc/cron.d/cron.allow  
If the cron.allow file is not owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**# chown root /etc/cron.d/cron.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22390  
**Group Title:** GEN003245  
**Rule ID:** SV-26550r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003245  
**Rule Title:**The at.allow file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files. Unauthorized modification of the at.allow file could result in Denial of Service to authorized at users and the granting of the ability to run at jobs to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/cron.d/at.allow  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/cron.d/at.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22391  
**Group Title:** GEN003250  
**Rule ID:** SV-26553r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003250  
**Rule Title:**The cron.allow file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the group of the cron.allow is not set to root, bin, or sys, the possibility exists for an unauthorized user to view or edit the list of users permitted to use cron. Unauthorized modification of this file could cause Denial of Service to authorized cron users or provide unauthorized users with the ability to run cron jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the file.  
  
Procedure:  
# ls -lL /etc/cron.d/cron.allow  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the file.  
  
Procedure:  
# chgrp root /etc/cron.d/cron.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22392  
**Group Title:** GEN003252  
**Rule ID:** SV-26556r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003252  
**Rule Title:**The at.deny file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  The at daemon control files restrict access to scheduled job manipulation and must be protected. Unauthorized modification of the at.deny file could result in Denial of Service to authorized at users or provide unauthorized users with the ability to run at jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/cron.d/at.deny  
If the file has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the file.  
# chmod 0600 /etc/cron.d/at.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22393  
**Group Title:** GEN003255  
**Rule ID:** SV-26560r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003255  
**Rule Title:**The at.deny file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  The "at" daemon control files restrict access to scheduled job manipulation and must be protected. Unauthorized modification of the at.deny file could result in Denial of Service to authorized "at" users or provide unauthorized users with the ability to run "at" jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/cron.d/at.deny  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/cron.d/at.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4430  
**Group Title:** GEN003260  
**Rule ID:** SV-27371r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003260  
**Rule Title:**The cron.deny file must be owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  Cron daemon control files restrict the scheduling of automated tasks and must be protected.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the cron.deny file.  
  
# ls -lL /etc/cron.d/cron.deny  
If the cron.deny file is not owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the ownership of the cron.deny file to root, sys, or bin.  
  
# chown root /etc/cron.d/cron.deny  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22394  
**Group Title:** GEN003270  
**Rule ID:** SV-26563r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003270  
**Rule Title:**The cron.deny file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  Cron daemon control files restrict the scheduling of automated tasks and must be protected. Unauthorized modification of the cron.deny file could result in Denial of Service to authorized cron users or could provide unauthorized users with the ability to run cron jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the file.  
  
Procedure:  
# ls -lL /etc/cron.d/cron.deny  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the file to root, sys, or bin.  
  
Procedure:  
# chgrp root /etc/cron.d/cron.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-984  
**Group Title:** GEN003280  
**Rule ID:** SV-27376r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003280  
**Rule Title:**Access to the at utility must be controlled via the at.allow and/or at.deny file(s).  
  
  
**Vulnerability Discussion:**  The at facility selectively allows users to execute jobs at deferred times. It is usually used for one-time jobs. The at.allow file selectively allows access to the at facility. If there is no at.allow file, there is no ready documentation of who is allowed to submit at jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check for the existence of at.allow and at.deny files.  
# ls -lL /etc/cron.d/at.allow  
# ls -lL /etc/cron.d/at.deny  
If neither file exists, this is a finding.  
  
  
**Fix Text:**Create at.allow and/or at.deny files containing appropriate lists of users to be allowed or denied access to the "at" daemon.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-985  
**Group Title:** GEN003300  
**Rule ID:** SV-27380r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003300  
**Rule Title:**The at.deny file must not be empty if it exists.  
  
  
**Vulnerability Discussion:**  On some systems, if there is no at.allow file and there is an empty at.deny file, then the system assumes everyone has permission to use the at facility. This could create an insecure setting in the case of malicious users or system intruders.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# more /etc/cron.d/at.deny  
If the at.deny file exists and is empty, this is a finding.  
  
**Fix Text:**Add appropriate users to the at.deny file, or remove the empty at.deny file if an at.allow file exists.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-986  
**Group Title:** GEN003320  
**Rule ID:** SV-27384r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003320  
**Rule Title:**Default system accounts (with the exception of root) must not be listed in the at.allow file or must be included in the at.deny file if the at.allow file does not exist.  
  
  
**Vulnerability Discussion:**  Default accounts, such as bin, sys, adm, uucp, daemon, and others, should never have access to the at facility. This would create a possible vulnerability open to intruders or malicious users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
# more /etc/cron.d/at.allow  
If default accounts (such as bin, sys, adm, and others) are listed in the at.allow file, this is a finding.  
  
  
**Fix Text:**Remove the default accounts (such as bin, sys, adm, and others) from the at.allow file.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-987  
**Group Title:** GEN003340  
**Rule ID:** SV-27388r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003340  
**Rule Title:**The at.allow file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  Permissions more permissive than 0600 (read and write for the owner) may allow unauthorized or malicious access to the at.allow and/or at.deny files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the at.allow file.  
# ls -lL /etc/cron.d/at.allow  
If the at.allow file has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the at.allow file.  
# chmod 0600 /etc/cron.d/at.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-988  
**Group Title:** GEN003360  
**Rule ID:** SV-40411r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003360  
**Rule Title:**The "at" daemon must not execute group-writable or world-writable programs.  
  
  
**Vulnerability Discussion:**  If the "at" facility executes world-writable or group-writable programs, it is possible for the programs to be accidentally or maliciously changed or replaced without the owner's intent or knowledge. This would cause a system security breach.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List the "at" jobs on the system.  
Procedure:  
# ls -la /var/spool/cron/atjobs  
  
For each "at" job file, determine which programs are executed.  
Procedure:  
# more <at job file>  
  
Check each program executed by "at" for group- or world-writable permissions.  
Procedure:  
# ls -la <at program file>  
  
If "at" executes group- or world-writable programs, this is a finding.  
  
**Fix Text:**Remove group-write and world-write permissions from files executed by "at" jobs.  
Procedure:  
# chmod go-w <file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-989  
**Group Title:** GEN003380  
**Rule ID:** SV-40412r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003380  
**Rule Title:**The "at" daemon must not execute programs in, or subordinate to, world-writable directories.  
  
  
**Vulnerability Discussion:**  If "at" programs are located in or subordinate to world-writable directories, they become vulnerable to removal and replacement by malicious users or system intruders.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List any "at" jobs on the system.  
Procedure:  
# ls /var/spool/cron/atjobs  
  
For each "at" job, determine which programs are executed.  
Procedure:  
# more <at job file>  
  
Check the directory containing each program executed by "at" for world-writable permissions.  
Procedure:  
# ls -la <at program file directory>  
  
If "at" executes programs in world-writable directories, this is a finding.  
  
**Fix Text:**Remove the world-writable permission from directories containing programs executed by "at".  
  
Procedure:  
# chmod o-w <at program directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4364  
**Group Title:** GEN003400  
**Rule ID:** SV-40391r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003400  
**Rule Title:**The "at" directory must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  If the "at" directory has a mode more permissive than 0755, unauthorized users could be allowed to view or to edit files containing sensitive information within the "at" directory. Unauthorized modifications could result in Denial of Service to authorized "at" jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the "at" directory.  
  
Procedure:  
# ls -ld /var/spool/cron/atjobs  
  
If the directory mode is more permissive than 0755, this is a finding.  
  
**Fix Text:**Change the mode of the "at" directory to 0755.  
  
Procedure:  
# chmod 0755 < at directory >     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22395  
**Group Title:** GEN003410  
**Rule ID:** SV-26566r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003410  
**Rule Title:**The "at" directory must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  If the "at" directory has an extended ACL, unauthorized users could be allowed to view or to edit files containing sensitive information within the "at" directory. Unauthorized modifications could result in Denial of Service to authorized "at" jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the directory.  
# ls -lLd /var/spool/cron/atjobs  
If the permissions include a "+", the directory has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /var/spool/cron/atjobs     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4365  
**Group Title:** GEN003420  
**Rule ID:** SV-39886r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003420  
**Rule Title:**The "at" directory must be owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the owner of the "at" directory is not root, bin, or sys, unauthorized users could be allowed to view or edit files containing sensitive information within the directory.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the "at" directory.  
  
Procedure:  
# ls -ld /var/spool/cron/atjobs   
  
If the directory is not owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the owner of the "at" directory to root, bin, or sys.  
  
Procedure:  
# chown root /var/spool/cron/atjobs     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22396  
**Group Title:** GEN003430  
**Rule ID:** SV-40414r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003430  
**Rule Title:**The "at" directory must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the "at" directory's group owner is not root, bin, or sys, unauthorized users could be allowed to view or edit files containing sensitive information within the directory.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the "at" directory.  
  
Procedure:  
# ls -lLd /var/spool/cron/atjobs  
  
If the "at" directory is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the "at" directory to root, bin, or sys.  
  
Procedure:  
# chgrp sys /var/spool/cron/atjobs     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4366  
**Group Title:** GEN003440  
**Rule ID:** SV-40416r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003440  
**Rule Title:**"At" jobs must not set the umask to a value less restrictive than 077.  
  
  
**Vulnerability Discussion:**  The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask is often represented as a 4-digit number, the first digit representing special access modes is typically ignored or required to be 0.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Determine what "at" jobs exist on the system.  
Procedure:  
# ls /var/spool/cron/atjobs  
  
If there are no "at" jobs present, this is not applicable.  
  
Determine if any of the "at" jobs or any scripts referenced execute the umask command. Check for any umask setting more permissive than 077.  
  
# grep umask <at job or referenced script>  
  
If any "at" job or referenced script sets umask to a value more permissive than 077, this is a finding.  
  
**Fix Text:**Edit "at" jobs or referenced scripts to remove umask commands setting umask to a value less restrictive than 077.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4367  
**Group Title:** GEN003460  
**Rule ID:** SV-27392r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003460  
**Rule Title:**The at.allow file must be owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the owner of the at.allow file is not set to root, bin, or sys, unauthorized users could be allowed to view or edit sensitive information contained within the file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /etc/cron.d/at.allow  
If the at.allow file is not owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the owner of the at.allow file.  
# chown root /etc/cron.d/at.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22397  
**Group Title:** GEN003470  
**Rule ID:** SV-26570r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003470  
**Rule Title:**The at.allow file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the group owner of the at.allow file is not set to root, bin, or sys, unauthorized users could be allowed to view or edit the list of users permitted to run at jobs. Unauthorized modification could result in Denial of Service to authorized at users or provide unauthorized users with the ability to run at jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the file.  
  
Procedure:  
# ls -lL /etc/cron.d/at.allow  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the file.  
  
Procedure:  
# chgrp root /etc/cron.d/at.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4368  
**Group Title:** GEN003480  
**Rule ID:** SV-27396r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003480  
**Rule Title:**The at.deny file must be owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the owner of the at.deny file is not set to root, bin, or sys, unauthorized users could be allowed to view or edit sensitive information contained within the file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /etc/cron.d/at.deny  
If the at.deny file is not owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the owner of the at.deny file.  
# chown root /etc/cron.d/at.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22398  
**Group Title:** GEN003490  
**Rule ID:** SV-26573r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003490  
**Rule Title:**The at.deny file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the group owner of the at.deny file is not set to root, bin, or sys, unauthorized users could be allowed to view or edit sensitive information contained within the file. Unauthorized modification could result in Denial of Service to authorized "at" users or provide unauthorized users with the ability to run "at" jobs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the file.  
  
Procedure:  
# ls -lL /etc/cron.d/at.deny  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the at.deny file to root, bin, or sys.  
  
Procedure:  
# chgrp root /etc/cron.d/at.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11996  
**Group Title:** GEN003500  
**Rule ID:** SV-27400r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003500  
**Rule Title:**Process core dumps must be disabled unless needed.  
  
  
**Vulnerability Discussion:**  Process core dumps contain the memory in use by the process when it crashed. Process core dump files can be of significant size and their use can result in file systems filling to capacity, which may result in Denial of Service. Process core dumps can be useful for software debugging.   
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the process core dump configuration.  
# coreadm |grep enabled  
OR  
# egrep "COREADM\_.\*\_ENABLED" /etc/coreadm.conf.  
  
If any lines are returned by coreadm or if any lines are not set to no in /etc/coreadm.conf, this is a finding.  
  
# grep coredumpsize /etc/system  
If the value is 1, this is a finding.  
  
**Fix Text:**Change the process core dump configuration.  
# coreadm -d global  
# coreadm -d process  
# coreadm -d global-setid  
# coreadm -d proc-setid  
# coreadm -d log  
  
Edit /etc/system and remove the coredumpsize parameter.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22399  
**Group Title:** GEN003501  
**Rule ID:** SV-26576r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003501  
**Rule Title:**The system must be configured to store any process core dumps in a specific, centralized directory.  
  
  
**Vulnerability Discussion:**  Specifying a centralized location for core file creation allows for the centralized protection of core files. Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If process core dump creation is not configured to use a centralized directory, core dumps may be created in a directory that does not have appropriate ownership or permissions configured, which could result in unauthorized access to the core dumps.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify a directory is defined for process core dumps.  
  
# grep COREADM\_GLOB\_PATTERN /etc/coreadm.conf  
  
If the parameter is not an absolute path (does not start with a slash [/]), this is a finding.  
  
**Fix Text:**Change the core file pattern.  
# coreadm -i /var/core/core.%f.%p     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22400  
**Group Title:** GEN003502  
**Rule ID:** SV-26579r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003502  
**Rule Title:**The centralized process core dump data directory must be owned by root.  
  
  
**Vulnerability Discussion:**  Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the centralized process core dump data directory is not owned by root, the core dumps contained in the directory may be subject to unauthorized access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the defined directory for process core dumps.  
  
# coreadm | grep "global core file pattern"  
OR  
# grep COREADM\_GLOB\_PATTERN /etc/coreadm.conf  
  
Check the ownership of the directory.  
# ls -lLd [core file directory]  
If the directory is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the core file directory.  
# chown root [core file directory]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22401  
**Group Title:** GEN003503  
**Rule ID:** SV-26582r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003503  
**Rule Title:**The centralized process core dump data directory must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the centralized process core dump data directory is not group-owned by a system group, the core dumps contained in the directory may be subject to unauthorized access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the defined directory for process core dumps.  
  
# coreadm | grep "global core file pattern"  
OR   
# grep COREADM\_GLOB\_PATTERN /etc/coreadm.conf  
  
Check the group ownership of the directory.  
# ls -lLd [core file directory]  
If the directory is not group-owned by root, this is a finding.  
  
**Fix Text:**Change the group-owner of the core file directory.  
# chgrp root [core file directory]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22402  
**Group Title:** GEN003504  
**Rule ID:** SV-26596r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003504  
**Rule Title:**The centralized process core dump data directory must have mode 0700 or less permissive.  
  
  
**Vulnerability Discussion:**  Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the process core dump data directory has a mode more permissive than 0700, unauthorized users may be able to view or to modify sensitive information contained any process core dumps in the directory.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the defined directory for process core dumps.  
  
# coreadm | grep "global core file pattern"  
OR  
# grep COREADM\_GLOB\_PATTERN /etc/coreadm.conf  
  
Check the permissions of the directory.  
# ls -lLd [core file directory]  
If the directory has a mode more permissive than 0700, this is a finding.  
  
**Fix Text:**Change the mode of the core file directory.  
# chmod 0700 [core file directory]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22403  
**Group Title:** GEN003505  
**Rule ID:** SV-26602r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003505  
**Rule Title:**The centralized process core dump data directory must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the process core dump data directory has an extended ACL, unauthorized users may be able to view or to modify sensitive information contained any process core dumps in the directory.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the defined directory for process core dumps.  
  
# coreadm | grep "global core file pattern"  
OR  
# grep COREADM\_GLOB\_PATTERN /etc/coreadm.conf  
  
Check the permissions of the directory.  
# ls -lLd [core file directory]  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the directory.  
# chmod A- [core file directory]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22404  
**Group Title:** GEN003510  
**Rule ID:** SV-26605r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003510  
**Rule Title:**Kernel core dumps must be disabled unless needed.  
  
  
**Vulnerability Discussion:**  Kernel core dumps may contain the full contents of system memory at the time of the crash. Kernel core dumps may consume a considerable amount of disk space and may result in Denial of Service by exhausting the available space on the target file system. The kernel core dump process may increase the amount of time a system is unavailable due to a crash. Kernel core dumps can be useful for kernel debugging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify savecore is not used.  
# dumpadm | grep 'Savecore enabled'  
If the value is true, this is a finding.  
  
OR  
  
# grep DUMPADM\_ENABLE /etc/dumpadm.conf  
If the value is yes, this is a finding.  
  
**Fix Text:**Disable savecore.  
# dumpadm -n     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11997  
**Group Title:** GEN003520  
**Rule ID:** SV-27407r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003520  
**Rule Title:**The kernel core dump data directory must be owned by root.  
  
  
**Vulnerability Discussion:**  Kernel core dumps may contain the full contents of system memory at the time of the crash. As the system memory may contain sensitive information, it must be protected accordingly. If the kernel core dump data directory is not owned by root, the core dumps contained in the directory may be subject to unauthorized access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the kernel core dump data directory.  
  
# ls -ld /var/crash  
OR  
# ls -ld `grep DUMPADM\_SAVDIR /etc/dumpadm.conf | cut -d= -f2`  
  
If the kernel core dump data directory is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the kernel core dump data directory to root.   
# chown root /var/crash     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22405  
**Group Title:** GEN003521  
**Rule ID:** SV-26610r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003521  
**Rule Title:**The kernel core dump data directory must be group-owned by root.  
  
  
**Vulnerability Discussion:**  Kernel core dumps may contain the full contents of system memory at the time of the crash. As the system memory may contain sensitive information, it must be protected accordingly. If the kernel core dump data directory is not group-owned by a system group, the core dumps contained in the directory may be subject to unauthorized access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine the kernel core dump data directory.   
  
# dumpadm | grep "Savecore directory"  
OR  
# grep DUMPADM\_SAVDIR /etc/dumpadm.conf  
  
Check ownership of the core dump data directory.  
# ls -l [savecore directory]  
If the directory is not group-owned by root, this is a finding.  
  
**Fix Text:**Change the group-owner of the kernel core dump data directory.  
# chgrp root [kernel core dump data directory]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22406  
**Group Title:** GEN003522  
**Rule ID:** SV-26614r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003522  
**Rule Title:**The kernel core dump data directory must have mode 0700 or less permissive.  
  
  
**Vulnerability Discussion:**  Kernel core dumps may contain the full contents of system memory at the time of the crash. As the system memory may contain sensitive information, it must be protected accordingly. If the mode of the kernel core dump data directory is more permissive than 0700, unauthorized users may be able to view or to modify kernel core dump data files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine the kernel core dump data directory.   
  
# dumpadm | grep "Savecore directory"  
OR  
# grep DUMPADM\_SAVDIR /etc/dumpadm.conf  
  
Check the permissions of the kernel core dump data directory.  
# ls -l [savecore directory]  
If the directory has a mode more permissive than 0700, this is a finding.  
  
**Fix Text:**Change the group-owner of the kernel core dump data directory.  
# chmod 0700 [kernel core dump data directory]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22407  
**Group Title:** GEN003523  
**Rule ID:** SV-26618r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003523  
**Rule Title:**The kernel core dump data directory must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Kernel core dumps may contain the full contents of system memory at the time of the crash. As the system memory may contain sensitive information, it must be protected accordingly. If there is an extended ACL for the kernel core dump data directory, unauthorized users may be able to view or to modify kernel core dump data files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine the kernel core dump data directory.  
  
# dumpadm | grep "Savecore directory"  
OR  
# grep DUMPADM\_SAVDIR /etc/dumpadm.conf  
  
Check the kernel core dump data directory permissions.  
# ls -ld [savecore directory]  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [kernel core dump directory]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11999  
**Group Title:** GEN003540  
**Rule ID:** SV-27412r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003540  
**Rule Title:**The system must implement non-executable program stacks.  
  
  
**Vulnerability Discussion:**  A common type of exploit is the stack buffer overflow. An application receives, from an attacker, more data than it is prepared for and stores this information on its stack, writing beyond the space reserved for it. This can be designed to cause execution of the data written on the stack. One mechanism to mitigate this vulnerability is for the system to not allow the execution of instructions in sections of memory identified as part of the stack.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2, ECSC-1  
  
**Check Content:**    
Determine if the system implements non-executable program stacks.  
# grep noexec\_user\_stack /etc/system  
If the noexec\_user\_stack is not set to 1, this is a finding.  
  
**Fix Text:**Edit /etc/system and set the noexec\_user\_stack parameter to 1. Restart the system for the setting to take effect.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12001  
**Group Title:** GEN003580  
**Rule ID:** SV-27416r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003580  
**Rule Title:**The system must use initial TCP sequence numbers most resistant to sequence number guessing attacks.  
  
  
**Vulnerability Discussion:**  One use of initial TCP sequence numbers is to verify bidirectional communication between two hosts, which provides some protection against spoofed source addresses being used by the connection originator. If the initial TCP sequence numbers for a host can be determined by an attacker, it may be possible to establish a TCP connection from a spoofed source address without bidirectional communication.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# grep "TCP\_STRONG\_ISS=2" /etc/default/inetinit  
If this variable is not set, this is a finding.  
  
**Fix Text:**Edit /etc/default/inetinit and set the TCP\_STRONG\_ISS parameter to 2.     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12002  
**Group Title:** GEN003600  
**Rule ID:** SV-27420r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003600  
**Rule Title:**The system must not forward IPv4 source-routed packets.  
  
  
**Vulnerability Discussion:**  Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv4 forwarding is enabled and the system is functioning as a router.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# ndd /dev/ip ip\_forward\_src\_routed  
If the returned value is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not forward IPv4 source-routed packets.  
Procedure:  
# ndd /dev/ip ip\_forward\_src\_routed 0  
  
This command must also be added to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23741  
**Group Title:** GEN003601  
**Rule ID:** SV-28639r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003601  
**Rule Title:**TCP backlog queue sizes must be set appropriately.  
  
  
**Vulnerability Discussion:**  To provide some mitigation to TCP DoS attacks, the TCP backlog queue sizes must be set to at least 1280 or in accordance with product-specific guidelines.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Procedure:  
# ndd /dev/tcp tcp\_conn\_req\_max\_q0  
  
If the returned value is not 1280 or greater, this is a finding.  
  
Procedure:  
# ndd /dev/tcp tcp\_conn\_req\_max\_q  
  
If the returned value is not 1024, this is a finding.  
  
**Fix Text:**Procedure:  
# ndd -set /dev/tcp tcp\_conn\_req\_max\_q0 1280  
# ndd -set /dev/tcp tcp\_conn\_req\_max\_q 1024  
  
Ensure these commands are also present in system startup scripts.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22409  
**Group Title:** GEN003602  
**Rule ID:** SV-26621r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003602  
**Rule Title:**The system must not process ICMP timestamp requests.  
  
  
**Vulnerability Discussion:**  The processing of Internet Control Message Protocol (ICMP) timestamp requests increases the attack surface of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system does not respond to ICMP timestamp requests.  
# ndd /dev/ip ip\_respond\_to\_timestamp  
If the result is not 0, this is a finding.  
  
**Fix Text:**Disable ICMP timestamp responses on the system.  
# ndd -set /dev/ip ip\_respond\_to\_timestamp 0  
Also add this command to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22410  
**Group Title:** GEN003603  
**Rule ID:** SV-26622r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003603  
**Rule Title:**The system must not respond to ICMPv4 echoes sent to a broadcast address.  
  
  
**Vulnerability Discussion:**  Responding to broadcast Internet Control Message Protocol (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system does not respond to ICMP ECHO\_REQUESTs set to broadcast addresses.  
# ndd /dev/ip ip\_respond\_to\_echo\_broadcast  
If the result is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not respond to ICMP ECHO\_REQUESTs sent to broadcast addresses.  
# ndd -set /dev/ip ip\_respond\_to\_echo\_broadcast 0  
Also add this command to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22411  
**Group Title:** GEN003604  
**Rule ID:** SV-26624r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003604  
**Rule Title:**The system must not respond to ICMP timestamp requests sent to a broadcast address.  
  
  
**Vulnerability Discussion:**  The processing of Internet Control Message Protocol (ICMP) timestamp requests increases the attack surface of the system. Responding to broadcast ICMP timestamp requests facilitates network mapping and provides a vector for amplification attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system does not respond to ICMP timestamp requests set to broadcast addresses.  
# ndd /dev/ip ip\_respond\_to\_echo\_broadcast  
If the result is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not respond to ICMP timestamp requests sent to broadcast addresses.  
# ndd -set /dev/ip ip\_respond\_to\_echo\_broadcast 0  
Also add this command to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22412  
**Group Title:** GEN003605  
**Rule ID:** SV-26626r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003605  
**Rule Title:**The system must not apply reversed source routing to TCP responses.  
  
  
**Vulnerability Discussion:**  Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system does not apply reversed source routing to TCP responses.  
# ndd /dev/tcp tcp\_rev\_src\_routes  
If the result is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not apply reversed source routing to TCP responses.  
# ndd -set /dev/tcp tcp\_rev\_src\_routes 0  
Also add this command to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22413  
**Group Title:** GEN003606  
**Rule ID:** SV-29709r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003606  
**Rule Title:**The system must prevent local applications from generating source-routed packets.  
  
  
**Vulnerability Discussion:**  Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for an IPF rule blocking outgoing source-routed packets.  
  
Procedure:  
# ipfstat -o   
  
Examine the list for rules such as:  
block out log quick all with opt lsrr  
block out log quick all with opt ssrr  
  
If the listed rules do not block both lsrr and ssrr options, this is a finding.  
  
**Fix Text:**Edit /etc/ipf/ipf.conf and add rules to block outgoing source-routed packets, such as:   
  
block out log quick all with opt lsrr  
block out log quick all with opt ssrr  
  
Reload the IPF rules.  
Procedure:  
  
# ipf -Fa -A -f /etc/ipf/ipf.conf     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22414  
**Group Title:** GEN003607  
**Rule ID:** SV-29711r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003607  
**Rule Title:**The system must not accept source-routed IPv4 packets.  
  
  
**Vulnerability Discussion:**  Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the handling of source-routed traffic destined to the system itself, not to traffic forwarded by the system to another, such as when IPv4 forwarding is enabled and the system is functioning as a router.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for an IPF rule blocking incoming source-routed packets.   
  
Procedure: # ipfstat -i   
  
Examine the list for rules such as:   
block in log quick all with opt lsrr  
block in log quick all with opt ssrr  
  
If the listed rules do not block incoming traffic with both lsrr and ssrr options, this is a finding.  
  
**Fix Text:**Edit /etc/ipf/ipf.conf and add rules to block incoming source-routed packets, such as:   
  
block in log quick all with opt lsrr   
block in log quick all with opt ssrr  
  
Reload the IPF rules.  
Procedure:  
# ipf -Fa -A -f /etc/ipf/ipf.conf     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22415  
**Group Title:** GEN003608  
**Rule ID:** SV-29603r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003608  
**Rule Title:**Proxy ARP must not be enabled on the system.  
  
  
**Vulnerability Discussion:**  Proxy ARP allows a system to respond to ARP requests on one interface on behalf of hosts connected to another interface. If this function is enabled when not required, addressing information may be leaked between the attached network segments.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system has non-local published ARP entries.  
  
Procedure:  
# arp -a  
  
If any entries have the flag P, they are non-local published entries, and this is a finding.  
  
**Fix Text:**Remove non-local published ARP entries from the system.  
  
Procedure:  
# arp -d <host>  
  
Check system initialization files for any commands creating published ARP entries (such as "arp -s <host> <ether> pub" or "arp -f") and removing them.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22416  
**Group Title:** GEN003609  
**Rule ID:** SV-26630r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003609  
**Rule Title:**The system must ignore IPv4 ICMP redirect messages.  
  
  
**Vulnerability Discussion:**  ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system does not accept IPv4 ICMP redirect messages.  
  
Procedure:  
# ndd -get /dev/ip ip\_ignore\_redirect  
  
If the result is not 1, this is a finding.  
  
**Fix Text:**Configure the system to not accept IPv4 ICMP redirect messages.  
  
Procedure:  
# ndd -set /dev/ip ip\_ignore\_redirect 1  
  
This command must also be added to a system startup script.     
  
**CCI:**CCI-001503  
  
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22417  
**Group Title:** GEN003610  
**Rule ID:** SV-26632r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003610  
**Rule Title:**The system must not send IPv4 ICMP redirects.  
  
  
**Vulnerability Discussion:**  ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table that could reveal portions of the network topology.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system does not send IPv4 ICMP redirect messages.  
  
Procedure:  
# ndd /dev/ip ip\_send\_redirects  
  
If the result is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not send IPv4 ICMP redirect messages.  
  
Procedure:  
# ndd -set /dev/ip ip\_send\_redirects 0  
  
Also add this command to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22418  
**Group Title:** GEN003611  
**Rule ID:** SV-29773r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003611  
**Rule Title:**The system must log martian packets.  
  
  
**Vulnerability Discussion:**  Martian packets are packets containing addresses known by the system to be invalid. Logging these messages allows the SA to identify misconfigurations or attacks in progress.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Determine if the system is configured to log martian packets. Examine the IPF rules on the system.  
  
Procedure:  
# ipfstat -i  
  
There must be rules logging inbound traffic containing invalid source addresses, which minimally include the system's own addresses and broadcast addresses for attached subnets. If such rules do not exist, this is a finding.  
  
**Fix Text:**Configure the system to log martian packets using IPF. Add rules logging inbound traffic containing invalid source addresses, which minimally include the system's own addresses and broadcast addresses for attached subnets.  
  
For example, consider a system with a single network connection having IP address 192.168.1.10 with a local subnet broadcast address of 192.168.1.255. Packets with source addresses of 192.168.1.10 and 192.168.1.255 must be logged if received by the system from the network connection.  
  
Edit /etc/ipf/ipf.conf and add the following rules, substituting local addresses and interface names:  
block in log quick on ce0 from 192.168.1.10 to any  
block in log quick on ce0 from 192.168.1.255 to any  
  
Reload the IPF rules.  
Procedure:  
# ipf -Fa -A -f /etc/ipf/ipf.conf     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22421  
**Group Title:** GEN003619  
**Rule ID:** SV-42308r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003619  
**Rule Title:**The system must not be configured for network bridging.  
  
  
**Vulnerability Discussion:**  Some systems have the ability to bridge or switch frames (link-layer forwarding) between multiple interfaces. This can be useful in a variety of situations but, if enabled when not needed, has the potential to bypass network partitioning and security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Ask the system administrator if network bridging software is installed on the system or the system is configured for network bridging. If network bridging software is installed or the system is configured for network bridging, this is a finding.  
  
**Fix Text:**Remove the network bridging software and configuration from the system.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12003  
**Group Title:** GEN003620  
**Rule ID:** SV-28618r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003620  
**Rule Title:**A separate file system must be used for user home directories (such as /home or equivalent).  
  
  
**Vulnerability Discussion:**  The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the /export/home path is a separate file system.  
# grep /export/home /etc/vfstab  
If no result is returned, /export/home is not on a separate file system and this is a finding.  
  
**Fix Text:**Migrate the /export/home path onto a separate file system.     
  
**CCI:**CCI-001208  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23738  
**Group Title:** GEN003623  
**Rule ID:** SV-28628r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003623  
**Rule Title:**The system must use a separate file system for the system audit data path.  
  
  
**Vulnerability Discussion:**  The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine the audit log data path.  
# grep "^dir:" /etc/security/audit\_control  
Determine if the audit log data path is a separate filesystem.  
# grep <audit data path> /etc/vfstab  
If no result is returned, the audit data path is not on a separate filesystem and this is a finding.  
  
**Fix Text:**Migrate the system audit data path onto a separate file system.     
  
**CCI:**CCI-001208  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23739  
**Group Title:** GEN003624  
**Rule ID:** SV-28632r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003624  
**Rule Title:**The system must use a separate filesystem for /tmp (or equivalent).  
  
  
**Vulnerability Discussion:**  The use of separate filesystems for different paths can protect the system from failures resulting from a filesystem becoming full or failing.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the /tmp path is a separate file system.  
# grep /tmp /etc/vfstab  
If no result is returned, /tmp is not on a separate file system, this is a finding.  
If the returned result indicates that /tmp is mounted on a memory or swap based file system, this is not a finding  
  
  
**Fix Text:**Migrate the /tmp path onto a separate file system.     
  
**CCI:**CCI-001208  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4304  
**Group Title:** GEN003640  
**Rule ID:** SV-40021r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003640  
**Rule Title:**The root file system must employ journaling or another mechanism ensuring file system consistency.  
  
  
**Vulnerability Discussion:**  File system journaling, or logging, can allow reconstruction of file system data after a system crash, thus, preserving the integrity of data that may have otherwise been lost. Journaling file systems typically do not require consistent checks upon booting after a crash, which can improve system availability. Some file systems employ other mechanisms to ensure consistency which also satisfy this requirement.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Logging should be enabled for those types of files systems that do not turn on logging by default.   
  
Procedure:  
# mount -v  
  
UFS, JFS, VXFS, HFS, XFS, reiserfs, EXT3 and EXT4 all turn logging on by default and will not be a finding. The ZFS file system uses other mechanisms to provide for file system consistency, and will not be a finding. For other file systems types, if the root file system does not have the 'logging' option, this is a finding. If the 'nolog' option is set on the root file system, this is a finding.  
  
  
**Fix Text:**Implement file system journaling for the root file system, or use a file system using other mechanisms to ensure consistency. If the root file system supports journaling, enable it. If the file system does not support journaling or another mechanism to ensure consistency, a migration to a different file system will be necessary.     
  
**CCI:**CCI-000553  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22422  
**Group Title:** GEN003650  
**Rule ID:** SV-26638r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003650  
**Rule Title:**All local file systems must employ journaling or another mechanism ensuring file system consistency.  
  
  
**Vulnerability Discussion:**  File system journaling, or logging, can allow reconstruction of file system data after a system crash, thus preserving the integrity of data that may have otherwise been lost. Journaling file systems typically do not require consistent checks upon booting after a crash, which can improve system availability. Some file systems employ other mechanisms to ensure consistency which also satisfy this requirement.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify local file systems use journaling or another mechanism ensuring file system consistency.  
  
Procedure:  
# mount | grep '^/dev/' | grep -v '(logging|vxfs|zfs)'  
  
If a mount is listed, this is a finding.  
  
**Fix Text:**Convert local file systems to use journaling or another mechanism ensuring file system consistency.     
  
**CCI:**CCI-000553  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12004  
**Group Title:** GEN003660  
**Rule ID:** SV-12505r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003660  
**Rule Title:**The system must log authentication informational data.  
  
  
**Vulnerability Discussion:**  Monitoring and recording successful and unsuccessful logins assists in tracking unauthorized access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check /etc/syslog.conf and verify the auth facility is logging both the notice and info level messages by using one of the procedures below.  
  
# grep "auth.notice" /etc/syslog.conf  
# grep "auth.info" /etc/syslog.conf  
OR  
# grep 'auth.\*' /etc/syslog.conf  
  
If auth.\* is not found, and either auth.notice or auth.info is not found, this is a finding.  
  
**Fix Text:**Edit /etc/syslog.conf and add local log destinations for auth.\* or both auth.notice and auth.info.     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12005  
**Group Title:** GEN003700  
**Rule ID:** SV-27426r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003700  
**Rule Title:**Inetd and xinetd must be disabled or removed if no network services utilizing them are enabled.  
  
  
**Vulnerability Discussion:**  Unnecessary services should be disabled to decrease the attack surface of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if inetd is running,  
# svcs -a | grep inetd  
If inetd is not running, this check is not a finding.  
# inetadm | grep -v disabled  
If no enabled/online services are found, yet the inetd daemon is running, this is a finding.  
  
**Fix Text:**Disable the inetd service.  
  
Procedure:  
# svcadm disable inetd     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-821  
**Group Title:** GEN003720  
**Rule ID:** SV-39883r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003720  
**Rule Title:**The inetd.conf file must be owned by root or bin.  
  
  
**Vulnerability Discussion:**  Failure to give ownership of sensitive files or utilities to root provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of inetd.conf file.  
  
Procedure:  
# ls -lL /etc/inet/inetd.conf  
  
This is a finding if any of the above files or directories are not owned by root or bin.  
  
**Fix Text:**Change the ownership of the inetd.conf file to root or bin.  
  
Procedure:  
# chown root /etc/inet/inetd.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22423  
**Group Title:** GEN003730  
**Rule ID:** SV-39884r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003730  
**Rule Title:**The inetd.conf file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  Failure to give ownership of sensitive files or utilities to system groups may provide unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the inetd.conf file.  
  
Procedure:  
# ls -alL /etc/inet/inetd.conf  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the inetd.conf file.  
Procedure:  
# chgrp sys /etc/inet/inetd.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-822  
**Group Title:** GEN003740  
**Rule ID:** SV-39885r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003740  
**Rule Title:**The inetd.conf file must have mode 0440 or less permissive.  
  
  
**Vulnerability Discussion:**  The Internet service daemon configuration files must be protected as malicious modification could cause Denial of Service or increase the attack surface of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of inetd.conf file.  
# ls -lL /etc/inet/inetd.conf  
If the mode of the file is more permissive than 0440, this is a finding.  
  
**Fix Text:**Change the mode of the inetd.conf file.  
# chmod 0440 /etc/inet/inetd.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22424  
**Group Title:** GEN003745  
**Rule ID:** SV-26653r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003745  
**Rule Title:**The inetd.conf file must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  The Internet service daemon configuration files must be protected as malicious modification could cause Denial of Service or increase the attack surface of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the inetd configuration file.  
# ls -lL /etc/inet/inetd.conf  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/inet/inetd.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-823  
**Group Title:** GEN003760  
**Rule ID:** SV-823r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003760  
**Rule Title:**The services file must be owned by root or bin.  
  
  
**Vulnerability Discussion:**  Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the services file.  
  
Procedure:  
# ls -lL /etc/services  
  
If the services file is not owned by root or bin, this is a finding.  
  
**Fix Text:**Change the ownership of the services file to root or bin.  
  
Procedure:  
# chown root /etc/services     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22427  
**Group Title:** GEN003770  
**Rule ID:** SV-39903r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003770  
**Rule Title:**The services file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  Failure to give ownership of system configuration files to root or a system group provides the designated owner and unauthorized users with the potential to change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the services file.  
  
Procedure:  
# ls -lL /etc/services  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group-owner of the services file.  
  
Procedure:  
# chgrp root /etc/services     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-824  
**Group Title:** GEN003780  
**Rule ID:** SV-824r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003780  
**Rule Title:**The services file must have mode 0444 or less permissive.  
  
  
**Vulnerability Discussion:**  The services file is critical to the proper operation of network services and must be protected from unauthorized modification. Unauthorized modification could result in the failure of network services.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the services file.  
  
Procedure:  
# ls -lL /etc/services  
  
If the services file has a mode more permissive than 0444, this is a finding.  
  
**Fix Text:**Change the mode of the services file to 0444 or less permissive.  
  
Procedure:  
# chmod 0444 /etc/services     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22428  
**Group Title:** GEN003790  
**Rule ID:** SV-26660r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003790  
**Rule Title:**The services file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  The services file is critical to the proper operation of network services and must be protected from unauthorized modification. If the services file has an extended ACL, it may be possible for unauthorized users to modify the file. Unauthorized modification could result in the failure of network services.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the /etc/services file.  
# ls -lL /etc/services  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/services     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1011  
**Group Title:** GEN003800  
**Rule ID:** SV-27430r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003800  
**Rule Title:**Inetd or xinetd logging/tracing must be enabled.  
  
  
**Vulnerability Discussion:**  Inetd or xinetd logging and tracing allows the system administrators to observe the IP addresses connecting to their machines and to observe what network services are being sought. This provides valuable information when trying to find the source of malicious users and potential malicious users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3, ECSC-1  
  
**Check Content:**    
Verify the default value of the inet service property tcp\_trace.  
# inetadm -p |grep tcp\_trace  
  
If the tcp\_trace inet service property is not set or is set to FALSE, this is a finding.  
  
Verify that all enabled inetd-managed processes have the tcp\_trace inet service property set to the default value or TRUE.  
# inetadm | grep enabled | awk '{print $NF}' | xargs inetadm -l | more  
  
If any enabled inetd-managed processes have the tcp\_trace inet service property set to FALSE, this is a finding.  
  
**Fix Text:**Enable logging or tracing for inetd.  
  
Procedure:  
# inetadm -M tcp\_trace=TRUE  
  
Set the tcp\_trace inet service property to the default for all enabled inetd-managed services.  
  
# inetadm | grep enabled | awk '{print $NF}' | xargs -I X inetadm -m X tcp\_trace=  
  
(Note: The trailing '=' instructs inetd to use the default value for tcp\_trace.)     
  
**CCI:**CCI-000134  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22429  
**Group Title:** GEN003810  
**Rule ID:** SV-26664r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003810  
**Rule Title:**The portmap or rpcbind service must not be running unless needed.  
  
  
**Vulnerability Discussion:**  The portmap and rpcbind services increase the attack surface of the system and should only be used when needed. The portmap or rpcbind services are used by a variety of services using remote procedure calls (RPCs).  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the status of the rpcbind service.  
  
# svcs network/rpc/bind  
  
If the service is online and is not documented as required, this is a finding.  
  
**Fix Text:**Disable the portmap service.  
# svcadm disable network/rpc/bind     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22430  
**Group Title:** GEN003815  
**Rule ID:** SV-40810r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003815  
**Rule Title:**The portmap or rpcbind service must not be installed unless needed.  
  
  
**Vulnerability Discussion:**  The portmap and rpcbind services increase the attack surface of the system and should only be used when needed. The portmap or rpcbind services are used by a variety of services using Remote Procedure Calls (RPCs).  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system needs the portmap service to operate, this is not applicable. The rpcbind program is part of a core Solaris package and cannot be removed. Verify the permissions on the rpcbind file.  
# ls -lL /usr/sbin/rpcbind  
If the rpcbind service is not required and the rpcbind file has non-zero permissions, this is a finding.  
  
**Fix Text:**Remove all permissions from the rpcbind file.  
  
Procedure:  
# chmod 0000 /usr/sbin/rpcbind     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4687  
**Group Title:** GEN003820  
**Rule ID:** SV-27435r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN003820  
**Rule Title:**The rsh daemon must not be running.  
  
  
**Vulnerability Discussion:**  The rshd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  EBRU-1  
  
**Check Content:**    
# svcs network/shell  
If the service is enabled, this is a finding.  
  
  
**Fix Text:**Disable the remote shell service and restart inetd.  
Procedure:  
# svcadm disable network/shell  
# svcadm refresh inetd     
  
**CCI:**CCI-000068  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22431  
**Group Title:** GEN003825  
**Rule ID:** SV-26668r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003825  
**Rule Title:**The rshd service must not be installed.  
  
  
**Vulnerability Discussion:**  The rshd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1  
  
**Check Content:**    
Check if the SUNWrcmdr package is installed.  
  
Procedure:  
# pkginfo SUNWrcmdr  
  
If the package is installed, this is a finding.  
  
**Fix Text:**Remove the SUNWrcmdr package.  
  
Procedure:  
# pkgrm SUNWrcmdr     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22432  
**Group Title:** GEN003830  
**Rule ID:** SV-39863r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003830  
**Rule Title:**The rlogind service must not be running.  
  
  
**Vulnerability Discussion:**  The rlogind process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1  
  
**Check Content:**    
Determine if the rlogind service is running.   
# svcs rlogin  
  
If the rlogin service is enabled, this is a finding.  
  
**Fix Text:**Disable the rlogind service.   
  
# svcadm disable rlogin  
# svcadm refresh inetd  
  
    
  
**CCI:**CCI-000068  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22433  
**Group Title:** GEN003835  
**Rule ID:** SV-26670r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003835  
**Rule Title:**The rlogind service must not be installed.  
  
  
**Vulnerability Discussion:**  The rlogind process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1  
  
**Check Content:**    
Check if the SUNWrcmdr package is installed.  
  
Procedure:  
# pkginfo SUNWrcmdr  
  
If the package is installed, this is a finding.  
  
**Fix Text:**Remove the SUNWrcmdr package.  
  
Procedure:  
# pkgrm SUNWrcmdr     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4688  
**Group Title:** GEN003840  
**Rule ID:** SV-27438r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN003840  
**Rule Title:**The rexec daemon must not be running.  
  
  
**Vulnerability Discussion:**  The rexecd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.  
  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  EBRP-1, ECSC-1  
  
**Check Content:**    
# svcs rexec  
If the service is enabled, this is a finding.  
  
**Fix Text:**# svcadm disable rexec  
# svcadm refresh inetd  
    
  
**CCI:**CCI-001435  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22434  
**Group Title:** GEN003845  
**Rule ID:** SV-26674r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003845  
**Rule Title:**The rexecd service must not be installed.  
  
  
**Vulnerability Discussion:**  The rexecd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check if the SUNWrcmdr package is installed.  
  
Procedure:  
# pkginfo SUNWrcmdr  
  
If the package is installed, this is a finding.  
  
**Fix Text:**Remove the SUNWrcmdr package.  
  
Procedure:  
# pkgrm SUNWrcmdr     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24386  
**Group Title:** GEN003850  
**Rule ID:** SV-39864r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN003850  
**Rule Title:**The telnet daemon must not be running.  
  
  
**Vulnerability Discussion:**  The telnet daemon provides a typically unencrypted remote access service which does not provide for the confidentiality and integrity of user passwords or the remote session. If a privileged user were to log on using this service, the privileged user password could be compromised.  
  
**Mitigations:**   
GEN003850  
  
**Mitigation Control:**   
If an enabled telnet daemon is configured to only allow encrypted sessions, such as with Kerberos or the use of encrypted network tunnels, the risk of exposing sensitive information is mitigated, and this is not a finding.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1  
  
**Check Content:**    
Determine if the telnet daemon is running.   
  
# svcs telnet  
  
If the telnet service is enabled, this is a finding.  
  
**Fix Text:**Disable the telnet daemon.   
  
# svcadm disable telnet  
# svcadm refresh inetd  
    
  
**CCI:**CCI-000197  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4701  
**Group Title:** GEN003860  
**Rule ID:** SV-27441r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003860  
**Rule Title:**The system must not have the finger service active.  
  
  
**Vulnerability Discussion:**  The finger service provides information about the system's users to network clients. This information could expose information that could be used in subsequent attacks.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1, EBRU-1  
  
**Check Content:**    
# svcs finger  
If the finger service is not disabled, this is a finding.  
  
**Fix Text:**Disable the finger service and restart inetd.  
Procedure:  
# svcadm disable finger  
# svcadm refresh inetd     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12049  
**Group Title:** GEN003865  
**Rule ID:** SV-40811r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003865  
**Rule Title:**Network analysis tools must not be installed.  
  
  
**Vulnerability Discussion:**  Network analysis tools allow for the capture of network traffic visible to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPA-1  
  
**Check Content:**    
Determine if any network analysis tools are installed.  
  
Procedure:  
# find / -name ethereal  
# find / -name wireshark  
# find / -name tshark  
# find / -name netcat  
# find / -name tcpdump  
# find / -name snoop  
  
If any network analysis tools are found, this is a finding.  
  
**Fix Text:**Remove the network analysis tool binary from the system. The snoop binary is part of the SUNWrcmdc package, which may also be removed if none of its components are required.  
  
Procedure:  
# rm <binary>  
# pkgrm SUNWrcmdc     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-827  
**Group Title:** GEN003900  
**Rule ID:** SV-40457r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003900  
**Rule Title:**The hosts.lpd file (or equivalent) must not contain a "+" character.  
  
  
**Vulnerability Discussion:**  Having the "+" character in the hosts.lpd (or equivalent) file allows all hosts to use local system print resources.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Solaris uses the "IPP" print service and can also use the Samba print service. Verify remote host access is limited.  
  
Procedure:  
# grep -i Listen /etc/apache/httpd-standalone-ipp.conf  
The /etc/apache/httpd-standalone-ipp.conf file must not contain a Listen \*:<port> or equivalent line.  
If the network address of the "Listen" line is unrestricted, this is a finding.  
  
# grep -i "Allow From" /etc/apache/httpd-standalone-ipp.conf  
The "Allow From" line within the "<Location />" element should limit access to the printers to @LOCAL and specific hosts.  
If the "Allow From" line contains "All", this is a finding.   
  
Verify guest access to printers shared via Samba is restricted according to GEN006235.  
  
**Fix Text:**Configure IPP to use only the localhost or specified remote hosts.  
  
Procedure:  
Modify the /etc/apache/httpd-standalone-ipp.conf file to "Listen" only to the local machine or a known set of hosts (i.e., Listen localhost:631).  
Modify the /etc/apache/httpd-standalone-ipp.conf file "<Location />" element to "Deny From All" and "Allow from 127.0.0.1" or allowed host addresses.  
  
Restart the IPP service:  
# svcadm restart ipp-listener     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-828  
**Group Title:** GEN003920  
**Rule ID:** SV-37455r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003920  
**Rule Title:**The hosts.lpd (or equivalent) file must be owned by root.  
  
  
**Vulnerability Discussion:**  Failure to give ownership of the hosts.lpd file to root provides the designated owner, and possible unauthorized users, with the potential to modify the hosts.lpd file. Unauthorized modifications could disrupt access to local printers from authorized remote hosts or permit unauthorized remote access to local printers.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the print service configuration files.   
Procedure:  
# ls -lL /etc/apache/httpd-standalone-ipp.conf /etc/printers.conf /etc/sfw/smb.conf  
If the owner of the files is not root, this is a finding.  
  
**Fix Text:**Change the owner of the print service configuration files.  
Procedure:  
# chown root /etc/apache/httpd-standalone-ipp.conf /etc/printers.conf /etc/sfw/smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22435  
**Group Title:** GEN003930  
**Rule ID:** SV-37456r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003930  
**Rule Title:**The hosts.lpd (or equivalent) file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  Failure to give group ownership of the hosts.lpd (or equivalent) file to root, bin, sys, or system provides the members of the owning group and possible unauthorized users, with the potential to modify the hosts.lpd file. Unauthorized modifications could disrupt access to local printers from authorized remote hosts or permit unauthorized remote access to local printers.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the print service configuration files.  
  
Procedure:  
# ls -lL /etc/printers.conf /etc/apache/httpd-standalone-ipp.conf /etc/sfw/smb.conf  
  
If the files are not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the print service configuration files.   
Procedure:   
# chgrp bin /etc/apache/httpd-standalone-ipp.conf  
# chgrp root /etc/printers.conf /etc/sfw/smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-829  
**Group Title:** GEN003940  
**Rule ID:** SV-37457r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003940  
**Rule Title:**The hosts.lpd (or equivalent) must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the hosts.lpd (or equivalent) file may permit unauthorized modification. Unauthorized modifications could disrupt access to local printers from authorized remote hosts or permit unauthorized remote access to local printers.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the print service configuration files.  
  
Procedure:  
# ls -lL /etc/apache/httpd-standalone-ipp.conf /etc/printers.conf /etc/sfw/smb.conf  
  
If the mode of any of the print service configuration file is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the print service configuration files to 0644 or less permissive.  
  
Procedure:  
# chmod 0644 /etc/apache/httpd-standalone-ipp.conf /etc/printers.conf /etc/sfw/smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22436  
**Group Title:** GEN003950  
**Rule ID:** SV-26678r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003950  
**Rule Title:**The hosts.lpd (or equivalent) file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the hosts.lpd (or equivalent) file may permit unauthorized modification. Unauthorized modifications could disrupt access to local printers from authorized remote hosts or permit unauthorized remote access to local printers.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the print service configuration files.  
  
Procedure:  
# ls -lL /etc/apache/httpd-standalone-ipp.conf /etc/printers.conf /etc/sfw/smb.conf  
  
If the permissions on any file include a '+', the file has an extended ACL and this is a finding.  
  
  
**Fix Text:**Remove the extended ACLs from the files.  
# chmod A- /etc/apache/httpd-standalone-ipp.conf /etc/printers.conf /etc/sfw/smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4369  
**Group Title:** GEN003960  
**Rule ID:** SV-28392r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003960  
**Rule Title:**The traceroute command owner must be root.  
  
  
**Vulnerability Discussion:**  If the traceroute command owner has not been set to root, an unauthorized user could use this command to obtain knowledge of the network topology inside the firewall. This information may allow an attacker to determine trusted routers and other network information possibly leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /usr/sbin/traceroute  
If the traceroute command is not owned by root, this is a finding.  
  
  
**Fix Text:**Change the owner of the traceroute command to root.  
Example procedure:  
# chown root /usr/sbin/traceroute  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4370  
**Group Title:** GEN003980  
**Rule ID:** SV-28395r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003980  
**Rule Title:**The traceroute command must be group-owned by sys, bin, or root.  
  
  
**Vulnerability Discussion:**  If the group owner of the traceroute command has not been set to a system group, unauthorized users could have access to the command and use it to gain information regarding a network's topology inside of the firewall. This information may allow an attacker to determine trusted routers and other network information possibly leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the traceroute file.  
  
Procedure:  
# ls -lL /usr/sbin/traceroute  
  
If the traceroute command is not group-owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the group-owner of the traceroute command to root.  
  
Procedure:  
# chgrp root /usr/sbin/traceroute     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4371  
**Group Title:** GEN004000  
**Rule ID:** SV-28399r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004000  
**Rule Title:**The traceroute file must have mode 0700 or less permissive.  
  
  
**Vulnerability Discussion:**  If the mode of the traceroute executable is more permissive than 0700, malicious code could be inserted by an attacker and triggered whenever the traceroute command is executed by authorized users. Additionally, if an unauthorized user is granted executable permissions to the traceroute command, it could be used to gain information about the network topology behind the firewall. This information may allow an attacker to determine trusted routers and other network information that may lead to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /usr/sbin/traceroute  
If the traceroute command has a mode more permissive than 0700, this is a finding.  
  
  
**Fix Text:**Change the mode of the traceroute command.  
# chmod 0700 /usr/sbin/traceroute  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22437  
**Group Title:** GEN004010  
**Rule ID:** SV-26682r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004010  
**Rule Title:**The traceroute file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  If an extended ACL exists on the traceroute executable file, it may provide unauthorized users with access to the file. Malicious code could be inserted by an attacker and triggered whenever the traceroute command is executed by authorized users. Additionally, if an unauthorized user is granted executable permissions to the traceroute command, it could be used to gain information about the network topology behind the firewall. This information may allow an attacker to determine trusted routers and other network information possibly leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the /usr/sbin/traceroute file.  
# ls -lL /usr/contrib/bin/traceroute  
  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /usr/sbin/traceroute     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4382  
**Group Title:** GEN004220  
**Rule ID:** SV-4382r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN004220  
**Rule Title:**Administrative accounts must not run a web browser, except as needed for local service administration.  
  
  
**Vulnerability Discussion:**  If a web browser flaw is exploited while running as a privileged user, the entire system could be compromised.  
  
Specific exceptions for local service administration should be documented in site-defined policy. These exceptions may include HTTP(S)-based tools used for the administration of the local system, services, or attached devices. Examples of possible exceptions are HP’s System Management Homepage (SMH), the CUPS administrative interface, and Sun's StorageTek Common Array Manager (CAM) when these services are running on the local system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Look in the root account home directory for a .netscape or a .mozilla directory. If none exists, this is not a finding. If there is one, verify with the root users and the IAO what the intent of the browsing is. Some evidence may be obtained by using the browser to view cached pages under the .netscape directory.  
  
**Fix Text:**Enforce policy requiring administrative accounts use web browsers only for local service administration.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-831  
**Group Title:** GEN004360  
**Rule ID:** SV-40493r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004360  
**Rule Title:**The alias file must be owned by root.  
  
  
**Vulnerability Discussion:**  If the alias file is not owned by root, an unauthorized user may modify the file to add aliases to run malicious code or redirect email.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the alias file on the system.  
  
Procedure:  
# egrep '^O(A| AliasFile)' /etc/mail/sendmail.cf  
  
If the "alias file" is an NIS or LDAP map, this check is not applicable. The default location is /etc/mail/aliases.  
  
Check the ownership of the alias file.  
  
Procedure:  
# ls -lL <alias file>  
  
If the alias file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/mail/aliases file (or equivalent, such as /usr/lib/aliases) to root.  
  
Procedure:  
# chown root /etc/mail/aliases     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22438  
**Group Title:** GEN004370  
**Rule ID:** SV-37458r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004370  
**Rule Title:**The aliases file must be group-owned by root, sys, smmsp, or bin.  
  
  
**Vulnerability Discussion:**  If the alias file is not group-owned by root or a system group, an unauthorized user may modify the file to add aliases to run malicious code or redirect email.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the alias files on the system.  
  
Procedure:  
# egrep '^O(A| AliasFile)' /etc/mail/sendmail.cf  
  
If the "alias file" is an NIS or LDAP map, this check is not applicable. The default location is /etc/mail/aliases.  
  
Check the group ownership of the alias file and the hashed version of it used by sendmail.  
  
Procedure:  
# ls -lL /etc/mail/aliases /etc/mail/aliases.db  
  
If the file is not group-owned by root, sys, smmsp, or bin, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/mail/aliases files.  
  
Procedure:  
# chgrp bin /etc/mail/aliases   
# chgrp smmsp /etc/mail/aliases.db     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-832  
**Group Title:** GEN004380  
**Rule ID:** SV-40651r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004380  
**Rule Title:**The alias file must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the aliases file may permit unauthorized modification. If the alias file is modified by an unauthorized user, they may modify the file to run malicious code or redirect email.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the alias files on the system.  
  
Procedure:  
# egrep '^O(A| AliasFile)' /etc/mail/sendmail.cf  
  
If the alias file is an NIS or LDAP map, this check is not applicable. The default location is /etc/mail/aliases.  
  
Check the permissions of the alias file and the hashed version of it used by sendmail.  
  
Procedure:  
# ls -lL /etc/mail/aliases /etc/mail/aliases.db  
  
If the alias files have a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/mail/aliases files (or equivalent, such as /usr/lib/aliases) to 0644.  
  
Procedure:  
# chmod 0644 /etc/mail/aliases /etc/mail/aliases.db     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22439  
**Group Title:** GEN004390  
**Rule ID:** SV-26687r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004390  
**Rule Title:**The alias file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the aliases file may permit unauthorized modification. If the alias file is modified by an unauthorized user, they may modify the file to run malicious code or redirect email.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the alias files on the system.  
  
Procedure:  
# egrep '^O(A| AliasFile)' /etc/mail/sendmail.cf  
  
If the "alias file" is an NIS or LDAP map, this check is not applicable. The default location is /etc/mail/aliases.  
  
Check the permissions of the alias file and the hashed version of it used by sendmail.  
  
Procedure:  
# ls -lL /etc/mail/aliases /etc/mail/aliases.db  
  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the files.  
# chmod A- /etc/mail/aliases /etc/mail/aliases.db     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-833  
**Group Title:** GEN004400  
**Rule ID:** SV-833r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN004400  
**Rule Title:**Files executed through a mail aliases file must be owned by root and must reside within a directory owned and writable only by root.  
  
  
**Vulnerability Discussion:**  If a file executed through a mail aliases file is not owned and writable only by root, it may be subject to unauthorized modification. Unauthorized modification of files executed through aliases may allow unauthorized users to attain root privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the aliases file on the system.  
  
Procedure:  
# find / -name aliases -depth -print  
# more < aliases file location >  
  
Examine the aliases file for any directories or paths that may be utilized.  
  
Procedure:  
# ls -lL < path >  
  
Check if the file or parent directory is owned by root. If not, this is a finding.  
  
**Fix Text:**Edit the /etc/mail/aliases file (alternatively, /usr/lib/sendmail.cf). Locate the entries executing a program. They will appear similar to the following line.  
  
Aliasname: : /usr/local/bin/ls (or some other program name)  
  
Ensure root owns the programs and the directory(ies) they reside in by using the chown command to change owner to root.  
Procedure:  
# chown root filename     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22440  
**Group Title:** GEN004410  
**Rule ID:** SV-39904r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004410  
**Rule Title:**Files executed through a mail aliases file must be group-owned by root, bin, or sys, and must reside within a directory group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If a file executed through a mail aliases file is not group-owned by root or a system group, it may be subject to unauthorized modification. Unauthorized modification of files executed through aliases may allow unauthorized users to attain root privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Examine the contents of the /etc/mail/aliases file.  
For each file referenced, check the group ownership of the file.  
  
Procedure:  
# ls -lL <file referenced from aliases>  
  
If the group owner of any file is not root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the file referenced from /etc/mail/aliases.  
  
Procedure:  
# chgrp root <file referenced from aliases>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-834  
**Group Title:** GEN004420  
**Rule ID:** SV-834r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004420  
**Rule Title:**Files executed through a mail aliases file must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  If a file executed through a mail alias file has permissions greater than 0755, it can be modified by an unauthorized user and may contain malicious code or instructions possibly compromising the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the aliases file on the system.  
Procedure:  
# find / -name aliases -depth -print  
  
Examine the aliases file for any directories or paths that may be utilized.  
Procedure:  
# more <aliases file location>  
  
Check the permissions for any paths referenced.  
Procedure:  
# ls -lL <path>  
  
If any file referenced from the aliases file has a mode more permissive than 0755, this is a finding.  
  
  
**Fix Text:**Use the chmod command to change the access permissions for files executed from the alias file.  
For example:  
  
# chmod 0755 < filename >     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22441  
**Group Title:** GEN004430  
**Rule ID:** SV-26696r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004430  
**Rule Title:**Files executed through a mail aliases file must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Excessive permissions on files executed through a mail alias file could result in modification by an unauthorized user, execution of malicious code, and/or system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Examine the contents of the /etc/mail/aliases file.  
For each file referenced, check the permissions of the file.  
# ls -lL [file referenced from aliases]  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [file referenced from aliases]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-835  
**Group Title:** GEN004440  
**Rule ID:** SV-835r2\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004440  
**Rule Title:**Sendmail logging must not be set to less than nine in the sendmail.cf file.  
  
  
**Vulnerability Discussion:**  If Sendmail is not configured to log at level 9, system logs may not contain the information necessary for tracking unauthorized use of the Sendmail service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check if Sendmail logging is set to level 9.  
  
Procedure:  
# grep "O L" /etc/mail/sendmail.cf  
  
OR  
  
# grep LogLevel /etc/mail/sendmail.cf  
  
If logging is set to less than 9, this is a finding.  
  
**Fix Text:**Edit the sendmail.conf file, locate the "O L" or LogLevel entry and change it to 9.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-836  
**Group Title:** GEN004460  
**Rule ID:** SV-41546r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004460  
**Rule Title:**The system syslog service must log informational and more severe SMTP service messages.  
  
  
**Vulnerability Discussion:**  If informational and more severe SMTP service messages are not logged, malicious activity on the system may go unnoticed.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3, ECSC-1  
  
**Check Content:**    
Check the syslog configuration file for mail.crit logging configuration.  
  
Procedure:  
# more /etc/syslog.conf  
  
Verify a line similar to one of the following lines is present in syslog.conf is configured so that critical mail log data is logged. (Critical log data may also be captured by a remote log host in accordance with GEN005460.)  
  
mail.crit /var/adm/messages  
\*.crit /var/log/messages  
  
Less severe syslog levels (err, warning, info, and debug) may be substituted for crit, since they will also capture crit level syslog messages. If syslog is not configured to log critical Sendmail messages, this is a finding.  
  
**Fix Text:**Edit the syslog.conf file and add a configuration line specifying an appropriate destination for mail.crit syslogs.     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-837  
**Group Title:** GEN004480  
**Rule ID:** SV-837r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004480  
**Rule Title:**The SMTP service log file must be owned by root.  
  
  
**Vulnerability Discussion:**  If the SMTP service log file is not owned by root, then unauthorized personnel may modify or delete the file to hide a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Locate any mail log files by checking the syslog configuration file.  
  
Procedure:  
# more /etc/syslog.conf  
  
Identify any log files configured for the mail service at any severity level, or those configured for all services. Check the ownership of these log files.  
  
Procedure:  
# ls -lL <file location>  
  
If any mail log file is not owned by root, this is a finding.  
  
**Fix Text:**Change the ownership of the Sendmail log file.  
# chown root <sendmail log file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-838  
**Group Title:** GEN004500  
**Rule ID:** SV-838r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004500  
**Rule Title:**The SMTP service log file must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  If the SMTP service log file is more permissive than 0644, unauthorized users may be allowed to change the log file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the SMTP service log file.  
  
Procedure:  
# more /etc/syslog.conf  
  
Check the configuration to determine which log files contain logs for mail.crit, mail.debug, or \*.crit.  
  
Procedure:  
# ls -lL <file location>  
  
If the log file permissions are greater than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the SMTP service log file.  
  
Procedure:  
# chmod 0644 <sendmail log file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22442  
**Group Title:** GEN004510  
**Rule ID:** SV-26700r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004510  
**Rule Title:**The SMTP service log file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  If the SMTP service log file has an extended ACL, unauthorized users may be allowed to access or to modify the log file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Examine /etc/syslog.conf and determine the log file(s) receiving logs for mail.crit, mail.debug, mail.\*, or \*.crit.  
Check the permissions on these log files.  
# ls -lL [log file]  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [log file]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12006  
**Group Title:** GEN004540  
**Rule ID:** SV-42309r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004540  
**Rule Title:**The SMTP service HELP command must not be enabled.  
  
  
**Vulnerability Discussion:**  The HELP command should be disabled to mask version information. The version of the SMTP service software could be used by attackers to target vulnerabilities present in specific software versions.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check if Help is disabled in Sendmail.  
  
Procedure:  
# telnet <host> 25  
> help  
  
If the help command returns any Sendmail version information, this is a finding.  
  
If telnet is unavailable for testing, check the value of the HelpFile parameter in the sendmail.cf file.  
  
# grep HelpFile /etc/mail/sendmail.cf  
  
If the contents of the file indicated by the HelpFile parameter contains any Sendmail version information, this is a finding.  
  
**Fix Text:**To disable the SMTP HELP command, clear the Sendmail help file.  
# echo > /etc/mail/helpfile     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4384  
**Group Title:** GEN004560  
**Rule ID:** SV-42310r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004560  
**Rule Title:**The SMTP services SMTP greeting must not provide version information.  
  
  
**Vulnerability Discussion:**  The version of the SMTP service can be used by attackers to plan an attack based on vulnerabilities present in the specific version.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for the Sendmail version being displayed in the greeting.  
  
# telnet localhost 25  
  
If a version number is displayed, this is a finding.  
  
If telnet is unavailable for testing, check the value of the SmtpGreetingMessage parameter in the sendmail.cf file.  
  
# grep SmtpGreetingMessage /etc/mail/sendmail.cf  
  
If the value of the SmtpGreetingMessage parameter contains the $v or $Z macros, this is a finding.  
  
**Fix Text:**Ensure Sendmail or its equivalent has been configured to mask the version information. If necessary, change the O SmtpGreetingMessage line in the /etc/mail/sendmail.cf file as noted below.  
O SmtpGreetingMessage=$j Sendmail $v/$Z; $b  
Change it to:  
O SmtpGreetingMessage= Mail Server Ready ; $b     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4385  
**Group Title:** GEN004580  
**Rule ID:** SV-39827r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004580  
**Rule Title:**The system must not use .forward files.  
  
  
**Vulnerability Discussion:**  The .forward file allows users to automatically forward mail to another system. Use of .forward files could allow the unauthorized forwarding of mail and could potentially create mail loops which could degrade system performance.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Search for any .forward files on the system.  
  
# find / -name .forward -print  
  
This is considered a finding if any .forward files are found on the system.  
  
**Fix Text:**Remove .forward files from the system.   
  
# rm .forward  
  
Update the sendmail.cf file to ignore .forward files by adding   
ForwardPath="".  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4689  
**Group Title:** GEN004600  
**Rule ID:** SV-39819r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN004600  
**Rule Title:**The SMTP service must be an up-to-date version.  
  
  
**Vulnerability Discussion:**  The SMTP service version on the system must be current to avoid exposing vulnerabilities present in unpatched versions.  
  
**Responsibility:**  System Administrator  
**IAControls:**  VIVM-1  
  
**Check Content:**    
Determine the version of the SMTP service software, using a non-privileged account.  
$ /usr/lib/sendmail -d0 -bt < /dev/null  
(Note: While this command will report the sendmail version almost immediately, it will take several moments to return to the shell prompt. Press ctrl-C to terminate the sendmail process.)  
  
Version 8.14.4 is the latest required version.  
Version 8.14.4+Sun is available from Oracle for Solaris.  
  
If the sendmail version is not at least 8.14.4 or Oracle's latest version, this is a finding.  
  
**Fix Text:**Obtain and install the latest version of Sendmail from Oracle through normal software update processes, as implemented locally.     
  
**CCI:**CCI-001230  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4690  
**Group Title:** GEN004620  
**Rule ID:** SV-42311r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN004620  
**Rule Title:**The Sendmail server must have the debug feature disabled.  
  
  
**Vulnerability Discussion:**  Debug mode is a feature present in older versions of Sendmail which, if not disabled, may allow an attacker to gain access to a system through the Sendmail service.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for an enabled debug command provided by the SMTP service.  
  
Procedure:  
# telnet localhost 25  
debug  
  
If the command does not return a 500 error code of command unrecognized, this is a finding.  
  
If telnet is unavailable for testing, check the version of sendmail. Run the following as a non-privileged user.  
  
$ echo \$Z | /usr/sbin/sendmail -bt -d0  
  
If the version reported is less than 8.6, this is a finding.  
  
**Fix Text:**Obtain and install a more recent version of Sendmail, which does not implement the DEBUG feature.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4691  
**Group Title:** GEN004640  
**Rule ID:** SV-42312r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN004640  
**Rule Title:**The SMTP service must not have a uudecode alias active.  
  
  
**Vulnerability Discussion:**  A common configuration for older Mail Transfer Agents (MTAs) includes an alias for the decode user. All mail sent to this user is sent to the uudecode program, which automatically converts and stores files. By sending mail to decode or uudecode aliases present on some systems, a remote attacker may be able to create or overwrite files on the remote host. This could possibly be used to gain remote access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SMTP service for an active decode command.  
  
Procedure:  
# telnet localhost 25  
decode  
  
If the command does not return a 500 error code of command unrecognized, this is a finding.  
  
If telnet is unavailable for testing, check for the existence of the decode and uudecode aliases in the sendmail aliases file.  
  
Find the active sendmail aliases file.  
# grep AliasFile /etc/mail/sendmail.cf  
(The aliases file is usually at /etc/mail/aliases)  
Look for decode aliases in the aliases file.  
# grep decode /etc/mail/aliases  
  
If there is an uncommented decode or uudecode alias in the aliases file, this is a finding.  
  
**Fix Text:**Comment out active decode and uudecode aliases in the aliases file.  
  
# vi /usr/mail/aliases  
  
Activate updated aliases file.  
  
# newaliases     
  
**CCI:**CCI-001230  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4692  
**Group Title:** GEN004660  
**Rule ID:** SV-4692r2\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004660  
**Rule Title:**The SMTP service must not have the EXPN feature active.  
  
  
**Vulnerability Discussion:**  The SMTP EXPN function allows an attacker to determine if an account exists on a system, providing significant assistance to a brute-force attack on user accounts. EXPN may also provide additional information concerning users on the system, such as the full names of account owners.  
  
**False Positives:**   
False positives may occur with the SMTP EXPN check. According to RFC821, it is acceptable for a server to respond with a 250 (success) or 550 (failure) when the server supports the EXPN command. For example, some servers return "550 EXPN command not available", meaning the command is not supported and the machine is not vulnerable. However, a result of "550 That is a mailing list, not a user" would be a failure code, but not an indication of an error, and the machine would be vulnerable. If false positive is suspected, check the log file for the response from the server.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if EXPN is disabled.  
  
Procedure:  
# telnet localhost 25  
expn root  
  
If the command does not return a 500 error code of command unrecognized, this is a finding.  
  
OR  
  
Locate the sendmail.cf configuration file.  
  
Procedure:  
# find / -name sendmail.cf -print  
# grep -v "^#" <sendmail.cf location> | egrep -i "(goaway|noexpn)"  
  
Verify the EXPN command is disabled with an entry in the sendmail.cf file that reads as one of the following:  
  
Opnoexpn  
O PrivacyOptions=noexpn  
Opgoaway  
O PrivacyOptions=goaway  
  
(Other privacy options, such as novrfy or noetrn, may be included in the same line, separated by commas. The goaway option encompasses a number of privacy options, including noexpn.) If the EXPN command is not disabled, this is a finding.  
  
**Fix Text:**Edit the sendmail.cf file and add Opnoexpn option.  
Restart the Sendmail service.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4693  
**Group Title:** GEN004680  
**Rule ID:** SV-4693r2\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004680  
**Rule Title:**The SMTP service must not have the VRFY feature active.  
  
  
**Vulnerability Discussion:**  The VRFY (Verify) command allows an attacker to determine if an account exists on a system, providing significant assistance to a brute-force attack on user accounts. VRFY may provide additional information about users on the system, such as the full names of account owners.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if VRFY is disabled.  
  
Procedure:  
# telnet localhost 25  
vrfy root  
  
If the command does not return a 500 error code of command unrecognized, this is a finding.  
  
OR  
  
Locate the sendmail.cf configuration file.  
  
Procedure:  
# find / -name sendmail.cf -print  
# grep -v "^#" <sendmail.cf location> |grep -i "(goaway|vrfy)"  
  
Verify the VRFY command is disabled with an entry in the sendmail.cf file that reads as one of the following:  
  
Opnovrfy  
O PrivacyOptions=novrfy  
Opgoaway  
O PrivacyOptions=goaway  
  
(Other privacy options, such as noexpn or noetrn, may be included in the same line, separated by commas. The goaway option encompasses a number of privacy options, including novrfy.) If the VRFY command is not disabled, this is a finding.  
  
**Fix Text:**If Sendmail is running, add the line Opnovrfy to the Sendmail configuration file, usually located in /etc/sendmail.cf. For other mail servers, contact the vendor for information on how to disable the verify command. Newer versions of Sendmail are available at http://www.sendmail.org or from ftp://ftp.cs.berkeley.edu/ucb/sendmail.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4694  
**Group Title:** GEN004700  
**Rule ID:** SV-4694r2\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004700  
**Rule Title:**The Sendmail service must not have the wizard backdoor active.  
  
  
**Vulnerability Discussion:**  Very old installations of the Sendmail mailing system contained a feature whereby a remote user connecting to the SMTP port can enter the WIZ command and be given an interactive shell with root privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Locate the sendmail.cf configuration file and check for wiz configuration.  
  
Procedure:  
# find / -name sendmail.cf -print  
# grep -v "^#" <sendmail.cf location> |grep -i wiz  
  
If an entry is found for wiz, this is a finding.  
  
**Fix Text:**If the WIZ command is enabled on Sendmail, it should be disabled by adding this line to the sendmail.cf configuration file (it must be typed in uppercase).  
  
OW\*  
  
For the change to take effect, kill the Sendmail process, refreeze the sendmail.cf file, and restart the Sendmail process.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23952  
**Group Title:** GEN004710  
**Rule ID:** SV-28908r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004710  
**Rule Title:**Mail relaying must be restricted.  
  
  
**Vulnerability Discussion:**  If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending SPAM or other unauthorized activity.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system uses Sendmail, locate the sendmail.cf file.  
Procedure:  
# find / -name sendmail.cf  
  
Determine if Sendmail only binds to loopback addresses by examining the DaemonPortOptions configuration options.  
Procedure:  
# grep -i "O DaemonPortOptions" </path/to/sendmail.cf>  
  
If there are uncommented DaemonPortOptions lines, and all such lines specify system loopback addresses, this is not a finding.  
  
Otherwise, determine if Sendmail is configured to allow open relay operation.  
Procedure:  
# find / -name sendmail.mc  
# grep -i promiscuous\_relay </path/to/sendmail.mc>  
  
If the promiscuous relay feature is enabled, this is a finding.  
  
If the system uses Postfix, locate the main.cf file.  
Procedure:  
# find / -name main.cf  
  
Determine if Postfix only binds to loopback addresses by examining the inet\_interfaces line.  
Procedure:  
# grep inet\_interfaces </path/to/main.cf>  
  
If inet\_interfaces is set to loopback-only or contains only loopback addresses, such as 127.0.0.1 and [::1], Postfix is not listening on external network interfaces, this is not a finding.  
  
Otherwise, determine if Postfix is configured to restrict clients permitted to relay mail by examining the smtpd\_client\_restrictions line.  
Procedure:  
# grep smtpd\_client\_restrictions </path/to/main.cf>  
  
If the smtpd\_client\_restrictions line is missing, or does not contain reject, this is a finding. If the line contains permit before reject, this is a finding.   
  
If the system is using other SMTP software, consult the software's documentation for procedures to verify mail relaying is restricted.  
  
**Fix Text:**If the system uses Sendmail, edit the sendmail.mc file and remove the promiscuous\_relay configuration. Rebuild the sendmail.cf file from the modified sendmail.mc and restart the service. If the system does not need to receive mail from external hosts, add one or more DaemonPortOptions lines referencing system loopback addresses (such as "O DaemonPortOptions=Addr=127.0.0.1,Port=smtp,Name=MTA") and remove lines containing non-loopback addresses. Restart the service.  
  
If the system uses Postfix, edit the main.cf file and add or edit the smtpd\_client\_restrictions line to have contents permit mynetworks, reject or a similarly restrictive rule. If the system does not need to receive mail from external hosts, add or edit the inet\_interfaces line to have contents loopback-only or a set of loopback addresses for the system. Restart the service.  
  
If the system is using other SMTP software, consult the software's documentation for procedures to restrict mail relaying.     
  
**CCI:**CCI-001305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12010  
**Group Title:** GEN004800  
**Rule ID:** SV-28635r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004800  
**Rule Title:**Unencrypted FTP must not be used on the system.  
  
  
**Vulnerability Discussion:**  FTP is typically unencrypted and, therefore, presents confidentiality and integrity risks. FTP may be protected by encryption in certain cases, such as when used in a Kerberos environment. SFTP and FTPS are encrypted alternatives to FTP.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Perform the following to determine if unencrypted FTP is enabled.  
  
# svcs ftp  
  
If FTP is enabled, ask the SA if it is encrypted. If it is not, this is a finding.  
  
**Fix Text:**# svcadm disable ftp  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-846  
**Group Title:** GEN004820  
**Rule ID:** SV-846r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004820  
**Rule Title:**Anonymous FTP must not be active on the system unless authorized.  
  
  
**Vulnerability Discussion:**  Due to the numerous vulnerabilities inherent in anonymous FTP, it is recommended that it not be used. If anonymous FTP must be used on a system, the requirement must be authorized and approved in the system accreditation package.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Attempt to log into this host with a user name of anonymous and a password of guest (also try the password of guest@mail.com). If the logon is successful, this is a finding.  
  
Procedure:  
# ftp localhost  
Name: anonymous  
530 Guest login not allowed on this machine.  
  
  
**Fix Text:**Configure the FTP service to not permit anonymous logins.     
  
**CCI:**CCI-001475  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4702  
**Group Title:** GEN004840  
**Rule ID:** SV-4702r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004840  
**Rule Title:**If the system is an anonymous FTP server, it must be isolated to the DMZ network.  
  
  
**Vulnerability Discussion:**  Anonymous FTP is a public data service which is only permitted in a server capacity when located on the DMZ network.  
  
**Responsibility:**  Information Assurance Officer  
**IAControls:**  EBBD-1, EBBD-2, EBBD-3, ECSC-1  
  
**Check Content:**    
Use the command ftp to connect the system's FTP service. Attempt to log into this host with a user name of anonymous and a password of guest (also try the password of guest@mail.com). If the logon is not successful, this check is not applicable.  
  
Ask the SA if the system is located on a DMZ network. If the system is not located on a DMZ network, this is a finding.  
  
**Fix Text:**Move the system to a DMZ network.     
  
**CCI:**CCI-000787  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-840  
**Group Title:** GEN004880  
**Rule ID:** SV-28404r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004880  
**Rule Title:**The ftpusers file must exist.  
  
  
**Vulnerability Discussion:**  The ftpusers file contains a list of accounts not allowed to use FTP to transfer files. If this file does not exist, then unauthorized accounts can utilize FTP.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check for the existence of the ftpusers file.  
# ls -l /etc/ftpd/ftpusers  
If the ftpusers file does not exist, this is a finding.  
  
**Fix Text:**Create a /etc/ftpd/ftpusers file containing a list of accounts not authorized for FTP.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-841  
**Group Title:** GEN004900  
**Rule ID:** SV-28407r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004900  
**Rule Title:**The ftpusers file must contain account names not allowed to use FTP.  
  
  
**Vulnerability Discussion:**  The ftpusers file contains a list of accounts that are not allowed to use FTP to transfer files. If the file does not contain the names of all accounts not authorized to use FTP, then unauthorized use of FTP may take place.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the contents of the ftpusers file.  
  
Procedure:  
# more /etc/ftpd/ftpusers  
  
If the system has accounts not allowed to use FTP that are not listed in the ftpusers file, this is a finding.  
  
**Fix Text:**Add accounts not allowed to use FTP to the /etc/ftpd/ftpusers file.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-842  
**Group Title:** GEN004920  
**Rule ID:** SV-28410r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004920  
**Rule Title:**The ftpusers file must be owned by root.  
  
  
**Vulnerability Discussion:**  If the file ftpusers is not owned by root, an unauthorized user may modify the file to allow unauthorized accounts to use FTP.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the ftpusers file.  
# ls -l /etc/ftpd/ftpusers  
If the ftpusers file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the ftpusers file to root.  
# chown root /etc/ftpd/ftpusers  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22444  
**Group Title:** GEN004930  
**Rule ID:** SV-39905r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004930  
**Rule Title:**The ftpusers file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the ftpusers file is not group-owned by root or a system group, an unauthorized user may modify the file to allow unauthorized accounts to use FTP.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the ftpusers file.  
  
Procedure:  
# ls -lL /etc/ftpd/ftpusers /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the ftpusers file.  
  
Procedure:  
# chgrp root /etc/ftpusers     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-843  
**Group Title:** GEN004940  
**Rule ID:** SV-28413r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004940  
**Rule Title:**The ftpusers file must have mode 0640 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the ftpusers file could permit unauthorized modification. Unauthorized modification could result in Denial of Service to authorized FTP users or permit unauthorized users to access the FTP service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the ftpusers file.  
# ls -l /etc/ftpd/ftpusers  
If the ftpusers file has a mode more permissive than 0640, this is a finding.  
  
**Fix Text:**Change the mode of the ftpusers file to 0640.  
# chmod 0640 /etc/ftpd/ftpusers     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22445  
**Group Title:** GEN004950  
**Rule ID:** SV-26707r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004950  
**Rule Title:**The ftpusers file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the ftpusers file could permit unauthorized modification. Unauthorized modification could result in Denial of Service to authorized FTP users or permit unauthorized users to access the FTP service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the /etc/ftpd/ftpusers file.  
# ls -lL /etc/ftpd/ftpusers  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/ftpd/ftpusers     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-845  
**Group Title:** GEN004980  
**Rule ID:** SV-40816r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004980  
**Rule Title:**The FTP daemon must be configured for logging or verbose mode.  
  
  
**Vulnerability Discussion:**  The -l option allows basic logging of connections. The verbose (on HP) and the debug (on Solaris) allow logging of what files the FTP session transferred. This extra logging makes it possible to easily track which files are being transferred onto or from a system. If they are not configured, the only option for tracking is the audit files. The audit files are much harder to read. If auditing is not properly configured, then there would be no record at all of the file transfer transactions.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Verify the FTP daemon is invoked with the -l option by SMF.  
# inetadm -l ftp | grep in.ftpd  
If the exec name-value pair does not include the -l option for in.ftpd, this is a finding.  
  
**Fix Text:**Add the -l option to the exec name-value pair used by SMF to invoke the FTP daemon.  
# inetadm -m ftp exec="/usr/sbin/in.ftpd [other options] -l"  
Refresh inetd.  
# svcadm refresh inetd     
  
**CCI:**CCI-000130  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4387  
**Group Title:** GEN005000  
**Rule ID:** SV-4387r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005000  
**Rule Title:**Anonymous FTP accounts must not have a functional shell.  
  
  
**Vulnerability Discussion:**  If an anonymous FTP account has been configured to use a functional shell, attackers could gain access to the shell if the account is compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the shell for the anonymous FTP account.  
  
Procedure:  
# grep "^ftp" /etc/passwd  
  
This is a finding if the seventh field is empty (the entry ends with a ':') or if the seventh field does not contain one of the following.  
  
/bin/false  
/dev/null  
/usr/bin/false  
/bin/true  
/sbin/nologin  
  
**Fix Text:**Configure anonymous FTP accounts to use a non-functional shell. If necessary, edit the /etc/passwd file to remove any functioning shells associated with the FTP account and replace them with non-functioning shells, such as, /dev/null.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4388  
**Group Title:** GEN005020  
**Rule ID:** SV-39838r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005020  
**Rule Title:**The anonymous FTP account must be configured to use chroot or a similarly isolated environment.  
  
  
**Vulnerability Discussion:**  If an anonymous FTP account does not use a chroot or similarly isolated environment, the system may be more vulnerable to exploits against the FTP service. Such exploits could allow an attacker to gain shell access to the system and view, edit, or remove sensitive files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
The default Solaris FTP daemon, in.ftpd, uses the ftp user's home directory as the chroot base for anonymous FTP. If any files and directories within the ftp user's home directory are owned by any user other than root, or if any subdirectory other than pub has permissions more permissive than 0111, this is a finding.  
  
**Fix Text:**Run the ftpconfig(1M) command to set up a chroot-ed environment for anonymous FTP with appropriate constraints.  
  
# ftpconfig < anonymous FTP home directory>     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12011  
**Group Title:** GEN005040  
**Rule ID:** SV-12512r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005040  
**Rule Title:**All FTP users must have a default umask of 077.  
  
  
**Vulnerability Discussion:**  The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask is stored as a 4-digit number, the first digit representing special access modes is typically ignored or required to be 0.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the umask setting for the FTP user.  
  
Procedure:  
# su - ftp  
$ umask  
  
If the umask value does not return 077, this is a finding.  
  
**Fix Text:**Edit the initialization files for the FTP user and set the umask to 077.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-847  
**Group Title:** GEN005080  
**Rule ID:** SV-28419r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005080  
**Rule Title:**The TFTP daemon must operate in secure mode which provides access only to a single directory on the host file system.  
  
  
**Vulnerability Discussion:**  Secure mode limits TFTP requests to a specific directory. If TFTP is not running in secure mode, it may be able to write to any file or directory and may seriously impair system integrity, confidentiality, and availability.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if TFTPD is running in secure mode.  
# grep tftp /etc/inet/inetd.conf  
If any returned service line does not use the -s parameter to TFTPD, this is a finding.  
  
**Fix Text:**Edit /etc/inet/inetd.conf and add the -s parameter to TFTPD.  
# inetconv     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-848  
**Group Title:** GEN005100  
**Rule ID:** SV-40392r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005100  
**Rule Title:**The TFTP daemon must have mode 0755 or less permissive.  
  
  
**Vulnerability Discussion:**  If TFTP runs with the setuid or setgid bit set, it may be able to write to any file or directory and may seriously impair system integrity, confidentiality, and availability.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Check the mode of the TFTP daemon.  
  
Procedure:  
  
# ls -lL /usr/sbin/in.tftpd  
  
If the mode of the file is more permissive than 0755, this is a finding.  
  
**Fix Text:**Change the mode of the TFTP daemon.  
  
Procedure:  
# chmod 0755 /usr/sbin/in.tftpd     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-849  
**Group Title:** GEN005120  
**Rule ID:** SV-39825r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005120  
**Rule Title:**The TFTP daemon must be configured to vendor specifications, including a dedicated TFTP user account, a non-login shell, such as /bin/false, and a home directory owned by the TFTP user.  
  
  
**Vulnerability Discussion:**  If TFTP has a valid shell, it increases the likelihood of someone logging to the TFTP account and compromising the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the tftp service is enabled.  
  
# svcs tftp  
  
If the tftp service is not installed or enabled, this check is not applicable.  
  
Check the /etc/passwd file to determine if TFTP is configured properly.  
  
Procedure:  
# grep tftp /etc/passwd  
  
If a "tftp" user account does not exist and TFTP is active, this is a finding.  
  
Check the user shell for the "tftp" user. If it is not /bin/false or equivalent, this is a finding.  
  
Check the home directory assigned to the "tftp" user. If no home directory is set, or the directory specified is not dedicated to the use of the TFTP service, this is a finding.  
  
  
  
**Fix Text:**Create a TFTP user account if none exists.  
Assign a non-login shell to the TFTP user account, such as /bin/false.  
Assign a home directory to the TFTP user account.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4695  
**Group Title:** GEN005140  
**Rule ID:** SV-28423r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005140  
**Rule Title:**Any active TFTP daemon must be authorized and approved in the system accreditation package.  
  
  
**Vulnerability Discussion:**  TFTP is a file transfer protocol often used by embedded systems to obtain configuration data or software. The service is unencrypted and does not require authentication of requests. Data available using this service may be subject to unauthorized access or interception.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSW-1  
  
**Check Content:**    
Determine if the TFTP daemon is active.  
# svcs svc:/network/tftp/\*  
If TFTP is found enabled, it is a finding if it is not documented using site-defined procedures.  
  
**Fix Text:**Disable the TFTP daemon.  
# svcadm disable svc:/network/tftp/\*  
# svcadm refresh inetd  
If TFTP is found enabled, it is a finding if it is not documented.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-850  
**Group Title:** GEN005160  
**Rule ID:** SV-850r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005160  
**Rule Title:**Any X Windows host must write .Xauthority files.  
  
  
**Vulnerability Discussion:**  .Xauthority files ensure the user is authorized to access the specific X Windows host. If .Xauthority files are not used, it may be possible to obtain unauthorized access to the X Windows host.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check for .Xauthority files being utilized by looking for such files in the home directory of a user that uses X.  
  
Procedure:  
# cd ~someuser  
# ls -la .Xauthority  
  
If the .Xauthority file does not exist, ask the SA if the user is using X Windows. If the user is utilizing X Windows and the .Xauthority file does not exist, this is a finding.  
  
**Fix Text:**Ensure the X Windows host is configured to write .Xauthority files into user home directories. Edit the Xaccess file. Ensure the line that writes the .Xauthority file is uncommented.     
  
**CCI:**CCI-000297  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12014  
**Group Title:** GEN005180  
**Rule ID:** SV-12515r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005180  
**Rule Title:**All .Xauthority files must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  .Xauthority files ensure the user is authorized to access the specific X Windows host. Excessive permissions may permit unauthorized modification of these files, which could lead to Denial of Service to authorized access or allow unauthorized access to be obtained.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the file permissions for the .Xauthority files in the home directories of users of X.  
  
Procedure:  
# cd ~<X user>  
# ls -lL .Xauthority  
  
If the file mode is more permissive than 0600, this is finding.  
  
  
**Fix Text:**Change the mode of the .Xauthority files.  
  
Procedure:  
# chmod 0600 .Xauthority     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22446  
**Group Title:** GEN005190  
**Rule ID:** SV-26711r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005190  
**Rule Title:**The .Xauthority files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  .Xauthority files ensure the user is authorized to access the specific X Windows host. Extended ACLs may permit unauthorized modification of these files, which could lead to Denial of Service to authorized access or allow unauthorized access to be obtained.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the file permissions for the .Xauthority files.  
# ls -lL .Xauthority  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- .Xauthority     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4697  
**Group Title:** GEN005200  
**Rule ID:** SV-4697r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005200  
**Rule Title:**X displays must not be exported to the world.  
  
  
**Vulnerability Discussion:**  Open X displays allow an attacker to capture keystrokes and to execute commands remotely. Many users have their X Server set to xhost +, permitting access to the X Server by anyone, from anywhere.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If X Windows is not used on the system, this is not applicable.  
  
Check the output of the xhost command from an X terminal.  
  
Procedure:  
$ xhost  
If the output reports access control is enabled (and possibly lists the hosts that can receive X Window logins), this is not a finding. If the xhost command returns a line indicating access control is disabled, this is a finding.  
  
NOTE: It may be necessary to define the display if the command reports it cannot open the display.   
  
Procedure:  
$ DISPLAY=MachineName:0.0; export DISPLAY  
MachineName may be replaced with an Internet Protocol Address. Repeat the check procedure after setting the display.  
  
**Fix Text:**If using an xhost-type authentication the xhost - command can be used to remove current trusted hosts and then selectively allow only trusted hosts to connect with xhost + commands. A cryptographically secure authentication, such as provided by the xauth program, is always preferred. Refer to your X11 server's documentation for further security information.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12016  
**Group Title:** GEN005220  
**Rule ID:** SV-12517r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005220  
**Rule Title:**.Xauthority or X\*.hosts (or equivalent) file(s) must be used to restrict access to the X server.  
  
  
**Vulnerability Discussion:**  If access to the X server is not restricted, a user's X session may be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Determine if the X server is running.  
Procedure:  
# ps -ef |grep X  
  
Determine if xauth is being used.  
Procedure:  
# xauth  
xauth> list  
  
If the above command sequence does not show any host other than the localhost, then xauth is not being used.  
  
Search the system for an X\*.hosts files, where \* is a display number that may be used to limit X window connections. If no files are found, X\*.hosts files are not being used. If the X\*.hosts files contain any unauthorized hosts, this is a finding.  
  
If both xauth and X\*.hosts files are not being used, this is a finding.  
  
**Fix Text:**Create an X\*.hosts file, where \* is a display number that may be used to limit X window connections. Add the list of authorized X clients to the file.     
  
**CCI:**CCI-000297  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12017  
**Group Title:** GEN005240  
**Rule ID:** SV-12518r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005240  
**Rule Title:**The .Xauthority utility must only permit access to authorized hosts.  
  
  
**Vulnerability Discussion:**  If unauthorized clients are permitted access to the X server, a user's X session may be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the X Window system access is limited to authorized clients.  
  
Procedure:  
# xauth  
xauth> list  
  
Ask the SA if the clients listed are authorized. If any are not, this is a finding.  
  
**Fix Text:**Remove unauthorized clients from the xauth configuration.  
# xauth remove <display name>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12018  
**Group Title:** GEN005260  
**Rule ID:** SV-12519r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005260  
**Rule Title:**X Window System connections that are not required must be disabled.  
  
  
**Vulnerability Discussion:**  If unauthorized clients are permitted access to the X server, a user's X session may be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the X Window system is running.  
  
Procedure:  
# ps -ef |grep X  
  
Ask the SA if the X Window system is an operational requirement. If it is not, this is a finding.  
  
**Fix Text:**Disable the X Windows server on the system.     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4696  
**Group Title:** GEN005280  
**Rule ID:** SV-28428r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005280  
**Rule Title:**The system must not have the UUCP service active.  
  
  
**Vulnerability Discussion:**  The UUCP utility is designed to assist in transferring files, executing remote commands, and sending email between UNIX systems over phone lines and direct connections between systems. The UUCP utility is a primitive and arcane system with many security issues. There are alternate data transfer utilities/products that can be configured to more securely transfer data by providing for authentication, as well as encryption.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# svcs uucp  
If UUCP is found enabled, this is a finding.  
  
**Fix Text:**# svcadm disable uucp  
# svcadm refresh inetd     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-993  
**Group Title:** GEN005300  
**Rule ID:** SV-40281r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005300  
**Rule Title:**SNMP communities, users, and passphrases must be changed from the default.  
  
  
**Vulnerability Discussion:**  Whether active or not, default SNMP passwords, users, and passphrases must be changed to maintain security. If the service is running with the default authenticators, then anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s).  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAAC-1  
  
**Check Content:**    
Check the SNMP configuration for default passwords.  
  
Locate and examine the SNMP configuration.  
Procedure:  
# more /etc/sma/snmp/snmpd.conf /var/sma\_snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /usr/sfw/lib/sma\_snmp/snmpd.conf  
  
Identify any community names or user password configuration. If any community name or password is set to a default value, such as public, private, snmp-trap, password, or any value which does not meet DISA password requirements, this is a finding.  
  
**Fix Text:**Change the default passwords. To change them, locate the snmpd.conf file and edit it. Locate the line system-group-read-community which has a default password of public and make the password something more random (less guessable). Make the same changes for the lines that read system-group-write-community, read-community, write-community, trap, and trap-community. Read the information in the file carefully. The trap is defining who to send traps to, for instance, by default. It is not a password, but the name of a host.     
  
**CCI:**CCI-000178  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22447  
**Group Title:** GEN005305  
**Rule ID:** SV-26715r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005305  
**Rule Title:**The SNMP service must use only SNMPv3 or its successors.  
  
  
**Vulnerability Discussion:**  SNMP Versions 1 and 2 are not considered secure. Without the strong authentication and privacy provided by the SNMP Version 3 User-based Security Model (USM), an attacker or other unauthorized users may gain access to detailed system management information and use the information to launch attacks against the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1  
  
**Check Content:**    
Verify the SNMP daemon is not configured to use the v1 or v2c security models.  
# egrep '(v1|v2c|community|com2sec)' /etc/sma/snmp/snmpd.conf /var/sma\_snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /usr/sfw/lib/sma\_snmp/snmpd.conf | grep -v '^#'  
If any configuration is found, this is a finding.  
  
**Fix Text:**Edit non-compliant snmpd.conf files and remove references to the v1, v2c, community, or com2sec. Restart the SNMP service.  
# svcadm restart svc:/application/management/sma:default     
  
**CCI:**CCI-001435  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-994  
**Group Title:** GEN005320  
**Rule ID:** SV-40262r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005320  
**Rule Title:**The snmpd.conf file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  The snmpd.conf file contains authenticators and must be protected from unauthorized access and modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the SNMP daemon configuration files.  
Procedure:  
# ls -lL /etc/sma/snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /var/sma\_snmp/snmpd.conf /usr/sfw/lib/sma\_snmp/snmpd.conf  
  
If any of the snmpd.conf files have a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the SNMP daemon configuration file to 0600.   
  
Procedure:  
# chmod 0600 <snmpd.conf>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-995  
**Group Title:** GEN005340  
**Rule ID:** SV-40817r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005340  
**Rule Title:**Management Information Base (MIB) files must have mode 0640 or less permissive.  
  
  
**Vulnerability Discussion:**  The ability to read the MIB file could impart special knowledge to an intruder or malicious user about the ability to extract compromising information about the system or network.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the modes for all Management Information Base (MIB) files on the system.  
  
# find /etc/sma/snmp/ /etc/snmp/conf/ /var/sma\_snmp/ /usr/sfw/lib/sma\_snmp/ -type f | grep -i mib | egrep -v '\.conf$' | xargs ls -lL  
  
If any file is returned that does not have mode 0640 or less permissive, this is a finding.  
  
**Fix Text:**Change the mode of MIB files to 0640.  
  
Procedure:  
# chmod 0640 <mib file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22450  
**Group Title:** GEN005350  
**Rule ID:** SV-26727r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005350  
**Rule Title:**Management Information Base (MIB) files must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  The ability to read the MIB file could impart special knowledge to an intruder or malicious user about the ability to extract compromising information about the system or network.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the modes for all Management Information Base (MIB) files on the system.  
  
# find /etc/sma/snmp/ /etc/snmp/conf/ /var/sma\_snmp/ /usr/sfw/lib/sma\_snmp/ -type f | grep -i mib | egrep -v '\.conf$' | xargs ls -lL  
  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- [mib file]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12019  
**Group Title:** GEN005360  
**Rule ID:** SV-40274r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005360  
**Rule Title:**The snmpd.conf files must be owned by root.  
  
  
**Vulnerability Discussion:**  The snmpd.conf files contain authenticators and must be protected from unauthorized access and modification. If the files are not owned by root, they may be subject to access and modification from unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine the owner of the SNMP configuration files.   
  
Procedure:  
  
# ls -lL /etc/sma/snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /var/sma\_snmp/snmpd.conf /usr/sfw/lib/sma\_snmp/snmpd.conf  
  
If the snmpd.conf files are not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the snmpd.conf file to root.  
  
Procedure:  
# chown root <snmpd.conf file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22451  
**Group Title:** GEN005365  
**Rule ID:** SV-26733r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005365  
**Rule Title:**The snmpd.conf file must be group-owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  The snmpd.conf file contains authenticators and must be protected from unauthorized access and modification. If the file is not group-owned by a system group, it may be subject to access and modification from unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the SNMP configuration files.  
  
Procedure:  
# ls -lL /etc/sma/snmp/snmpd.conf /var/sma\_snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /usr/sfw/lib/sma\_snmp/snmpd.conf  
  
If the files are not group-owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the group ownership of the SNMP configuration file.  
  
Procedure:  
# chgrp root /etc/sma/snmp/snmpd.conf /var/sma\_snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /usr/sfw/lib/sma\_snmp/snmpd.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22452  
**Group Title:** GEN005375  
**Rule ID:** SV-26737r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005375  
**Rule Title:**The snmpd.conf file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  The snmpd.conf file contains authenticators and must be protected from unauthorized access and modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the SNMP configuration files.  
# ls -lL/etc/sma/snmp/snmpd.conf /var/sma\_snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /usr/sfw/lib/sma\_snmp/snmpd.conf  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the files.  
# chmod A- /etc/sma/snmp/snmpd.conf /var/sma\_snmp/snmpd.conf /etc/snmp/conf/snmpd.conf /usr/sfw/lib/sma\_snmp/snmpd.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4392  
**Group Title:** GEN005380  
**Rule ID:** SV-4392r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005380  
**Rule Title:**If the system is a Network Management System (NMS) server, it must only run the NMS and any software required by the NMS.  
  
  
**Vulnerability Discussion:**  Installing extraneous software on a system designated as a dedicated Network Management System (NMS) server poses a security threat to the system and the network. Should an attacker gain access to the NMS through unauthorized software, the entire network may be susceptible to malicious activity.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPA-1  
  
**Check Content:**    
Ask the SA if this is an NMS server. If it is an NMS server, then ask what other applications run on it. If there is anything other than network management software and DBMS software used only for the storage and inquiry of NMS data, this is a finding.  
  
**Fix Text:**Ensure only authorized software is loaded on a designated NMS server. Authorized software is limited to the NMS software itself, a database management system for the NMS server if necessary, and network management software.     
  
**CCI:**CCI-001208  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22453  
**Group Title:** GEN005390  
**Rule ID:** SV-26740r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005390  
**Rule Title:**The /etc/syslog.conf file must have mode 0640 or less permissive.  
  
  
**Vulnerability Discussion:**  Unauthorized users must not be allowed to access or modify the /etc/syslog.conf file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the syslog configuration file.  
# ls -lL /etc/syslog.conf  
If the mode of the file is more permissive than 0640, this is a finding.  
  
**Fix Text:**Change the permissions of the syslog configuration file.  
# chmod 0640 /etc/syslog.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22454  
**Group Title:** GEN005395  
**Rule ID:** SV-26743r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005395  
**Rule Title:**The /etc/syslog.conf file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Unauthorized users must not be allowed to access or modify the /etc/syslog.conf file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the syslog configuration file.  
# ls -lL /etc/syslog.conf  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/syslog.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4393  
**Group Title:** GEN005400  
**Rule ID:** SV-4393r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005400  
**Rule Title:**The /etc/syslog.conf file must be owned by root.  
  
  
**Vulnerability Discussion:**  If the /etc/syslog.conf file is not owned by root, unauthorized users could be allowed to view, edit, or delete important system messages handled by the syslog facility.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/syslog.conf ownership.  
  
# ls -lL /etc/syslog.conf  
  
If /etc/syslog.conf is not owned by root, this is a finding.  
  
**Fix Text:**Use the chown command to set the owner to root.  
# chown root /etc/syslog.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4394  
**Group Title:** GEN005420  
**Rule ID:** SV-39892r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005420  
**Rule Title:**The /etc/syslog.conf file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the group owner of /etc/syslog.conf is not root, bin, or sys, unauthorized users could be permitted to view, edit, or delete important system messages handled by the syslog facility.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/syslog.conf group ownership.  
  
Procedure:  
# ls -lL /etc/syslog.conf  
  
If /etc/syslog.conf is not group-owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/syslog.conf file to root, bin, or sys.  
  
Procedure:  
# chgrp root /etc/syslog.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12020  
**Group Title:** GEN005440  
**Rule ID:** SV-41515r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005440  
**Rule Title:**The system must not be used as a syslog server (log host) for systems external to the enclave.  
  
  
**Vulnerability Discussion:**  Syslog messages are typically unencrypted and may contain sensitive information and are, therefore, restricted to the enclave.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Ask the SA if the log host server is collecting data for hosts outside the local enclave. If it is, this is a finding.  
  
**Fix Text:**Configure the hosts outside of the local enclave to not log to this system.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22455  
**Group Title:** GEN005450  
**Rule ID:** SV-26745r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005450  
**Rule Title:**The system must use a remote syslog server (log host).  
  
  
**Vulnerability Discussion:**  A syslog server (log host) receives syslog messages from one or more systems. This data can be used as an authoritative log source in the event a system is compromised and its local logs are suspect.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Check the syslog configuration file for remote syslog servers.  
# grep '@' /etc/syslog.conf | grep -v '^#'  
If no line is returned, this is a finding.  
  
**Fix Text:**Edit the syslog configuration file and add an appropriate remote syslog server.     
  
**CCI:**CCI-000136  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4395  
**Group Title:** GEN005460  
**Rule ID:** SV-4395r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005460  
**Rule Title:**The system must only use remote syslog servers (log hosts) justified and documented using site-defined procedures.  
  
  
**Vulnerability Discussion:**  If a remote log host is in use and it has not been justified and documented with the IAO, sensitive information could be obtained by unauthorized users without the SA's knowledge. A remote log host is any host to which the system is sending syslog messages over a network.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Examine the syslog.conf file for any references to remote log hosts.  
# grep -v "^#" /etc/syslog.conf | grep '@'  
Destination locations beginning with an @ represent log hosts. If the log host name is a local alias, such as log host, consult the /etc/hosts or other name databases as necessary to obtain the canonical name or address for the log host. Determine if the host referenced is a log host documented using site-defined procedures. If an undocumented log host is referenced, this is a finding.  
  
**Fix Text:**Remove, replace, or document the referenced undocumented log host.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12021  
**Group Title:** GEN005480  
**Rule ID:** SV-28431r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005480  
**Rule Title:**The syslog daemon must not accept remote messages unless it is a syslog server documented using site-defined procedures.  
  
  
**Vulnerability Discussion:**  Unintentionally running a syslog server accepting remote messages puts the system at increased risk. Malicious syslog messages sent to the server could exploit vulnerabilities in the server software itself, could introduce misleading information in to the system's logs, or could fill the system's storage leading to a Denial of Service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# svcprop system-log | grep log\_from\_remote  
  
If the config/log\_from\_remote value is not false, this is a finding.  
  
  
**Fix Text:**# svccfg -s system-log setprop config/log\_from\_remote=false  
# svcadm refresh system-log     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4295  
**Group Title:** GEN005500  
**Rule ID:** SV-39817r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005500  
**Rule Title:**The SSH daemon must be configured to only use the SSHv2 protocol.  
  
  
**Vulnerability Discussion:**  SSHv1 is not a DoD-approved protocol and has many well-known vulnerability exploits. Exploits of the SSH daemon could provide immediate root access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1, ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for allowed protocol versions.   
  
# grep -i protocol /etc/ssh/sshd\_config | grep -v '^#'   
  
If the variables Protocol 2,1 or Protocol 1 are defined on a line without a leading comment, this is a finding.  
  
**Fix Text:**Edit the configuration file and modify the Protocol line to look like:  
  
Protocol 2  
  
Reload sshd:  
kill -HUP <PID of sshd>     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22456  
**Group Title:** GEN005501  
**Rule ID:** SV-26749r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005501  
**Rule Title:**The SSH client must be configured to only use the SSHv2 protocol.  
  
  
**Vulnerability Discussion:**  SSHv1 is not a DoD-approved protocol and has many well-known vulnerability exploits. Exploits of the SSH client could provide access to the system with the privileges of the user running the client.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1  
  
**Check Content:**    
Check the SSH client configuration for allowed protocol versions.  
# grep -i protocol /etc/ssh/ssh\_config | grep -v '^#'   
If the returned protocol configuration allows versions less than 2, this is a finding.  
  
**Fix Text:**Edit the /etc/ssh/ssh\_config file and add or edit a Protocol configuration line that does not allow versions less than 2.     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22457  
**Group Title:** GEN005504  
**Rule ID:** SV-26750r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005504  
**Rule Title:**The SSH daemon must only listen on management network addresses unless authorized for uses other than management.  
  
  
**Vulnerability Discussion:**  The SSH daemon should only listen on network addresses designated for management traffic. If the system has multiple network interfaces and SSH listens on addresses not designated for management traffic, the SSH service could be subject to unauthorized access. If SSH is used for purposes other than management, such as providing an SFTP service, the list of approved listening addresses may be documented.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for listening network addresses.  
# grep -i Listen /etc/ssh/sshd\_config | grep -v '^#'  
If no configuration is returned, or if a returned Listen configuration contains addresses not designated for management traffic, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration to specify listening network addresses designated for management traffic.     
  
**CCI:**CCI-000069  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22458  
**Group Title:** GEN005505  
**Rule ID:** SV-41035r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005505  
**Rule Title:**The SSH daemon must be configured to only use FIPS 140-2 approved ciphers.  
  
  
**Vulnerability Discussion:**  DoD information systems are required to use FIPS 140-2 approved ciphers. SSHv2 ciphers meeting this requirement are 3DES and AES.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Check the SSH daemon configuration for allowed ciphers.  
# grep -i ciphers /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, or the returned ciphers list contains any cipher not starting with 3des or aes, this is a finding.  
  
**Fix Text:**Edit /etc/ssh/sshd\_config and change or set the Ciphers line to the following.  
  
Ciphers aes128-ctr, aes192-ctr, aes256-ctr     
  
**CCI:**CCI-000068  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22459  
**Group Title:** GEN005506  
**Rule ID:** SV-26752r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005506  
**Rule Title:**The SSH daemon must be configured to not use Cipher-Block Chaining (CBC) ciphers.  
  
  
**Vulnerability Discussion:**  The Cipher-Block Chaining (CBC) mode of encryption as implemented in the SSHv2 protocol is vulnerable to chosen plain text attacks and must not be used.  
  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for allowed ciphers.  
# grep -i ciphers /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, or the returned ciphers list contains any cipher ending with cbc, this is a finding.  
  
  
**Fix Text:**Edit /etc/ssh/sshd\_config and add or edit the "Ciphers" line. Only include ciphers that start with "3des" or "aes" and do not contain "cbc". For the list of available ciphers for the particular version of your software, consult the sshd\_config manpage.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22460  
**Group Title:** GEN005507  
**Rule ID:** SV-26753r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005507  
**Rule Title:**The SSH daemon must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.  
  
  
**Vulnerability Discussion:**  DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Check the SSH daemon configuration for allowed MACs.  
  
Procedure:  
# grep -i macs /etc/ssh/sshd\_config | grep -v '^#'   
  
If no lines are returned, or the returned MACs list contains any MAC other than hmac-sha1, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and remove any MACs other than hmac-sha1. If necessary, add a MACs line.     
  
**CCI:**CCI-001453  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22461  
**Group Title:** GEN005510  
**Rule ID:** SV-26754r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005510  
**Rule Title:**The SSH client must be configured to only use FIPS 140-2 approved ciphers.  
  
  
**Vulnerability Discussion:**  DoD information systems are required to use FIPS 140-2 approved ciphers. SSHv2 ciphers meeting this requirement are 3DES and AES.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Check the SSH client configuration for allowed ciphers.  
# grep -i ciphers /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, the returned ciphers list contains any cipher not starting with 3des or aes, this is a finding.  
  
**Fix Text:**Edit /etc/ssh/ssh\_config and add or edit the "Ciphers" line. Only include ciphers that start with "3des" or "aes" and do not contain "cbc". For the list of available ciphers for the particular version of your software, consult the ssh\_config manpage.     
  
**CCI:**CCI-000068  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22462  
**Group Title:** GEN005511  
**Rule ID:** SV-26755r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005511  
**Rule Title:**The SSH client must be configured to not use CBC-based ciphers.  
  
  
**Vulnerability Discussion:**  The Cipher-Block Chaining (CBC) mode of encryption as implemented in the SSHv2 protocol is vulnerable to chosen plain text attacks and must not be used.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH client configuration for allowed ciphers.  
# grep -i ciphers /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, or the returned ciphers list contains any cipher ending with cbc, this is a finding.  
  
**Fix Text:**Edit /etc/ssh/ssh\_config and add or edit the "Ciphers" line. Only include ciphers that start with "3des" or "aes" and do not contain "cbc". For the list of available ciphers for the particular version of your software, consult the ssh\_config manpage.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22463  
**Group Title:** GEN005512  
**Rule ID:** SV-26756r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005512  
**Rule Title:**The SSH client must be configured to only use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hash algorithms.  
  
  
**Vulnerability Discussion:**  DoD information systems are required to use FIPS 140-2 approved cryptographic hash functions.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Check the SSH client configuration for allowed MACs.  
# grep -i macs /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, or the returned MACs list contains any MAC other than hmac-sha1, this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and remove any MACs other than hmac-sha1. If necessary, add a MACs line.     
  
**CCI:**CCI-001453  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22470  
**Group Title:** GEN005521  
**Rule ID:** SV-26763r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005521  
**Rule Title:**The SSH daemon must restrict login ability to specific users and/or groups.  
  
  
**Vulnerability Discussion:**  Restricting SSH logins to a limited group of users, such as system administrators, prevents password-guessing and other SSH attacks from reaching system accounts and other accounts not authorized for SSH access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the SSH daemon configuration for the AllowGroups setting.  
# grep -i AllowGroups /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and add an AllowGroups directive.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22471  
**Group Title:** GEN005522  
**Rule ID:** SV-26764r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005522  
**Rule Title:**The SSH public host key files must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  If a public host key file is modified by an unauthorized user, the SSH service may be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions for SSH public host key files.  
# ls -lL /etc/ssh/\*key.pub  
If any file has a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the permissions for the SSH public host key files.  
# chmod 0644 /etc/ssh/\*key.pub     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22472  
**Group Title:** GEN005523  
**Rule ID:** SV-26765r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005523  
**Rule Title:**The SSH private host key files must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  If an unauthorized user obtains the private SSH host key file, the host could be impersonated.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions for SSH private host key files.  
# ls -lL /etc/ssh/\*key  
If any file has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the permissions for the SSH private host key files.  
# chmod 0600 /etc/ssh/\*key     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22473  
**Group Title:** GEN005524  
**Rule ID:** SV-26766r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005524  
**Rule Title:**The SSH daemon must not permit GSSAPI authentication unless needed.  
  
  
**Vulnerability Discussion:**  GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system’s GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Ask the SA if GSSAPI authentication is used for SSH authentication to the system. If so, this is not applicable.  
  
Check the SSH daemon configuration for the GSSAPI authentication setting.  
# grep -i GSSAPIAuthentication /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, or the setting is set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and set (add if necessary) a GSSAPIAuthentication directive set to no.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22474  
**Group Title:** GEN005525  
**Rule ID:** SV-26767r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005525  
**Rule Title:**The SSH client must not permit GSSAPI authentication unless needed.  
  
  
**Vulnerability Discussion:**  GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system’s GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH clients configuration for the GSSAPI authentication setting.  
# grep -i GSSAPIAuthentication /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, or the setting is set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and set (add if necessary) a GSSAPIAuthentication directive set to no.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22485  
**Group Title:** GEN005536  
**Rule ID:** SV-40400r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005536  
**Rule Title:**The SSH daemon must perform strict mode checking of home directory configuration files.  
  
  
**Vulnerability Discussion:**  If other users have access to modify user-specific SSH configuration files, they may be able to log into the system as another user.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the SSH daemon configuration for the StrictModes setting.  
# grep -i StrictModes /etc/ssh/sshd\_config | grep -v '^#'  
If the setting is present and not set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and change the StrictModes setting value to yes or remove it entirely.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22487  
**Group Title:** GEN005538  
**Rule ID:** SV-40396r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005538  
**Rule Title:**The SSH daemon must not allow rhosts RSA authentication.   
  
  
**Vulnerability Discussion:**  If SSH permits rhosts RSA authentication, a user may be able to log in based on the keys of the host originating the request and not any user-specific authentication.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for the RhostsRSAAuthentication setting.  
# grep -i RhostsRSAAuthentication /etc/ssh/sshd\_config | grep -v '^#'  
If the setting is set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and change the RhostsRSAAuthentication setting value to no or remove it entirely.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22488  
**Group Title:** GEN005539  
**Rule ID:** SV-26787r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005539  
**Rule Title:**The SSH daemon must not allow compression or must only allow compression after successful authentication.  
  
  
**Vulnerability Discussion:**  If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for the Compression setting.  
# grep -i Compression /etc/ssh/sshd\_config | grep -v '^#'   
If the setting is not present, or set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and add or edit the Compression setting value to no or delayed.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12022  
**Group Title:** GEN005540  
**Rule ID:** SV-40279r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005540  
**Rule Title:**The SSH daemon must be configured for IP filtering.  
  
  
**Vulnerability Discussion:**  The SSH daemon must be configured for IP filtering to provide a layered defense against connection attempts from unauthorized addresses.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1, ECWM-1  
  
**Check Content:**    
Check the TCP wrappers configuration files to determine if SSHD is configured to use TCP wrappers.  
  
Procedure:  
# egrep '^[^#:]\*(ALL|sshd)' /etc/hosts.deny  
# egrep '^[^#:]\*(ALL|sshd)' /etc/hosts.allow  
  
If neither of the hosts.deny or hosts.allow files exist, this is a finding.  
If no entries are returned, the TCP wrappers are not configured for SSHD, this is a finding.  
  
**Fix Text:**Add appropriate IP restrictions for SSH to the /etc/hosts.deny and/or /etc/hosts.allow files.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22489  
**Group Title:** GEN005550  
**Rule ID:** SV-40280r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005550  
**Rule Title:**The SSH daemon must be configured with the Department of Defense (DoD) login banner.  
  
  
**Vulnerability Discussion:**  Failure to display the DoD logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.  
  
The SSH service must be configured to display the DoD logon warning banner through the SSH daemon configuration.  
  
The SSH daemon may also be used to provide SFTP service. The warning banner configuration for SSH will apply to SFTP.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECWM-1  
  
**Check Content:**    
Verify the SSH daemon is configured for logon warning banners.  
# grep -i banner /etc/ssh/sshd\_config | grep -v '^#'  
# cat [banner file]  
Verify the Banner configuration line is present and the file it references contains a login warning banner.  
  
If the SSH daemon is not configured to display a logon warning banner, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and add (or edit) a banner setting referencing a file containing a logon warning banner.  
  
DoD Login Banners:  
  
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."  
  
OR  
  
"I've read & consent to terms in IS user agreem't."     
  
**CCI:**CCI-000048  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4397  
**Group Title:** GEN005560  
**Rule ID:** SV-30079r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005560  
**Rule Title:**The system must be configured with a default gateway for IPv4 if the system uses IPv4, unless the system is a router.  
  
  
**Vulnerability Discussion:**  If a system has no default gateway defined, the system is at increased risk of man-in-the-middle, monitoring, and Denial of Service attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for an IPv4 default route.  
  
Procedure:  
# netstat -r |grep default  
  
If a default route is not defined, this is a finding.  
  
**Fix Text:**Create or edit /etc/defaultrouter to contain the default gateway address.  
  
Procedure (for a default gateway of 192.168.3.1):  
# echo "192.168.3.1" > /etc/defaultrouter  
  
Restart the system for the setting to take effect.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22490  
**Group Title:** GEN005570  
**Rule ID:** SV-26804r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005570  
**Rule Title:**The system must be configured with a default gateway for IPv6 if the system uses IPv6, unless the system is a router.  
  
  
**Vulnerability Discussion:**  If a system has no default gateway defined, the system is at increased risk of man-in-the-middle, monitoring, and Denial of Service attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for a default route for IPv6.  
# netstat -f inet6 -r | grep default  
If the system uses IPv6, and no results are returned, this is a finding.  
  
**Fix Text:**Add a default route for IPv6.  
# route add -inet6 default <gateway>  
Add this command to an init script.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4398  
**Group Title:** GEN005580  
**Rule ID:** SV-4398r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005580  
**Rule Title:**A system used for routing must not run other network services or applications.  
  
  
**Vulnerability Discussion:**  Installing extraneous software on a system designated as a dedicated router poses a security threat to the system and the network. Should an attacker gain access to the router through the unauthorized software, the entire network is susceptible to malicious activity.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSP-1  
  
**Check Content:**    
Ask the SA if the system is a designated router. If it is not, this is not applicable.  
  
Check the system for non-routing network services.  
  
Procedure:  
# netstat -a | grep -i listen  
# ps -ef  
  
If non-routing services, including Web servers, file servers, DNS servers, or applications servers, but excluding management services, such as SSH and SNMP, are running on the system, this is a finding.  
  
**Fix Text:**Ensure only authorized software is loaded on a designated router. Authorized software will be limited to the most current version of routing protocols and SSH for system administration purposes.     
  
**CCI:**CCI-001208  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22665  
**Group Title:** GEN005590  
**Rule ID:** SV-39878r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005590  
**Rule Title:**The system must not be running any routing protocol daemons, unless the system is a router.  
  
  
**Vulnerability Discussion:**  Routing protocol daemons are typically used on routers to exchange network topology information with other routers. If this software is used when not required, system network information may be unnecessarily transmitted across the network.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for any running routing protocol daemons.  
# svcs -a | grep online | egrep '(ospf|route|bgp|zebra|quagga)'  
OR  
# ps -ef | egrep '(ospf|route|bgp|zebra|quagga)'  
If any routing protocol daemons are listed, this is a finding.  
  
**Fix Text:**Disable any routing protocol daemons.  
  
# svcadm disable <routing protocol daemon>     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12023  
**Group Title:** GEN005600  
**Rule ID:** SV-28581r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005600  
**Rule Title:**IP forwarding for IPv4 must not be enabled, unless the system is a router.  
  
  
**Vulnerability Discussion:**  If the system is configured for IP forwarding and is not a designated router, it could be used to bypass network security by providing a path for communication not filtered by network devices.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system is configured for IPv4 forwarding.  
# svcs | grep svc:/network/ipv4-forwarding  
If the service is enabled, this is a finding.  
  
**Fix Text:**Disable IPv4 forwarding on the system.  
# svcadm disable svc:/network/ipv4-forwarding  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22491  
**Group Title:** GEN005610  
**Rule ID:** SV-26810r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005610  
**Rule Title:**The system must not have IP forwarding for IPv6 enabled, unless the system is an IPv6 router.  
  
  
**Vulnerability Discussion:**  If the system is configured for IP forwarding and is not a designated router, it could be used to bypass network security by providing a path for communication not filtered by network devices.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check if the system is configured for IPv6 forwarding.  
# ndd /dev/ip6 ip6\_forwarding  
If the value is not 0, this is a finding.  
  
**Fix Text:**Disable IPv6 forwarding.  
# ndd -set /dev/ip6 ip6\_forwarding 0  
Edit startup scripts as necessary; add this command or remove commands setting the value to 1.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-928  
**Group Title:** GEN005740  
**Rule ID:** SV-28444r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005740  
**Rule Title:**The NFS export configuration file must be owned by root.  
  
  
**Vulnerability Discussion:**  Failure to give ownership of the NFS export configuration file to root provides the designated owner and possible unauthorized users with the potential to change system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the dfstab file.  
  
Example:  
# ls -lL /etc/dfs/dfstab   
  
If the export configuration file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the dfstab file to root.  
  
Example:  
# chown root /etc/dfs/dfstab     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22492  
**Group Title:** GEN005750  
**Rule ID:** SV-26813r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005750  
**Rule Title:**The NFS export configuration file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  Failure to give group ownership of the NFS export configuration file to root or system groups provides the designated group owner and possible unauthorized users with the potential to change system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the NFS export configuration file.  
  
Procedure:  
# ls -lL /etc/dfs/dfstab  
  
If the file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the NFS export configuration file.  
  
Procedure:  
# chgrp root /etc/dfs/dfstab     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-929  
**Group Title:** GEN005760  
**Rule ID:** SV-28446r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005760  
**Rule Title:**The NFS export configuration file must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the NFS export configuration file could allow unauthorized modification of the file, which could result in Denial of Service to authorized NFS exports and the creation of additional unauthorized exports.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2, ECLP-1  
  
**Check Content:**    
# ls -lL /etc/dfs/dfstab   
If the file has a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the permissions of the dfstab file to 664 or less permissive.  
  
# chmod 0644 /etc/dfs/dfstab     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22493  
**Group Title:** GEN005770  
**Rule ID:** SV-26816r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005770  
**Rule Title:**The NFS exports configuration file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files. Excessive permissions on the NFS export configuration file could allow unauthorized modification of the file, which could result in Denial of Service to authorized NFS exports and the creation of additional unauthorized exports.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the NFS export configuration file.  
# ls -lL /etc/dfs/dfstab  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/dfs/dfstab     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-931  
**Group Title:** GEN005800  
**Rule ID:** SV-40303r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005800  
**Rule Title:**All NFS-exported system files and system directories must be owned by root.  
  
  
**Vulnerability Discussion:**  Failure to give ownership of sensitive files or directories to root provides the designated owner and possible unauthorized users with the potential to access sensitive information or change system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for NFS exported file systems.  
  
Procedure:  
# exportfs -v  
OR  
# more /etc/dfs/sharetab  
  
This will display all of the exported file systems. For each file system displayed, check the ownership.  
  
Procedure:  
# ls -lLa <exported file system path>  
  
If the files and directories are not owned by root, this is a finding.  
  
**Fix Text:**Change the ownership of exported file systems not owned by root.  
  
Procedure:  
# chown root <path>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22496  
**Group Title:** GEN005810  
**Rule ID:** SV-26821r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005810  
**Rule Title:**All NFS exported system files and system directories must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  Failure to give group ownership of sensitive files or directories to root provides the members of the owning group with the potential to access sensitive information or change system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
List the exports.  
# cat /etc/dfs/dfstab  
OR  
# more /etc/dfs/sharetab  
  
For each export, check the ownership information.  
# ls -ldL <export>  
If the directory is not group-owned by root, this is a finding.  
  
**Fix Text:**Change the group owner of the export directory.  
# chgrp root <export>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-932  
**Group Title:** GEN005820  
**Rule ID:** SV-40304r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005820  
**Rule Title:**The NFS anonymous UID and GID must be configured to values that have no permissions.  
  
  
**Vulnerability Discussion:**  When an NFS server is configured to deny remote root access, a selected UID and GID are used to handle requests from the remote root user. The UID and GID should be chosen from the system to provide the appropriate level of non-privileged access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1, IAIA-1, IAIA-2  
  
**Check Content:**    
Check if the anon option is set correctly for exported file systems.  
  
List exported file systems.  
# exportfs -v  
OR  
# more /etc/dfs/sharetab  
  
Each of the exported file systems should include an entry for the 'anon=' option set to -1 or an equivalent (60001, 60002, 65534, or 65535). If an appropriate 'anon=' setting is not present for an exported file system, this is a finding.  
  
**Fix Text:**Edit /etc/dfs/dfstab and add the "anon=-1" option for exports lacking it. Re-export the filesystems.     
  
**CCI:**CCI-000062  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-933  
**Group Title:** GEN005840  
**Rule ID:** SV-40305r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005840  
**Rule Title:**The NFS server must be configured to restrict file system access to local hosts.  
  
  
**Vulnerability Discussion:**  The NFS access option limits user access to the specified level. This assists in protecting exported file systems. If access is not restricted, unauthorized hosts may be able to access the system's NFS exports.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the permissions on exported NFS file systems.  
  
Procedure:  
# exportfs -v  
OR  
# more /etc/dfs/sharetab  
  
If the exported file systems do not contain the rw or ro options specifying a list of hosts or networks, this is a finding.  
  
**Fix Text:**Edit /etc/dfs/dfstab and add ro and/or rw options (as appropriate) specifying a list of hosts or networks which are permitted access. Re-export the file systems.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-934  
**Group Title:** GEN005860  
**Rule ID:** SV-40306r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005860  
**Rule Title:**The system's NFS export configuration must not have the sec option set to none (or equivalent); additionally, the default authentication must not to be set to none.  
  
  
**Vulnerability Discussion:**  If sec=none on Solaris, all NFS requests are mapped to an unknown/common user instead of being processed according to the provided UID.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAN-1  
  
**Check Content:**    
Perform the following on NFS servers:  
  
# grep "^default" /etc/nfssec.conf  
  
Check to ensure the second column does not equal 0. This would indicate the default is set to none. Perform the following to check currently exported file systems.  
  
# more /etc/dfs/dfstab  
  
If the option sec=none is set on any of the exported file systems, this is a finding.  
  
**Fix Text:**Edit the /etc/dfs/dfstab file and add the sec=XXX option to the share line as an option. XXX must be a valid option for the system other than none.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-935  
**Group Title:** GEN005880  
**Rule ID:** SV-40307r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005880  
**Rule Title:**The NFS server must not allow remote root access.  
  
  
**Vulnerability Discussion:**  If the NFS server allows root access to local file systems from remote hosts, this access could be used to compromise the system.  
  
**Responsibility:**  Information Assurance Officer  
**IAControls:**  EBRP-1  
  
**Check Content:**    
Determine if the NFS server is exporting with the root access option.  
  
Procedure:  
# exportfs -v | grep "root="  
OR  
# more /etc/dfs/sharetab  
  
If an export with the root option is found, this is a finding.  
  
**Fix Text:**Edit the /etc/dfs/dfstab file and remove the root= option from all exports. Re-export the file systems.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-936  
**Group Title:** GEN005900  
**Rule ID:** SV-28452r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005900  
**Rule Title:**The nosuid option must be enabled on all NFS client mounts.  
  
  
**Vulnerability Discussion:**  Enabling the nosuid mount option prevents the system from granting owner or group-owner privileges to programs with the setuid or setgid bit set. If the system does not restrict this access, users with unprivileged access to the local system may be able to acquire privileged access by executing setuid or setgid files located on the mounted NFS file system.  
  
**Responsibility:**  Information Assurance Officer  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Check the system for NFS mounts not using the nosuid option.  
  
Procedure:  
# mount -v | grep " type nfs " | grep -v nosetuid  
OR  
# grep nfs /etc/mnttab | grep -v nosuid | grep -v :vold  
  
If the mounted file systems do not have the nosetuid/nosuid option, this is a finding. NOTE: Mount options for the volume management daemon (vold) are controlled by the /etc/rmmount.conf file.  
  
**Fix Text:**Edit /etc/vfstab and add the nosuid option for all NFS file systems. Remount the NFS file systems to make the change take effect.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12024  
**Group Title:** GEN006000  
**Rule ID:** SV-41525r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006000  
**Rule Title:**The system must not have a public Instant Messaging (IM) client installed.  
  
  
**Vulnerability Discussion:**  Public Instant Messaging (IM) systems are not approved for use and may result in the unauthorized distribution of information. IM clients provide a way for a user to send a message to one or more other users in real time. Additional capabilities may include file transfer and support for distributed game playing. Communication between clients and associated directory services are managed through messaging servers. Commercial IM clients include AOL Instant Messenger (AIM), MSN Messenger, and Yahoo! Messenger.  
  
IM clients present a security issue when the clients route messages through public servers. The obvious implication is potentially sensitive information could be intercepted or altered in the course of transmission. This same issue is associated with the use of public email servers. In order to reduce the potential for disclosure of sensitive Government information and to ensure the validity of official government information, IM clients connecting to public IM services will not be installed. Clients used to access internal or DoD-controlled IM services are permitted.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECIM-1  
  
**Check Content:**    
If an IM client is installed, ask the SA if it has access to any public domain IM servers. If it does have access to public servers, this is a finding.  
  
  
  
**Fix Text:**Uninstall the IM client from the system, or configure the client to only connect to DoD-approved IM services.  
    
  
**CCI:**CCI-000366  
  
  
**CCI:**CCI-001154  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12025  
**Group Title:** GEN006040  
**Rule ID:** SV-12526r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006040  
**Rule Title:**The system must not have any peer-to-peer file-sharing application installed.  
  
  
**Vulnerability Discussion:**  Peer-to-peer file-sharing software can result in the unintentional exfiltration of information. There are also many legal issues associated with these types of utilities including copyright infringement or other intellectual property issues. The ASD Memo "Use of Peer-to-Peer (P2P) File-Sharing Applications across the DoD" states the following:  
  
“P2P file-sharing applications are authorized for use on DoD networks with approval by the appropriate Designated Approval Authority (DAA). Documented requirements, security architecture, configuration management process, and a training program for users are all requirements within the approval process. The unauthorized use of application or services, including P2P applications, is prohibited, and such applications or services must be eliminated.”  
  
P2P applications include, but are not limited to, the following:  
  
-Napster,  
-Kazaa,  
-ARES,  
-Limewire,  
-IRC Chat Relay, and  
-BitTorrent.  
  
**Responsibility:**  Designated Approving Authority  
**IAControls:**  DCPD-1, ECSC-1  
  
**Check Content:**    
Ask the SA if any peer-to-peer file-sharing applications are installed. Some examples of these applications include:  
  
- Napster,  
- Kazaa,  
- ARES,  
- Limewire,  
- IRC Chat Relay, and  
- BitTorrent.  
  
If any of these applications are installed, this is a finding.  
  
**Fix Text:**Uninstall the peer-to-peer file sharing application(s) from the system.     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4321  
**Group Title:** GEN006060  
**Rule ID:** SV-4321r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006060  
**Rule Title:**The system must not run Samba unless needed.  
  
  
**Vulnerability Discussion:**  Samba is a tool used for the sharing of files and printers between Windows and UNIX operating systems. It provides access to sensitive files and, therefore, poses a security risk if compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPD-1, ECSC-1  
  
**Check Content:**    
Check the system for a running Samba server.  
  
Procedure:  
# ps -ef |grep smbd  
  
If the Samba server is running, ask the SA if the Samba server is operationally required. If it is not, this is a finding.  
  
**Fix Text:**If there is no functional need for Samba and the daemon is running, disable the daemon by killing the process ID as noted from the output of ps -ef |grep smbd. The utility should also be removed or not installed if there is no functional requirement.     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1026  
**Group Title:** GEN006080  
**Rule ID:** SV-42313r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006080  
**Rule Title:**The Samba Web Administration Tool (SWAT) must be restricted to the local host or require SSL.  
  
  
**Vulnerability Discussion:**  SWAT is a tool used to configure Samba. As it modifies Samba configuration, which can impact system security, it must be protected from unauthorized access. SWAT authentication may involve the root password, which must be protected by encryption when traversing the network.  
  
Restricting access to the local host allows for the use of SSH TCP forwarding, if configured, or administration by a web browser on the local system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  EBRP-1, ECCT-1, ECCT-2  
  
**Check Content:**    
Verify the SWAT daemon is running under inetd.  
  
# svcs swat  
  
If SWAT is disabled or not installed, this is not applicable.  
  
Verify that TCP\_wrappers is enabled for the SWAT daemon.  
  
# inetadm -l swat | grep tcp\_wrappers  
  
If the tcp\_wrappers value is unset or is set to FALSE, this is a finding.  
  
Verify access to the SWAT daemon is limited to localhost through the use of TCP\_Wrappers.  
  
# more /etc/hosts.allow  
# more /etc/hosts.deny  
  
If the hosts.allow and hosts.deny access control files are configured such that remote access to SWAT is enabled, this is a finding.  
  
Ask the SA if SSH port forwarding is used to enable remote access to SWAT. If it is, this is not a finding. If all access to SWAT is via localhost using a local web browser, this is not a finding.  
  
**Fix Text:**Enable tcp\_wrappers for the SWAT daemon.  
# inetadm -m swat tcp\_wrappers=true  
OR  
# inetadm -M tcp\_wrappers=true  
Relfresh the inetd daemon.  
# svcadm refresh inetd  
  
Configure the hosts.allow and hosts.deny files to limit access to SWAT to localhost.  
Example:  
# echo ALL: ALL >> /etc/hosts.deny  
# echo swat: localhost >> /etc/hosts.allow     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1027  
**Group Title:** GEN006100  
**Rule ID:** SV-40291r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006100  
**Rule Title:**The smb.conf file must be owned by root.  
  
  
**Vulnerability Discussion:**  The smb.conf file allows access to other machines on the network and grants permissions to certain users. If it is owned by another user, the file may be maliciously modified and the Samba configuration could be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the /etc/smb.conf file.  
  
Procedure:  
# ls -l /etc/sfw/smb.conf  
  
If the smb.conf file is not owned by root, this is a finding.  
  
**Fix Text:**Change the ownership of the smb.conf file.  
  
Procedure:  
# chown root /etc/sfw/smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1056  
**Group Title:** GEN006120  
**Rule ID:** SV-39890r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006120  
**Rule Title:**The smb.conf file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  If the group owner of the smb.conf file is not root or a system group, the file may be maliciously modified and the Samba configuration could be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the smb.conf file.  
  
Procedure:  
# ls -l /etc/sfw/smb.conf  
  
If an smb.conf file is not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group owner of the smb.conf file.  
  
Procedure:  
# chgrp root /etc/sfw/smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1028  
**Group Title:** GEN006140  
**Rule ID:** SV-40294r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006140  
**Rule Title:**The smb.conf file must have mode 0644 or less permissive.  
  
  
**Vulnerability Discussion:**  If the smb.conf file has excessive permissions, the file may be maliciously modified and the Samba configuration could be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the smb.conf file.  
  
Procedure:  
# ls -lL /etc/sfw/smb.conf file  
  
If the smb.conf has a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the smb.conf file to 0644 or less permissive.  
  
Procedure:  
# chmod 0644 /etc/sfw/smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22497  
**Group Title:** GEN006150  
**Rule ID:** SV-26824r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006150  
**Rule Title:**The smb.conf file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Excessive permissions could endanger the security of the Samba configuration file and, ultimately, the system and network.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the Samba configuration file.  
# ls -lL /etc/sfw/smb.conf  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/sfw/smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1029  
**Group Title:** GEN006160  
**Rule ID:** SV-40284r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006160  
**Rule Title:**The smbpasswd file must be owned by root.  
  
  
**Vulnerability Discussion:**  If the smbpasswd file is not owned by root, the smbpasswd file may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the smbpasswd file.  
  
# ls -lL /etc/sfw/private/smbpasswd  
  
If the smbpasswd file is not owned by root, this is a finding.  
  
**Fix Text:**Use the chown command to configure the smb passwd file.  
# chown root /etc/sfw/private/smbpasswd     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1058  
**Group Title:** GEN006180  
**Rule ID:** SV-40287r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006180  
**Rule Title:**The smbpasswd file must be group-owned by root.  
  
  
**Vulnerability Discussion:**  If the smbpasswd file is not group-owned by root, the smbpasswd file may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check smbpasswd ownership.  
  
# ls -lL /etc/sfw/private/smbpasswd  
  
If smbpasswd is not group-owned by root, this is a finding.  
  
**Fix Text:**Use the chgrp command to ensure the group owner of the smbpasswd file is root.  
  
# chgrp root /etc/sfw/private/smbpasswd     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1059  
**Group Title:** GEN006200  
**Rule ID:** SV-40289r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006200  
**Rule Title:**The smbpasswd file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  If the smbpasswd file has a mode more permissive than 0600, the smbpasswd file may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check smbpasswd mode.  
  
Procedure:  
# ls -lL /etc/sfw/private/smbpasswd   
  
If smbpasswd has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the smbpasswd file to 0600.  
  
Procedure:  
# chmod 0600 /etc/sfw/private/smbpasswd     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22498  
**Group Title:** GEN006210  
**Rule ID:** SV-26828r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006210  
**Rule Title:**The smbpasswd file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  If the permissions of the smbpasswd file are too permissive, the smbpasswd file may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the Samba configuration file.  
# ls -lL /etc/sfw/private/smbpasswd  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/sfw/private/smbpasswd     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1030  
**Group Title:** GEN006220  
**Rule ID:** SV-40298r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006220  
**Rule Title:**The smb.conf file must use the hosts option to restrict access to Samba.  
  
  
**Vulnerability Discussion:**  Samba increases the attack surface of the system and must be restricted to communicate only with systems requiring access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Examine the smb.conf file.  
  
# more /etc/sfw/smb.conf  
  
If the hosts option is not present to restrict access to a list of authorized hosts and networks, this is a finding.  
  
**Fix Text:**Edit the smb.conf file and set the hosts option to permit only authorized hosts to access Samba.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22499  
**Group Title:** GEN006225  
**Rule ID:** SV-40295r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006225  
**Rule Title:**Samba must be configured to use an authentication mechanism other than "share."  
  
  
**Vulnerability Discussion:**  Samba share authentication does not provide for individual user identification and must not be used.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the security mode of the Samba configuration.  
# grep -i security /etc/sfw/smb.conf  
If the security mode is share, this is a finding.  
  
**Fix Text:**Edit the /etc/sfw/smb.conf file and change the security setting to user or another valid setting other than share.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22500  
**Group Title:** GEN006230  
**Rule ID:** SV-40296r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006230  
**Rule Title:**Samba must be configured to use encrypted passwords.  
  
  
**Vulnerability Discussion:**  Samba must be configured to protect authenticators. If Samba passwords are not encrypted for storage, plain-text user passwords may be read by those with access to the Samba password file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the encryption setting of the Samba configuration.  
# grep -i 'encrypt passwords' /etc/sfw/smb.conf  
If the setting is not present, or not set to yes, this is a finding.  
  
**Fix Text:**Edit the /etc/sfw/smb.conf file and change the encrypt passwords setting to yes.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22501  
**Group Title:** GEN006235  
**Rule ID:** SV-40297r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006235  
**Rule Title:**Samba must be configured to not allow guest access to shares.  
  
  
**Vulnerability Discussion:**  Guest access to shares permits anonymous access and is not permitted.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the encryption setting for the Samba configuration.  
# grep -i 'guest ok' /etc/sfw/smb.conf  
If the setting exists and is set to yes, this is a finding.  
  
**Fix Text:**Edit the /etc/sfw/smb.conf file and change the guest ok setting to no.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1023  
**Group Title:** GEN006240  
**Rule ID:** SV-1023r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006240  
**Rule Title:**The system must not run an Internet Network News (INN) server.  
  
  
**Vulnerability Discussion:**  Internet Network News (INN) servers access Usenet newsfeeds and store newsgroup articles. INN servers use the Network News Transfer Protocol (NNTP) to transfer information from the Usenet to the server and from the server to authorized remote hosts.  
  
If this function is necessary to support a valid mission requirement, its use must be authorized and approved in the system accreditation package.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# ps -ef | egrep "innd|nntpd"  
  
If an INN server is running, this is a finding.  
  
  
**Fix Text:**Disable the INN server.     
  
**CCI:**CCI-000381  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4273  
**Group Title:** GEN006260  
**Rule ID:** SV-4273r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006260  
**Rule Title:**The /etc/news/hosts.nntp (or equivalent) must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the hosts.nntp file may allow unauthorized modification which could lead to Denial-of-Service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/news/hosts.nntp permissions.  
  
# ls -lL /etc/news/hosts.nntp  
  
If /etc/news/hosts.nntp has a mode more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the /etc/news/hosts.nntp file to 0600.  
  
# chmod 0600 /etc/news/hosts.nntp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22502  
**Group Title:** GEN006270  
**Rule ID:** SV-26835r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006270  
**Rule Title:**The /etc/news/hosts.nntp file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files. Excessive permissions on the hosts.nntp file may allow unauthorized modification which could lead to Denial of Service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/news/hosts.nntp  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/news/hosts.nntp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4274  
**Group Title:** GEN006280  
**Rule ID:** SV-4274r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006280  
**Rule Title:**The /etc/news/hosts.nntp.nolimit (or equivalent) must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the hosts.nntp.nolimit file may allow unauthorized modification which could lead to Denial-of-Service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/news/hosts.nntp.nolimit permissions.  
  
# ls -lL /etc/news/hosts.nntp.nolimit  
  
If /etc/news/hosts.nntp.nolimit has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of /etc/news/hosts.nntp.nolimit to 0600.  
# chmod 0600 /etc/news/hosts.nntp.nolimit     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22503  
**Group Title:** GEN006290  
**Rule ID:** SV-26842r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006290  
**Rule Title:**The /etc/news/hosts.nntp.nolimit file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files. Excessive permissions on the hosts.nntp.nolimit file may allow unauthorized modification which could lead to Denial of Service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/news/hosts.nntp.nolimit  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/news/hosts.nntp.nolimit     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4275  
**Group Title:** GEN006300  
**Rule ID:** SV-4275r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006300  
**Rule Title:**The /etc/news/nnrp.access (or equivalent) must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the nnrp.access file may allow unauthorized modification which could lead to Denial-of-Service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/news/nnrp.access permissions.  
  
# ls -lL /etc/news/nnrp.access  
  
If /etc/news/nnrp.access has a mode more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the /etc/news/nnrp.access file to 0600.  
# chmod 0600 /etc/news/nnrp.access     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22504  
**Group Title:** GEN006310  
**Rule ID:** SV-26846r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006310  
**Rule Title:**The /etc/news/nnrp.access file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files. Excessive permissions on the nnrp.access file may allow unauthorized modification which could lead to Denial of Service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/news/nnrp.access  
If the permissions include a "+", the file has an extended ACL and this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/news/nnrp.access     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4276  
**Group Title:** GEN006320  
**Rule ID:** SV-4276r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006320  
**Rule Title:**The /etc/news/passwd.nntp file (or equivalent) must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  File permissions more permissive than 0600 for /etc/news/passwd.nntp may allow access to privileged information by system intruders or malicious users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/news/passwd.nntp permissions.  
  
# ls -lL /etc/news/passwd.nntp  
  
If /etc/news/passwd.nntp has a mode more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the /etc/news/passwd.nntp file.  
# chmod 0600 /etc/news/passwd.nntp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22505  
**Group Title:** GEN006330  
**Rule ID:** SV-26850r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006330  
**Rule Title:**The /etc/news/passwd.nntp file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  Extended ACLs may provide excessive permissions on the /etc/news/passwd.nntp file, which may permit unauthorized access or modification to the NNTP configuration.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/news/passwd.nntp  
If the permissions include a "+", the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# chmod A- /etc/news/passwd.nntp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4277  
**Group Title:** GEN006340  
**Rule ID:** SV-40487r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006340  
**Rule Title:**Files in /etc/news must be owned by root.  
  
  
**Vulnerability Discussion:**  If critical system files are not owned by a privileged user, system integrity could be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the files in /etc/news.  
  
Procedure:  
# ls -al /etc/news  
  
If the /etc/news directory or any files in it are not owned by root, this is a finding.  
  
**Fix Text:**Change the ownership of the /etc/news directory and the files in it to root.  
  
Procedure:  
# chown -R root /etc/news     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4278  
**Group Title:** GEN006360  
**Rule ID:** SV-40489r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006360  
**Rule Title:**The files in /etc/news must be group-owned by root.  
  
  
**Vulnerability Discussion:**  If critical system files do not have a privileged group owner, system integrity could be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/news directory and files group ownership.  
  
Procedure:  
# ls -al /etc/news  
  
If the /etc/news directory and the files in it are not group-owned by root, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/news directory and the files in it to root.  
  
Procedure:  
# chgrp -R root /etc/news     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4399  
**Group Title:** GEN006380  
**Rule ID:** SV-4399r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN006380  
**Rule Title:**The system must not use UDP for NIS/NIS+.  
  
  
**Vulnerability Discussion:**  Implementing NIS or NIS+ under UDP may make the system more susceptible to a Denial of Service attack and does not provide the same quality of service as TCP.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system does not use NIS or NIS+, this is not applicable.  
  
Check if NIS or NIS+ is implemented using UDP.  
  
Procedure:  
# rpcinfo -p | grep yp | grep udp  
  
If NIS or NIS+ is implemented using UDP, this is a finding.  
  
**Fix Text:**Configure the system to not use UDP for NIS and NIS+. Consult vendor documentation for the required procedure.     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-867  
**Group Title:** GEN006400  
**Rule ID:** SV-867r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006400  
**Rule Title:**The Network Information System (NIS) protocol must not be used.  
  
  
**Vulnerability Discussion:**  Due to numerous security vulnerabilities existing within NIS, it must not be used. Possible alternative directory services are NIS+ and LDAP.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Perform the following to determine if NIS is active on the system.  
  
# ps -ef | egrep '(ypbind|ypserv)'  
  
If NIS is found active on the system, this is a finding.  
  
**Fix Text:**Disable the use of NIS. Possible replacements are NIS+ and LDAP.     
  
**CCI:**CCI-001435  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12026  
**Group Title:** GEN006420  
**Rule ID:** SV-12527r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006420  
**Rule Title:**NIS maps must be protected through hard-to-guess domain names.  
  
  
**Vulnerability Discussion:**  The use of hard-to-guess NIS domain names provides additional protection from unauthorized access to the NIS directory information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the domain name for NIS maps.  
  
Procedure:  
# domainname  
  
If the name returned is simple to guess, such as the organization name, building, or room name, etc., this is a finding.  
  
**Fix Text:**Change the NIS domain name to a value difficult to guess. Consult vendor documentation for the required procedure.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-926  
**Group Title:** GEN006460  
**Rule ID:** SV-28453r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006460  
**Rule Title:**Any NIS+ server must be operating at security level 2.  
  
  
**Vulnerability Discussion:**  If the NIS+ server is not operating in, at least, security level 2, there is no encryption and the system could be penetrated by intruders and/or malicious users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system is not using NIS+, this is not applicable.  
  
Check the system to determine if NIS+ security level 2 is implemented.  
  
Procedure:  
# niscat cred.org\_dir   
  
If the second column does not contain DES, the system is not using NIS+ security level 2, and this is a finding.  
  
**Fix Text:**Ensure the NIS+ server is operating at security level 2 by editing /usr/lib/nis/nisserver and ensuring the line containing SEC= is set to the numeral 2, for example:  
  
SEC=2 # 2=DES or 3=RSA  
  
Security Level 0 is designed for testing and initial setup of the NIS+ namespace. When running at level 0, the daemon does not enforce access control. Any client is allowed to perform any operation, including updates and deletions.  
  
Security level 1 accepts AUTH\_SYS and AUTH\_DES credentials for authenticating clients and authorizing them to perform NIS+ operations. This is not a secure mode of operation since AUTH\_SYS credentials are easily forged. It should not be used on networks in which any untrusted user may potentially have access. Security level 2 accepts only AUTH\_DES credentials for authentication and authorization. This is the highest level of security currently provided by the NIS+ service and the default security level if the -S option is not used.     
  
**CCI:**CCI-001435  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-782  
**Group Title:** GEN006480  
**Rule ID:** SV-41526r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006480  
**Rule Title:**The system must have a host-based intrusion detection tool installed.  
  
  
**Vulnerability Discussion:**  Without a host-based intrusion detection tool, there is no system-level defense when an intruder gains access to a system or network. Additionally, a host-based intrusion detection tool can provide methods to immediately lock out detected intrusion attempts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECID-1  
  
**Check Content:**    
A few applications providing host-based network intrusion protection are:  
  
- Dragon Squire by Enterasys Networks,  
- ITA by Symantec,  
- Hostsentry by Psionic Software,  
- Logcheck by Psionic Software,  
- RealSecure agent by ISS, and  
- Swatch by Stanford University.  
  
Ask the SA or IAO if a host-based intrusion detection application is loaded on the system.  
  
Determine if the application is loaded on the system.  
  
Procedure:  
# find / -name <daemon name> -print   
  
  
  
Determine if the application is active on the system.  
  
Procedure:  
# ps -ef | grep <daemon name>   
  
If no host-based intrusion detection system is installed on the system, this is a finding.  
  
  
**Fix Text:**Install a host-based intrusion detection tool.  
    
  
**CCI:**CCI-001259  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12028  
**Group Title:** GEN006560  
**Rule ID:** SV-41530r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006560  
**Rule Title:**The system vulnerability assessment tool, host-based intrusion detection tool, and file integrity tool must notify the SA and the IAO of a security breach or a suspected security breach.  
  
  
**Vulnerability Discussion:**  Timely notifications of potential security compromises minimize the potential damage.  
  
Minimally, the system must log these events and the SA and the IAO will receive the notifications during the daily system log review. If feasible, active alerting (such as email or paging) should be employed consistent with the site’s established operations management systems and procedures.  
  
**Responsibility:**  Information Assurance Officer  
**IAControls:**  ECAT-1, ECAT-2  
  
**Check Content:**    
For each security tool on the system, determine if the tool is configured to notify the IAO and SA of any detected security problem. If such notifications are not configured, this is a finding.  
  
**Fix Text:**Configure the security tools on the system to notify the IAO and SA when any security issues are detected.     
  
**CCI:**CCI-000366  
  
  
**CCI:**CCI-001266  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22506  
**Group Title:** GEN006565  
**Rule ID:** SV-26857r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006565  
**Rule Title:**The system package management tool must be used to verify system software periodically.  
  
  
**Vulnerability Discussion:**  Verification using the system package management tool can be used to determine that system software has not been tampered with.  
  
This requirement is not applicable to systems not using package management tools.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Check the root crontab (crontab -l) for the presence of a package check command, such as, pkgchk -n.  
  
If no such cron job is found, this is a finding.  
  
**Fix Text:**Add a cron job to run a package verification command, such as, pkgchk -n.     
  
**CCI:**CCI-000366  
  
  
**CCI:**CCI-000698  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22507  
**Group Title:** GEN006570  
**Rule ID:** SV-26858r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN006570  
**Rule Title:**The file integrity tool must be configured to verify ACLs.  
  
  
**Vulnerability Discussion:**  ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
If using AIDE, verify the configuration contains the acl option for all monitored files and directories. Here is an example AIDE configuration fragment.  
  
SampleRule = p+i+l+n+u+g+s+m+c+acl+xattrs+sha256  
/bin SampleRule  
  
If the acl option is not present, this is a finding.  
  
If using a different file integrity tool, check the configuration per tool documentation.  
  
**Fix Text:**If using AIDE, edit the configuration and add the acl option for all monitored files and directories.  
  
If using a different file integrity tool, configure ACL checking per the tool's documentation.     
  
**CCI:**CCI-001297  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22508  
**Group Title:** GEN006571  
**Rule ID:** SV-26860r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN006571  
**Rule Title:**The file integrity tool must be configured to verify extended attributes.  
  
  
**Vulnerability Discussion:**  Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
If using AIDE, verify the configuration contains the xattrs option for all monitored files and directories. Here is an example AIDE configuration fragment.  
  
SampleRule = p+i+l+n+u+g+s+m+c+acl+xattrs+sha256  
/bin SampleRule  
  
If the xattrs option is not present, this is a finding.  
  
If using a different file integrity tool, check the configuration per tool documentation.  
  
**Fix Text:**If using AIDE, edit the configuration and add the xattrs option for all monitored files and directories.  
  
If using a different file integrity tool, configure extended attributes checking per the tool's documentation.     
  
**CCI:**CCI-001297  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22509  
**Group Title:** GEN006575  
**Rule ID:** SV-26861r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN006575  
**Rule Title:**The file integrity tool must use FIPS 140-2 approved cryptographic hashes for validating file contents.  
  
  
**Vulnerability Discussion:**  File integrity tools often use cryptographic hashes for verifying that file contents have not been altered. These hashes must be FIPS 140-2 approved.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If using AIDE, verify the configuration contains the sha256 or sha512 options for all monitored files and directories. Here is an example AIDE configuration fragment.  
  
SampleRule = p+i+l+n+u+g+s+m+c+acl+xattrs+sha256  
/bin SampleRule  
  
If either the sha256 or sha512 option is not present, this is a finding.  
  
If using a different file integrity tool, check the configuration per tool documentation.  
  
**Fix Text:**If using AIDE, edit the configuration and add the sha256 or sha512 option for all monitored files and directories.  
  
If using a different file integrity tool, configure FIPS 140-2 approved cryptographic hashes per the tool's documentation.     
  
**CCI:**CCI-001297  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-940  
**Group Title:** GEN006580  
**Rule ID:** SV-28459r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006580  
**Rule Title:**The system must use an access control program.  
  
  
**Vulnerability Discussion:**  Access control programs (such as TCP\_WRAPPERS) provide the ability to enhance system security posture.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  EBRU-1  
  
**Check Content:**    
# svcprop -p defaults inetd | grep tcp\_wrappers  
  
This should return a line with the following:  
  
defaults/tcp\_wrappers boolean true  
  
If the above line contains the word false, this is a finding.  
  
  
  
**Fix Text:**Enable tcp\_wrappers.  
# svccfg -s svc:/network/inetd setprop defaults/tcp\_wrappers=true  
# svcadm refresh inetd     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-941  
**Group Title:** GEN006600  
**Rule ID:** SV-941r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006600  
**Rule Title:**The system's access control program must log each system access attempt.  
  
  
**Vulnerability Discussion:**  If access attempts are not logged, then multiple attempts to log on to the system by an unauthorized user may go undetected.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Normally, TCPD logs to the mail facility in /etc/syslog.conf. Determine if syslog is configured to log events by TCPD.  
  
Procedure:  
# more /etc/syslog.conf  
  
Look for entries similar to the following:  
mail.debug                         /var/adm/maillog  
mail.none                               /var/adm/maillog  
mail.\*                               /var/log/mail  
auth.info                               /var/log/messages  
  
The above entries would indicate mail alerts are being logged. If no entries for mail exist, then TCPD is not logging and this is a finding.  
  
**Fix Text:**Configure the access restriction program to log every access attempt. Ensure the implementation instructions for TCP\_WRAPPERS are followed, so system access attempts are logged into the system log files. If an alternate application is used, it must support this function.     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12030  
**Group Title:** GEN006620  
**Rule ID:** SV-41532r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006620  
**Rule Title:**The system's access control program must be configured to grant or deny system access to specific hosts.  
  
  
**Vulnerability Discussion:**  If the system's access control program is not configured with appropriate rules for allowing and denying access to system network resources, services may be accessible to unauthorized hosts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2, ECSC-1  
  
**Check Content:**    
Check for the existence of the /etc/hosts.allow and /etc/hosts.deny files.  
  
Procedure:  
# ls -la /etc/hosts.allow  
# ls -la /etc/hosts.deny  
  
If either file does not exist, this is a finding.  
  
Check for the presence of a default deny entry.  
  
Procedure:  
# grep "ALL: ALL" /etc/hosts.deny  
  
If the "ALL: ALL" entry is not present in the /etc/hosts.deny file, any TCP service from a host or network not matching other rules will be allowed access. If the entry is not in /etc/hosts.deny, this is a finding.  
  
**Fix Text:**Edit the /etc/hosts.allow and /etc/hosts.deny files to configure access restrictions.  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12765  
**Group Title:** GEN006640  
**Rule ID:** SV-28461r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006640  
**Rule Title:**The system must use and update a DoD-approved virus scan program.  
  
  
**Vulnerability Discussion:**  Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems. Virus scanning software is available to DoD on the JTF-GNO web site.  
  
The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.  
  
If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECVP-1  
  
**Check Content:**    
Check for the existence of the McAfee command line scan tool to be executed daily in the cron file. Additional tools specific for each operating system are also available and will have to be manually reviewed if installed. In addition, the definitions file should not be older than 14 days.   
  
Check if uvscan is scheduled to run.  
# grep uvscan /var/spool/cron/crontabs/\*  
  
Perform the following command to ensure the virus definition signature files are not older than 14 days.  
  
# ls -la clean.dat names.dat scan.dat  
  
If a virus scanner is not being run daily or the virus definitions are older than 14 days, this is a finding.  
  
**Fix Text:**Install McAfee command line virus scan tool, or an appropriate alternative from https://www.jtfgno.mil. Ensure the virus signature definition files are no older than 14 days. Updates are also available from https://www.jtfgno.mil. Ensure the command line virus scan tool is run on a regular basis using a utility, such as cron.     
  
**CCI:**CCI-001668  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22530  
**Group Title:** GEN007480  
**Rule ID:** SV-26894r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007480  
**Rule Title:**The Reliable Datagram Sockets (RDS) protocol must be disabled or not installed unless required.  
  
  
**Vulnerability Discussion:**  The Reliable Datagram Sockets (RDS) protocol is a relatively new protocol developed by Oracle for communication between the nodes of a cluster. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes may be able to cause the system to dynamically load a protocol handler by opening a socket using the protocol.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Ask the SA if RDS is required by application software running on the system. If so, this is not applicable.  
  
Verify the RDS protocol handler is not installed.  
# pkginfo | grep SUNWrds  
If no results are returned, this is not a finding.  
  
Verify the RDS protocol handler is prevented from dynamic loading.  
# grep "exclude: rds" /etc/system  
If no result is returned, this is a finding.  
  
**Fix Text:**Remove the RDS protocol handler package.  
# pkgrm SUNWrds  
  
OR  
  
Prevent the RDS protocol handler from dynamic loading.  
# echo "exclude: rds" >> /etc/system     
  
**CCI:**CCI-000382  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22533  
**Group Title:** GEN007540  
**Rule ID:** SV-26902r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007540  
**Rule Title:**The Transparent Inter-Process Communication (TIPC) protocol must be disabled or not installed.  
  
  
**Vulnerability Discussion:**  The Transparent Inter-Process Communication (TIPC) protocol is a relatively new cluster communications protocol developed by Ericsson. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes may be able to cause the kernel to dynamically load a protocol handler by opening a socket using the protocol.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the TIPC protocol handler package is not installed.  
# pkginfo | grep SUNWtipc  
If the TIPC protocol handler package is not installed, this is not a finding  
  
Verify the TIPC protocol handler is prevented from dynamic loading.  
# grep "exclude: tipc" /etc/system  
If no result is returned, this is a finding.  
  
**Fix Text:**Remove the TIPC protocol handler package.  
# pkgrm SUNWtipc  
  
OR  
  
Prevent the TIPC protocol handler from dynamic loading.  
# echo "exclude: tipc" >> /etc/system     
  
**CCI:**CCI-000382  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22541  
**Group Title:** GEN007700  
**Rule ID:** SV-42321r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007700  
**Rule Title:**The IPv6 protocol handler must not be bound to the network stack unless needed.  
  
  
**Vulnerability Discussion:**  IPv6 is the next version of the Internet protocol. Binding this protocol to the network stack increases the attack surface of the host.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Ask the SA if the system is on an IPv6 network. If so, this is not applicable.  
  
Verify there are no IPv6 addresses bound to network interfaces.  
  
# ifconfig -a6  
  
If there are any IPv6 addresses bound to network interfaces, this is a finding.  
  
Verify the IPv6 Neighbor Discovery Protocol (NDP) daemon is not running.  
  
# ps -ef | grep in.ndp  
  
If the NDP daemon is running, this is a finding.  
  
**Fix Text:**Disable the IPv6 Neighbor Discovery Protocol daemon.  
  
# svcadm disable ndp  
  
Remove all IPv6 addresses from network interfaces. Perform the following for every interface with an IPv6 address bound to it.  
  
# ifconfig < interface > inet6 down unplumb  
  
Remove all IPv6 network interface configuration.  
  
# rm /etc/hostname6.\*     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22545  
**Group Title:** GEN007780  
**Rule ID:** SV-26921r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007780  
**Rule Title:**The system must not have 6to4 enabled.  
  
  
**Vulnerability Discussion:**  6to4 is an IPv6 transition mechanism that involves tunneling IPv6 packets encapsulated in IPv4 packets on an ad-hoc basis. This is not a preferred transition strategy and increases the attack surface of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# ifconfig -a  
If a tunnel interface is displayed with an IPv4 tunnel source address, an IPv6 interface address, and no tunnel destination address, this is a finding.  
  
**Fix Text:**Disable the active 6to4 tunnel.  
# ifconfig <tunnel> down  
  
Check the /etc/hostname\* files for startup configuration for the tunnel, and edit or delete as appropriate to prevent the tunnel creation on startup.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22547  
**Group Title:** GEN007820  
**Rule ID:** SV-26927r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007820  
**Rule Title:**The system must not have IP tunnels configured.  
  
  
**Vulnerability Discussion:**  IP tunneling mechanisms can be used to bypass network filtering.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for any IP tunnels.  
# ifconfig -a | grep 'ip.\*tun'  
If any results are returned, this is a finding.  
  
**Fix Text:**Disable the tunnels.  
# ifconfig <tunnel> down  
Remove the startup configuration for the tunnels.  
# rm /etc/hostname.<tunnel>     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22548  
**Group Title:** GEN007840  
**Rule ID:** SV-26931r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007840  
**Rule Title:**The DHCP client must be disabled if not needed.  
  
  
**Vulnerability Discussion:**  DHCP allows for the unauthenticated configuration of network parameters on the system by exchanging information with a DHCP server.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify no interface is configured to use DHCP.  
# ls /etc/dhcp.\*  
If any file is found, this is a finding.  
  
**Fix Text:**Delete the DHCP client configuration.  
# rm /etc/dhcp.\*     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22550  
**Group Title:** GEN007860  
**Rule ID:** SV-26937r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007860  
**Rule Title:**The system must ignore IPv6 ICMP redirect messages.  
  
  
**Vulnerability Discussion:**  ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages modify the host's route table and are unauthenticated. An illicit ICMP redirect message could result in a man-in-the-middle attack.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system is configured to ignore IPv6 ICMP redirect messages.  
# ndd /dev/ip6 ip6\_ignore\_redirect  
If the returned value is not 1, this is a finding.  
  
**Fix Text:**Configure the system to ignore IPv6 ICMP redirect messages.  
# ndd -set /dev/ip6 ip6\_ignore\_redirect 1  
Also add this command to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22551  
**Group Title:** GEN007880  
**Rule ID:** SV-26938r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007880  
**Rule Title:**The system must not send IPv6 ICMP redirects.  
  
  
**Vulnerability Discussion:**  ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table revealing portions of the network topology.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system is configured to not send IPv6 ICMP redirect messages.  
# ndd /dev/ip6 ip6\_send\_redirects  
If the returned value is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not send IPv6 ICMP redirect messages.  
# ndd -set /dev/ip6 ip6\_send\_redirects 0  
  
Also, add this command to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22552  
**Group Title:** GEN007900  
**Rule ID:** SV-26227r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007900  
**Rule Title:**The system must use an appropriate reverse-path filter for IPv6 network traffic, if the system uses IPv6.  
  
  
**Vulnerability Discussion:**  Reverse-path filtering provides protection against spoofed source addresses by causing the system to discard packets with source addresses for which the system has no route or if the route does not point towards the interface on which the packet arrived. Depending on the role of the system, reverse-path filtering may cause legitimate traffic to be discarded and, therefore, should be used with a more permissive mode or filter, or not at all. Whenever possible, reverse-path filtering should be used.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system uses a reverse-path filter for IPv6 network traffic. If it does not, this is a finding.  
  
**Fix Text:**Configure the system to use a reverse-path filter for IPv6 network traffic.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22553  
**Group Title:** GEN007920  
**Rule ID:** SV-26940r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007920  
**Rule Title:**The system must not forward IPv6 source-routed packets.  
  
  
**Vulnerability Discussion:**  Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the forwarding of source-routed traffic, such as when IPv6 forwarding is enabled and the system is functioning as a router.   
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system is configured to not forward IPv6 source-routed packets.  
# ndd /dev/ip6 ip6\_forward\_src\_routed  
If the returned value is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not forward IPv6 source-routed packets.  
# ndd -set /dev/ip6 ip6\_forward\_src\_routed 0  
  
Also, add this command to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22554  
**Group Title:** GEN007940  
**Rule ID:** SV-42323r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007940  
**Rule Title:**The system must not accept source-routed IPv6 packets.  
  
  
**Vulnerability Discussion:**  Source-routed packets allow the source of the packet to suggest that routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the handling of source-routed traffic destined to the system itself, not to traffic forwarded by the system to another, such as when IPv6 forwarding is enabled and the system is functioning as a router.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system is configured to not forward IPv6 source-routed packets.  
# ndd /dev/ip6 ip6\_forward\_src\_routed  
If the returned value is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not forward IPv6 source-routed packets.  
# ndd -set /dev/ip6 ip6\_forward\_src\_routed 0  
  
Also, add this command to a system startup script.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23972  
**Group Title:** GEN007950  
**Rule ID:** SV-29785r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007950  
**Rule Title:**The system must not respond to ICMPv6 echo requests sent to a broadcast address.  
  
  
**Vulnerability Discussion:**  Responding to broadcast ICMP echo requests facilitates network mapping and provides a vector for amplification attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system is configured to ignore IPv6 multicast ICMP echo-requests.  
  
Procedure:  
# ndd -get /dev/ip ip6\_respond\_to\_echo\_multicast  
  
If the result is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not respond to IPv6 multicast ICMP echo-requests.  
  
Procedure:  
# ndd -set /dev/ip ip6\_respond\_to\_echo\_multicast 0  
  
This command must also be added to a system startup script.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22555  
**Group Title:** GEN007980  
**Rule ID:** SV-41038r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007980  
**Rule Title:**If the system is using LDAP for authentication or account information, the system must use a TLS connection using FIPS 140-2 approved cryptographic algorithms.  
  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. Communication between an LDAP server and a host using LDAP requires protection.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Check if the system is using NSS LDAP.  
# grep -v '^#' /etc/nsswitch.conf | grep ldap  
If no lines are returned, this vulnerability is not applicable.  
  
Verify TLS is used for client authentications to the server  
# grep "NS\_LDAP\_AUTH=" /var/ldap/ldap\_client\_file  
If any of the authentication methods used do not begin with "tls:", this is a finding.  
  
Retrieve the list of LDAP servers.  
# grep "NS\_LDAP\_SERVERS=" /var/ldap/client\_file  
Use the certutil to verify the cipher(s) used for every server.  
# certutil -L -n < host nickname > -d /var/ldap  
If any of the TLS connections do not use FIPS 140-2 approved cryptographic algorithms, this is a finding.  
  
**Fix Text:**Configure all LDAP authentications and connections to be encrypted using TLS and FIPS 140-2 approved cryptographic algorithms.     
  
**CCI:**CCI-001453  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22559  
**Group Title:** GEN008060  
**Rule ID:** SV-40726r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008060  
**Rule Title:**If the system is using LDAP for authentication or account information the LDAP client configuration file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the permissions of the files.  
# ls -lL /var/ldap/ldap\_client\_file /var/ldap/ldap\_client\_cred  
If the mode of either file is more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the permissions of the files.  
# chmod 0600 /var/ldap/ldap\_client\_file /var/ldap/ldap\_client\_cred     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22560  
**Group Title:** GEN008080  
**Rule ID:** SV-40727r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008080  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP configuration file must be owned by root.  
  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the ownership of the files.  
# ls -lL /var/ldap/ldap\_client\_file /var/ldap/ldap\_client\_cred  
If the files are not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the files.  
# chown root /var/ldap/ldap\_client\_file /var/ldap/ldap\_client\_cred     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22561  
**Group Title:** GEN008100  
**Rule ID:** SV-39906r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008100  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP configuration file must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the files.  
  
Procedure:  
# ls -lL /var/ldap/ldap\_client\_file /var/ldap/ldap\_client\_cred  
  
If the files are not group-owned by root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group-owner of the files to root, bin, or sys.  
  
Procedure:  
# chgrp root /var/ldap/ldap\_client\_file /var/ldap/ldap\_client\_cred     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22562  
**Group Title:** GEN008120  
**Rule ID:** SV-40728r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008120  
**Rule Title:**If the system is using LDAP for authentication or account information, the /etc/ldap.conf (or equivalent) file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the permissions of the files.  
# ls -lL /var/ldap/ldap\_client\_file /var/ldap/ldap\_client\_cred  
If the permissions include a "+", the files have an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the files.  
# chmod A- /var/ldap/ldap\_client\_file /var/ldap/ldap\_client\_cred     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22563  
**Group Title:** GEN008140  
**Rule ID:** SV-40755r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008140  
**Rule Title:**If the system is using LDAP for authentication or account information, the TLS certificate authority file and/or directory (as appropriate) must be owned by root.  
  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check if the system is using NSS LDAP.  
# grep -v '^#' /etc/nsswitch.conf | grep ldap  
If no lines are returned, this vulnerability is not applicable.  
  
Verify the ownership of the certificate database files.  
# ls -lL /var/ldap/cert8.db /var/ldap/key3.db /var/ldap/secmod.db  
If the owner of any of the files is not root, this is a finding.  
  
**Fix Text:**Change the ownership of the certificate database files.  
# chown root /var/ldap/cert8.db /var/ldap/key3.db /var/ldap/secmod.db     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22564  
**Group Title:** GEN008160  
**Rule ID:** SV-39907r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008160  
**Rule Title:**If the system is using LDAP for authentication or account information, the TLS certificate authority file and/or directory (as appropriate) must be group-owned by root, bin, or sys.  
  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check if the system is using NSS LDAP.  
# grep -v '^#' /etc/nsswitch.conf | grep ldap  
If no lines are returned, this vulnerability is not applicable.  
  
Verify the group ownership of the certificate database files.  
# ls -lL /var/ldap/cert8.db /var/ldap/key3.db /var/ldap/secmod.db  
If the group owner of any of the files is not root, bin, or sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the certificate database files.  
# chgrp root /var/ldap/cert8.db /var/ldap/key3.db /var/ldap/secmod.db     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22565  
**Group Title:** GEN008180  
**Rule ID:** SV-40760r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008180  
**Rule Title:**If the system is using LDAP for authentication or account information, the TLS certificate authority file and/or directory (as appropriate) must have mode 0644 (0755 for directories) or less permissive.  
  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check if the system is using NSS LDAP.  
# grep -v '^#' /etc/nsswitch.conf | grep ldap  
If no lines are returned, this vulnerability is not applicable.  
  
Verify the mode of the certificate database files.  
# ls -lL /var/ldap/cert8.db /var/ldap/key3.db /var/ldap/secmod.db  
If the mode of any of the files is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the certificate database files.  
# chmod 0644 /var/ldap/cert8.db /var/ldap/key3.db /var/ldap/secmod.db  
  
NOTE: Some SAs may prefer to set the permissions to 0600. This is acceptable.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22566  
**Group Title:** GEN008200  
**Rule ID:** SV-37427r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008200  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP TLS certificate authority file and/or directory (as appropriate) must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check if the system is using NSS LDAP.  
# grep -v '^#' /etc/nsswitch.conf | grep ldap  
If no lines are returned, this vulnerability is not applicable.  
  
Verify the permissions of the certificate database files.  
# ls -lL /var/ldap/cert8.db /var/ldap/key3.db /var/ldap/secmod.db  
If the permissions of any of the files contain a "+", and extended ACL is present, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the certificate database files.  
# chmod A- /var/ldap/cert8.db /var/ldap/key3.db /var/ldap/secmod.db     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22575  
**Group Title:** GEN008380  
**Rule ID:** SV-26250r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008380  
**Rule Title:**A root kit check tool must be run on the system at least weekly.  
  
  
**Vulnerability Discussion:**  Root kits are software packages designed to conceal the compromise of a system from the SA. Root kit checking tools examine a system for evidence that a root kit is installed. Dedicated root kit detection software or root kit detection capabilities included in anti-virus packages may be used to satisfy this requirement.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Ask the SA if a root kit check tool is run on the system weekly. If this is not performed, this is a finding.  
  
**Fix Text:**Create an automated job or establish a site-defined procedure to check the system weekly with a root kit check tool.     
  
**CCI:**CCI-001199  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22577  
**Group Title:** GEN008440  
**Rule ID:** SV-26965r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008440  
**Rule Title:**Automated file system mounting tools must not be enabled unless needed.  
  
  
**Vulnerability Discussion:**  Automated file system mounting tools may provide unprivileged users with the ability to access local media and network shares. If this access is not necessary for the system’s operation, it must be disabled to reduce the risk of unauthorized access to these resources.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the autofs service is needed, this vulnerability is not applicable.  
Check if the autofs service is running.  
# svcs svc:/system/filesystem/autofs  
If the autofs service is online this is a finding.  
  
**Fix Text:**Stop and disable the autofs service.  
# svcadm disable autofs  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22578  
**Group Title:** GEN008460  
**Rule ID:** SV-26968r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008460  
**Rule Title:**The system must have USB disabled unless needed.  
  
  
**Vulnerability Discussion:**  USB is a common computer peripheral interface. USB devices may include storage devices that could be used to install malicious software on a system or exfiltrate data.  
  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system needs USB, this vulnerability is not applicable.  
Verify the SUNWusb package is installed.  
# pkginfo SUNWusb  
If the package is installed, this is a finding.  
  
**Fix Text:**Remove the SUNWusb package.  
# pkgrm SUNWusb     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22579  
**Group Title:** GEN008480  
**Rule ID:** SV-26970r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008480  
**Rule Title:**The system must have USB Mass Storage disabled unless needed.  
  
  
**Vulnerability Discussion:**  USB is a common computer peripheral interface. USB devices may include storage devices that could be used to install malicious software on a system or exfiltrate data.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system needs USB storage, this vulnerability is not applicable.  
  
Use the usbsecure.pl script to determine if USB storage is enabled. If USB storage is enabled, this is a finding.  
  
The script should be obtained from an authoritative channel. A link to the script from the Sun Developers Network is http://developers.sun.com/solaris/driverdev/reference/codesamples/usb\_security/index.html  
  
**Fix Text:**Use the usbsecure.pl script to disable USB storage.  
  
The script should be obtained from an authoritative channel. A link to the script from the Sun Developers Network is http://developers.sun.com/solaris/driverdev/reference/codesamples/usb\_security/index.html     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22580  
**Group Title:** GEN008500  
**Rule ID:** SV-26972r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008500  
**Rule Title:**The system must have IEEE 1394 (Firewire) disabled unless needed.  
  
  
**Vulnerability Discussion:**  Firewire is a common computer peripheral interface. Firewire devices may include storage devices that could be used to install malicious software on a system or exfiltrate data.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system needs IEEE 1394 (Firewire), this is not applicable.  
Check if the firewire module is not disabled.  
# grep 'exclude: s1394' /etc/system  
If no results are returned, this is a finding.  
  
**Fix Text:**Disable the firewire module.  
  
# echo "exclude: s1394" >> /etc/system  
  
Reboot for the changes to take effect.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22582  
**Group Title:** GEN008520  
**Rule ID:** SV-26974r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008520  
**Rule Title:**The system must employ a local firewall.  
  
  
**Vulnerability Discussion:**  A local firewall protects the system from exposing unnecessary or undocumented network services to the local enclave. If a system within the enclave is compromised, firewall protection on an individual system continues to protect it from attack.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system is using a local firewall.  
# svcs network/ipfilter  
If the service is not online, this is a finding.  
  
**Fix Text:**Enable the system's local firewall.  
# svcadm enable network/ipfilter     
  
**CCI:**CCI-001118  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22583  
**Group Title:** GEN008540  
**Rule ID:** SV-26976r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008540  
**Rule Title:**The system's local firewall must implement a deny-all, allow-by-exception policy.  
  
  
**Vulnerability Discussion:**  A local firewall protects the system from exposing unnecessary or undocumented network services to the local enclave. If a system within the enclave is compromised, firewall protection on an individual system continues to protect it from attack.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the firewall rules for a default deny rule.   
# ipfstat -i  
  
An example of a default deny rule is:  
block in log quick on ne3 from any to any.  
  
If there is no default deny rule, this is a finding.  
  
**Fix Text:**Edit /etc/ipf/ipf.conf and add a default deny rule.  
Restart the ipfilter service.  
# svcadm restart network/ipfilter     
  
**CCI:**CCI-001109  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1013  
**Group Title:** GEN008600  
**Rule ID:** SV-1013r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN008600  
**Rule Title:**The system must be configured to only boot from the system boot device.  
  
  
**Vulnerability Discussion:**  The ability to boot from removable media is the same as being able to boot into single user or maintenance mode without a password. This ability could allow a malicious user to boot the system and perform changes possibly compromising or damaging the system. It could also allow the system to be used for malicious purposes by a malicious anonymous user.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system is configured to boot from devices other than the system startup media. If so, this is a finding.  
  
In most cases, this will require access to the BIOS or system controller. The exact procedure will be hardware-dependent, and the SA should be consulted to identify the specific configuration. In the event the BIOS or system controller is not accessible without adversely impacting (e.g., restarting) the system, the SA may be interviewed to determine compliance with the requirement.  
  
**Fix Text:**Configure the system to only boot from system startup media.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4246  
**Group Title:** GEN008620  
**Rule ID:** SV-4246r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008620  
**Rule Title:**System BIOS or system controllers supporting password protection must have administrator accounts/passwords configured, and no others.  
  
  
**Vulnerability Discussion:**  A system's BIOS or system controller handles the initial startup of a system and its configuration must be protected from unauthorized modification. When the BIOS or system controller supports the creation of user accounts or passwords, such protections must be used and accounts/passwords only assigned to system administrators. Failure to protect BIOS or system controller settings could result in Denial-of-Service or compromise of the system resulting from unauthorized configuration changes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
On systems with a BIOS or system controller, verify a supervisor or administrator password is set. If a password is not set, this is a finding.  
  
If the BIOS or system controller supports user-level access in addition to supervisor/administrator access, determine if this access is enabled. If so, this is a finding.  
  
The exact procedure will be hardware-dependent, and the SA should be consulted to identify the specific configuration. In the event the BIOS or system controller is not accessible without adversely impacting (e.g., restarting) the system, the SA may be interviewed to determine compliance with the requirement.  
  
**Fix Text:**Access the system's BIOS or system controller. Set a supervisor/administrator password if one has not been set. Disable a user-level password if one has been set.     
  
**CCI:**CCI-000213  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4247  
**Group Title:** GEN008640  
**Rule ID:** SV-41534r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN008640  
**Rule Title:**The system must not use removable media as the boot loader.  
  
  
**Vulnerability Discussion:**  Malicious users with removable boot media can gain access to a system configured to use removable media as the boot loader.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Ask the SA if the system uses removable media for the boot loader. If it does, this is a finding.  
  
**Fix Text:**Configure the system to use a bootloader installed on fixed media.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4248  
**Group Title:** GEN008660  
**Rule ID:** SV-4248r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN008660  
**Rule Title:**For systems capable of using GRUB, the system must be configured with GRUB as the default boot loader unless another boot loader has been authorized, justified, and documented using site-defined procedures.  
  
  
**Vulnerability Discussion:**  GRUB is a versatile boot loader used by several platforms providing authentication for access to the system or boot loader.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Determine if the system uses the GRUB boot loader.  
# ls -l /boot/grub.conf /etc/grub.conf /boot/grub/grub.conf  
If the file does not exist, this is a finding.  
  
**Fix Text:**Configure the system to use the GRUB bootloader.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4255  
**Group Title:** GEN008680  
**Rule ID:** SV-4255r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN008680  
**Rule Title:**If the system boots from removable media, it must be stored in a safe or similarly secured container.  
  
  
**Vulnerability Discussion:**  Storing the boot loader on removable media in an insecure location could allow a malicious user to modify the systems boot instructions or boot to an insecure operating system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  PESS-1  
  
**Check Content:**    
Ask the SA if the system boots from removable media. If so, ask if the boot media is stored in a secure container when not in use. If it is not, this is a finding.  
  
**Fix Text:**Store the system boot media in a secure container when not in use.     
  
**CCI:**CCI-001208  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4249  
**Group Title:** GEN008700  
**Rule ID:** SV-4249r2\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN008700  
**Rule Title:**The system boot loader must require authentication.  
  
  
**Vulnerability Discussion:**  If the system's boot loader does not require authentication, users with console access to the system may be able to alter the system boot configuration or boot the system into single user or maintenance mode, which could result in Denial-of-Service or unauthorized privileged access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
For GRUB:  
  
Check the /etc/grub.conf or /boot/grub/menu.lst files.  
  
Procedure:  
# more /boot/grub/menu.lst  
  
Check for a password configuration line, such as the one below.  
password --md5 <password-hash>  
  
This line should be just below the line beginning with "timeout". Please note <password-hash> will be replaced by the actual MD5 encrypted password. If the password line is not in either of the files, this is a finding.  
  
**Fix Text:**The GRUB console boot loader can be configured to use an MD5 encrypted password by adding password --md5 password-hash to the /boot/grub.conf file. Use /sbin/grub-md5-crypt to generate MD5 passwords from the command line.     
  
**CCI:**CCI-000213  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24624  
**Group Title:** GEN008710  
**Rule ID:** SV-42317r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008710  
**Rule Title:**The system boot loader must protect passwords using an MD5 or stronger cryptographic hash.  
  
  
**Vulnerability Discussion:**  If system boot loader passwords are compromised, users with console access to the system may be able to alter the system boot configuration or boot the system into single user or maintenance mode, which could result in Denial-of-Service or unauthorized privileged access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the boot configuration for password settings.  
  
Procedure:  
  
Obtain the location of the active GRUB menu file.  
# bootadm list-menu  
  
List any password configuration from the active menu file (substitute the file determined above in place of the example file provided below, if necessary).  
# grep password /rpool/boot/grub/menu.lst  
  
Check for a password configuration line, such as:  
password --md5 <password-hash>  
  
If the boot loader passwords are not protected using an MD5 hash or stronger, this is a finding.  
  
**Fix Text:**Configure the GRUB bootloader to require a password.  
  
Procedure:  
  
Obtain the location of the active GRUB menu file.  
# bootadm list-menu  
  
Create a password hash using GRUB. The location of the GRUB binary may be different based on the specific system.  
# /boot/grub/bin/grub  
grub> md5crypt  
Password: <password>  
Encrypted: <password hash>  
grub> quit  
  
The encrypted password hash will be returned.  
  
Edit the GRUB menu configuration file, and add a line such as the following, substituting the password hash obtained above:  
  
password --md5 <password hash>     
  
**CCI:**CCI-000213  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4250  
**Group Title:** GEN008720  
**Rule ID:** SV-4250r2\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008720  
**Rule Title:**The system's boot loader configuration file(s) must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  File permissions greater than 0600 on boot loader configuration files could allow an unauthorized user to view or modify sensitive information pertaining to system boot instructions.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/grub.conf permissions.  
  
# ls -lL /etc/grub.conf  
  
If /etc/grub.conf has a mode more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the grub.conf file to 0600.  
  
# chmod 0600 /etc/grub.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22585  
**Group Title:** GEN008740  
**Rule ID:** SV-26985r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008740  
**Rule Title:**The system's boot loader configuration file(s) must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files. If extended ACLs are present on the system's boot loader configuration file(s), these files may be vulnerable to unauthorized access or modification, which could compromise the system's boot process.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lLd /boot/grub/grub.conf  
  
If the permissions of the file or directory contain "+", an extended ACL is present, and this is a finding.  
  
**Fix Text:**If the file with the extended ACL resides on a UFS filesystem:  
# getfacl /boot/grub/grub.conf  
Remove each ACE from the file.   
# setfacl -r [ACE] /boot/grub/grub.conf  
  
If the file with the extended ACL resides on a ZFS filesystem:   
# chmod A- /boot/grub/grub.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22586  
**Group Title:** GEN008760  
**Rule ID:** SV-26987r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008760  
**Rule Title:**The system's boot loader configuration files must be owned by root.  
  
  
**Vulnerability Discussion:**  The system's boot loader configuration files are critical to the integrity of the system and must be protected. Unauthorized modification of these files resulting from improper ownership could compromise the system's boot loader configuration.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the file.  
# ls -lLd /boot/grub/grub.conf  
If the owner of the file is not root, this is a finding.  
  
**Fix Text:**Change the ownership of the file.  
# chown root /boot/grub/grub.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22587  
**Group Title:** GEN008780  
**Rule ID:** SV-26989r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008780  
**Rule Title:**The system's boot loader configuration file(s) must be group-owned by root, bin, sys, or system.  
  
  
**Vulnerability Discussion:**  The system's boot loader configuration files are critical to the integrity of the system and must be protected. Unauthorized modifications resulting from improper group ownership may compromise the boot loader configuration.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the file.  
# ls -lLd /boot/grub/grub.conf  
If the group owner of the file is not root, this is a finding.  
  
**Fix Text:**Change the group ownership of the file.  
# chgrp root /boot/grub/grub.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22588  
**Group Title:** GEN008800  
**Rule ID:** SV-26991r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008800  
**Rule Title:**The system package management tool must cryptographically verify the authenticity of software packages during installation.  
  
  
**Vulnerability Discussion:**  To prevent the installation of software from unauthorized sources, the system package management tool must use cryptographic algorithms to verify the packages are authentic.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify package signature validation is not disabled.  
# grep "authentication=quit" /var/sadm/install/admin/default  
If no configuration is returned, this is a finding.  
  
**Fix Text:**Edit /var/sadm/install/admin/default and set the authentication setting to quit.     
  
**CCI:**CCI-000351  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22589  
**Group Title:** GEN008820  
**Rule ID:** SV-40814r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008820  
**Rule Title:**The system package management tool must not automatically obtain updates.  
  
  
**Vulnerability Discussion:**  System package management tools can obtain a list of updates and patches from a package repository and make this information available to the SA for review and action. Using a package repository outside of the organization's control, presents a risk that malicious packages could be introduced.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system package management tool is configured to automatically obtain updated packages using the cron or at utilities.  
  
# grep smpatch /var/spool/cron/crontabs/\* /var/spool/cron/atjobs/\*  
  
If smpatch is called with the add, update, or remove subcommands, this is a finding.  
  
**Fix Text:**Disable any cron or at jobs running smpatch.  
  
# crontab -e < user running smpatch >  
# atrm < id of at job running smpatch >     
  
**CCI:**CCI-001233  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24347  
**Group Title:** GEN009120  
**Rule ID:** SV-30004r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009120  
**Rule Title:**The system, if capable, must be configured to require the use of a CAC, PIV compliant hardware token, or Alternate Logon Token (ALT) for authentication.  
  
  
**Vulnerability Discussion:**  In accordance with CTO 07-015 PKI authentication is required. This provides stronger, two-factor authentication than using a username/password.  
  
NOTE: The following are exempt from this, however, they must meet all password requirements and must be documented with the IAO:  
  
- SIPRNET systems.  
- Stand-alone systems.  
- Application Accounts.  
- Students or unpaid employees (such as, interns) who are not eligible to receive or not in receipt of a CAC, PIV, or ALT.  
- Warfighters and support personnel located at operational tactical locations conducting wartime operations that are not collocated with RAPIDS workstations to issue CAC; are not eligible for CAC or do not have the capability to use ALT.  
- Test systems that have an Interim Approval to Test (IATT) and provide protection via separate VPN, firewall, or security measures preventing access to network and system components from outside the protection boundary documented in the IATT.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Consult vendor documentation to determine if the system is capable of CAC authentication. If it is not, this is not applicable.  
  
Interview the SA to determine if all accounts not exempted by policy are using CAC authentication. If non-exempt accounts are not using CAC authentication, this is a finding.  
  
  
**Fix Text:**Consult vendor documentation to determine the procedures necessary for configuring CAC authentication. Configure all accounts required by policy to use CAC authentication.     
  
**CCI:**CCI-000768  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**UNCLASSIFIED**