**UNCLASSIFIED**

**Red Hat Enterprise Linux 5 Security Technical Implementation Guide**

**Version: 1**

**Release: 1**

**2 Aug 2012**

**XSL Release 6/19/2012     Sort by:   STIGID**  
**Description:** The Red Hat Enterprise Linux 5 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-22341  
**Group Title:** GEN000000-LNX001431  
**Rule ID:** SV-37143r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX001431  
**Rule Title:**The /etc/gshadow file must be owned by root.  
  
  
**Vulnerability Discussion:**  The /etc/gshadow file is critical to system security and must be owned by a privileged user. The /etc/gshadow file contains a list of system groups and hashes for group passwords.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the /etc/gshadow file is owned by root.  
# ls -l /etc/gshadow  
If the file is not owned by root, this is a finding.  
  
  
  
**Fix Text:**Change the owner of the /etc/gshadow file to root.  
# chown root /etc/gshadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22342  
**Group Title:** GEN000000-LNX001432  
**Rule ID:** SV-37164r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX001432  
**Rule Title:**The /etc/gshadow file must be group-owned by root.   
  
  
**Vulnerability Discussion:**  The /etc/gshadow file is critical to system security and must be protected from unauthorized modification. The /etc/gshadow file contains a list of system groups and hashes for group passwords.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the /etc/gshadow file is group-owned by root.  
# ls -l /etc/gshadow  
If the file is not group-owned by root, this is a finding.  
  
**Fix Text:**Change the group-owner of the /etc/gshadow file to root.  
# chgrp root /etc/gshadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22343  
**Group Title:** GEN000000-LNX001433  
**Rule ID:** SV-37170r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX001433  
**Rule Title:**The /etc/gshadow file must have mode 0400.  
  
  
**Vulnerability Discussion:**  The /etc/gshadow file is critical to system security and must be protected from unauthorized modification. The /etc/gshadow file contains a list of system groups and hashes for group passwords.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/gshadow file.  
# ls -l /etc/gshadow  
If the file mode is more permissive than 0400, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/gshadow file to 0400 or less permissive.  
# chmod 0400 /etc/gshadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22344  
**Group Title:** GEN000000-LNX001434  
**Rule ID:** SV-37176r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX001434  
**Rule Title:**The /etc/gshadow file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  The /etc/gshadow file is critical to system security and must be protected from unauthorized modification. The /etc/gshadow file contains a list of system groups and hashes for group passwords.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/gshadow has no extended ACL.  
# ls -l /etc/gshadow  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/gshadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22349  
**Group Title:** GEN000000-LNX001476  
**Rule ID:** SV-37386r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX001476  
**Rule Title:**The /etc/gshadow file must not contain any group password hashes.  
  
  
**Vulnerability Discussion:**  Group passwords are typically shared and should not be used.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the /etc/gshadow file for password hashes.  
# cut -d : -f 2 /etc/gshadow | egrep -v '^(x|!!)$'  
If any password hashes are returned, this is a finding.  
  
  
  
**Fix Text:**Edit /etc/gshadow and change the password field to an exclamation point (!) to lock the group password.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4268  
**Group Title:** GEN000000-LNX00320  
**Rule ID:** SV-37181r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN000000-LNX00320  
**Rule Title:**The system must not have special privilege accounts, such as shutdown and halt.  
  
  
**Vulnerability Discussion:**  If special privilege accounts are compromised, the accounts could provide privileges to execute malicious commands on a system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAAC-1  
  
**Check Content:**    
Perform the following to check for unnecessary privileged accounts:  
  
# grep "^shutdown" /etc/passwd  
# grep "^halt" /etc/passwd  
# grep "^reboot" /etc/passwd  
  
If any unnecessary privileged accounts exist this is a finding.  
  
**Fix Text:**Remove any special privilege accounts, such as shutdown and halt, from the /etc/passwd and /etc/shadow files using the "userdel" or "system-config-users" commands.     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000764  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1021  
**Group Title:** GEN000000-LNX00360  
**Rule ID:** SV-37207r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00360  
**Rule Title:**The X server must have the correct options enabled.  
  
  
**Vulnerability Discussion:**  Without the correct options enabled, the Xwindows system would be less secure and there would be no screen timeout.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the options of the running Xwindows server are correct.  
  
Procedure:  
Get the running xserver information  
  
# ps -ef |grep X  
  
If the response contains /usr/bin/Xorg:0   
  
/usr/bin/Xorg:0 -br -audit 0 -auth /var/gdm/:0.Xauth -nolisten tcp vt7  
  
this is indicative of Xorg starting through gdm. This is the default on RHEL.  
  
Examine the Xorg line:  
  
If the "-auth" option is missing this would be a finding.  
If the "-audit" option is missing or not set to 4, this is a finding.  
If the "-s" option is missing or greater than 15, this is a finding.  
  
  
If the response to the grep contains X:0   
  
/usr/bin/X:0  
  
this indicates the X server was started with the xinit command with no associated .xserverrc in the home directory of the user. No options are selected by default. This is a finding.  
  
Otherwise if there are options on the X:0 line:  
If the "-auth" option is missing this is a finding   
If the "-audit" option is missing or not set to 4, this is a finding.  
If the "-s" option is missing or greater than 15, this is a finding.  
  
**Fix Text:**Enable the following options: -audit (at level 4), -auth and -s with 15 minutes as the timeout value.  
  
Procedure for gdm:  
Edit /etc/gdm/custom.conf and add the following:  
[server-Standard]   
name=Standard server  
command=/usr/bin/Xorg -br -audit 4 -s 15  
chooser=false  
handled=true  
flexible=true  
priority=0  
  
Procedure for xinit:  
Edit or create a .xserverrc file in the users home directory containing the startup script for xinit.  
This script must have an exec line with at least these options:  
  
exec /usr/bin/X -audit 4 -s 15 -auth <Xauth file> &  
  
The <Xauth file> is created using the "xauth" command and is customarily located in the users home directory with the name ".Xauthority".     
  
**CCI:**CCI-000032  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1022  
**Group Title:** GEN000000-LNX00380  
**Rule ID:** SV-37217r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00380  
**Rule Title:**An X server must have none of the following options enabled: -ac, -core (except for debugging purposes), or -nolock.   
  
  
**Vulnerability Discussion:**  These options will detract from the security of the Xwindows system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the options of the running Xwindows server are correct.  
  
Procedure:  
  
Get the running xserver information  
  
# ps -ef |grep X  
  
If the response contains /usr/bin/Xorg:0   
  
/usr/bin/Xorg:0 -br -audit 0 -auth /var/gdm/:0.Xauth -nolisten tcp vt7  
  
this is indicative of Xorg starting through gdm. This is the default window manager on RHEL.  
  
If the "-ac" option is found, this is a finding.  
If the "-core" option is found, this is a finding.  
If the "-nolock" option is found, this is a finding.  
  
  
If the response to the grep contains X:0   
  
/usr/bin/X:0  
  
Examine the X:0 line:  
  
If the "-ac" option is found, this is a finding.  
If the "-core" option is found, this is a finding.  
If the "-nolock" option is found, this is a finding.  
  
**Fix Text:**Disable the unwanted options:   
Procedure:  
For gdm:  
Remove the -ac, -core and -nolock options by creating a "command" entry in the /etc/gdm/custom.conf file with the options removed.  
  
For Xwindows started by xinit:  
Create or modify the .xserverrc script in the users home directory to remove the -ac, -core and -nolock options from the exec /usr/bin/X command.     
  
**CCI:**CCI-000032  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1025  
**Group Title:** GEN000000-LNX00400  
**Rule ID:** SV-37224r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00400  
**Rule Title:**The /etc/access.conf file must be owned by root.  
  
  
**Vulnerability Discussion:**  The /etc/access.conf file contains entries restricting access from the system console by authorized System Administrators. If the file is owned by a user other than root, it could compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check access configuration ownership:  
  
# ls -lL /etc/security/access.conf  
  
If this file exists and is not owned by root, this is a finding.  
  
**Fix Text:**Follow the correct configuration parameters for access configuration file. Use the chown command to configure it properly.   
(for example:  
# chown root /etc/security/access.conf   
).     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1054  
**Group Title:** GEN000000-LNX00420  
**Rule ID:** SV-37227r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00420  
**Rule Title:**The /etc/access.conf file must have a privileged group owner.  
  
  
**Vulnerability Discussion:**  Depending on the access restrictions of the /etc/access.conf file, if the group owner were not a privileged group, it could endanger system security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check access configuration group ownership:  
  
# ls -lL /etc/security/access.conf  
  
If this file exists and has a group-owner that is not a privileged user, this is a finding.  
  
**Fix Text:**Use the chgrp command to ensure the group owner is root, sys, or bin.  
(for example:  
# chgrp root /etc/security/access.conf  
  
).     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1055  
**Group Title:** GEN000000-LNX00440  
**Rule ID:** SV-37243r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00440  
**Rule Title:**The /etc/access.conf file must have mode 0640 or less permissive.  
  
  
**Vulnerability Discussion:**  If the access permissions are more permissive than 0640, system security could be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check access configuration mode:  
  
# ls -lL /etc/security/access.conf  
  
If this file exists and has a mode more permissive than 0640, this is a finding.  
  
**Fix Text:**Use the chmod command to set the permissions to 0640.  
(for example:  
# chmod 0640 /etc/security/access.conf  
  
).     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22595  
**Group Title:** GEN000000-LNX00450  
**Rule ID:** SV-26998r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00450  
**Rule Title:**The access.conf file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  If the access permissions are more permissive than 0640, system security could be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
# ls -lL /etc/security/access.conf  
If the permissions of the file or directory contain a '+', an extended ACL is present. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/security/access.conf     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4334  
**Group Title:** GEN000000-LNX00480  
**Rule ID:** SV-37253r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00480  
**Rule Title:**The /etc/sysctl.conf file must be owned by root.  
  
  
**Vulnerability Discussion:**  The sysctl.conf file specifies the values for kernel parameters to be set on boot. These settings can affect the system's security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/sysctl.conf ownership.  
# ls -lL /etc/sysctl.conf   
If /etc/sysctl.conf is not owned by root, this is a finding.  
  
**Fix Text:**Use the chown command to change the owner of /etc/sysctl.conf to root:  
# chown root /etc/sysctl.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4335  
**Group Title:** GEN000000-LNX00500  
**Rule ID:** SV-37257r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00500  
**Rule Title:**The /etc/sysctl.conf file must be group-owned by root.  
  
  
**Vulnerability Discussion:**  The sysctl.conf file specifies the values for kernel parameters to be set on boot. These settings can affect the system's security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/sysctl.conf group ownership:   
# ls -lL /etc/sysctl.conf   
If /etc/sysctl.conf is not group-owned by root, this is a finding.  
  
**Fix Text:**Use the chgrp command to change the group owner of /etc/sysctl.conf to root:  
# chgrp root /etc/sysctl.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4336  
**Group Title:** GEN000000-LNX00520  
**Rule ID:** SV-37258r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00520  
**Rule Title:**The /etc/sysctl.conf file must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  The sysctl.conf file specifies the values for kernel parameters to be set on boot. These settings can affect the system's security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/sysctl.conf permissions:  
  
# ls -lL /etc/sysctl.conf  
  
If /etc/sysctl.conf has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Use the chmod command to change the mode of the /etc/sysctl.conf file.  
# chmod 0600 /etc/sysctl.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22596  
**Group Title:** GEN000000-LNX00530  
**Rule ID:** SV-26999r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00530  
**Rule Title:**The /etc/sysctl.conf file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  The sysctl.conf file specifies the values for kernel parameters to be set on boot. These settings can affect the system's security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
  
# ls -lL /etc/sysctl.conf  
  
If the permissions of the file or directory contain a '+', an extended ACL is present. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/sysctl.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4339  
**Group Title:** GEN000000-LNX00560  
**Rule ID:** SV-37316r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN000000-LNX00560  
**Rule Title:**The Linux NFS Server must not have the insecure file locking option.  
  
  
**Vulnerability Discussion:**  Insecure file locking could allow for sensitive data to be viewed or edited by an unauthorized user.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Determine if an NFS server is running on the system by:  
  
# ps -ef |grep nfsd  
  
If an NFS server is running, confirm it is not configured with the insecure\_locks option by:  
  
# exportfs -v  
  
The example below would be a finding:  
  
/misc/export speedy.example.com(rw,insecure\_locks)  
  
**Fix Text:**Remove the "insecure\_locks" option from all NFS exports on the system.  
  
Procedure:  
  
Edit /etc/exports and remove all instances of the insecure\_locks option.  
  
Re-export the file systems to make the setting take effect.  
# exportfs -a     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000764  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4342  
**Group Title:** GEN000000-LNX00580  
**Rule ID:** SV-37327r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN000000-LNX00580  
**Rule Title:**The x86 CTRL-ALT-DELETE key sequence must be disabled.  
  
  
**Vulnerability Discussion:**  Undesirable reboots can occur if the CTRL-ALT-DELETE key sequence is not disabled. Such reboots may cause a loss of data or loss of access to critical information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify that reboot using the CTRL-ALT-DELETE key sequence has been disabled by performing:  
  
# grep ctrlaltdel /etc/inittab  
  
If the line returned does not specify "/usr/bin/logger", or is not commented out, this is a finding.  
  
**Fix Text:**Ensure the CTRL-ALT-DELETE key sequence has been disabled and attempts to use the sequence are logged.  
In the /etc/inittab file replace:  
ca::ctrlaltdel:/sbin/shutdown -t3 -r now  
with  
ca:nil:ctrlaltdel:/usr/bin/logger -p security.info "Ctrl-Alt-Del was pressed"  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4346  
**Group Title:** GEN000000-LNX00600  
**Rule ID:** SV-37339r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00600  
**Rule Title:**The Linux PAM system must not grant sole access to admin privileges to the first user who logs into the console.  
  
  
**Vulnerability Discussion:**  If an unauthorized user has been granted privileged access while logged in at the console, the security posture of a system could be greatly compromised. Additionally, such a situation could deny legitimate root access from another terminal.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Ensure the pam\_console.so module is not configured in any files in /etc/pam.d by:  
  
      # cd /etc/pam.d  
      # grep pam\_console.so \*  
  
Or  
  
      #       ls -la /etc/security/console.perms  
  
If either the pam\_console.so entry or the file /etc/security/console.perms is found then this is a finding.  
  
  
**Fix Text:**Configure PAM to not grant sole access of administrative privileges to the first user logged in at the console.   
  
Identify any instances of pam\_console.  
  
# cd /etc/pam.d  
# grep pam\_console.so \*  
  
For any files containing an un-commented reference to pam\_console.so, edit the file and remove or comment out the reference.  
  
Remove the console.perms file if it exists:  
# rm /etc/security/console.perms     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12038  
**Group Title:** GEN000000-LNX00620  
**Rule ID:** SV-37340r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00620  
**Rule Title:**The /etc/securetty file must be group-owned by root, sys, or bin.  
  
  
**Vulnerability Discussion:**  The securetty file contains the list of terminals permitting direct root logins. It must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/securetty group ownership:  
  
# ls -lL /etc/securetty  
  
If /etc/securetty is not group owned by root, sys, or bin, then this is a finding.  
  
  
**Fix Text:**Change the group-owner of /etc/securetty to root, sys, or bin.  
Example:  
# chgrp root /etc/securetty     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12039  
**Group Title:** GEN000000-LNX00640  
**Rule ID:** SV-37341r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00640  
**Rule Title:**The /etc/securetty file must be owned by root.  
  
  
**Vulnerability Discussion:**  The securetty file contains the list of terminals permitting direct root logins. It must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/securetty ownership.  
  
Procedure:  
# ls -lL /etc/securetty  
  
If /etc/securetty is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/securetty file to root.  
  
Procedure:  
# chown root /etc/securetty     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12040  
**Group Title:** GEN000000-LNX00660  
**Rule ID:** SV-37342r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-LNX00660  
**Rule Title:**The /etc/securetty file must have mode 0640 or less permissive.  
  
  
**Vulnerability Discussion:**  The securetty file contains the list of terminals permitting direct root logins. It must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/securetty permissions.  
  
Procedure:  
# ls -lL /etc/securetty  
  
If /etc/securetty has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/securetty file to 0600.  
  
Procedure:  
# chmod 0600 /etc/securetty     
  
**CCI:**CCI-000225  
  
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22598  
**Group Title:** GEN000000-LNX00720  
**Rule ID:** SV-27001r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000000-LNX00720  
**Rule Title:**Auditing must be enabled at boot by setting a kernel parameter.  
  
  
**Vulnerability Discussion:**  If auditing is enabled late in the boot process, the actions of startup scripts may not be audited. Some audit systems also maintain state information only available if auditing is enabled before a given process is created.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for the audit=1 kernel parameter.  
# grep 'audit=1' /proc/cmdline  
If no results are returned, this is a finding.  
  
**Fix Text:**Edit the grub bootloader file /boot/grub/grub.conf or /boot/grub/menu.lst by appending the "audit=1" parameter to the kernel boot line.  
Reboot the system for the change to take effect.     
  
**CCI:**CCI-000032  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22584  
**Group Title:** GEN000000-LNX00800  
**Rule ID:** SV-26978r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000000-LNX00800  
**Rule Title:**The system must use a Linux Security Module configured to limit the privileges of system services.  
  
  
**Vulnerability Discussion:**  Linux Security Modules such as SELinux and AppArmor can be used to provide protection from software exploits by explicitly defining the privileges permitted to each software package.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check if SELinux is enabled with at least a "targeted" policy.  
  
# grep ^SELINUX /etc/sysconfig/selinux  
  
If the SELINUX option is not set to "enforcing", this is a finding.  
If the SELINUXTYPE option is not set to "targeted" or "strict", this is a finding.  
  
If the use of the system is incompatible with the confines of SELinux this rule may be waived.  
  
**Fix Text:**Enable one of the SELinux policies.  
Edit /etc/sysconfig/selinux and set the value of the SELINUX option to "enforcing" and SELINUXTYPE to "targeted" or "strict".  
Restart the system.     
  
**CCI:**CCI-000032  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-756  
**Group Title:** GEN000020  
**Rule ID:** SV-37350r1\_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:**    
Check if the system requires a password for entering single-user mode.  
# grep ':S:' /etc/inittab  
If /sbin/sulogin is not listed, this is a finding.  
  
**Fix Text:**Edit /etc/inittab and set sulogin to run in single-user mode.  
Example line in /etc/inittab:  
~:S:wait:/sbin/sulogin     
  
**CCI:**CCI-000213  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11940  
**Group Title:** GEN000100  
**Rule ID:** SV-27049r1\_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:**    
Check the version of the operating system.  
  
Example:  
# cat /etc/redhat-release  
  
Vendor End-of-Support Information:  
Red Hat Enterprise 5: 31 Mar 2014  
  
Check with the vendor for additional information.  
  
If the version installed 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-27059r1\_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:**    
Obtain the list of available package updates from Red Hat. Check the available package updates have been installed on the system.  
  
Use the "rpm" command to list the packages installed on the system.  
Example:  
# rpm -qa -last  
  
If updated packages are available and applicable to the system and have not been installed, this is a finding.  
  
One source for the list of Red Hat updates is available at https://access.redhat.com/security/updates/active/  
  
**Fix Text:**Install the patches or updated packages available from the vendor.     
  
**CCI:**CCI-001227  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-27250  
**Group Title:** GEN000140-2  
**Rule ID:** SV-34549r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000140-2  
**Rule Title:**A file integrity baseline including cryptographic hashes must be created.  
  
  
**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:**    
Verify a system integrity baseline exists. The Advanced Intrusion Detection Environment (AIDE) is included in the distribution of RHEL. Other host intrusion detection system (HIDS) software is available but must be checked manually.  
  
Procedure:  
# grep DBDIR /etc/aide.conf  
  
If /etc/aide.conf does not exist AIDE has not been installed. Unless another HIDS is used on the system, this is a finding.  
  
Examine the response for "database" this indicates the location of the system integrity baseline database used as input to a comparison.   
# ls -la <DBDIR>  
  
If no "database" file as defined in /etc/aide.conf exists a system integrity baseline has not been created, this is a finding.  
  
Examine /etc/aide.conf to ensure some form of cryptographic hash (i.e. md5,rmd168,sha256) is used for files. In the default /etc/aide.conf the "NORMAL" or "LSPP" rules which are used for virtually all files DO include some form of cryptographic hash.  
  
If the site has defined rules to replace the functionality provided by the default "NORMAL" and "LSPP" rules but DOES NOT include cryptographic hashes, this is a finding.  
  
Otherwise, if any element used to define the "NORMAL" and "LSPP" rules has been modified resulting in cryptographic hashes not being used, this is a finding.  
  
If any other modification to the default /etc/aide.conf file have been made resulting in rules which do not include cryptographic hashes on appropriate files, this is a finding.  
  
**Fix Text:**Use AIDE to create a file integrity baseline, including cryptographic hashes, for the system.  
  
Configure the /etc/aide.conf file to ensure some form of cryptographic hash (e.g., md5,rmd168,sha256) is used for files. In the default /etc/aide.conf the "NORMAL" or "LSPP" rules which are used for virtually all files DO include some form of cryptographic hash.     
  
**CCI:**CCI-000293  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-27251  
**Group Title:** GEN000140-3  
**Rule ID:** SV-34550r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000140-3  
**Rule Title:**A file integrity baseline including cryptographic hashes must be 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:**    
Verify a system integrity baseline is maintained. The baseline has been updated to be consistent with the latest approved system configuration changes. The Advanced Intrusion Detection Environment (AIDE) is included in the distribution of RHEL-5. Other host intrusion detection system (HIDS) software is available but must be checked manually.  
  
Procedure:  
# grep DBDIR /etc/aide.conf  
  
If /etc/aide.conf does not exist AIDE has not been installed. Unless another HIDS is used on the system, this is a finding.  
  
Examine the response for "database" indicates the location of the system integrity baseline database used as input to a comparison.   
# ls -la <DBDIR>  
  
If the no "database" file as defined in /etc/aide.conf a system integrity baseline has not been created, this is a finding.  
  
Ask the SA when the last approved system configuration changes occurred. If the modification date of the AIDE database is prior to the last approved configuration change, this is a finding.  
  
  
  
**Fix Text:**Regularly rebuild the integrity baseline, including cryptographic hashes, for the system to be consistent with the latest approved system configuration.  
  
Procedure:  
After an approved modification to the system configuration has been made perform:  
  
# aide -u  
This will update the database.     
  
**CCI:**CCI-000293  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11945  
**Group Title:** GEN000220  
**Rule ID:** SV-38178r1\_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, binaries and other critical system files 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 an automated job, scheduled to run weekly or more frequently, to run the file integrity tool to check for unauthorized additions to system libraries. The check can be done using Advanced Intrusion Detection Environment (AIDE) which is part of the Red Hat Enterprise Linux (RHEL) distribution. Other file integrity software may be used but must be checked manually.   
  
Procedure:  
Check the root crontab (crontab -l) and the global crontabs in /etc/crontab, /etc/cron.d/\* for the presence of an "aide" job to run at least weekly, which should have asterisks (\*) in columns 3, 4, and 5.  
  
Check the weekly cron directory (/etc/cron.weekly) for any script running "aide --check" or "aide -C" or simply "aide". If there is not, this is a finding.  
  
NOTE: For MAC I systems, increase the frequency to daily.  
  
  
**Fix Text:**Establish an automated job, scheduled to run weekly or more frequently, to run "aide --check" which is the file integrity tool to check for unauthorized 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-37402r1\_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 (i.e., it has 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 if NTP running:  
# ps -ef | egrep "xntpd|ntpd"  
  
Check if "ntpd -qg" scheduled to run:  
# grep "ntpd -qg" /var/spool/cron/\*  
# grep "ntpd -qg" /etc/cron.d/\*  
# grep "ntpd -qg" /etc/cron.daily/\*  
# grep "ntpd -qg" /etc/cron.hourly/\*  
# grep "ntpd -qg" /etc/cron.monthly/\*  
# grep "ntpd -qg" /etc/cron.weekly/\*  
  
If NTP is running or "ntpd -qg" is found:  
  
# more /etc/ntp.conf  
  
Confirm the timeservers and peers or multicast client (as applicable) are local or authoritative U.S. DoD sources appropriate for the level of classification which the network operates.  
  
If a non-local/non-authoritative time-server is used, this is a finding.  
  
**Fix Text:**Use an authoritative local time server or a time server operated by the U.S. government. Ensure all systems in the facility feed from one or more local time servers which feed from the authoritative U.S. government time server.     
  
**CCI:**CCI-001492  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22290  
**Group Title:** GEN000241  
**Rule ID:** SV-26292r1\_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 (i.e., it has 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 (crontab -l) and the global crontabs in /etc/crontab, /etc/cron.d/\* for the presence of an "ntpd -qg" job to run at least daily, which should have asterisks (\*) in columns 3, 4, and 5.  
  
Check the daily cron directory (/etc/cron.daily) for any script running "ntpd -qg".  
  
Check for a running NTP daemon.  
# ps ax | grep ntpd  
  
If none of the above checks are successful, this is a finding.  
  
**Fix Text:**Enable the NTP daemon for continuous synchronization.  
# service ntpd start ; chkconfig ntpd on  
  
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-37412r1\_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 (i.e., it has 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 (crontab -l) and the global crontabs in /etc/crontab, /etc/cron.d/\*, or scripts in the /etc/cron.daily directory for the presence of an "ntpd -qg" job. If the "ntpd -qg" 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/ntp.conf | egrep -v '(127.127.1.0|127.127.1.1)'  
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 "ntpd -qg", add additional NTP servers to the cron job running "ntpd -qg".  
  
If using the NTP daemon, add an additional "server" line to /etc/ntp.conf for each additional NTP server.     
  
**CCI:**CCI-000160  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22292  
**Group Title:** GEN000244  
**Rule ID:** SV-37413r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000244  
**Rule Title:**The system must use local time sources 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 providing 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 (i.e., it has 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 (crontab -l) and the global crontabs in /etc/crontab, /etc/cron.d/\*, or scripts in the /etc/cron.daily directory for the presence of an "ntpd -qg" job. If the "ntpd -qg" command is invoked with NTP servers outside of the enclave, this is a finding.  
  
Check the NTP daemon configuration for NTP servers.  
# grep ^server /etc/ntp.conf | grep -v 127.127.1.1  
If an NTP server is listed outside of the enclave, this is a finding.  
  
**Fix Text:**If using "ntpd -qg", remove NTP servers external to the enclave from the cron job running "ntpd -qg".  
  
If using the NTP daemon, remove the "server" line from /etc/ntp.conf for each NTP server external to the enclave.     
  
**CCI:**CCI-000160  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22294  
**Group Title:** GEN000250  
**Rule ID:** SV-37415r1\_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:**    
Check the ownership of the NTP configuration file.  
# ls -l /etc/ntp.conf  
If the owner is not root, this is a finding.  
  
**Fix Text:** Change the owner of the NTP configuration file.  
# chown root /etc/ntp.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22295  
**Group Title:** GEN000251  
**Rule ID:** SV-37416r1\_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 -lL /etc/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/ntp.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22296  
**Group Title:** GEN000252  
**Rule ID:** SV-37417r1\_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:**    
Check the mode for the NTP configuration file is not more permissive than 0640.  
# ls -l /etc/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 more restrictive.  
# chmod 0640 /etc/ntp.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22297  
**Group Title:** GEN000253  
**Rule ID:** SV-37418r1\_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 the NTP configuration file has no extended ACL.  
# ls -l /etc/ntp.conf  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the NTP configuration file.  
# setfacl --remove-all /etc/ntp.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-760  
**Group Title:** GEN000280  
**Rule ID:** SV-37419r1\_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.  
  
**Documentable:** YES   
**Responsibility:**  Information Assurance Officer  
**IAControls:**  ECSC-1, IAIA-1  
  
**Check Content:**    
Use the last command to check for multiple accesses to an account from different workstations/IP addresses.  
  
# last -R  
  
If users log directly onto accounts, rather than using the switch user (su) command from their own named account to access them, this is a finding (such as logging directly on to oracle).  
  
Verify with the SA or the IAO on documentation for users/administrators to log into their own accounts first and then switch user (su) to the account to be shared has been maintained including requirements and procedures. If no such documentation exists, this is a finding.   
  
**Fix Text:**Use the switch user (su) command from a named account login to access shared accounts. Document requirements and procedures for users/administrators to log into their own accounts first and then switch user (su) to the account to be shared.     
  
**CCI:**CCI-000770  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4269  
**Group Title:** GEN000290  
**Rule ID:** SV-38176r1\_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   
  
Obtain a list of authorized accounts from the IAO. If any unnecessary accounts are found on the system, this is a finding.  
  
**Fix Text:**Remove all unnecessary accounts from the /etc/passwd file before connecting a system to the network. Other accounts that are associated with a service not in use should also be removed.     
  
**CCI:**CCI-000012  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29376  
**Group Title:** GEN000290-1  
**Rule ID:** SV-38177r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000290-1  
**Rule Title:**The system must not have the unnecessary "games" account.  
  
  
**Vulnerability Discussion:**  Accounts that provide 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.  
  
**IAControls:**  IAAC-1  
  
**Check Content:**    
Check the system for the unnecessary "games" accounts.  
  
Procedure:  
# grep ^games /etc/passwd  
If this account exists, it is a finding.  
  
  
**Fix Text:**Remove the "games" account.  
  
Procedure:  
# userdel games     
  
**CCI:**CCI-000012  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-27275  
**Group Title:** GEN000290-2  
**Rule ID:** SV-34574r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000290-2  
**Rule Title:**The system must not have the unnecessary "news" account.  
  
  
**Vulnerability Discussion:**  Accounts that provide 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 the unnecessary "news" accounts.  
  
Procedure:  
# rpm -q inn  
If the "inn" is installed the "news" user is necessary and this is not a finding.  
  
# grep ^news /etc/passwd  
If this account exists and "inn" is not installed, this is a finding.  
  
**Fix Text:**Remove the "news" account from the /etc/passwd file before connecting a system to the network.     
  
**CCI:**CCI-000012  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-27276  
**Group Title:** GEN000290-3  
**Rule ID:** SV-34575r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000290-3  
**Rule Title:**The system must not have the unnecessary "gopher" account.  
  
  
**Vulnerability Discussion:**  Accounts that provide 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 the unnecessary "gopher" accounts.  
  
Procedure:  
# grep ^gopher /etc/passwd  
If this account exists, it is a finding.  
  
**Fix Text:**Remove the "gopher" account from the /etc/passwd file before connecting a system to the network.     
  
**CCI:**CCI-000012  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-27279  
**Group Title:** GEN000290-4  
**Rule ID:** SV-34578r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000290-4  
**Rule Title:**The system must not have the unnecessary "ftp" account.  
  
  
**Vulnerability Discussion:**  Accounts that provide 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 the unnecessary "ftp" accounts.  
  
Procedure:  
# rpm -q krb5-workstation  
An ftp server is part of "krb5-workstation". If it is installed the "ftp" user is necessary and this is not a finding.  
  
# rpm -q vsftp  
If the "vsftp" ftp server is installed the "ftp" user is necessary and this is not a finding.  
  
# grep ^ftp /etc/passwd  
If this account exists and no ftp server is installed which requires it, this is a finding.  
  
**Fix Text:**Remove the "ftp" account from the /etc/passwd file before connecting a system to the network.     
  
**CCI:**CCI-000012  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-761  
**Group Title:** GEN000300  
**Rule ID:** SV-27063r1\_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:  
# pwck -r  
  
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-27068r1\_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:  
  
# cut -d: -f3 /etc/passwd | uniq -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-37155r1\_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 for all accounts.  
  
# cut -d: -f 1,3 /etc/passwd | egrep ":[1-4][0-9]{2}$|:[0-9]{1,2}$"  
  
Confirm all accounts with a UID of 499 and below are used by a system account. If a UID reserved for system accounts (0 - 499) is used by a non-system account, then this is a finding.  
  
**Fix Text:**Change the UID numbers for non-system accounts with reserved UIDs (those less or equal to 499).     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-780  
**Group Title:** GEN000360  
**Rule ID:** SV-37157r1\_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.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Confirm all accounts with a GID of 499 and below are used by a system account.   
  
Procedure:  
List all the users with a GID of 0-499.  
# cut -d: -f 1,4 /etc/passwd|egrep ":[1-4][0-9]{2}$|:[0-9]{1,2}$"  
  
If a GID reserved for system accounts (0 - 499) 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 499).     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-781  
**Group Title:** GEN000380  
**Rule ID:** SV-27072r1\_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 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:  
# pwck -r  
If GIDs referenced in /etc/passwd are not defined in /etc/group are returned, this is a finding.  
  
**Fix Text:**Add a group to the system for each GID referenced without a corresponding group.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-763  
**Group Title:** GEN000400  
**Rule ID:** SV-37169r1\_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 logon 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 login 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-37171r1\_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 logon 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:**    
Access the graphical desktop environment(s) provided by the system and attempt to log in. 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:**Configure the system to display one of the DoD login banners prior to, or as part of, the graphical desktop environment login process.  
  
Procedure:  
Modify /usr/share/gdm/themes/RHEL/RHEL.xml by adding the following xml after the first two "pixmap" entries.  
  
<item type="rect" id="custom-dod-banner">  
<pos anchor="nw" x="20%" y="10" width="80%" height="100%"/>  
<box>  
<item type="label">  
<normal font="Sans Bold 9" color="#ffffff"/>  
<text>  
Insert the "approved text" here based on the character limitations imposed by the system.  
</text>  
</item>  
</box>  
</item>  
  
  
Approved 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-28606r1\_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 to 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:**Provide the proper text for the DoD banner to be presented by the FTP server to the user.  
  
For vsftp:  
Examine the /etc/vsftp.conf file for the "banner\_file" entry. (i.e. banner\_file = /etc/banner/vsftp)  
  
For gssftp:  
Examine the /etc/xinetd.d/gssftp file for the "banner" entry. (i.e. banner = /etc/banner/gssftp)  
  
For both:  
Add the banner entry if one is not found.  
  
Modify or create the referenced banner file to contain one of the following 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-765  
**Group Title:** GEN000440  
**Rule ID:** SV-37178r1\_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 assists 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 all logon attempts are being logged.  
  
Procedure:  
Verify successful logins are being logged:  
# last -R | more   
If the command does not return successful logins, this is a finding.  
  
Verify if unsuccessful logons are being logged:   
# lastb -R | more  
If the command does not return unsuccessful logins, this is a finding.  
  
**Fix Text:**Make sure the collection files exist.  
Procedure:  
If there are no successful logins being returned from the "last" command, create /var/log/wtmp:  
# touch /var/log/wtmp  
  
If there are no unsuccessful logins being returned from the "lastb" command, create /var/log/btmp:  
# touch /var/log/btmp     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22298  
**Group Title:** GEN000450  
**Rule ID:** SV-37182r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000450  
**Rule Title:**The system must limit users to 10 simultaneous system logins, or a site-defined number, in accordance with operational requirements.  
  
  
**Vulnerability Discussion:**  Limiting simultaneous user logins can insulate the system from denial of service problems caused by excessive logins. Automated login processes operating improperly or maliciously may result in an exceptional number of simultaneous login sessions.  
  
If the defined value of 10 logins does not meet operational requirements, the site may define the permitted number of simultaneous login sessions based on operational requirements.  
  
This limit is for the number of simultaneous login sessions for EACH user account. This is NOT a limit on the total number of simultaneous login sessions on the system.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for a default maxlogins line in the /etc/security/limits.conf and /etc/security/limits.d/\* files.  
  
Procedure:  
#grep maxlogins /etc/security/limits.conf /etc/security/limits.d/\*  
  
The default maxlimits should be set to a max of 10 or a documented site defined number:  
  
\* - maxlogins 10  
  
If no such line exists, this is a finding.  
  
**Fix Text:**Add a "maxlogins" line such as "\* hard maxlogins 10" to /etc/security/limits.conf or a file in /etc/security/limits.d. The enforced maximum should be defined by site requirements and policy.     
  
**CCI:**CCI-000054  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22299  
**Group Title:** GEN000452  
**Rule ID:** SV-37187r1\_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:**    
Check that pam\_lastlog is used and not silent, or that the SSH daemon is configured to display last login information.  
  
# grep pam\_lastlog /etc/pam.d/sshd  
If pam\_lastlog is present, and does not have the "silent" option, this is not a finding.  
  
# grep -i PrintLastLog /etc/ssh/sshd\_config  
  
If PrintLastLog is not present in the configuration, this is not a finding. This is the default setting.  
If PrintLastLog is present in the configuration and set to "yes" (case insensitive), this is not a finding.  
Otherwise, this is a finding.  
  
**Fix Text:**Implement pam\_lastlog, or enable PrintLastLog in the SSH daemon.  
  
To enable pam\_lastlog, add a line such as "session required pam\_lastlog.so" to /etc/pam.d/sshd.  
  
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-37203r1\_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:**    
Check the pam\_tally configuration.  
# more /etc/pam.d/system-auth   
Confirm the following line is configured, before any "auth sufficient" lines:  
auth required pam\_tally2.so deny=3   
If no such line is found, this is a finding.  
  
**Fix Text:**By default link /etc/pam.d/system-auth points to /etc/pam.d/system-auth-ac which is the file maintained by the authconfig utility. In order to add pam options other than those available via the utility create /etc/pam.d/system-auth-local with the options and including system-auth-ac. In order to set the account lockout to three failed attempts the content should be similar to:  
  
auth required pam\_access.so  
auth required pam\_tally2.so deny=3  
auth include system-auth-ac  
account required pam\_tally2.so  
account include system-auth-ac  
password include system-auth-ac  
session include system-auth-ac  
  
Once system-auth-local is written reset the /etc/pam.d/system-auth to point to system-auth-local. This is necessary because authconfig writes directly to system-auth-ac so any changes made by hand will be lost if authconfig is run.     
  
**CCI:**CCI-000044  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-768  
**Group Title:** GEN000480  
**Rule ID:** SV-37213r1\_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 value of the FAIL\_DELAY variable and the ability to use it.  
  
Procedure:  
# grep FAIL\_DELAY /etc/login.defs   
If the value does not exist, or is less than 4, this is a finding.  
  
Check for the use of pam\_faildelay.  
# grep pam\_faildelay /etc/pam.d/system-auth\*  
If pam\_faildelay.so module is not present, this is a finding.  
  
If pam\_faildelay is present only in /etc/pam.d/system-auth-ac:  
ensure that /etc/pam.d/system-auth includes /etc/pam.d/system-auth-ac.  
#grep system-auth-ac /etc/pam.d/system-auth  
  
This should return:  
auth include system-auth-ac  
account include system-auth-ac  
password include system-auth-ac  
session include system-auth-ac  
  
/etc/pam.d/system-auth-ac should only be included by /etc/pam.d/system-auth. All other pam files should include /etc/pam.d/system-auth.   
  
If pam\_faildelay is not defined in /etc/pam.d/system-auth either directly or through inclusion of system-auth-ac, this is a finding.  
  
**Fix Text:**Add the pam\_faildelay module and set the FAIL\_DELAY variable.  
  
Procedure:  
  
Edit /etc/login.defs and set the value of the FAIL\_DELAY variable to 4 or more.  
  
The default link /etc/pam.d/system-auth points to /etc/pam.d/system-auth-ac which is the file maintained by the authconfig utility. In order to add pam options other than those available via the utility create or modify /etc/pam.d/system-auth-local with the options and including system-auth-ac. For example:  
  
auth required pam\_access.so  
auth optional pam\_faildelay.so delay=4000000  
auth include system-auth-ac  
account include system-auth-ac  
password include system-auth-ac  
session include system-auth-ac  
  
Once system-auth-local is written ensure the /etc/pam.d/system-auth points to system-auth-local. This is necessary because authconfig writes directly to system-auth-ac so any manual changes made will be lost if authconfig is run.     
  
**CCI:**CCI-000043  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4083  
**Group Title:** GEN000500  
**Rule ID:** SV-29796r1\_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. Applications requiring continuous, real-time screen display (i.e., network management products) require the following and need to be documented with the IAO. -The logon session does not have administrator rights. -The display station (i.e., keyboard, monitor, etc.) is located in a controlled access area.   
  
  
**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:**    
For the Gnome screen saver, check the idle\_activation\_enabled flag.  
  
Procedure:  
# gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --get /apps/gnome-screensaver/idle\_activation\_enabled  
If this does not return "true" and a documented exception has not been made by the IAO, this is a finding.  
  
**Fix Text:**For the Gnome screen saver, set the idle\_activation\_enabled flag.  
Procedure:  
# gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type bool --set /apps/gnome-screensaver/idle\_activation\_enabled true  
    
  
**CCI:**CCI-000057  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-27283  
**Group Title:** GEN000500-2  
**Rule ID:** SV-34582r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000500-2  
**Rule Title:**The graphical desktop environment must set the idle timeout to no more than 15 minutes.  
  
  
**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:**    
For the Gnome screen saver, check the idle\_delay setting.  
  
Procedure:  
# gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --get /apps/gnome-screensaver/idle\_delay  
If this does not return 15 or less, this is a finding.  
  
**Fix Text:**For the Gnome screen saver, set idle\_delay to 15.  
  
Procedure:  
# gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type int --set /apps/gnome-screensaver/idle\_delay 15     
  
**CCI:**CCI-000057  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-27284  
**Group Title:** GEN000500-3  
**Rule ID:** SV-34583r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000500-3  
**Rule Title:**Graphical desktop environments provided by the system must have automatic lock enabled.  
  
  
**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:**    
For the Gnome screen saver, check the lock\_enabled flag.  
  
Procedure:  
# gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --get /apps/gnome-screensaver/lock\_enabled  
If this does not return "true", this is a finding.  
  
**Fix Text:**For the Gnome screen saver, set the lock\_enabled flag.  
  
Procedure:  
# gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type bool --set /apps/gnome-screensaver/lock\_enabled true     
  
**CCI:**CCI-000057  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22301  
**Group Title:** GEN000510  
**Rule ID:** SV-37222r1\_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. Some screensaver themes available but not included in the RHEL distribution use a snapshot of the current screen as a graphic. This theme does not qualify as a publicly-viewable pattern. If the session lock pattern is not publicly-viewable this is a finding.  
  
**Fix Text:**Configure the system to display a publicly-viewable pattern during a session lock. This is done graphically by selecting a screensaver theme using gnome-screensaver-preferences command. Any of the themes distributed with RHEL may be used including "Blank Screen".     
  
**CCI:**CCI-000061  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-769  
**Group Title:** GEN000520  
**Rule ID:** SV-37232r1\_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.  
Verify documentation exists for the requirement and justification of the application. If no documentation exists, this is a finding.  
Execute "ps -ef | more" to determine which user owns the process(es) associated with the application. If the owner is root, this is a finding.  
  
**Fix Text:**Configure the system so the owner of a session requires 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 and 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-37239r1\_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.  
# cat /etc/shadow | cut -d ':' -f 4 | grep -v 1  
If any results are returned, this is a finding.  
  
**Fix Text:** Change the minimum time period between password changes for each user account to 1 day.  
# passwd -n 1 <user name>     
  
**CCI:**CCI-000198  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-770  
**Group Title:** GEN000560  
**Rule ID:** SV-37259r1\_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 the system will not log in accounts with blank passwords.  
# grep nullok /etc/pam.d/system-auth /etc/pam.d/system-auth-ac  
If an entry for nullok is found, this is a finding on Linux.  
  
**Fix Text:**Edit /etc/pam.d/system-auth and remove the "nullok" setting.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11947  
**Group Title:** GEN000580  
**Rule ID:** SV-37260r1\_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.  
  
Procedure:  
Check the password minlen option  
# grep pam\_cracklib.so /etc/pam.d/system-auth  
  
Confirm the minlen option is set to at least 14 as in the example below:  
  
password required pam\_cracklib.so minlen=14  
  
There may be other options on the line. If no such line is found, or the minlen is less than 14 this is a finding.   
  
**Fix Text:**Edit "/etc/pam.d/system-auth" to include the line:  
  
password required pam\_cracklib.so minlen=14  
  
prior to the "password include system-auth-ac" line.     
  
**CCI:**CCI-000205  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22302  
**Group Title:** GEN000585  
**Rule ID:** SV-37261r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000585  
**Rule Title:**The system must enforce compliance of the entire password during authentification.  
  
  
**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  
# cut -d ':' -f2 /etc/shadow  
  
If any password hash is present that does not have an initial underscore (\_) or dollar sign ($) character, this is a finding.  
  
  
**Fix Text:**Change the passwords for all accounts using non-compliant password hashes.   
  
(This requires GEN000590 is already met.)     
  
**CCI:**CCI-000205  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22303  
**Group Title:** GEN000590  
**Rule ID:** SV-26313r1\_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 algorithm used for password hashing is of the SHA-2 family.  
# egrep "password .\* pam\_unix.so" /etc/pam.d/system-auth-ac  
If the line indicates the hash algorithm is not set to sha256 or sha512, this is a finding.  
  
**Fix Text:**Change the default password algorithm.  
# authconfig --passalgo=sha512 --update     
  
**CCI:**CCI-000803  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22304  
**Group Title:** GEN000595  
**Rule ID:** SV-26316r1\_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:**    
Check all password hashes in /etc/passwd or /etc/shadow begin with '$5$' or '$6$'.  
  
Procedure:  
# cut -d ':' -f2 /etc/passwd  
# cut -d ':' -f2 /etc/shadow  
  
Any password hashes present not beginning with '$5$' or '$6$', is a finding.  
  
**Fix Text:** Change the passwords for all accounts using non-compliant password hashes.   
  
(This requires GEN000590 is already met.)     
  
**CCI:**CCI-000196  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11948  
**Group Title:** GEN000600  
**Rule ID:** SV-41826r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000600  
**Rule Title:**The system must require passwords 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 ucredit setting.  
# grep ucredit /etc/pam.d/system-auth  
If ucredit is not set to -1, this is a finding.  
  
**Fix Text:**Edit "/etc/pam.d/system-auth" to include the line:  
  
password required pam\_cracklib.so ucredit=-1  
  
prior to the "password include system-auth-ac" line.     
  
**CCI:**CCI-000192  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-27285  
**Group Title:** GEN000600-2  
**Rule ID:** SV-34584r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000600-2  
**Rule Title:**Global settings defined in system-auth must be applied in the pam.d definition files.   
  
  
**Vulnerability Discussion:**  Pam global requirements are generally defined in the /etc/pam.d/system-auth or /etc/pam.d/system-auth-ac file. In order for the requirements to be applied the file containing them must be included directly or indirectly in each program's definition file in /etc/pam.d  
  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system-auth settings are being applied.  
  
Procedure:  
Verify the additional pam.d requirements are in use.  
  
The file "/etc/pam.d/system-auth-ac" is auto generated by "authconfig". Any manual changes made to it will be lost next time "authconfig" is run.   
Check to see if the systems default of the symlink "/etc/pam.d/system-auth" pointing to "/etc/pam.d/system-auth-ac" has been changed.  
  
# ls -l /etc/pam.d/system-auth  
  
If the symlink points to "/etc/pam.d/system-auth-ac", manual changes cannot be protected. This is a finding.  
  
# grep system-auth-ac /etc/pam.d/system-auth  
  
The local system-auth file pointed to by "/etc/pam.d/system-auth" must contain "/etc/pam.d/system-auth-ac" for the auth, account, password, and session lines. If it does not then the parameters maintained by "authconfig" will not be applied, this is a finding.  
  
**Fix Text:**In the default distribution of RHEL "/etc/pam.d/system-auth" is a symlink "/etc/pam.d/system-auth-ac" which is an autogenerated file. When a site adds password requirements a new system-auth-local file must be created with only the additional requirements and includes for auth, account, passwd and session pointing to "/etc/pam.d/system-auth-ac". Then the symlink "/etc/system-auth" is modified to point to "/etc/pam.d/system-auth-local". This way any changes made do not get lost when "/etc/pam.d/system-auth-ac" is regenerated and each program's pam.d definition file need only have "include system-auth" for auth, account, passwd and session, as needed, in order to assure the password requirements will be applied to it.  
    
  
**CCI:**CCI-000192  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22305  
**Group Title:** GEN000610  
**Rule ID:** SV-26321r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000610  
**Rule Title:**The system must require passwords contain at least one lowercase 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 /etc/pam.d/system-auth for lcredit setting.  
  
Procedure:  
Check the password lcredit option  
# grep pam\_cracklib.so /etc/pam.d/system-auth  
  
Confirm the lcredit option is set to -1 as in the example:  
  
password required pam\_cracklib.so lcredit=-1  
  
There may be other options on the line. If no such line is found, or the lcredit is not -1 this is a finding.   
  
**Fix Text:** Edit "/etc/pam.d/system-auth" to include the line:  
  
password required pam\_cracklib.so lcredit=-1  
  
prior to the "password include system-auth-ac" line.     
  
**CCI:**CCI-000193  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11972  
**Group Title:** GEN000620  
**Rule ID:** SV-37281r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000620  
**Rule Title:**The system must require passwords 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 dcredit setting.  
  
Procedure:  
Check the password dcredit option  
# grep pam\_cracklib.so /etc/pam.d/system-auth  
  
Confirm the dcredit option is set to -1 as in the example:  
  
password required pam\_cracklib.so dcredit=-1  
  
There may be other options on the line. If no such line is found, or the dcredit option is not -1 this is a finding.   
  
**Fix Text:**Edit "/etc/pam.d/system-auth" to include the line:  
  
password required pam\_cracklib.so dcredit=-1  
  
prior to the "password include system-auth-ac" line.     
  
**CCI:**CCI-000194  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11973  
**Group Title:** GEN000640  
**Rule ID:** SV-37287r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000640  
**Rule Title:**The system must require passwords 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 ocredit setting.  
  
Procedure:  
Check the password ocredit option  
# grep pam\_cracklib.so /etc/pam.d/system-auth  
  
Confirm the ocredit option is set to -1 as in the example:  
  
password required pam\_cracklib.so ocredit=-1  
  
There may be other options on the line. If no such line is found, or the ocredit is not -1 this is a finding.   
  
**Fix Text:**Edit "/etc/pam.d/system-auth" to include the line:  
  
password required pam\_cracklib.so ocredit=-1  
  
prior to the "password include system-auth-ac" line.     
  
**CCI:**CCI-001619  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11975  
**Group Title:** GEN000680  
**Rule ID:** SV-37294r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000680  
**Rule Title:**The system must require passwords 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 maxrepeat setting.  
  
Procedure:  
Check the password maxrepeat configuration  
# grep pam\_cracklib.so /etc/pam.d/system-auth  
  
If the maxrepeat option is missing, this is a finding.  
If the maxrepeat option is set to more than 3, this is a finding.  
  
**Fix Text:** Edit "/etc/pam.d/system-auth" to include the line:  
  
password required pam\_cracklib.so maxrepeat=3  
  
prior to the "password include system-auth-ac" line.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11976  
**Group Title:** GEN000700  
**Rule ID:** SV-37298r1\_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.  
# more /etc/shadow  
If the max days field is equal to 0 or greater than 60 for any user, this is a finding.  
  
**Fix Text:**Set the max days field to 60 for all user accounts.  
# passwd -x 60 <user>     
  
**CCI:**CCI-000180  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11977  
**Group Title:** GEN000740  
**Rule ID:** SV-37302r1\_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 or are locked. If SA indicates passwords for automated processing accounts are not changed once per year or are not locked, this is a finding.  
  
**Fix Text:** Implement or establish procedures to change the passwords of automated processing accounts at least once per year or lock them.     
  
**CCI:**CCI-000199  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22306  
**Group Title:** GEN000750  
**Rule ID:** SV-37304r1\_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 that 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/pam.d/system-auth for a pam\_cracklib parameter difok.   
  
Procedure:  
# grep difok /etc/pam.d/system-auth  
If difok is not present, or has a value less than 4, this is a finding.  
  
Check for system-auth-ac inclusions.  
# grep -c system-auth-ac /etc/pam.d/\*  
  
If the system-auth-ac file is included anywhere  
# more /etc/pam.d/system-auth-ac | grep difok  
  
If system-auth-ac is included anywhere and difok is not present, or has a value less than 4, this is a finding.  
  
Ensure the passwd command uses the system-auth settings.  
# grep system-auth /etc/pam.d/passwd  
If a line "password include system-auth" is not found then the password checks in system-auth will not be applied to new passwords.  
  
**Fix Text:**If /etc/pam.d/system-auth references /etc/pam.d/system-auth-ac refer to the man page for system-auth-ac for a description of how to add options not configurable with authconfig. Edit /etc/pam.d/system-auth and add or edit a pam\_cracklib entry with an difok parameter set equal to or greater than 4.     
  
**CCI:**CCI-000195  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-918  
**Group Title:** GEN000760  
**Rule ID:** SV-37314r1\_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 that have no entries in the "last" log. Check the date in the "last" log to verify it is within the last 35 days or the maximum numbers of days set by the site if more restrictive. If an inactive 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.   
  
The passwd command can also be used to list a status for an account. For example, the following may be used to provide status information on each local account:  
  
# cut -d: -f1 /etc/passwd | xargs -n1 passwd -S  
  
If an inactive account is found not disabled, this is a finding.  
  
**Fix Text:**All inactive accounts will have /sbin/nologin (or an equivalent), as the default shell in the /etc/passwd file and have the password disabled. Examine the user 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 or the maximum number of days set by the site, not to exceed 35 days, then disable the accounts using system-config-users tool. Alternately place a shell field of /sbin/nologin /bin/false or /dev/null in the passwd file entry for the account.     
  
**CCI:**CCI-000017  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22307  
**Group Title:** GEN000790  
**Rule ID:** SV-37318r1\_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 that uses 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/pam.d/system-auth for pam\_cracklib configuration.  
  
Procedure:  
# grep pam\_cracklib /etc/pam.d/system-auth\*  
If pam\_cracklib is not present. This is a finding.  
  
If pam\_cracklib is present only in /etc/pam.d/system-auth-ac:  
ensure that /etc/pam.d/system-auth includes /etc/pam.d/system-auth-ac.  
#grep system-auth-ac /etc/pam.d/system-auth  
  
This should return:  
auth include system-auth-ac  
account include system-auth-ac  
password include system-auth-ac  
session include system-auth-ac  
  
/etc/pam.d/system-auth-ac should only be included by /etc/pam.d/system-auth. All other pam files should include /etc/pam.d/system-auth.   
  
If pam\_cracklib is not defined in /etc/pam.d/system-auth either directly or through inclusion of system-auth-ac, this is a finding.  
  
Ensure the passwd command uses the system-auth settings.  
# grep system-auth /etc/pam.d/passwd  
  
If a line "password include system-auth" is not found then the password checks in system-auth will not be applied to new passwords, this is a finding.  
  
**Fix Text:**If /etc/pam.d/system-auth references /etc/pam.d/system-auth-ac refer to the man page for system-auth-ac for a description of how to add options not configurable with authconfig. Edit /etc/pam.d/system-auth and configure pam\_cracklib by adding a line such as "password required pam\_cracklib.so"     
  
**CCI:**CCI-000189  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4084  
**Group Title:** GEN000800  
**Rule ID:** SV-37323r1\_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:**    
# ls /etc/security/opasswd  
If /etc/security/opasswd does not exist, then this is a finding.  
  
# grep password /etc/pam.d/system-auth| grep pam\_unix.so | grep remember  
If the "remember" option in /etc/pam.d/system-auth is not 5 or greater, this is a finding.  
  
Check for system-auth-ac inclusions.  
# grep -c system-auth-ac /etc/pam.d/\*  
  
If the system-auth-ac file is included anywhere  
# more /etc/pam.d/system-auth-ac | grep password | grep pam\_unix.so | grep remember  
  
If in /etc/pam.d/system-auth-ac is referenced by another file and the "remember" option is not set to 5 or greater this is a finding.  
  
**Fix Text:**Create the password history file.  
# touch /etc/security/opasswd  
# chown root:root /etc/security/opasswd  
# chmod 0600 /etc/security/opasswd  
  
Enable password history.  
If /etc/pam.d/system-auth references /etc/pam.d/system-auth-ac refer to the man page for system-auth-ac for a description of how to add options not configurable with authconfig. Edit /etc/pam.d/system-auth to include the remember option on the "password pam\_unix" lines set to at least 5.     
  
**CCI:**CCI-000200  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22308  
**Group Title:** GEN000850  
**Rule ID:** SV-37345r1\_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:**    
Check /etc/pam.d/su uses pam\_wheel.  
# grep pam\_wheel /etc/pam.d/su  
If pam\_wheel is not present, or is commented out, this is a finding.  
  
**Fix Text:**Edit /etc/pam.d/su and uncomment or add a line such as "auth required pam\_wheel.so". If necessary, create a "wheel" group and add administrative users to the group.     
  
**CCI:**CCI-000009  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-773  
**Group Title:** GEN000880  
**Rule ID:** SV-37347r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000880  
**Rule Title:**The root account must be the only account having a UID of 0.  
  
  
**Vulnerability Discussion:**  If an account has a UID of 0, it has root authority. Multiple accounts with a 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:  
# cat /etc/passwd | awk -F":" '{print$1":"$3":"}' | grep ":0:"  
  
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-37349r1\_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 root places in its default directory. It also gives root the same discretionary access control for root's home directory as for the other 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 /roothome).  
  
Procedure:  
# mkdir /rootdir  
# chown root /rootdir  
# chgrp root /rootdir  
# chmod 700 /rootdir  
# cp -r /.??\* /rootdir/.  
  
Then, 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. Ensure you are in the "/" directory when executing the "cp" command.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-775  
**Group Title:** GEN000920  
**Rule ID:** SV-37355r1\_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 check will be marked "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-37358r1\_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 unix permissions of the files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the root account's home directory has no extended ACL.  
  
# grep "^root" /etc/passwd | awk -F":" '{print $6}'  
  
# ls -ld <root home directory>  
  
If the permissions include a '+' the directory has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the root account's home directory.  
# setfacl --remove-all <root home directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-776  
**Group Title:** GEN000940  
**Rule ID:** SV-37360r1\_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:  
# 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 ~/.profile,~/.bashrc (assuming root shell is bash). 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-37363r1\_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:**    
Check 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-37364r1\_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:**    
Check 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-37372r1\_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:  
# ls -ld `echo $PATH | sed "s/:/ /g"`  
  
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, do 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-37374r1\_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 /etc/securetty  
# more /etc/securetty  
If the file does not exist, or contains more than "console" or a single "tty" device this is a finding.  
  
**Fix Text:**Create if needed and set the contents of /etc/securetty to a "console" or "tty" device.  
# echo console > /etc/securetty  
or  
# echo tty1 > /etc/securetty     
  
**CCI:**CCI-000770  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4298  
**Group Title:** GEN001000  
**Rule ID:** SV-37376r1\_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:**    
Check /etc/securetty  
# more /etc/securetty  
If the file does not exist, or contains more than "console" or a single "tty" device this is a finding.  
  
**Fix Text:**Create if needed and set the contents of /etc/securetty to a "console" or "tty" device.  
# echo console > /etc/securetty  
or   
# echo tty1 > /etc/securetty     
  
**CCI:**CCI-000070  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11979  
**Group Title:** GEN001020  
**Rule ID:** SV-37377r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001020  
**Rule Title:**The root account must not be used for direct log in.  
  
  
**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 root is used for direct logins.  
  
Procedure:  
# last root | grep -v reboot  
  
If any direct login records for root are listed, this is a finding.  
  
**Fix Text:**Enforce policy requiring all root account access is attained by first logging into a user account and then becoming root preferably through the use of "sudo" which provides traceability to the command level. If that is not workable then using "su" to access the root account will provide traceability to the login user.     
  
**CCI:**CCI-000770  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11980  
**Group Title:** GEN001060  
**Rule ID:** SV-37378r1\_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 log files to determine if access to the root account is being logged.  
  
Procedure:  
Examine /etc/syslog.conf to confirm the location to which "authpriv" messages will be directed. The default syslog.conf uses /var/log/messages and /var/log/secure but this needs to be confirmed.  
  
# grep @ /etc/syslog.conf  
If a line starting with "\*.\*" is returned then all syslog messages will be sent to system whose address appears after the "@". In this case syslog may or may not be configured to also log "authpriv" messages locally.  
  
# grep authpriv /etc/syslog.conf  
If any lines are returned which do not start with "#" the "authpriv" messages will be sent to the indicated files or remote systems.  
  
Try to "su -" and enter an incorrect password.  
  
If there are no records indicating the authentication failure, this is a finding.  
  
**Fix Text:**Troubleshoot the system logging configuration to provide for logging of root account login attempts.  
Procedure:  
Edit /etc/syslog.conf to make sure "authpriv.\*" messages are directed to a file or remote system.  
Examine /etc/audit/audit.rules to ensure user authentication messages have not been specifically excluded.  
There remove any entries that correspond to:  
-a exclude,never -Fmsgtype=USER\_START  
-a exclude,never -Fmsgtype=USER\_LOGIN  
-a exclude,never -Fmsgtype=USER\_AUTH  
-a exclude,never -Fmsgtype=USER\_END  
-a exclude,never -Fmsgtype=USER\_ACCT     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1062  
**Group Title:** GEN001080  
**Rule ID:** SV-37380r1\_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:**    
Determine if root's shell executable resides on a dedicated file system.  
  
Procedure:  
Find the location of the root user's shell  
  
# grep "^root" /etc/passwd|cut -d: -f7|cut -d/ -f2  
  
The result is the top level directory under / where the shell resides (e.g., usr)  
Check if it is on a dedicated file system.  
  
# grep /<top level directory> /etc/fstab  
  
If /<top level directory> is on a dedicated file system, this is a finding.  
  
**Fix Text:**Change the root account's shell to one present on the / file system.   
  
Procedure:  
Edit /etc/passwd and change the shell for the root account to one present on the / file system (such as /bin/sh, assuming /bin is not on a separate file system). If the system does not store shell configuration in the /etc/passwd file, consult vendor documentation for the correct procedure for the system.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1046  
**Group Title:** GEN001100  
**Rule ID:** SV-37150r1\_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-37156r1\_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 sshd\_config file and set the PermitRootLogin option to "no".     
  
**CCI:**CCI-000770  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-784  
**Group Title:** GEN001140  
**Rule ID:** SV-37159r1\_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/lbin /usr/usb /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-37161r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001160  
**Rule Title:**All files and directories must have a valid owner.  
  
  
**Vulnerability Discussion:**  Un-owned files and directories may be unintentionally inherited if a user is assigned the same UID as the UID of the un-owned files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the system for files with no assigned owner.  
  
Procedure:  
# find / -nouser   
  
If any files have no assigned owner, this is a finding.  
  
Caution should be used when centralized authorization is used because valid files may appear as unowned due to communication issues.  
  
  
  
  
**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-37165r1\_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   
If any files are found, this is a finding.  
  
  
  
**Fix Text:**Change the group-owner for each file without a valid group-owner.  
# chgrp avalidgroup /tmp/a-file-without-a-valid-group-owner     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-786  
**Group Title:** GEN001180  
**Rule ID:** SV-37194r1\_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.  
# find /usr/sbin -type f -perm +022 -exec stat -c %a:%n {} \;  
  
This will return the octal permissions and name of all files that are group or world writable.  
If any network services daemon listed is world or group writable (either or both of the 2 lowest order digits contain a 2, 3 or 6), 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.  
  
  
  
**Fix Text:**Change the mode of the network services daemon.  
# chmod go-w <path>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22313  
**Group Title:** GEN001190  
**Rule ID:** SV-37199r1\_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:**    
Check network services daemon files have no extended ACLs.  
  
# ls -la /usr/sbin  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
Note: Network daemons not residing in these directories must also be checked.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /usr/sbin/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-794  
**Group Title:** GEN001200  
**Rule ID:** SV-37205r1\_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 world-writable.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/usb, /sbin, and /usr/sbin.   
  
Procedure:  
# DIRS="/etc /bin /usr/bin /usr/lbin /usr/usb /sbin /usr/sbin";for DIR in $DIRS;do find $DIR -type f -perm +022 -exec stat -c %a:%n {} \;;done  
  
This will return the octal permissions and name of all group or world writable files. If any file listed is world or group writable (either or both of the 2 lowest order digits contain a 2, 3 or 6), 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 taking into account necessary GIUD and SUID bits.  
  
Procedure:  
# chmod go-w <filename>     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22314  
**Group Title:** GEN001210  
**Rule ID:** SV-37210r1\_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:**    
Check all system command files have no extended ACLs.  
# ls -lL /etc /bin /usr/bin /usr/lbin /usr/usb /sbin /usr/sbin  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all [file with extended ACL]     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-795  
**Group Title:** GEN001220  
**Rule ID:** SV-37216r1\_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/usb /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-37220r1\_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/usb /sbin /usr/sbin  
  
If any system file, program, or directory is not 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-37228r1\_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 files.  
  
Procedure:  
# ls -lL /var/log /var/log/syslog /var/adm  
  
With the exception of /var/log/wtmp, if any of the log files 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.     
  
**CCI:**CCI-001314  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22315  
**Group Title:** GEN001270  
**Rule ID:** SV-37233r1\_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 system log files have no extended ACLs.  
  
Procedure:  
# ls -lL /var/log  
  
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 providing access beyond the needs of authorized software, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
  
Procedure:  
# setfacl --remove-all [file with extended ACL]     
  
**CCI:**CCI-001314  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-792  
**Group Title:** GEN001280  
**Rule ID:** SV-37234r1\_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 to compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the mode of the manual page files.  
  
Procedure:  
# ls -lL /usr/share/man /usr/share/info /usr/share/infopage  
  
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/to/manpage     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22316  
**Group Title:** GEN001290  
**Rule ID:** SV-37238r1\_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 to compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify all manual page files have no extended ACLs.  
# ls -lL /usr/share/man /usr/share/info /usr/share/infopage  
If the permissions include a '+', the file has an extended ACL this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /usr/share/man/\* /usr/share/info/\* /usr/share/infopage/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-793  
**Group Title:** GEN001300  
**Rule ID:** SV-37241r1\_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:  
# DIRS="/usr/lib /lib";for DIR in $DIRS;do find $DIR -type f -perm +022 -exec stat -c %a:%n {} \;;done  
  
This will return the octal permissions and name of all group or world writable files.  
If any file listed is world or group writable (either or both of the 2 lowest order digits contain a 2, 3 or 6), this is a finding.  
  
  
  
**Fix Text:**Change the mode of library files to 0755 or less permissive.  
  
Procedure (example):  
# chmod go-w </path/to/library-file>  
  
Note: Library files should have an extension of ".a" or a ".so" extension, possibly followed by a version number.     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22317  
**Group Title:** GEN001310  
**Rule ID:** SV-37250r1\_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/\* | grep "+ "  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and has not been approved by the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /usr/lib/\* /lib/\*     
  
**CCI:**CCI-001499  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-789  
**Group Title:** GEN001320  
**Rule ID:** SV-37267r1\_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 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 -la /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, sys or bin.   
  
Procedure (example):  
# chown root <filename>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-790  
**Group Title:** GEN001340  
**Rule ID:** SV-41577r1\_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 -la /var/yp/\*  
  
If the file group ownership is not root, sys, or bin, this is a finding.  
  
  
**Fix Text:**Perform the following to change NIS file ownership.  
  
# chown root /var/yp/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-791  
**Group Title:** GEN001360  
**Rule ID:** SV-37272r1\_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 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 permissions.  
  
# ls -la /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 (example):  
# chmod 0755 <filename>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22318  
**Group Title:** GEN001361  
**Rule ID:** SV-37277r1\_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 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 -lL /var/yp/\*  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /var/yp/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22319  
**Group Title:** GEN001362  
**Rule ID:** SV-37280r1\_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.  
# 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-37286r1\_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-37291r1\_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.  
# ls -l /etc/resolv.conf  
If the file mode is not 0644, this is a finding.  
  
  
**Fix Text:**Change the mode of the /etc/resolv.conf file to 0644.  
# chmod 0644 /etc/resolv.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22322  
**Group Title:** GEN001365  
**Rule ID:** SV-37307r1\_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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/resolv.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22323  
**Group Title:** GEN001366  
**Rule ID:** SV-37309r1\_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.  
# 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-37315r1\_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-37321r1\_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.  
# ls -l /etc/hosts  
If the file mode is not 0644, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the /etc/hosts file to 0644.  
# chmod 0644 /etc/hosts     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22326  
**Group Title:** GEN001369  
**Rule ID:** SV-37324r1\_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 -l /etc/hosts  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/hosts     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22327  
**Group Title:** GEN001371  
**Rule ID:** SV-37326r1\_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.  
# 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-37330r1\_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-37332r1\_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.  
# ls -l /etc/nsswitch.conf  
If the file mode is not 0644, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the /etc/nsswitch.conf file to 0644 or less permissive.  
# chmod 0644 /etc/nsswitch.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22330  
**Group Title:** GEN001374  
**Rule ID:** SV-37334r1\_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.  
# ls -l /etc/nsswitch.conf  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/nsswitch.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22332  
**Group Title:** GEN001378  
**Rule ID:** SV-37336r1\_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.  
# 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-37337r1\_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-37344r1\_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 passwd file is writable by a group-owner or the world, the risk of passwd file compromise is increased. The passwd 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     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22334  
**Group Title:** GEN001390  
**Rule ID:** SV-37346r1\_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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/passwd     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22335  
**Group Title:** GEN001391  
**Rule ID:** SV-37351r1\_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.  
# 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-37352r1\_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-37354r1\_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.  
# 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-37357r1\_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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/group     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-797  
**Group Title:** GEN001400  
**Rule ID:** SV-37361r1\_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 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 /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 (or equivalent) file.  
# chown root /etc/shadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22339  
**Group Title:** GEN001410  
**Rule ID:** SV-37365r1\_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-37368r1\_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 0400 /etc/shadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22340  
**Group Title:** GEN001430  
**Rule ID:** SV-37371r1\_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 -l /etc/shadow  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/shadow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-899  
**Group Title:** GEN001440  
**Rule ID:** SV-37375r1\_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-37379r1\_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 without a 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.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22347  
**Group Title:** GEN001470  
**Rule ID:** SV-37381r1\_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-37383r1\_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.  
# cut -d : -f 2 /etc/group | egrep -v '^(x|!)$'  
If any password hashes are returned, this is a 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-37154r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001480  
**Rule Title:**All user home directories must have mode 0750 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on home directories allow unauthorized access to user files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the home directory mode of each user in /etc/passwd.  
  
Procedure:  
# cut -d: -f6 /etc/passwd|sort|uniq|xargs -n1 ls -ld  
  
If a user 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 user home directories to 0750 or less permissive.  
  
Procedure (example):  
# chmod 0750 <home directory>  
  
Note: Application directories are allowed and may need 0755 permissions (or greater) for correct operation.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22350  
**Group Title:** GEN001490  
**Rule ID:** SV-37162r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001490  
**Rule Title:**User home directories must not have extended ACLs.  
  
  
**Vulnerability Discussion:**  Excessive permissions on home directories allow unauthorized access to user files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify user 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.  
# setfacl --remove-all [user home directory with extended ACL]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-902  
**Group Title:** GEN001500  
**Rule ID:** SV-37163r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001500  
**Rule Title:**All interactive user 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 home directory listed in the /etc/passwd file.  
  
Procedure:  
# cut -d : -f 6 /etc/passwd | xargs -n1 ls -ld   
  
If any user 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-37168r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001520  
**Rule Title:**All interactive user home directories must be group-owned by the home directory owner's primary group.  
  
  
**Vulnerability Discussion:**  If the Group Identifier (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   
  
If any user 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 home directories to the primary group of the assigned user.  
  
Procedure:  
Find the primary group of the user (GID) which is the fourth field of the user entry in /etc/passwd.  
  
# chgrp <GID> <user home directory>  
  
Document all changes.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-914  
**Group Title:** GEN001540  
**Rule ID:** SV-37175r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001540  
**Rule Title:**All files and directories contained in interactive user 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:**  System Administrator  
**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.  
  
Procedure:  
# find /<usershomedirectory> ! -fstype nfs ! -user <username> ! \( -name .bashrc -o -name .bash\_login -o -name .bash\_logout -o -name .bash\_profile -o -name .cshrc -o -name .kshrc -o -name .login -o -name .logout -o -name .profile -o -name .tcshrc -o -name .env -o -name .dtprofile -o -name .dispatch -o -name .emacs -o -name .exrc \) -exec ls -ld {} \;  
  
If user home directories contain files or directories not owned by the home directory owner, this is a finding.  
  
  
  
**Fix Text:**Change the ownership of files and directories in user home directories to the owner of the home directory.   
  
Procedure:  
# chown accountowner filename     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22351  
**Group Title:** GEN001550  
**Rule ID:** SV-37180r1\_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 ~username -printf %G\\n | sort | uniq  
3. Obtain the list of GIDs where the user is a member.  
# id -G username  
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 of which the home directory's owner is a member.  
# chgrp <group with user as member> <file with bad group ownership>  
Document all changes.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-915  
**Group Title:** GEN001560  
**Rule ID:** SV-37183r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001560  
**Rule Title:**All files and directories contained in user home directories must have mode 0750 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions allow unauthorized access to user files.  
  
  
**Documentable:** YES   
**Responsibility:**  Information Assurance Officer  
**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 ! \( -name .bashrc -o -name .bash\_login -o -name .bash\_logout -o -name .bash\_profile -o -name .cshrc -o -name .kshrc -o -name .login -o -name .logout -o -name .profile -o -name .tcshrc -o -name .env -o -name .dtprofile -o -name .dispatch -o -name .emacs -o -name .exrc \) \( -perm -0001 -o -perm -0002 -o -perm -0004 -o -perm -0020 -o -perm -2000 -o -perm -4000 \) -exec ls -ld {} \;  
  
If user 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 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-37188r1\_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 user home directories for files with extended ACLs.  
# cut -d : -f 6 /etc/passwd | xargs -n1 -IDIR ls -alLR DIR  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all <user file with extended ACL>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-906  
**Group Title:** GEN001580  
**Rule ID:** SV-37192r1\_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.  
# cd /etc  
# ls -lL rc\*  
# cd /etc/init.d  
# ls -l  
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 research why they are world-writable.  
  
Procedure:   
# chmod 755 <startup file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22353  
**Group Title:** GEN001590  
**Rule ID:** SV-37196r1\_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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all <run control script with extended ACL>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-907  
**Group Title:** GEN001600  
**Rule ID:** SV-37202r1\_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' library search paths.  
# grep -r PATH /etc/rc\* /etc/init.d  
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, 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-37211r1\_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.  
# grep -r LD\_LIBRARY\_PATH /etc/rc\* /etc/init.d  
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, 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-37215r1\_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.  
# grep -r LD\_PRELOAD /etc/rc\* /etc/init.d  
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, 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-38154r1\_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-37264r1\_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  
  
Alternatively:  
# find /etc -name "[SK][0-9]\*"|xargs stat -L -c %U:%n  
  
If any run control script is not owned by root or bin, this is a finding.  
  
**Fix Text:**Change the ownership of the run control script(s) with incorrect ownership.  
# find /etc -name "[SK][0-9]\*"|xargs stat -L -c %U:%n|egrep -v "^root:"|cut -d: -f2|xargs chown root     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4090  
**Group Title:** GEN001680  
**Rule ID:** SV-37269r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001680  
**Rule Title:**All system start-up files must be group-owned by root, sys, bin, other, or system.  
  
  
**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  
  
Alternatively:  
# find /etc -name "[SK][0-9]\*"|xargs stat -L -c %G:%n|egrep -v "^(root|sys|bin|other):"  
If any run control script is not group-owned by root, sys, bin, or other system groups, 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>  
# find /etc -name "[SK][0-9]\*"|xargs stat -L -c %G:%n|egrep -v "^(root|sys|bin|other):"|cut -d: -f2|xargs chgrp root     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4091  
**Group Title:** GEN001700  
**Rule ID:** SV-37270r1\_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 indicating 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  
# ls -l <executed program>  
  
Alternatively:  
# for FILE in `egrep -r "/" /etc/rc.\* /etc/init.d|awk '/^.\*[^\/][0-9A-Za-z\_\/]\*/{print $2}'|egrep "^/"|sort|uniq`;do if [ -e $FILE ]; then stat -L -c '%U:%n' $FILE;fi;done  
  
This provides a list of files referenced by initialization scripts and their associated UIDs.  
If any file is run by an initialization file and 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, sys, or other.  
# chown root <executed file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11981  
**Group Title:** GEN001720  
**Rule ID:** SV-37275r1\_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/bashrc  
# ls -l /etc/csh.cshrc  
# ls -l /etc/csh.login  
# ls -l /etc/csh.logout  
# ls -l /etc/environment  
# ls -l /etc/ksh.kshrc  
# ls -l /etc/profile  
# ls -l /etc/suid\_profile  
# ls -l /etc/profile.d/\*  
  
  
If global initialization files 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-37279r1\_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 -l /etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\* 2>null|grep "\+ "  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
  
# ls -l etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\* 2>null|grep "\+ "|sed "s/^.\* \///g"|xargs setfacl --remove-all     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11982  
**Group Title:** GEN001740  
**Rule ID:** SV-37283r1\_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.  
  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of global initialization files.  
  
Procedure:  
# ls -lL etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\*  
This should show information for each file. Examine to ensure the owner is always root  
  
or:  
# ls etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\* 2>null|xargs stat -L -c %U:%n|egrep -v "^root"  
  
This will show you only the owner and filename of files not owned by root.  
  
If any global initialization file is not owned by root, this is a finding.  
  
**Fix Text:**Change the ownership of global initialization files with incorrect ownership.  
  
Procedure:  
# chown root <global initialization files>  
  
or:  
# ls etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\* 2>null|xargs stat -L -c %U:%n|egrep -v "^root"|cut -d: -f2|xargs chown root  
will set the owner of all files not currently owned by root to root.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11983  
**Group Title:** GEN001760  
**Rule ID:** SV-37285r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001760  
**Rule Title:**All global initialization files must be group-owned by root, sys, bin, other, system, or the system default.  
  
  
**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/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\*   
  
This should show information for each file. Examine to ensure the group is always root  
  
or:  
# ls -lL etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\* 2>null|sed "s/^[^\/]\*//"|xargs stat -L -c %G:%n|egrep -v "^(root|sys|bin|other):"  
will show you only the group and filename of files not owned by one of the approved groups.  
  
If any global initialization file is not group-owned by root, sys, bin, other, system, or the system default, 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>  
or:  
# ls -lL /etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\* 2>null|sed "s/^[^\/]\*//"|xargs stat -L -c %G:%n|egrep -v "^(root|sys|bin|other):"|cut -d: -f2|xargs chgrp root  
will set the group of all files not currently owned by an approved group to root.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-825  
**Group Title:** GEN001780  
**Rule ID:** SV-37289r1\_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/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\*   
  
If no 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-37292r1\_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-37297r1\_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 startup parameters and possibly jeopardize user 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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all [skeleton file with extended ACL]  
or:  
# ls -lL /etc/skel|grep "\+ "|sed "s/^.\* \//|xargs setfacl --remove-all  
will remove all ACLs from the files.  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11984  
**Group Title:** GEN001820  
**Rule ID:** SV-37300r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001820  
**Rule Title:**All skeleton files and directories (typically in /etc/skel) must be owned by root or 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 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 skeleton files ownership.  
# ls -alL /etc/skel  
If a skeleton file is not owned by root or bin, this is a finding.  
  
**Fix Text:**Change the ownership of skeleton files with incorrect mode:  
# chown root <skeleton file>  
or  
# ls -L /etc/skel|xargs stat -L -c %U:%n|egrep -v "^(root|bin):"|cut -d: -f2|chown root   
will change all files not owned by root or bin to root.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22358  
**Group Title:** GEN001830  
**Rule ID:** SV-37237r1\_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, sys, system, or other.  
  
  
**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, bin, sys, system, or other this is a finding.  
  
**Fix Text:**Change the group-owner of the skeleton file to root, bin, sys, system, or other.  
  
Procedure:  
# chgrp <group> /etc/skel/[skeleton file]  
or:  
# ls -L /etc/skel|xargs stat -L -c %G:%n|egrep -v "^(root|bin|sy|sytem|other):"|cut -d: -f2|chgrp root  
will change the group of all files not already one of the approved group to root.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11985  
**Group Title:** GEN001840  
**Rule ID:** SV-37420r1\_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 PATH /etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\*  
  
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, 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-37246r1\_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.  
  
Procedure:  
# grep LD\_LIBRARY\_PATH /etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\*  
  
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, 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-37248r1\_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.  
# grep -r LD\_PRELOAD /etc/bashrc /etc/csh.cshrc /etc/csh.login /etc/csh.logout /etc/environment /etc/ksh.kshrc /etc/profile /etc/suid\_profile /etc/profile.d/\*  
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, this is a finding.  
  
**Fix Text:**Edit the global initialization file and remove the relative path entry from the library preload variable.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-904  
**Group Title:** GEN001860  
**Rule ID:** SV-37430r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001860  
**Rule Title:**All local initialization files must be owned by the home directory's 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:  
# 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 ! -user <username> -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 filenames 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-37252r1\_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.  
  
Procedure:  
# FILES=" .login .cshrc .logout .profile .bash\_profile .bashrc .bash\_logout .env .dtprofile .dispatch .emacs .exrc";  
# for PWLINE in `cut -d: -f4,6 /etc/passwd`; do HOMEDIR=$(echo ${PWLINE}|cut -d: -f2);GROUP=$(echo ${PWLINE} | cut -d: -f1);for INIFILE in $FILES;do stat -c %g/%G:%n ${HOMEDIR}/${INIFILE} 2>null|egrep -v "${GROUP}";done;done  
  
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's local initialization file>  
  
Procedure:  
# FILES=".bashrc .bash\_login .bash\_logout .bash\_profile .cshrc .kshrc .login .logout .profile .tcshrc .env .dtprofile .dispatch .emacs .exrc";  
# for PWLINE in `cut -d: -f4,6 /etc/passwd`; do HOMEDIR=$(echo ${PWLINE}|cut -d: -f2);GROUP=$(echo ${PWLINE} | cut -d: -f1);for INIFILE in $FILES;do MATCH=$(stat -c %g/%G:%n ${HOMEDIR}/${INIFILE} 2>null|egrep -c -v "${GROUP}");if [ $MATCH != 0 ] ; then chgrp ${GROUP} ${HOMEDIR}/${INIFILE};fi;done;done     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-905  
**Group Title:** GEN001880  
**Rule ID:** SV-37431r1\_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>/.bashrc  
# ls -al /<usershomedirectory>/.bash\_login  
# ls -al /<usershomedirectory>/.bash\_logout  
# ls -al /<usershomedirectory>/.bash\_profile  
# ls -al /<usershomedirectory>/.cshrc  
# ls -al /<usershomedirectory>/.kshrc  
# ls -al /<usershomedirectory>/.login  
# ls -al /<usershomedirectory>/.logout  
# ls -al /<usershomedirectory>/.profile  
# ls -al /<usershomedirectory>/.tcshrc  
# 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 or the .dt directory is more permissive than 0755 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-37271r1\_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/.bashrc DIR/.bash\_login DIR/.bash\_logout DIR/.bash\_profile DIR/.cshrc DIR/.kshrc DIR/.login DIR/.logout DIR/.profile DIR/.env DIR/.dtprofile DIR/.dispatch DIR/.emacs DIR/.exrc  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all <local initialization file with extended ACL>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11986  
**Group Title:** GEN001900  
**Rule ID:** SV-37432r1\_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:**    
Verify local initialization files have executable search path containing only absolute paths or relative paths are necessary and documented.  
  
Procedure:  
# cut -d: -f6 /etc/passwd |xargs -n1 -IDIR find DIR -name ".\*" -type f -maxdepth 1 -exec grep -l 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, ask the SA or IAO if the relative path is required for the operation of a specific application. If it is not, this is a finding.  
  
**Fix Text:**Edit the local initialization file and remove the relative path entry from the executable search path variable. If this is not feasible, justify and document the necessity of having the relative path for a specific application.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22363  
**Group Title:** GEN001901  
**Rule ID:** SV-37305r1\_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.  
Procedure:  
# cut -d: -f6 /etc/passwd |xargs -n1 -IDIR find DIR -name ".\*" -type f -maxdepth 1 -exec grep -H 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, 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-37312r1\_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.  
  
Procedure:  
# cut -d: -f6 /etc/passwd |xargs -n1 -IDIR find DIR -name ".\*" -type f -maxdepth 1 -exec grep -H 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, 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-37433r1\_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 that destroy user files or otherwise compromise 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 and scripts executing from world writable directories.  
  
Procedure:  
For each home directory on the system make a list of files referenced within any local initialization script.  
Show the mode for each file and its parent directory.  
  
# FILES=".bashrc .bash\_login .bash\_logout .bash\_profile .cshrc .kshrc .login .logout .profile .tcshrc .env .dtprofile .dispatch .emacs .exrc";  
  
# for HOMEDIR in `cut -d: -f6 /etc/passwd|sort|uniq`;do for INIFILE in $FILES;do REFLIST=`egrep " [\"~]?/" ${HOMEDIR}/${INIFILE} 2>null|sed "s/.\*\([~ \"]\/[\.0-9A-Za-z\_\/\-]\*\).\*/\1/"`;for REFFILE in $REFLIST;do FULLREF=`echo $REFFILE|sed "s:\~:${HOMEDIR}:g"|sed "s:^\s\*::g"`;dirname $FULLREF|xargs stat -c "dir:%a:%n";stat -c "file:%a:%n" $FULLREF;done;done;done|sort|uniq  
  
This command outputs a list of files and directories and their associated access modes.  
  
If any local initialization file executes a world-writable program or script or a script from a world-writable directory, 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-37435r1\_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  
# grep + /<directorylocation>/.rhosts  
  
# find / -name .shosts  
# grep + /<directorylocation>/.shosts  
  
# find / -name hosts.equiv  
# grep + /<directorylocation>/hosts.equiv  
  
# find / -name shosts.equiv  
# grep + /<directorylocation>/shosts.equiv  
  
# 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-37436r1\_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:  
# find / -name .netrc  
# rm <.netrc file>     
  
**CCI:**CCI-000196  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4427  
**Group Title:** GEN002020  
**Rule ID:** SV-37437r1\_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 r-commands access control files.  
  
Procedure:  
# find / -name .rhosts  
# more /<directorylocation>/.rhosts  
  
# find / -name .shosts  
# more /<directorylocation>/.shosts  
  
# find / -name hosts.equiv  
# more /<directorylocation>/hosts.equiv  
  
# find / -name shosts.equiv  
# more /<directorylocation>/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-37370r1\_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.  
  
# find / -name .rhosts  
# find / -name .shosts  
# find / -name hosts.equiv  
# find / -name shosts.equiv  
  
If .rhosts, .shosts, hosts.equiv, or shosts.equiv are found and their use has not been documented and approved by the IAO, this is a finding.  
  
**Fix Text:**Remove all the r-commands access control files.  
  
Procedure:  
# find / -name .rhosts -exec rm {} \;  
# find / -name .shosts -exec rm {} \;  
# find / -name hosts.equiv -exec rm {} \;  
# find / -name shosts.equiv -exec rm {} \;     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4428  
**Group Title:** GEN002060  
**Rule ID:** SV-37385r1\_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:**    
  
Procedure:  
# ls -l /etc/hosts.equiv  
  
# ls -l /etc/ssh/shosts.equiv  
  
# find / -name .rhosts  
# ls -al <home directory>/.rhosts  
  
# find / -name .shosts  
# ls -al <home directory>/.shosts  
  
# find / -name .netrc  
# ls -al <home directory>/.netrc  
  
If the .rhosts, .shosts, hosts.equiv, or shosts.equiv files have permissions greater than 600, then this is a finding.  
If the /etc/hosts.equiv, or /etc/ssh/shosts.equiv files are not owned by root, this is a finding.  
  
Any .rhosts, .shosts and .netrc files outside of home directories have no meaning and are not subject to this rule  
If the ~/.rhosts or ~/.shosts are not owned by the owner of the home directory where they are immediately located or by root, this is a finding.  
  
**Fix Text:**Ensure the permission for these files is set to 600 or more restrictive and their owner is root or the same as the owner of the home directory in which they reside.  
  
Procedure:  
# chmod 600 /etc/hosts.equiv  
# chmod 600 /etc/ssh/shosts.equiv  
# chown root /etc/hosts.equiv  
# chown root /etc/ssh/shosts.equiv  
  
# find / -name .rhosts  
# chmod 600 /<home directory>/.rhosts  
# chown <home directory owner> <home directory>/.rhosts  
  
# find / -name .shosts  
# chmod 600 <directory location>/.shosts  
# chown <home directory owner> <home directory>/.shosts  
  
# find / -name .netrc  
# chmod 600 <directory location>/.netrc  
# chown <home directory owner> <home directory>/.netrc     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11989  
**Group Title:** GEN002100  
**Rule ID:** SV-37389r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002100  
**Rule Title:**The .rhosts file must not be supported in PAM.  
  
  
**Vulnerability Discussion:**  .rhosts files are used to specify a list of hosts 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.  
  
Example:  
# grep rhosts\_auth /etc/pam.d/\*  
  
If a rhosts\_auth entry is found, this is a finding.  
  
**Fix Text:**Edit the file(s) in /etc/pam.d referencing the rhosts\_auth module, and remove the references to the rhosts\_auth module.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-916  
**Group Title:** GEN002120  
**Rule ID:** SV-37390r1\_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 unsecure shell.  
  
**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. Consult vendor documentation for an appropriate list of system shells.  
  
Procedure:  
# echo "/bin/bash" >> /etc/shells  
# echo "/bin/csh" >> /etc/shells  
(Repeat as necessary for other shells.)     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-917  
**Group Title:** GEN002140  
**Rule ID:** SV-37393r1\_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 unsecure shell.  
  
**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:  
# for USHELL in `cut -d: -f7 /etc/passwd`; do if [ $(grep -c "${USHELL}" /etc/shells) == 0 ]; then echo "${USHELL} not in /etc/shells"; fi; done  
  
The /usr/bin/false, /bin/false, /dev/null, /sbin/nologin, /bin/sync, /sbin/halt, /sbin/shutdown, (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.  
  
Example:  
# chsh -s /bin/bash testuser     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-921  
**Group Title:** GEN002200  
**Rule ID:** SV-37396r1\_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 -l  
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-37399r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002210  
**Rule Title:**All shell files must be group-owned by root, bin, sys, or system.  
  
  
**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 -l  
  
Otherwise, check any shells found on the system.  
Procedure:  
# find / -name "\*sh" | xargs -n1 ls -l  
  
If a shell is not group-owned by root, bin, sys, or system, this is a finding.  
  
**Fix Text:**Change the group-owner of the shell to root, bin, sys, or system.  
  
Procedure:  
# chgrp root <shell>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-922  
**Group Title:** GEN002220  
**Rule ID:** SV-37403r1\_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 -l  
  
Otherwise, check any shells found on the system.  
# find / -name "\*sh" | xargs -n1 ls -l  
  
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-37405r1\_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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all [shell]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-923  
**Group Title:** GEN002260  
**Rule ID:** SV-37543r1\_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:**  Information Assurance Officer  
**IAControls:**  DCSW-1, ECSC-1  
  
**Check Content:**    
Ask the SA for the automated or manual process used to check for extraneous device files.   
  
Review the process to determine if the system is checked for extraneous device files on a weekly basis. If no weekly automated or manual process is in place, this is a finding. If the process is not identifying extraneous device files, 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. A list of device files can be generated with this command:  
# find / -type b -o -type c > device-file-list     
  
**CCI:**CCI-000318  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-924  
**Group Title:** GEN002280  
**Rule ID:** SV-37553r1\_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 world-writable device files existing anywhere on the system.  
  
Procedure:  
# find / -perm -2 -a \( -type b -o -type c \) > devicelist  
Check the permissions on the directories above subdirectories containing device files. If any of the device files or their parent directories are 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-37558r1\_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 {} \;  
  
Ask the SA to identify any device files used for backup purposes.  
  
If any device file(s) used for backup are writable by users other than root or the designated backup user, 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 <back device filename>  
  
Document all changes.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1048  
**Group Title:** GEN002320  
**Rule ID:** SV-37566r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002320  
**Rule Title:**Audio devices must have mode 0660 or less permissive.  
  
  
**Vulnerability Discussion:**  Audio and video devices that are globally accessible have proven to be another security hazard. 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 into a bugging device.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of audio devices.  
# ls -lL /dev/audio\* /dev/snd/\*  
If the mode of audio devices are more permissive than 660, this is a finding.  
  
**Fix Text:**Change the mode of audio devices.  
# chmod 0660 <audio device>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22367  
**Group Title:** GEN002330  
**Rule ID:** SV-37569r1\_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\* /dev/snd/\*  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all [device file]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1049  
**Group Title:** GEN002340  
**Rule ID:** SV-37575r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002340  
**Rule Title:**Audio devices must be owned by root.  
  
  
**Vulnerability Discussion:**  Audio and video devices globally accessible have proven to be another security hazard. 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 into a bugging device.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the owner of audio devices.  
# ls -lL /dev/audio\* /dev/snd/\*  
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-37577r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002360  
**Rule Title:**Audio devices must be group-owned by root, sys, bin, or system.  
  
  
**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\* /dev/snd/\*  
  
If the group-owner of an audio device is not root, sys, bin, or system, this is a finding.  
  
**Fix Text:**Change the group-owner of the audio device.  
  
Procedure:  
# chgrp root <audio device>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-801  
**Group Title:** GEN002380  
**Rule ID:** SV-37579r1\_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 allowing reading and writing of files, or shell escapes. Only default vendor-supplied executables should have the setuid bit set.  
  
**Documentable:** YES   
**Responsibility:**  Information Assurance Officer  
**IAControls:**  ECPA-1  
  
**Check Content:**    
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. Documentation must include the owner, group-owner, mode, ACL, and location of the files. If any undocumented file has its setuid bit set, this is a finding.  
  
**Fix Text:**Document the files with the suid bit set or unset the suid bit on the executable.     
  
**CCI:**CCI-000368  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-803  
**Group Title:** GEN002400  
**Rule ID:** SV-37592r1\_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 allowing reading and writing of files, or shell escapes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Ask the SA for the weekly automated or manual process 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.  
  
Review the process. If the process does not identify and report changes in setuid files, this is a finding.  
  
**Fix Text:**Establish a weekly automated or manual process to generate a list of suid files on the system and compare it with the prior list. To create a list of suid files:  
# find / -perm -4000 > suid-file-list     
  
**CCI:**CCI-000318  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-805  
**Group Title:** GEN002420  
**Rule ID:** SV-37607r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002420  
**Rule Title:**Removable media, remote file systems, and any file system not containing 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 not containing approved setuid files. Executing setuid files from untrusted file systems, or file systems not containing approved setuid files, increases the opportunity for unprivileged users to attain unauthorized administrative access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/mtab and verify the "nosuid" mount option is used on file systems mounted from removable media, network shares, or any other file system not containing approved setuid or setgid files. If any of these files systems do not mount with the "nosuid" option, it is a finding.  
  
**Fix Text:**Edit /etc/fstab and add the "nosuid" mount option to all file systems mounted from removable media or network shares, and any file system not containing approved setuid or setgid files.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22368  
**Group Title:** GEN002430  
**Rule ID:** SV-37623r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002430  
**Rule Title:**Removable media, remote file systems, and any file system not containing approved device files must be mounted with the "nodev" option.  
  
  
**Vulnerability Discussion:**  The "nodev" (or equivalent) mount option causes the system to not handle device files as system devices. This option must be used for mounting any file system not containing approved device files. Device files can provide direct access to system hardware and can compromise security if not protected.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check /etc/mtab and verify the "nodev" mount option is used on any filesystems mounted from removable media or network shares. If any filesystem mounted from removable media or network shares does not have this option, this is a finding.  
  
**Fix Text:**Edit /etc/fstab and add the "nodev" option to any filesystems mounted from removable media or network shares.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-802  
**Group Title:** GEN002440  
**Rule ID:** SV-37628r1\_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 allowing reading and writing of files, or shell escapes.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
List all setgid files on the system.  
Procedure:  
# find / -perm -2000 -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 setgid bit set have been documented. Documentation must include owner, group-owner, mode, ACL, and location. If any undocumented file has its setgid bit set, this is a finding.  
  
**Fix Text:**Document the files with the sgid bit set or unset the sgid bit on the executable.     
  
**CCI:**CCI-000368  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-804  
**Group Title:** GEN002460  
**Rule ID:** SV-37635r1\_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 allowing reading and writing of files, or shell escapes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Ask the SA 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:  
# find / -perm -2000 > setgid-file-list     
  
**CCI:**CCI-000318  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1010  
**Group Title:** GEN002480  
**Rule ID:** SV-37645r1\_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.  
  
Procedure:  
# find / -perm -2 -a \( -type d -o -type f \) -exec ls -ld {} \;  
  
If any world-writable files 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 on the system not required to be world-writable.  
  
Procedure:  
# chmod o-w <file>  
  
Document all changes     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-806  
**Group Title:** GEN002500  
**Rule ID:** SV-37647r1\_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:**    
Check 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-37888r1\_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-37893r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002540  
**Rule Title:**All public directories must be group-owned by root, sys, bin, or an application group.  
  
  
**Vulnerability Discussion:**  If a public directory has the sticky bit set and is not group-owned by a privileged 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, 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-37898r1\_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 initialization files for the configured umask value.  
Procedure:  
# grep umask /etc/\*   
  
Check local initialization files for the configured umask value.  
Procedure:   
# cut -d: -f6 /etc/passwd |xargs -n1 -IDIR find DIR -name ".\*" -type f -maxdepth 1 -exec grep umask {} \;  
  
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 Severity Code I finding.  
  
  
  
**Fix Text:**Edit local and global initialization files that contain "umask" and change them to use 077 instead of the current value.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-810  
**Group Title:** GEN002640  
**Rule ID:** SV-37903r1\_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) have been disabled.  
  
# cat /etc/shadow  
  
If an account's password field (which is the second field in the /etc/shadow file) is "\*", "\*LK\*", or is prefixed with a '!', the account is locked or disabled.  
  
If there are any unlocked default system accounts 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-27270r1\_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:**Start the auditd service and set it to start on boot.  
# service auditd start ; chkconfig auditd on     
  
**CCI:**CCI-000169  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-812  
**Group Title:** GEN002680  
**Rule ID:** SV-37912r1\_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.  
  
Procedure:  
# grep "^log\_file" /etc/audit/auditd.conf|sed s/^[^\/]\*//|xargs stat -c %U:%n  
  
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-37914r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002690  
**Rule Title:**System audit logs must be group-owned by root, bin, sys, or system.  
  
  
**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:**    
Check the group ownership of the audit logs.  
  
Procedure:  
# grep "^log\_file" /etc/audit/auditd.conf|sed s/^[^\/]\*//|xargs stat -c %G:%n  
  
If any audit log file is not group-owned by root, bin, sys, or system, 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-37916r1\_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.  
Procedure:  
# grep "^log\_file" /etc/audit/auditd.conf|sed s/^[^\/]\*//|xargs stat -c %a:%n  
  
If 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-37917r1\_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 system audit log files for extended ACLs.  
  
Procedure:  
# grep "^log\_file" /etc/audit/auditd.conf|sed s/^[^\/]\*//|xargs ls -l  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the system audit file(s).     
  
**CCI:**CCI-000163  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22370  
**Group Title:** GEN002715  
**Rule ID:** SV-26504r1\_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 /sbin/auditctl /sbin/auditd /sbin/ausearch /sbin/aureport /sbin/autrace /sbin/audispd   
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-26507r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002716  
**Rule Title:**System audit tool executables must be group-owned by root, bin, sys, or system.  
  
  
**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, sys, or system.  
  
Procedure:  
# ls -lL /sbin/auditctl /sbin/auditd /sbin/ausearch /sbin/aureport /sbin/autrace /sbin/audispd   
  
If any listed file is not group-owned by root, bin, sys, or system, this is a finding.  
  
**Fix Text:**Change the group-owner of the audit tool executable to root, bin, sys, or system.  
  
Procedure:  
# chgrp root <audit tool executable>     
  
**CCI:**CCI-001493  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22372  
**Group Title:** GEN002717  
**Rule ID:** SV-26510r1\_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 /sbin/auditctl /sbin/auditd /sbin/ausearch /sbin/aureport /sbin/autrace /sbin/audispd   
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-26513r1\_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 /sbin/auditctl /sbin/auditd /sbin/ausearch /sbin/aureport /sbin/autrace /sbin/audispd   
If the permissions include a '+' the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all [audit file]     
  
**CCI:**CCI-001493  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22374  
**Group Title:** GEN002719  
**Rule ID:** SV-26517r1\_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 e-mail 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 /etc/audit/auditd.conf has the disk\_full\_action and disk\_error\_action parameters set.  
  
Procedure:  
# grep disk\_full\_action /etc/audit/audit.conf  
  
If the disk\_full\_action parameter is missing or set to "suspend" or "ignore" this is a finding.  
  
# grep disk\_error\_action /etc/audit/audit.conf  
  
If the disk\_error\_action parameter is missing or set to "suspend" or "ignore" this is a finding.  
  
  
**Fix Text:**Edit /etc/audit/auditd.conf and set the disk\_full\_action and/or disk\_error\_action parameters to a valid setting of "syslog", "exec", "single" or "halt", adding the parameters if necessary.     
  
**CCI:**CCI-000139  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-814  
**Group Title:** GEN002720  
**Rule ID:** SV-38645r1\_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:**    
Verify auditd is configured to audit failed file access attempts.  
  
There must be an audit rule for each of the access syscalls logging all failed accesses (-F success=0) or there must both an "-F exit=-EPERM" and "-F exit=-EACCES" for each access syscall.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -e "-S creat" | grep -e "-F success=0"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -e "-S creat" | grep -e "-F exit=-EPERM"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -e "-S creat" | grep -e "-F exit=-EACCES"  
  
If an "-S creat" audit rule with "-F success" does not exist and no separate rules containing "-F exit=-EPERM" and "-F exit=-EACCES" for "creat" exist, then this is a finding.  
  
**Fix Text:**Edit the audit.rules file and add the following line(s) to enable auditing of failed attempts to access files and programs:  
  
either:  
-a exit,always -F arch=<ARCH> -S creat -F success=0  
  
or both:  
-a exit,always -F arch=<ARCH> -S creat -F exit=-EPERM  
-a exit,always -F arch=<ARCH> -S creat -F exit=-EACCES  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29236  
**Group Title:** GEN002720-2  
**Rule ID:** SV-37612r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002720-2  
**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 that auditd is configured to audit failed file access attempts.  
There must be an audit rule for each of the access syscalls that logs all failed accesses (-F success=0) or there must both an "-F exit=-EPERM" and "-F exit=-EACCES" for each access syscall.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S open" | grep "-F success=0"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S open" | grep "-F exit=-EPERM"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S open" | grep "-F exit=-EACCES"  
  
If an "-S open" audit rule with "-F success" does not exist and no separate rules containing "-F exit=-EPERM" and "-F exit=-EACCES" for "open" exist, then this is a finding.  
  
**Fix Text:**Edit the audit.rules file and add the following line(s) to enable auditing of failed attempts to access files and programs:  
  
either:  
-a exit,always -F arch=<ARCH> -S open -F success=0  
  
or both:  
-a exit,always -F arch=<ARCH> -S open -F exit=-EPERM  
-a exit,always -F arch=<ARCH> -S open -F exit=-EACCES  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000192  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29237  
**Group Title:** GEN002720-3  
**Rule ID:** SV-37614r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002720-3  
**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:**    
Verify auditd is configured to audit failed file access attempts.  
There must be an audit rule for each of the access syscalls logging all failed accesses (-F success=0) or there must both an "-F exit=-EPERM" and "-F exit=-EACCES" for each access syscall.  
  
Procedure:  
  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S openat" | grep "-F success=0"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S openat" | grep "-F exit=-EPERM"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S openat" | grep "-F exit=-EACCES"  
  
If an "-S openat" audit rule with "-F success" does not exist and no separate rules containing "-F exit=-EPERM" and "-F exit=-EACCES" for "openat" exist, then this is a finding.  
  
**Fix Text:**Edit the audit.rules file and add the following line(s) to enable auditing of failed attempts to access files and programs:  
  
either:  
-a exit,always -F arch=<ARCH> -S openat -F success=0  
  
or both:  
-a exit,always -F arch=<ARCH> -S openat -F exit=-EPERM  
-a exit,always -F arch=<ARCH> -S openat -F exit=-EACCES  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000192  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29238  
**Group Title:** GEN002720-4  
**Rule ID:** SV-37654r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002720-4  
**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:**    
Verify auditd is configured to audit failed file access attempts.  
There must be an audit rule for each of the access syscalls logging all failed accesses (-F success=0) or  
there must both an "-F exit=-EPERM" and "-F exit=-EACCES" for each access syscall.  
  
Procedure:  
  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S truncate" | grep "-F success=0"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S truncate" | grep "-F exit=-EPERM"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S truncate" | grep "-F exit=-EACCES"  
  
If an "-S truncate" audit rule with "-F success" does not exist and no separate rules containing "-F exit=-EPERM" and "-F exit=-EACCES" for "truncate" exist, then this is a finding.  
  
**Fix Text:**Edit the audit.rules file and add the following line(s) to enable auditing of failed attempts to access files and programs:  
  
either:  
-a exit,always -F arch=<ARCH> -S truncate -F success=0  
  
or both:  
-a exit,always -F arch=<ARCH> -S truncate -F exit=-EPERM  
-a exit,always -F arch=<ARCH> -S truncate -F exit=-EACCES  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000192  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29239  
**Group Title:** GEN002720-5  
**Rule ID:** SV-37655r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002720-5  
**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:**    
Verify auditd is configured to audit failed file access attempts.  
There must be an audit rule for each of the access syscalls logging all failed accesses (-F success=0) or  
there must both an "-F exit=-EPERM" and "-F exit=-EACCES" for each access syscall.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S ftruncate" | grep "-F success=0"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S ftruncate" | grep "-F exit=-EPERM"  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep "-S ftruncate" | grep "-F exit=-EACCES"  
  
If an "-S ftruncate" audit rule with "-F success" does not exist and no separate rules containing "-F exit=-EPERM" and "-F exit=-EACCES" for "ftruncate" exist, then this is a finding.  
  
**Fix Text:**Edit the audit.rules file and add the following line(s) to enable auditing of failed attempts to access files and programs:  
  
either:  
-a exit,always -F arch=<ARCH> -S ftruncate -F success=0  
  
or both:  
-a exit,always -F arch=<ARCH> -S ftruncate -F exit=-EPERM  
-a exit,always -F arch=<ARCH> -S ftruncate -F exit=-EACCES  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000192  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22375  
**Group Title:** GEN002730  
**Rule ID:** SV-26518r1\_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 e-mail or paging) should be employed consistent with the site’s established operations management systems and procedures.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check /etc/audit/auditd.conf for the space\_left\_action and action\_mail\_accnt parameters. If the space\_left\_action or the action\_mail\_accnt parameters are set to blanks, this is a finding.  
  
If the space\_left\_action is set to "syslog", the system logs the event, this is not a finding.  
  
If the space\_left\_action is set to "exec", the system executes a designated script. If this script informs the SA of the event, this is not a finding.  
  
If the space\_left\_action parameter is missing, this is a finding.  
If the space\_left\_action parameter is set to "ignore" or "suspend" no logging would be performed after the event, this is a finding.  
If the space\_left\_action parameter is set to "single" or "halt" this effectively stops the system causing a Denial of Service, this is a finding.  
  
If the space\_left\_action is set to "email" and the action\_mail\_acct parameter is not set to the e-mail address of the system administrator, this is a finding. The action\_mail\_acct parameter, if missing, defaults to "root". Note that if the email address of the system administrator is on a remote system "sendmail" must be available.  
  
  
  
**Fix Text:**Edit /etc/audit/auditd.conf and set the space\_left\_action parameter to a valid setting other than "ignore". If the space\_left\_action parameter is set to "email" set the action\_mail\_acct parameter to an e-mail address for the system administrator.     
  
**CCI:**CCI-000143  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-815  
**Group Title:** GEN002740  
**Rule ID:** SV-42185r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002740  
**Rule Title:**The audit system must be configured to audit files and programs deleted by the user.  
  
  
**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 file and directory deletions are audited.  
  
# cat /etc/audit.rules /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "unlink"  
  
If no results are returned, or the results do not contain "-S unlink", this is a finding.  
  
**Fix Text:**Edit the audit.rules file and add the following line to enable auditing of deletions:  
-a exit,always -S unlink  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29240  
**Group Title:** GEN002740-2  
**Rule ID:** SV-37656r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002740-2  
**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:**    
Check the system audit configuration to determine if file and directory deletions are audited.  
  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "rmdir"  
  
If no results are returned, or the results do not contain "-S rmdir", this is a finding.  
  
**Fix Text:**Edit the audit.rules file and add the following line to enable auditing of deletions:  
-a exit,always -S rmdir   
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22376  
**Group Title:** GEN002750  
**Rule ID:** SV-26519r1\_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:**    
Determine if execution of the useradd and groupadd executable are audited.  
# auditctl -l | egrep '(useradd|groupadd)'  
If either useradd or groupadd are not listed with a permissions filter of at least 'x', this is a finding.  
Determine if /etc/passwd, /etc/shadow, /etc/group, and /etc/gshadow are audited for appending.  
# auditctl -l | egrep '(/etc/passwd|/etc/shadow|/etc/group|/etc/gshadow)'  
If any of these are not listed with a permissions filter of at least 'a', this is a finding.  
  
**Fix Text:**Configure execute auditing of the useradd and groupadd executables.  
Add the following to audit.rules:  
-w /usr/sbin/useradd -p x -k useradd  
-w /usr/sbin/groupadd -p x -k groupadd  
Configure append auditing of the passwd, shadow, group, and gshadow files. Add the following to audit.rules:  
-w /etc/passwd -p a -k passwd  
-w /etc/shadow -p a -k shadow  
-w /etc/group -p a -k group  
-w /etc/gshadow -p a -k gshadow  
Restart the auditd service.     
  
**CCI:**CCI-000018  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22377  
**Group Title:** GEN002751  
**Rule ID:** SV-26520r1\_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:**    
Determine if execution of the usermod and groupmod executable are audited.  
# auditctl -l | egrep '(usermod|groupmod)'  
If either useradd or groupadd are not listed with a permissions filter of at least 'w', this is a finding.  
Determine if /etc/passwd, /etc/shadow, /etc/group, and /etc/gshadow are audited for writing.  
# auditctl -l | egrep '(/etc/passwd|/etc/shadow|/etc/group|/etc/gshadow)'  
If any of these are not listed with a permissions filter of at least 'w', this is a finding.  
  
**Fix Text:**Configure execute auditing of the usermod and groupmod executables. Add the following to the audit.rules file:  
-w /usr/sbin/usermod -p x -k usermod  
-w /usr/sbin/groupmod -p x -k groupmod  
Configure append auditing of the passwd, shadow, group, and gshadow files. Add the following to the audit.rules file:  
-w /etc/passwd -p w -k passwd  
-w /etc/shadow -p w -k shadow  
-w /etc/group -p w -k group  
-w /etc/gshadow -p w -k gshadow  
Restart the auditd service.     
  
**CCI:**CCI-001403  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22378  
**Group Title:** GEN002752  
**Rule ID:** SV-26521r1\_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:**    
Determine if execution of the passwd executable is audited.  
# auditctl -l | grep /usr/bin/passwd  
If passwd is not listed with a permissions filter of at least 'x', this is a finding.  
  
**Fix Text:**Configure execute auditing of the passwd executable. Add the following to the audit.rules file:  
-w /usr/bin/passwd -p x -k passwd  
  
Restart the auditd service.     
  
**CCI:**CCI-001404  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22382  
**Group Title:** GEN002753  
**Rule ID:** SV-26522r1\_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:**    
Determine if execution of the userdel and groupdel executable are audited.  
# auditctl -l | egrep '(userdel|groupdel)'  
If either userdel or groupdel are not listed with a permissions filter of at least 'x', this is a finding.  
  
  
  
**Fix Text:**Configure execute auditing of the userdel and groupdel executables. Add the following to the audit.rules file:  
-w /usr/sbin/userdel -p x   
-w /usr/sbin/groupdel -p x  
  
Restart the auditd service.     
  
**CCI:**CCI-001405  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29249  
**Group Title:** GEN002760-10  
**Rule ID:** SV-37665r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760-10  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "sched\_setscheduler"  
  
If the result does not contain "-S sched\_setscheduler", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>"restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>"restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
A Real Time Operating System (RTOS) provides specialized system scheduling which causes an inordinate number of messages to be produced when the sched\_setparam and set\_setscheduler are audited. This not only may degrade the system speed to an unusable level but obscures any forensic information which may otherwise have been useful.  
Unless the operating system is a Red Hat 5 based RTOS (including MRG and AS5300) the following should also be present in /etc/audit/audit.rules  
  
-a exit,always -F arch=<ARCH> -S sched\_setscheduler  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29241  
**Group Title:** GEN002760-2  
**Rule ID:** SV-37657r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760-2  
**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.  
  
Procedure:  
  
# cat /etc/audit/audit.rules | grep -i "audit.rules"  
  
If no results are returned, or the line does not start with "-w", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>"restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>"restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
Add the following lines to the audit.rules file to enable auditing of administrative, privileged, and security actions:  
  
-w /etc/audit.rules  
-w /etc/audit/audit.rules  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29242  
**Group Title:** GEN002760-3  
**Rule ID:** SV-37658r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760-3  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "adjtime"  
  
If the result does not contain "-S adjtime", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>"restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>"restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
Add the following lines to the audit.rules file to enable auditing of administrative, privileged, and security actions:  
  
-a exit,always -F arch=<ARCH> -S adjtime  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29243  
**Group Title:** GEN002760-4  
**Rule ID:** SV-37659r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760-4  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "settimeofday"  
  
If the result does not contain "-S settimeofday", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>"restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>"restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
Add the following lines to the audit.rules file to enable auditing of administrative, privileged, and security actions:  
  
-a exit,always -F arch=<ARCH> -S settimeofday  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29244  
**Group Title:** GEN002760-5  
**Rule ID:** SV-37660r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760-5  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "stime"  
  
If the result does not contain "-S stime", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>"restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>"restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
Add the following lines to the audit.rules file to enable auditing of administrative, privileged, and security actions:  
  
-a exit,always -F arch=<ARCH> -S stime  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29245  
**Group Title:** GEN002760-6  
**Rule ID:** SV-37661r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760-6  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "clock\_settime"  
  
If the result does not contain "-S clock\_settime", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>"restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>"restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
Add the following lines to the audit.rules file to enable auditing of administrative, privileged, and security actions:  
  
-a exit,always -F arch=<ARCH> -S clock\_settime  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29246  
**Group Title:** GEN002760-7  
**Rule ID:** SV-37662r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760-7  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "sethostname"  
  
If the result does not contain "-S sethostname", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>"restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>"restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
Add the following lines to the audit.rules file to enable auditing of administrative, privileged, and security actions:  
  
-a exit,always -F arch=<ARCH> -S sethostname  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29247  
**Group Title:** GEN002760-8  
**Rule ID:** SV-37663r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760-8  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "setdomain"  
  
If the result does not contain "-S setdomain", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>"restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>"restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
Add the following lines to the audit.rules file to enable auditing of administrative, privileged, and security actions:  
  
-a exit,always -F arch=<ARCH> -S setdomainname  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29248  
**Group Title:** GEN002760-9  
**Rule ID:** SV-37664r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760-9  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "sched\_setparam"  
  
If the result does not contain "-S sched\_setparam", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>"restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>"restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
A Real Time Operating System (RTOS) provides specialized system scheduling which causes an inordinate number of messages to be produced when the sched\_setparam and set\_setscheduler are audited. This not only may degrade the system speed to an unusable level but obscures any forensic information which may otherwise have been useful.  
Unless the operating system is a Red Hat 5 based RTOS (including MRG and AS5300) the following should also be present in /etc/audit/audit.rules  
  
-a exit,always -F arch=<ARCH> -S sched\_setparam  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000347  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-818  
**Group Title:** GEN002800  
**Rule ID:** SV-37944r1\_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:**    
The message types that are always recorded to /var/log/audit/audit.log include LOGIN,USER\_LOGIN,USER\_START,USER\_END among others and do not need to be added to audit\_rules.   
  
The log files /var/log/faillog and /var/log/lastlog must be protected from tampering of the login records.  
  
Procedure:  
  
#egrep "faillog|lastlog" /etc/audit/audit.rules|grep "-p (wa|aw)"  
  
If both /var/log/faillog and /var/log/lastlog entries do not exist, this is a finding.  
  
  
  
**Fix Text:**Ensure logins   
  
Procedure:  
Modify /etc/audit/audit.rules to contain:  
  
-w /var/log/faillog -p wa  
-w /var/log/lastlog -p wa  
  
    
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-819  
**Group Title:** GEN002820  
**Rule ID:** SV-27313r1\_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.  
  
Procedure:  
# cat /etc/audit.rules /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i " chmod "  
If "-S chmod" is not in the result, this is a finding  
  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S chmod  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29272  
**Group Title:** GEN002820-10  
**Rule ID:** SV-37716r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-10  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fsetxattr"  
  
If "-S fsetxattr" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S fsetxattr  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29274  
**Group Title:** GEN002820-11  
**Rule ID:** SV-37718r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-11  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "removexattr"  
  
If "-S removexattr" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S removexattr  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29275  
**Group Title:** GEN002820-12  
**Rule ID:** SV-37719r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-12  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "lremovexattr"  
  
If "-S lremovexattr" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S lremovexattr  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29279  
**Group Title:** GEN002820-13  
**Rule ID:** SV-37726r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-13  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fremovexattr"  
  
If "-S fremovexattr" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S fremovexattr  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29250  
**Group Title:** GEN002820-2  
**Rule ID:** SV-37666r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-2  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchmod"  
  
If "-S fchmod" is not in the result, this is a finding  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S fchmod  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29251  
**Group Title:** GEN002820-3  
**Rule ID:** SV-37667r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-3  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchmodat"  
  
If "-S fchmodat" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S fchmodat  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29252  
**Group Title:** GEN002820-4  
**Rule ID:** SV-37668r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-4  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "chown"  
  
If "-S chown" is not in the result, this is a finding.  
  
Additionally, the following rule is required in systems supporting the 32-bit syscall table (such as i686 and x86\_64):  
  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "chown32"  
  
If "-S chown32" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S chown  
  
Additionally, the following rule is required in systems supporting the 32-bit syscall table (such as i686 and x86\_64):  
-a exit,always -F arch=<ARCH> -S chown32  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29253  
**Group Title:** GEN002820-5  
**Rule ID:** SV-37669r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-5  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchown"  
If "-S fchown" is not in the result, this is a finding.  
  
Additionally, the following rule is required in systems supporting the 32-bit syscall table (such as i686 and x86\_64):  
  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchown32"  
  
If "-S fchown32" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S fchown  
  
Additionally, the following rule is required in systems supporting the 32-bit syscall table (such as i686 and x86\_64):  
-a exit,always -F arch=<ARCH> -S fchown32  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29255  
**Group Title:** GEN002820-6  
**Rule ID:** SV-37671r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-6  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchownat"  
  
If "-S fchownat" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S fchownat  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29257  
**Group Title:** GEN002820-7  
**Rule ID:** SV-37673r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-7  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "lchown"  
  
If "-S lchown" is not in the result, this is a finding.  
Additionally, the following rule is required in systems supporting the 32-bit syscall table (such as i686 and x86\_64):  
  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "lchown32"  
  
If "-S lchown32" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S lchown  
  
Additionally, the following rule is required in systems supporting the 32-bit syscall table (such as i686 and x86\_64):  
-a exit,always -F arch=<ARCH> -S lchown32  
  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29259  
**Group Title:** GEN002820-8  
**Rule ID:** SV-37677r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-8  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "setxattr"  
  
If "-S setxattr" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S setxattr  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29261  
**Group Title:** GEN002820-9  
**Rule ID:** SV-37681r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002820-9  
**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.  
  
Procedure:  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "lsetxattr"  
  
If "-S lsetxattr" is not in the result, this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Edit the audit.rules file and add the following lines to enable auditing of discretionary access control permissions modifications.  
-a exit,always -F arch=<ARCH> -S lsetxattr  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22383  
**Group Title:** GEN002825  
**Rule ID:** SV-38652r1\_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:**    
Determine if the init\_module syscall is audited.  
  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "init\_module"  
  
If the result does not contain "-S init\_module", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
Configure auditing of the init\_module syscalls.  
Add the following to the "etc/audit/audit.rules" or "etc/audit.rules" file:  
  
-a exit,always -S init\_module  
  
Restart the auditd service.  
# service auditd restart  
    
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29281  
**Group Title:** GEN002825-2  
**Rule ID:** SV-37728r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002825-2  
**Rule Title:**The audit system must be configured to audit the loading and unloading of dynamic kernel modules - delete\_module.  
  
  
**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, ECAR-2, ECAR-3  
  
**Check Content:**    
Determine if the delete\_module syscall is audited.  
  
# cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "delete\_module"  
  
If the result does not contain "-S delete\_module", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
Configure auditing of the delete\_module syscalls.  
Add the following to the "etc/audit/audit.rules" or "etc/audit.rules" file:  
  
-a exit,always -S delete\_module  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29284  
**Group Title:** GEN002825-3  
**Rule ID:** SV-37734r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002825-3  
**Rule Title:**The audit system must be configured to audit the loading and unloading of dynamic kernel modules - /sbin/insmod.  
  
  
**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, ECAR-2, ECAR-3  
  
**Check Content:**    
Determine if /sbin/insmod is audited.  
  
# cat /etc/audit/audit.rules | grep "/sbin/insmod"  
  
If the result does not start with "-w" and contain "-p x", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
  
Configure auditing of the /sbin/insmod, files.  
Add the following to the "etc/audit/audit.rules" or "etc/audit.rules" file:  
-w /sbin/insmod -p x  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29286  
**Group Title:** GEN002825-4  
**Rule ID:** SV-37738r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002825-4  
**Rule Title:**The audit system must be configured to audit the loading and unloading of dynamic kernel modules -/sbin/modprobe.  
  
  
**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, ECAR-2, ECAR-3  
  
**Check Content:**    
Determine if the /sbin/modprobe file is audited.  
  
# cat /etc/audit/audit.rules | grep "/sbin/modprobe"  
  
If the result does not start with "-w" and contain "-p x", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
Procedure:  
-w /sbin/modprobe -p x  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29288  
**Group Title:** GEN002825-5  
**Rule ID:** SV-37741r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002825-5  
**Rule Title:**The audit system must be configured to audit the loading and unloading of dynamic kernel modules - /sbin/rmmod  
  
  
**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, ECAR-2, ECAR-3  
  
**Check Content:**    
Determine if the /sbin/rmmod file is audited.  
  
# cat /etc/audit/audit.rules | grep "/sbin/rmmod"  
  
If the result does not start with "-w" and contain "-p x", this is a finding.  
  
**Fix Text:**The "-F arch=<ARCH>" restriction is required on dual-architecture systems (such as x86\_64). On dual-architecture systems, two separate rules must exist - one for each architecture supported. Use the generic architectures "b32" and "b64" for specifying these rules.  
On single architecture systems, the "-F arch=<ARCH>" restriction may be omitted, but if present must match either the architecture of the system or its corresponding generic architecture. The architecture of the system may be determined by running "uname -m". See the auditctl(8) manpage for additional details.  
Any restrictions (such as with "-F") beyond those provided in the example rules are not in strict compliance with this requirement, and are a finding unless justified and documented appropriately.  
The use of audit keys consistent with the provided example is encouraged to provide for uniform audit logs, however omitting the audit key or using an alternate audit key is not a finding.  
  
Procedure:  
Configure auditing of the /sbin/rmmod file.  
Add the following to the "etc/audit/audit.rules" or "etc/audit.rules" file:  
  
-w /sbin/rmmod -p x  
  
Restart the auditd service.  
# service auditd restart     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4357  
**Group Title:** GEN002860  
**Rule ID:** SV-37945r1\_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 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-37948r1\_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:**    
Verify the system is configured to forward all audit records to a remote server. If the system is not configured to provide this function, this is a finding.  
  
Procedure:  
Ensure the audit option for the kernel is enabled.  
  
# grep "audit" /boot/grub/grub.conf  
  
If the kernel does not have the "audit=1" option specified, this is a finding.  
  
Ensure the kernel auditing is active.  
  
# grep "active" /etc/audisp/plugins.d/syslog.conf  
  
If the "active" setting is either missing or not set to "yes", this is a finding.  
  
Ensure all audit records are forwarded to a remote server.  
  
# grep "\\*.\\*" /etc/syslog.conf |grep "@" (for syslog)  
or:  
# grep "\\*.\\*" /etc/rsyslog.conf | grep "@" (for rsyslog)  
  
If neither of these lines exist, it is a finding.  
  
**Fix Text:**Configure the system to send audit records to a remote server.   
  
Procedure:  
These instructions assume a known remote audit server is available to this system.   
Modify /etc/syslog.conf to contain a line sending all audit records to a remote audit server. The server is specified by placing an "@" before the DNS name or IP address in the line.   
  
\*.\* @<remote audit server>  
  
Edit the "active" line in /etc/audisp/plugins.d/syslog.conf so it shows "active = yes".  
  
Restart audit and syslog:  
# service auditd restart  
# service syslog restart     
  
**CCI:**CCI-000136  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-974  
**Group Title:** GEN002960  
**Rule ID:** SV-27320r1\_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.allow  
# ls -lL /etc/cron.deny  
If neither file exists, this is a finding.  
  
**Fix Text:**Create /etc/cron.allow and/or /etc/cron.deny with appropriate content.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-975  
**Group Title:** GEN002980  
**Rule ID:** SV-27326r1\_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 readable and/or writable cron.allow file by users 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.allow  
  
If the 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.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22384  
**Group Title:** GEN002990  
**Rule ID:** SV-37382r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002990  
**Rule Title:**The cron.allow file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  A readable and/or writeable cron.allow file by other users 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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:** Remove the extended ACL from the file.  
# setfacl --remove-all /etc/cron.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-976  
**Group Title:** GEN003000  
**Rule ID:** SV-37384r1\_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  
  
# ls /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls /etc/cron\*|grep -v deny  
  
If cron jobs exist under any of the above directories, use the following command to search for programs executed by cron:  
  
# more <cron job file>  
  
Perform a long listing of each program file found in the cron file to determine if the file is group-writable or world-writable.  
  
# 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-37388r1\_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  
  
# ls /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls /etc/cron\*|grep -v deny  
  
  
If cron jobs exist under any of the above directories, use the following command to search for programs executed by at:  
  
# more <cron job file>  
  
Perform a long listing of each directory containing program files found in the cron file to determine if the directory is world-writable.  
  
# 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-37392r1\_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  
  
# ls -lL /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls -lL /etc/cron\*|grep -v deny  
  
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>  
or   
# chown <user> <crontab file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22385  
**Group Title:** GEN003050  
**Rule ID:** SV-37400r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003050  
**Rule Title:**Crontab files must be group-owned by root, cron, 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.  
Procedure:  
  
# ls -lL /var/spool/cron  
  
# ls -lL /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls -lL /etc/cron\*|grep -v deny  
  
If the group owner is not root or the crontab owner's primary group, this is a finding.  
  
**Fix Text:**Change the group owner of the crontab file to root, cron, 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-27338r1\_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.allow  
# more /etc/cron.deny  
If a default system account (such as bin, sys, adm, or others, traditionally UID less than 500) is listed in the cron.allow file, or not listed in the cron.deny file and if no cron.allow file exists, this is a finding.  
  
**Fix Text:**Remove default system accounts (such as bin, sys, adm, or others, traditionally UID less than 500) 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-37466r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003080  
**Rule Title:**Crontab files must have mode 0600 or less permissive, and files in cron script directories must have mode 0700 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/  
# ls -lL /etc/cron.d/  
# ls -lL /etc/crontab  
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/\* /etc/cron.d/\* /etc/crontab     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29289  
**Group Title:** GEN003080-2  
**Rule ID:** SV-37745r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003080-2  
**Rule Title:**Files in cron script directories must have mode 0700 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 scripts in cron job directories.  
# ls -lL /etc/cron.daily/  
# ls -lL /etc/cron.hourly/  
# ls -lL /etc/cron.monthly/  
# ls -lL /etc/cron.weekly/  
If any cron script has a mode more permissive than 0700, this is a finding.  
  
**Fix Text:**Change the mode of the cron scripts.  
# chmod 0700 /etc/cron.daily/\* /etc/cron.hourly/\* /etc/cron.monthly/\* /etc/cron.weekly/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22386  
**Group Title:** GEN003090  
**Rule ID:** SV-37467r1\_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.  
Procedure:  
  
# ls -lL /var/spool/cron  
  
# ls -lL /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls -lL /etc/cron\*|grep -v deny  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all [crontab file]     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-979  
**Group Title:** GEN003100  
**Rule ID:** SV-37470r1\_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 directories.  
  
Procedure:  
# ls -ld /var/spool/cron  
  
# ls -ld /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls -ld /etc/cron\*|grep -v deny  
  
If the mode of any of the crontab directories is more permissive than 0755, this is a finding.  
  
**Fix Text:**Change the mode of the crontab directories.  
# chmod 0755 <crontab directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22387  
**Group Title:** GEN003110  
**Rule ID:** SV-37471r1\_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.  
  
Procedure:  
# ls -ld /var/spool/cron  
  
# ls -ld /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls -ld /etc/cron\*|grep -v deny  
  
If the permissions include a '+' the directory has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the directory.  
# setfacl --remove-all <crontab directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-980  
**Group Title:** GEN003120  
**Rule ID:** SV-37474r1\_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 directories.  
Procedure:  
  
# ls -ld /var/spool/cron  
  
# ls -ld /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls -ld /etc/cron\*|grep -v deny  
  
  
If the owner of any of the crontab directories is not root or bin, this is a finding.  
  
**Fix Text:**Change the mode of the crontab directories.  
# chown root <crontab directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-981  
**Group Title:** GEN003140  
**Rule ID:** SV-37476r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003140  
**Rule Title:**Cron and crontab directories must be group-owned by root, sys, bin or cron.  
  
  
**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 cron and crontab directories.  
  
Procedure:  
# ls -ld /var/spool/cron  
  
# ls -ld /etc/cron.d /etc/crontab /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls -ld /etc/cron\*|grep -v deny  
  
  
If a directory is not group-owned by root, sys, bin, or cron, this is a finding.  
  
**Fix Text:**Change the group owner of cron and crontab directories.  
# chgrp root <crontab directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-982  
**Group Title:** GEN003160  
**Rule ID:** SV-27352r1\_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:**    
# grep cron /etc/syslog.conf  
If cron logging is not configured, this is a finding.  
  
Check the configured cron log file found in the cron entry of /etc/syslog (normally /var/log/cron).  
# ls -lL /var/log/cron  
  
If this file does not exist, or is older than the last cron job, this is a finding.  
  
**Fix Text:**Edit /etc/syslog.conf and setup cron logging.     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-983  
**Group Title:** GEN003180  
**Rule ID:** SV-27357r1\_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.  
  
Procedure:  
Check the configured cron log file found in the cron entry in /etc/syslog (normally /var/log/cron).  
# grep cron /etc/syslog.conf  
# ls -lL /var/log/cron  
  
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/log/cron     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22388  
**Group Title:** GEN003190  
**Rule ID:** SV-37477r1\_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.  
  
Procedure:  
Check the configured cron log file found in the cron entry in /etc/syslog (normally /var/log/cron).  
# grep cron /etc/syslog.conf  
# ls -lL /var/log/cron  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /var/log/cron     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4358  
**Group Title:** GEN003200  
**Rule ID:** SV-27362r1\_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.deny  
If the cron.deny file does not exist this is not a finding.  
If the cron.deny file exists and the mode is more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the cron.deny file.  
# chmod 0600 /etc/cron.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22389  
**Group Title:** GEN003210  
**Rule ID:** SV-37486r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003210  
**Rule Title:**The cron.deny file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  If there are excessive file permissions for the cron.deny file, 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.deny  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/cron.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4360  
**Group Title:** GEN003220  
**Rule ID:** SV-37489r1\_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. A 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 more permissive than 077:  
  
Procedure:  
  
# ls -lL /var/spool/cron  
  
# ls -lL /etc/cron.d /etc/cron.daily /etc/cron.hourly /etc/cron.monthly /etc/cron.weekly  
or   
# ls -lL /etc/cron.\*|grep -v deny  
  
# 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 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-27369r1\_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.allow  
If the cron.allow file is not owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**# chown root /etc/cron.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22390  
**Group Title:** GEN003245  
**Rule ID:** SV-37495r1\_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/at.allow  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/at.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22391  
**Group Title:** GEN003250  
**Rule ID:** SV-37499r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003250  
**Rule Title:**The cron.allow file must be group-owned by root, bin, sys, or cron.  
  
  
**Vulnerability Discussion:**  If the group of the cron.allow is not set to root, bin, sys, or cron, 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.allow  
  
If the file exists and is not group-owned by root, bin, sys or cron, this is a finding.  
  
**Fix Text:**Change the group ownership of the file.  
  
Procedure:  
# chgrp root /etc/cron.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22392  
**Group Title:** GEN003252  
**Rule ID:** SV-26555r1\_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/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/at.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22393  
**Group Title:** GEN003255  
**Rule ID:** SV-26558r1\_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/at.deny  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/at.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4430  
**Group Title:** GEN003260  
**Rule ID:** SV-27374r1\_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:**    
# ls -lL /etc/cron.deny  
If the cron.deny file is not owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**# chown root /etc/cron.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22394  
**Group Title:** GEN003270  
**Rule ID:** SV-26562r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003270  
**Rule Title:**The cron.deny file must be group-owned by root, bin, sys, or cron.  
  
  
**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.deny  
  
If the file is not group-owned by root, bin, sys, this is a finding.  
  
**Fix Text:**Change the group ownership of the file.  
# chgrp root /etc/cron.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-984  
**Group Title:** GEN003280  
**Rule ID:** SV-37512r1\_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/at.allow  
# ls -lL /etc/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-37516r1\_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/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-37517r1\_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/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, traditionally UID less than 500) from the at.allow file.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-987  
**Group Title:** GEN003340  
**Rule ID:** SV-37518r1\_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, write and execute 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/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/at.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-988  
**Group Title:** GEN003360  
**Rule ID:** SV-37519r1\_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/at  
  
For each "at" job file, determine which programs are executed.  
  
Procedure:  
# more <at job file>  
  
Check the 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-37520r1\_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/at  
  
For each "at" job, determine which programs are executed by "at."  
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-37521r1\_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/at  
  
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-37523r1\_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/at  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the directory.  
# setfacl --remove-all /var/spool/at     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4365  
**Group Title:** GEN003420  
**Rule ID:** SV-37527r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003420  
**Rule Title:**The at directory must be owned by root, bin, sys, daemon, or cron.  
  
  
**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/at  
  
If the directory is not owned by root, sys, bin, daemon, or cron, this is a finding.  
  
Fix Text: Change the owner of the "at" directory to root, bin, sys, or system.  
  
**Fix Text:**Change the owner of the "at" directory to root, bin, sys, or system.  
  
Procedure:  
# chown <root or other system account> <"at" directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22396  
**Group Title:** GEN003430  
**Rule ID:** SV-37529r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003430  
**Rule Title:**The "at" directory must be group-owned by root, bin, sys, or cron.  
  
  
**Vulnerability Discussion:**  If the group of the "at" directory is not root, bin, sys, or cron, 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 file.  
  
Procedure:  
# ls -lL /var/spool/at  
  
If the file is not group-owned by root, bin, sys, daemon or cron, this is a finding.  
  
**Fix Text:**Change the group ownership of the file to root, bin, sys, daemon or cron.  
  
Procedure:  
# chgrp <root or other system group> <"at" directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4366  
**Group Title:** GEN003440  
**Rule ID:** SV-37531r1\_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. A 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/at  
  
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 that set umask to a value less restrictive than 077.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4367  
**Group Title:** GEN003460  
**Rule ID:** SV-37533r1\_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/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/at.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22397  
**Group Title:** GEN003470  
**Rule ID:** SV-26569r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003470  
**Rule Title:**The at.allow file must be group-owned by root, bin, sys, or cron.  
  
  
**Vulnerability Discussion:**  If the group owner of the at.allow file is not set to root, bin, sys, or cron, 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/at.allow  
  
If the file is not group-owned by root, bin, sys, or cron, this is a finding.  
  
**Fix Text:**Change the group ownership of the file.  
  
Procedure:  
# chgrp root /etc/at.allow     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4368  
**Group Title:** GEN003480  
**Rule ID:** SV-37535r1\_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/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/at.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22398  
**Group Title:** GEN003490  
**Rule ID:** SV-26572r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003490  
**Rule Title:**The at.deny file must be group-owned by root, bin, sys, or cron.  
  
  
**Vulnerability Discussion:**  If the group owner of the at.deny file is not set to root, bin, sys, or cron, 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/at.deny  
  
If the file is not group-owned by root, bin, sys, or cron, this is a finding.  
  
**Fix Text:**Change the group ownership of the at.deny file to root, sys, bin, or cron.  
  
Procedure:  
# chgrp root /etc/at.deny     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11996  
**Group Title:** GEN003500  
**Rule ID:** SV-37546r1\_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:**    
# ulimit -c  
If the above command does not return 0 and the enabling of core dumps has not been documented and approved by the IAO, this a finding.  
  
**Fix Text:**Edit /etc/security/limits.conf and set a hard limit for "core" to 0 for all users.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22404  
**Group Title:** GEN003510  
**Rule ID:** SV-26604r1\_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 the kdump service is not running.  
  
Procedure:  
# service kdump status  
If "Kdump is operational" is returned, this is a finding.  
  
**Fix Text:**Disable kdump.  
# service kdump stop  
# chkconfig kdump off     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11997  
**Group Title:** GEN003520  
**Rule ID:** SV-37570r1\_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  
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-26608r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003521  
**Rule Title:**The kernel core dump data directory must be group-owned by root, bin, sys, or system.  
  
  
**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 and check its ownership.  
  
Procedure:  
Examine /etc/kdump.conf. The "path" parameter, which defaults to /var/crash, determines the path relative to the crash dump device. The crash device is specified with a filesystem type and device, such as "ext3 /dev/sda2". Using this information, determine where this path is currently mounted on the system.  
# ls -ld <kernel dump data directory>  
If the directory is not group-owned by root, bin, sys, or system, 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-26612r1\_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 and check its permissions.  
  
Procedure:  
Examine /etc/kdump.conf. The "path" parameter, which defaults to /var/crash, determines the path relative to the crash dump device. The crash device is specified with a filesystem type and device, such as "ext3 /dev/sda2". Using this information, determine where this path is currently mounted on the system.  
# ls -l <kernel dump 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-26616r1\_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 and check its permissions.  
  
Procedure:  
Examine /etc/kdump.conf. The "path" parameter, which defaults to /var/crash, determines the path relative to the crash dump device. The crash device is specified with a filesystem type and device, such as "ext3 /dev/sda2". Using this information, determine where this path is currently mounted on the system.  
# ls -l <kernel dump directory>  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all <core file directory>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11999  
**Group Title:** GEN003540  
**Rule ID:** SV-27414r1\_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:**    
Verify "exec\_shield" and "randomize\_va\_space" have not been changed from the default "1" settings.  
  
Procedure:  
#sysctl kernel.exec-shield  
If the return value is not:   
kernel.exec-shield = 1  
this is a finding.  
  
  
#sysctl kernel.randomize\_va\_space  
If the return value is not:   
kernel.randomize\_va\_space = 1  
this is a finding.  
  
**Fix Text:**Examine /etc/sysctl.conf for "kernel.exec-shield" and "kernel.randomize\_va\_space" entries and if found remove them. The system default of "1" enables these modules.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22408  
**Group Title:** GEN003581  
**Rule ID:** SV-26620r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003581  
**Rule Title:**Network interfaces must not be configured to allow user control.  
  
  
**Vulnerability Discussion:**  Configuration of network interfaces should be limited to privileged users. Manipulation of network interfaces may result in a Denial of Service or bypass of network security mechanisms.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the system for user-controlled network interfaces.  
# grep -l '^USERCTL=yes' /etc/sysconfig/network-scripts/ifcfg\*   
If any results are returned, this is a finding.  
  
**Fix Text:**Edit the configuration for the user-controlled interface and remove the "USERCTL=yes" configuration line or set to "USERCTL=no".     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12002  
**Group Title:** GEN003600  
**Rule ID:** SV-29795r1\_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 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:**    
Verify the system does not accept source-routed IPv4 packets.  
  
Procedure:  
# grep [01] /proc/sys/net/ipv4/conf/\*/accept\_source\_route|egrep "default|all"  
  
If all of the returned lines do not end with 0, this is a finding.  
  
Note: The same setting is used by Linux for both the local acceptance and forwarding of source-routed IPv4 packets.  
  
**Fix Text:**Configure the system to not accept source-routed IPv4 packets.  
Edit /etc/sysctl.conf and add a setting for "net.ipv4.conf.all.accept\_source\_route=0" and "net.ipv4.conf.default.accept\_source\_route=0".   
  
Reload the sysctls.  
Procedure:  
# sysctl -p     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23741  
**Group Title:** GEN003601  
**Rule ID:** SV-37594r1\_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 Denial of Service 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:**    
# cat /proc/sys/net/ipv4/tcp\_max\_syn\_backlog  
If the result is not 1280 or greater, this is a finding.  
  
**Fix Text:**Edit /etc/sysctl.conf and add a setting for "net.ipv4.tcp\_max\_syn\_backlog=1280".  
  
Procedure:  
# sysctl -p     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22409  
**Group Title:** GEN003602  
**Rule ID:** SV-37601r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003602  
**Rule Title:**The system must not process Internet Control Message Protocol (ICMP) timestamp requests.  
  
  
**Vulnerability Discussion:**  The processing of (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  
  
Procedure:  
# grep "timestamp" /etc/sysconfig/iptables  
  
This should return entries for "timestamp-reply" and "timestamp\_request". Both should end with "-j DROP'. If either does not exist or does not "DROP" the message, this is a finding.  
  
**Fix Text:**Configure the system to not respond to ICMP TIMESTAMP\_REQUESTs. This is done by rejecting ICMP type 13 and 14 messages at the firewall.  
  
Procedure:  
Edit /etc/sysconfig/iptables to add:  
  
-A RH-Firewall-1-INPUT -p ICMP --icmp-type timestamp-request -j DROP  
-A RH-Firewall-1-INPUT -p ICMP --icmp-type timestamp-reply -j DROP  
  
Restart the firewall:  
# service iptables restart     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22410  
**Group Title:** GEN003603  
**Rule ID:** SV-37608r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003603  
**Rule Title:**The system must not respond to Internet Control Message Protocol v4 (ICMPv4) echoes sent to a broadcast address.  
  
  
**Vulnerability Discussion:**  Responding to broadcast (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.  
  
Procedure:  
# cat /proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts  
  
If the result is not 1, this is a finding.  
  
**Fix Text:**Configure the system to not respond to ICMP ECHO\_REQUESTs sent to broadcast addresses. Edit /etc/sysctl.conf and add a setting for "net.ipv4.icmp\_echo\_ignore\_broadcasts=1" and reload the sysctls.  
  
Procedure:  
# echo "net.ipv4.icmp\_echo\_ignore\_broadcasts=1" >> /etc/sysctl.conf  
# sysctl -p     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22411  
**Group Title:** GEN003604  
**Rule ID:** SV-29288r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003604  
**Rule Title:**The system must not respond to Internet Control Message Protocol (ICMP) timestamp requests sent to a broadcast address.  
  
  
**Vulnerability Discussion:**  The processing of (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.  
  
**Mitigations:**   
GEN000000-FW  
  
**Mitigation Control:**   
The system's firewall default-deny policy mitigates the risk from this vulnerability.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system does not respond to ICMP TIMESTAMP\_REQUESTs set to broadcast addresses.  
  
Procedure:  
# cat /proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts  
  
If the result is not 1, this is a finding.  
  
Note: The same parameter controls both ICMP ECHO\_REQUESTs and TIMESTAMP\_REQUESTs.  
  
**Fix Text:**Configure the system to not respond to ICMP TIMESTAMP\_REQUESTs sent to broadcast addresses. Edit /etc/sysctl.conf and add a setting for "net.ipv4.icmp\_echo\_ignore\_broadcasts=1" and reload the sysctls.  
  
Procedure:  
# echo "net.ipv4.icmp\_echo\_ignore\_broadcasts=1" >> /etc/sysctl.conf  
# sysctl -p     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22414  
**Group Title:** GEN003607  
**Rule ID:** SV-37622r1\_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 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 system, such as when IPv4 forwarding is enabled and the system is functioning as a router.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system does not accept source-routed IPv4 packets.  
  
Procedure:  
# grep [01] /proc/sys/net/ipv4/conf/\*/accept\_source\_route|egrep "default|all"  
  
If all of the resulting lines do not end with "0", this is a finding.  
  
**Fix Text:**Configure the system to not accept source-routed IPv4 packets.  
Edit /etc/sysctl.conf and add a setting for "net.ipv4.conf.all.accept\_source\_route=0" and "net.ipv4.conf.default.accept\_source\_route=0".   
  
Reload the sysctls.  
Procedure:  
# sysctl -p     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22415  
**Group Title:** GEN003608  
**Rule ID:** SV-37624r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003608  
**Rule Title:**Proxy Address Resolution Protocol (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:**    
Verify the system does not use proxy ARP.  
  
# grep [01] /proc/sys/net/ipv4/conf/\*/proxy\_arp|egrep "default|all"  
  
If all of the resulting lines do not end with "0", this is a finding.  
  
**Fix Text:**Configure the system to not use proxy ARP.  
Edit /etc/sysctl.conf and add a setting for "net.ipv4.conf.all.proxy\_arp=0" and "net.ipv4.conf.default.proxy\_arp=0".  
# sysctl -p     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22416  
**Group Title:** GEN003609  
**Rule ID:** SV-37626r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003609  
**Rule Title:**The system must ignore IPv4 Internet Control Message Protocol (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.  
  
# grep [01] /proc/sys/net/ipv4/conf/\*/accept\_redirects|egrep "default|all"  
  
If all of the resulting lines do not end with "0", this is a finding.  
  
**Fix Text:**Configure the system to not accept IPv4 ICMP redirect messages.  
Edit /etc/sysctl.conf and add a setting for "net.ipv4.conf.all.accept\_redirects=0" and "net.ipv4.conf.default.accept\_redirects=0".  
# sysctl -p     
  
**CCI:**CCI-001503  
  
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22417  
**Group Title:** GEN003610  
**Rule ID:** SV-37629r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003610  
**Rule Title:**The system must not send IPv4 Internet Control Message Protocol (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 possibly revealing portions of the network topology.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system does not send IPv4 ICMP redirect messages.  
  
# grep [01] /proc/sys/net/ipv4/conf/\*/send\_redirects|egrep "default|all"  
  
If all of the resulting lines do not end with "0", this is a finding.  
  
**Fix Text:**Configure the system to not send IPv4 ICMP redirect messages.  
Edit /etc/sysctl.conf and add a setting for "net.ipv4.conf.all.send\_redirects=0" and "net.ipv4.conf.default.send\_redirects=0".   
# sysctl -p  
    
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22418  
**Group Title:** GEN003611  
**Rule ID:** SV-37630r1\_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:**    
Verify the system logs martian packets.  
  
# grep [01] /proc/sys/net/ipv4/conf/\*/log\_martians|egrep "default|all"  
  
If all of the resulting lines do not end with "1", this is a finding.  
  
**Fix Text:**Configure the system to log martian packets.  
Edit /etc/sysctl.conf and add a setting for "net.ipv4.conf.all.log\_martians=1" and "net.ipv4.conf.default.log\_martians=1".   
  
Reload the sysctls.  
Procedure:  
# sysctl -p     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22419  
**Group Title:** GEN003612  
**Rule ID:** SV-37633r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003612  
**Rule Title:**The system must be configured to use TCP syncookies when experiencing a TCP SYN flood.  
  
  
**Vulnerability Discussion:**  A TCP SYN flood attack can cause Denial of Service by filling a system's TCP connection table with connections in the SYN\_RCVD state. Syncookies are a mechanism used to only track a connection when a subsequent ACK is received, verifying the initiator is attempting a valid connection and is not a flood source. This technique does not operate in a fully standards-compliant manner, but is only activated when a flood condition is detected, and allows defense of the system while continuing to service valid requests.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the system configured to use TCP syncookies when experiencing a TCP SYN flood.  
# cat /proc/sys/net/ipv4/tcp\_syncookies  
If the result is not "1", this is a finding.  
  
**Fix Text:**Configure the system to use TCP syncookies when experiencing a TCP SYN flood.  
Edit /etc/sysctl.conf and add a setting for "net.ipv4.tcp\_syncookies=1".   
# sysctl -p     
  
**CCI:**CCI-001092  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22421  
**Group Title:** GEN003619  
**Rule ID:** SV-37639r1\_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:**    
Verify the system is not configured for bridging.  
# ls /proc/sys/net/bridge  
If the directory exists, this is a finding.  
# lsmod | grep '^bridge '  
If any results are returned, this is a finding.  
  
Fix Text: Configure the system to not use bridging.  
  
  
**Fix Text:** Configure the system to not use bridging.  
# rmmod bridge  
Edit /etc/modprobe.conf and add a line such as "install bridge /bin/false" to prevent the loading of the bridge module.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12003  
**Group Title:** GEN003620  
**Rule ID:** SV-37640r1\_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 an 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 /home path is a separate filesystem.  
# grep "/home " /etc/fstab  
If no result is returned, /home is not on a separate filesystem this is a finding.  
  
**Fix Text:**Migrate the /home (or equivalent) path onto a separate file system.     
  
**CCI:**CCI-001208  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23736  
**Group Title:** GEN003621  
**Rule ID:** SV-37641r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003621  
**Rule Title:**The system must use a separate file system for /var.  
  
  
**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 if the /var path is a separate filesystem.  
# grep /var /etc/fstab  
If no result is returned, /var is not on a separate filesystem this is a finding.  
  
**Fix Text:**Migrate the /var path onto a separate file system.     
  
**CCI:**CCI-001208  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23738  
**Group Title:** GEN003623  
**Rule ID:** SV-37642r1\_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 if the /var/log/audit path is a separate filesystem.  
# grep /var/log/audit /etc/fstab  
If no result is returned, /var/log/audit is not on a separate filesystem this is a finding.  
  
**Fix Text:**Migrate the /var/log/audit path onto a separate filesystem.     
  
**CCI:**CCI-001208  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23739  
**Group Title:** GEN003624  
**Rule ID:** SV-37395r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003624  
**Rule Title:**The system must use a separate file system for /tmp (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.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the /tmp path is a separate filesystem.  
# egrep "[\t ]/tmp[\t ]" /etc/fstab  
If no result is returned, /tmp is not on a separate filesystem this is 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-37398r1\_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, preserving the integrity of data that may have otherwise been lost. Journaling file systems typically do not require consistency checks upon booting after a crash, which can improve system availability. Some file systems employ other mechanisms to ensure consistency also satisfying this requirement.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Logging should be enabled for those types of file systems not turning on logging by default.   
  
Procedure:  
# mount  
  
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 support journaling this is a finding. If the 'nolog' option is set on the root file system that does support journaling, this is a finding.  
  
  
  
**Fix Text:**Implement file system journaling for the root file system, or use a file system with other mechanisms to ensure file system consistency. If the root file system supports journaling, enable it. If the file system does not support journaling or another mechanism to ensure file system 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-37401r1\_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 preserving the integrity of data that may have otherwise been lost. Journaling file systems typically do not require consistency checks upon booting after a crash, which can improve system availability. Some file systems employ other mechanisms to ensure consistency also satisfying this requirement.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify local filesystems use journaling.  
# mount | grep '^/dev/' | egrep -v 'type (ext3|ext4|jfs|reiserfs|xfs|iso9660|udf)'  
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-37404r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003660  
**Rule Title:**The system must log informational authentication 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 authpriv facility is logging both the "notice" and "info" priority messages.  
  
Procedure:  
For a given action all messages of a higher severity or "priority" are logged. The three lowest priorities in ascending order are "debug", "info" and "notice". A priority of "info" will include "notice". A priority of "debug" includes both "info" and "notice".  
  
Enter/Input:  
# grep "authpriv.debug" /etc/syslog.conf  
# grep "authpriv.info" /etc/syslog.conf  
# grep "authpriv\.\\*" /etc/syslog.conf  
  
If an "authpriv.\*", "authpriv.debug", or "authpriv.info" entry is not found, this is a finding.  
  
  
  
  
**Fix Text:**Edit /etc/syslog.conf and add local log destinations for "authpriv.\*", "authpriv.debug" or "authpriv.info".     
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12005  
**Group Title:** GEN003700  
**Rule ID:** SV-27424r1\_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:**    
# ps -ef |grep xinetd  
If xinetd is not running, this check is not a finding.  
# grep -v "^#" /etc/xinetd.conf  
# grep disable /etc/xinetd.d/\* |grep no  
If no active services are found, and the inetd daemon is running, this is a finding.  
  
**Fix Text:**# service xinetd stop ; chkconfig xinetd off     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-821  
**Group Title:** GEN003720  
**Rule ID:** SV-37406r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003720  
**Rule Title:**The inetd.conf file, xinetd.conf file, and the xinetd.d directory 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 possibly weakening the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the owner of the xinetd configuration files.  
  
Procedure:  
# ls -lL /etc/xinetd.conf   
# ls -laL /etc/xinetd.d  
This is a finding if any of the above files or directories are not owned by root or bin.  
  
  
  
**Fix Text:**Change the owner of the xinetd configuration files.  
# chown root /etc/xinetd.conf /etc/xinetd.d/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22423  
**Group Title:** GEN003730  
**Rule ID:** SV-37407r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003730  
**Rule Title:**The inetd.conf file, xinetd.conf file, and the xinetd.d directory must be group-owned by root, bin, sys, or system.  
  
  
**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 possibly weakening the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the xinetd configuration files and directories.  
  
Procedure:  
# ls -alL /etc/xinetd.conf /etc/xinetd.d  
  
If a file or directory is not group-owned by root, bin, sys, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group-owner of the xinetd configuration files and directories.  
  
Procedure:  
# chgrp -R root /etc/xinetd.conf /etc/xinetd.d     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-822  
**Group Title:** GEN003740  
**Rule ID:** SV-37408r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003740  
**Rule Title:**The inetd.conf and xinetd.conf files 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 the xinetd configuration files.  
  
Procedure:  
# ls -lL /etc/xinetd.conf   
# ls -lL /etc/xinetd.d  
If the mode of the file(s) is more permissive than 0640, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the xinetd configuration files.  
# chmod 0640 /etc/xinetd.conf /etc/xinetd.d/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22424  
**Group Title:** GEN003745  
**Rule ID:** SV-37409r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003745  
**Rule Title:**The inetd.conf and xinetd.conf files 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 xinetd configuration files.   
  
Procedure:  
# ls -alL /etc/xinetd.conf  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/xinetd.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22425  
**Group Title:** GEN003750  
**Rule ID:** SV-37410r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003750  
**Rule Title:**The xinetd.d directory must have mode 0755 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 permissions of the xinetd configuration directories.  
# ls -dlL /etc/xinetd.d  
If the mode of the directory is more permissive than 0755, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the directory.  
# chmod 0755 /etc/xinetd.d     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22426  
**Group Title:** GEN003755  
**Rule ID:** SV-37411r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003755  
**Rule Title:**The xinetd.d directory must not have an extended ACL.  
  
  
**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 xinetd configuration files and directories.  
# ls -alL /etc/xinetd.conf /etc/xinetd.d  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/xinetd.d     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-823  
**Group Title:** GEN003760  
**Rule ID:** SV-37424r1\_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 possibly weakening 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-37425r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003770  
**Rule Title:**The services file must be group-owned by root, bin, sys, or system.  
  
  
**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 possibly weakening 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, sys, or system, 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-37426r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003780  
**Rule Title:**The services file must have mode 0644 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 0644, this is a finding  
  
**Fix Text:**Change the mode of the services file to 0644 or less permissive.  
  
Procedure:  
# chmod 0644 /etc/services     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22428  
**Group Title:** GEN003790  
**Rule ID:** SV-37438r1\_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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/services     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1011  
**Group Title:** GEN003800  
**Rule ID:** SV-37439r1\_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 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:**    
The /etc/xinetd.conf file and each file in the /etc/xinetd.d directory file should be examined for the following:   
  
Procedure:  
log\_type = SYSLOG authpriv  
log\_on\_success = HOST PID USERID EXIT  
log\_on\_failure = HOST USERID  
  
If xinetd is running and logging is not enabled, this is a finding.  
  
  
  
**Fix Text:**Edit each file in the /etc/xinetd.d directory and the /etc/xinetd.conf file to contain:  
log\_type = SYSLOG authpriv  
log\_on\_success = HOST PID USERID EXIT  
log\_on\_failure = HOST USERID  
  
The /etc/xinetd.conf file contains default values that will hold true for all services unless individually modified in the service's xinetd.d file.  
  
To make the new settings effective, restart the xinetd service:  
# service xinetd restart     
  
**CCI:**CCI-000134  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22429  
**Group Title:** GEN003810  
**Rule ID:** SV-26662r1\_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 portmap service.  
# service portmap status  
If the service is running, this is a finding.  
  
**Fix Text:**Shutdown and disable the portmap service.  
# service portmap stop; chkconfig portmap off     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22430  
**Group Title:** GEN003815  
**Rule ID:** SV-26666r1\_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:**    
Check if the portmap package is installed.  
# rpm -qa | grep portmap  
If a package is found, this is a finding.  
  
**Fix Text:**Remove the portmap package.  
# rpm -e portmap  
or   
# yum remove portmap     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4687  
**Group Title:** GEN003820  
**Rule ID:** SV-37441r1\_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:**    
Check to see if rshd is configured to run on startup.  
  
Procedure:  
# grep disable /etc/xinetd.d/rsh  
  
If /etc/xinetd.d/rsh exists and rsh is found to be enabled, this is a finding.  
  
  
**Fix Text:**Edit /etc/xinetd.d/rsh and set "disable=yes".     
  
**CCI:**CCI-000068  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22431  
**Group Title:** GEN003825  
**Rule ID:** SV-26667r1\_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 rsh-server package is installed.  
  
Procedure:  
# rpm -qa | grep rsh-server  
  
If a package is found, this is a finding.  
  
**Fix Text:**Remove the rsh-server package.  
  
Procedure:  
# rpm -e rsh-server     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22432  
**Group Title:** GEN003830  
**Rule ID:** SV-26671r1\_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:**    
Check the rlogind configuration.  
# cat /etc/xinetd.d/rlogin  
If the file exists and does not contain "disable = yes" this is a finding.  
  
**Fix Text:**Remove or disable the rlogin configuration and restart xinetd.  
# rm /etc/xinetd.d/rlogin ; service xinetd restart     
  
**CCI:**CCI-000068  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22433  
**Group Title:** GEN003835  
**Rule ID:** SV-26669r1\_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 rsh-server package is installed.  
  
Procedure:  
# rpm -qa | grep rsh-server  
  
If a package is found, this is a finding.  
  
**Fix Text:**Remove the rsh-server package.  
  
Procedure:  
# rpm -e rsh-server     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4688  
**Group Title:** GEN003840  
**Rule ID:** SV-37443r1\_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:**  Information Assurance Officer  
**IAControls:**  EBRP-1, ECSC-1  
  
**Check Content:**    
# grep disable /etc/xinetd.d/rexec  
If the service file exists and is not disabled, this is a finding.  
  
  
  
**Fix Text:** Edit /etc/xinetd.d/rexec and set "disable=yes"     
  
**CCI:**CCI-001435  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22434  
**Group Title:** GEN003845  
**Rule ID:** SV-26673r1\_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 rsh-server package is installed.  
  
Procedure:  
# rpm -qa | grep rsh-server  
  
If a package is found, this is a finding.  
  
**Fix Text:**Remove the rsh-server package.  
  
Procedure:  
# rpm -e rsh-server     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24386  
**Group Title:** GEN003850  
**Rule ID:** SV-37444r1\_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:**    
The telnet service included in the RHEL distribution is part of krb5-workstation. There are two versions of telnetd server provided. The xinetd.d file ekrb5-telnet allows only connections authenticated through kerberos. The xinetd.d krb5-telnet allows normal telnet connections as well as kerberized connections. Both are set to "disable = yes" by default. Ensure that neither is running.  
  
Procedure:  
Check if telnetd is running:  
  
# ps -ef |grep telnetd  
  
If the telnet daemon is running, this is a finding.  
  
Check if telnetd is enabled on startup:  
  
# chkconfig --list|grep telnet  
  
If an entry with "on" is found, this is a finding.  
  
**Fix Text:**Identify the telnet service running and disable it.  
  
Procedure:  
  
Disable the telnet server.  
# chkconfig telnet off  
  
Verify the telnet daemon is no longer running.  
# ps -ef |grep telnet     
  
**CCI:**CCI-000197  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4701  
**Group Title:** GEN003860  
**Rule ID:** SV-37445r1\_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 more information for potential used in subsequent attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1, EBRU-1  
  
**Check Content:**    
# grep disable /etc/xinetd.d/finger  
If the finger service is not disabled, this is a finding.  
  
  
  
**Fix Text:**Edit /etc/xinetd.d/finger and set "disable=yes"     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12049  
**Group Title:** GEN003865  
**Rule ID:** SV-37446r1\_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 nc  
# find / -name tcpdump  
# find / -name snoop  
  
If any network analysis tools are found, this is a finding  
  
**Fix Text:**Remove each network analysis tool binary from the system. Remove package items with a package manager, others remove the binary directly.  
  
Procedure:  
Find the binary file:  
# find / -name <Item to be removed>  
  
Find the package, if any, to which it belongs:  
# rpm -qf <binary file>  
  
Remove the package if it does not also include other software:  
# rpm -e <package name>  
or   
# yum remove <package name>  
  
If the item to be removed is not in a package, or the entire package cannot be removed because of other software it provides, remove the item's binary file.  
# rm <binary file>     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-827  
**Group Title:** GEN003900  
**Rule ID:** SV-37447r1\_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:**    
RHEL uses "cups" print service. Verify remote host access is limited.  
  
Procedure:  
# grep -i Listen /etc/cups/cupsd.conf   
The /etc/cups/cupsd.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/cups/cupsd.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  
  
**Fix Text:**Configure cups to use only the localhost or specified remote hosts.  
  
Procedure:   
Modify the /etc/cups/cupsd.conf file to "Listen" only to the local machine or a known set of hosts (i.e., Listen localhost:631).  
Modify the /etc/cups/cupsd.conf file "<Location />" element to "Deny From All" and "Allow from 127.0.0.1" or allowed host addresses.   
  
Restart cups:  
# service cups restart  
  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-828  
**Group Title:** GEN003920  
**Rule ID:** SV-37448r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003920  
**Rule Title:**The hosts.lpd (or equivalent) file must be owned by root, bin, sys, or lp.  
  
  
**Vulnerability Discussion:**  Failure to give ownership of the hosts.lpd file to root, bin, sys, or lp 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 file.  
  
Procedure:  
# ls -lL /etc/cups/printers.conf;  
  
If no print service configuration file is found, this is not applicable.  
If the owner of the file is not root, this is a finding  
  
**Fix Text:**Change the owner of the /etc/cups/printers.conf to root.   
  
Procedure:  
# chown root /etc/cups/printers.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22435  
**Group Title:** GEN003930  
**Rule ID:** SV-37449r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003930  
**Rule Title:**The hosts.lpd (or equivalent) file must be group-owned by root, bin, sys, or system.  
  
  
**Vulnerability Discussion:**  Failure to give group-ownership of the hosts.lpd 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 /etc/cups/printers.conf file.  
  
Procedure:  
# ls -lL /etc/cups/printers.conf  
  
If the file is not group-owned by lp, this is a finding.  
  
  
  
**Fix Text:**Change the group-owner of the printers.conf file.  
  
Procedure:  
# chgrp lp /etc/cups/printers.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-829  
**Group Title:** GEN003940  
**Rule ID:** SV-37461r1\_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 file.  
  
Procedure:  
# ls -lL /etc/cups/printers.conf  
  
If no print service configuration file is found, this is not applicable.  
If the mode of the print service configuration file is more permissive than 0664, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the /etc/cups/printers.conf file to 0664 or less permissive.  
  
Procedure:  
# chmod 0664 /etc/cups/printers.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22436  
**Group Title:** GEN003950  
**Rule ID:** SV-37462r1\_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 /etc/cups/printers.conf file.  
  
# ls -lL /etc/cups/printers.conf  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/cups/printers.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4369  
**Group Title:** GEN003960  
**Rule ID:** SV-37463r1\_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 potentially leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /bin/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:  
# chown root /bin/traceroute  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4370  
**Group Title:** GEN003980  
**Rule ID:** SV-37464r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003980  
**Rule Title:**The traceroute command must be group-owned by sys, bin, root, or system.  
  
  
**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 potentially 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 /bin/traceroute  
  
If the traceroute command is not group-owned by root, sys, bin, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group-owner of the traceroute command to root.  
  
Procedure:  
# chgrp root /bin/traceroute     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4371  
**Group Title:** GEN004000  
**Rule ID:** SV-37465r1\_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 potentially leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /bin/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 /bin/traceroute  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22437  
**Group Title:** GEN004010  
**Rule ID:** SV-37468r1\_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 potentially leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the /bin/traceroute file.  
# ls -lL /bin/traceroute  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /bin/traceroute     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4382  
**Group Title:** GEN004220  
**Rule ID:** SV-37469r1\_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 .mozilla directory. If none exists, this is not a finding. If there is one, verify with the root users and the IAO the intent of the browsing. If the browsing is not limited to authorized local services administration, this is a finding.  
  
**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-37472r1\_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 adding aliases to run malicious code or redirect e-mail.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the alias files.  
  
Procedure:  
for sendmail:  
# ls -lL /etc/aliases  
# ls -lL /etc/aliases.db  
If all the files are not owned by root, this is a finding.  
  
for postfix:  
Verify the location of the alias file.  
# postconf alias maps  
  
This will return the location of the "aliases" file, by default "/etc/postfix/aliases"  
  
# ls -lL <postfix aliases file>  
# ls -lL <postfix aliases.db file>  
If all the files are not owned by root, this is a finding.  
  
  
  
**Fix Text:**Change the owner of the /etc/aliases file to root.  
  
Procedure:  
for sendmail:  
# chown root /etc/aliases  
# chown root /etc/aliases.db  
  
for postfix  
# chown root /etc/postfix/aliases  
# chown root /etc/postfix/aliases.db  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22438  
**Group Title:** GEN004370  
**Rule ID:** SV-37473r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004370  
**Rule Title:**The aliases file must be group-owned by root, sys, bin, or system.  
  
  
**Vulnerability Discussion:**  If the alias file is not group-owned by root or a system group, an unauthorized user may modify the file adding aliases to run malicious code or redirect e-mail.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the alias files.  
  
Procedure:  
for sendmail:  
# ls -lL /etc/aliases  
If the files are not group-owned by root, this is a finding.  
  
# ls -lL /etc/aliases.db  
If the file is not group-owned by the same system group as sendmail, which is smmsp by default, this is a finding.  
  
for postfix:  
Verify the location of the alias file.  
# postconf alias maps  
  
This will return the location of the "aliases" file, by default "/etc/postfix/aliases"  
  
# ls -lL <postfix aliases file>  
If the files are not group-owned by root, this is a finding.  
  
# ls -lL <postfix aliases.db file>  
If the file is not group-owned by root, this is a finding.  
  
  
  
**Fix Text:**Change the group-owner of the /etc/aliases file.  
  
Procedure:  
for sendmail:  
# chgrp root /etc/aliases  
# chgrp smmsp /etc/aliases.db  
  
The aliases.db file must be owned by the same system group as sendmail, which is smmsp by default.  
  
for postfix  
# chgrp root /etc/postfix/aliases  
# chgrp root /etc/postfix/aliases.db     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-832  
**Group Title:** GEN004380  
**Rule ID:** SV-37475r1\_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 e-mail.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the alias file.  
  
Procedure:  
for sendmail:  
# ls -lL /etc/aliases /etc/aliases.db  
If an alias file has a mode more permissive than 0644, this is a finding.  
  
for postfix:  
Verify the location of the alias file.  
# postconf alias maps  
  
This will return the location of the "aliases" file, by default "/etc/postfix/aliases"  
  
# ls -lL <postfix aliases file> <postfix aliases.db file>  
If an alias file has a mode more permissive than 0644, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the alias files as needed to function. No higher than 0644.  
Procedure:  
for sendmail:  
# chmod 0644 /etc/aliases /etc/aliases.db  
  
for postfix (assuming the default postfix directory):  
# chmod 0644 /etc/postfix/aliases /etc/postfix/aliases.db     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22439  
**Group Title:** GEN004390  
**Rule ID:** SV-37488r1\_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 e-mail.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the alias file.  
  
Procedure:  
for sendmail:  
# ls -lL /etc/aliases /etc/aliases.db  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
for postfix:  
Verify the location of the alias file.  
# postconf alias maps  
  
This will return the location of the "aliases" file, by default "/etc/postfix/aliases"  
  
# ls -lL <postfix aliases file> <postfix aliases.db file>  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended permissions from the alias files.  
Procedure:  
for sendmail:  
# setfacl --remove-all /etc/aliases /etc/aliases.db  
  
for postfix (assuming the default postfix directory):  
# setfacl --remove-all /etc/postfix/aliases /etc/postfix/aliases.db     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-833  
**Group Title:** GEN004400  
**Rule ID:** SV-37491r1\_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:**    
Verify the ownership of files referenced within the sendmail aliases file.  
  
Procedure:  
# more /etc/aliases  
Examine the aliases file for any utilized directories or paths.  
  
# ls -lL <directory or file path>  
Check the owner for any paths referenced.   
Check if the file or parent directory is owned by root. If not, this is a finding.  
  
  
  
**Fix Text:**Edit the /etc/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 <file or directory name>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22440  
**Group Title:** GEN004410  
**Rule ID:** SV-37493r1\_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, sys, or system, and must reside within a directory group-owned by root, bin, sys, or system.  
  
  
**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/aliases file.  
  
Procedure:  
# more /etc/aliases  
Examine the aliases file for any utilized directories or paths.  
  
# ls -lL <file referenced from aliases>  
Check the permissions for any paths referenced.   
If the group owner of any file is not root, bin, sys, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group ownership of the file referenced from /etc/aliases.  
  
Procedure:  
# chgrp root <file referenced from aliases>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-834  
**Group Title:** GEN004420  
**Rule ID:** SV-37494r1\_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 aliases file has permissions greater than 0755, it can be modified by an unauthorized user and may contain malicious code or instructions potentially compromising the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Examine the contents of the /etc/aliases file.  
  
Procedure:  
# more /etc/aliases  
Examine the aliases file for any referenced programs, which are specified with the pipe (|) symbol.  
  
# ls -lL <file referenced from aliases>  
Check the permissions for any paths referenced.   
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-37496r1\_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 aliases 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/aliases file.  
  
Procedure:  
# more /etc/aliases  
Examine the aliases file for any utilized directories or paths.  
  
# ls -lL <file referenced from aliases>  
Check the permissions for any paths referenced.   
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all <file referenced from aliases>  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-835  
**Group Title:** GEN004440  
**Rule ID:** SV-37497r1\_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 nine:  
  
Procedure:  
for sendmail:  
# grep "O L" /etc/mail/sendmail.cf  
  
OR  
  
# grep LogLevel /etc/mail/sendmail.cf  
  
If logging is set to less than nine, this is a finding.  
  
for Postfix:  
This rule is not applicable to postfix which does not use "log levels" in the same fashion as sendmail.  
  
  
  
**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-37500r1\_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:  
# grep "mail\." /etc/syslog.conf   
  
If syslog is not configured to log critical sendmail messages ("mail.crit" or "mail.\*"), this is a finding.  
  
  
  
**Fix Text:**Check the syslog configuration file for mail.crit logging configuration.  
  
Procedure:  
# grep "mail\." /etc/syslog.conf   
  
If syslog is not configured to log critical sendmail messages ("mail.crit" or "mail.\*"), this is a finding.  
  
    
  
**CCI:**CCI-000126  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-837  
**Group Title:** GEN004480  
**Rule ID:** SV-37501r1\_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:  
The check procedure is the same for both sendmail and Postfix.  
Identify any log files configured for the "mail" service (excluding mail.none) at any severity level and check the ownership   
# egrep "mail\.[^n][^/]\*" /etc/syslog.conf|sed 's/^[^/]\*//'|xargs ls -lL  
  
If any mail log file is not owned by root, this is a finding.  
  
  
  
**Fix Text:**Change the ownership of the sendmail log file.  
  
Procedure:  
The fix procedure is the same for both sendmail and Postfix.  
# chown root <sendmail log file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-838  
**Group Title:** GEN004500  
**Rule ID:** SV-37502r1\_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:  
The check procedure is the same for both sendmail and Postfix.  
Identify any log files configured for the "mail" service (excluding mail.none) at any severity level and check the permissions   
# egrep "mail\.[^n][^/]\*" /etc/syslog.conf|sed 's/^[^/]\*//'|xargs ls -lL  
  
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:  
The fix procedure is the same for both sendmail and Postfix.  
# chmod 0644 <sendmail log file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22442  
**Group Title:** GEN004510  
**Rule ID:** SV-37503r1\_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".  
  
Procedure:  
This check is applicable to both Postfix or sendmail servers.  
Check the permissions on these log files.Identify any log files configured for "\*.crit" and the "mail" service (excluding mail.none) and at any severity level.  
# egrep "(\\*.crit|mail\.[^n][^/]\*)" /etc/syslog.conf|sed 's/^[^/]\*//'|xargs ls -lL  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**This fix is applicable to both Postfix and sendmail servers.  
Remove the extended ACL from the file.  
# setfacl --remove-all <log file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12006  
**Group Title:** GEN004540  
**Rule ID:** SV-37504r1\_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. This rule is for "sendmail" only and not applicable to "Postfix".  
  
Procedure:  
# telnet localhost 25  
> help  
  
If the help command returns any sendmail version information, this is a finding.  
  
  
  
**Fix Text:**To disable the SMTP HELP command, remove /etc/mail/helpfile.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4384  
**Group Title:** GEN004560  
**Rule ID:** SV-37505r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004560  
**Rule Title:**The SMTP service's 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:**    
To check for the version of either sendmail or Postfix being displayed in the greeting:  
  
# telnet localhost 25  
  
If a version number is displayed, this is a finding.  
  
  
  
**Fix Text:**Ensure sendmail or Postfix has been configured to mask the version information.  
  
Procedure  
for sendmail:  
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  
  
for Postfix:  
Examine the "smtpd\_banner" line of /etc/postfix/main.conf and remove any "$mail\_version" entry on it or comment the entire "smtpd\_banner" line to use the default value which does not display the version information.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4385  
**Group Title:** GEN004580  
**Rule ID:** SV-37506r1\_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:**    
Check forwarding capability from sendmail.  
  
Procedure:  
grep "0 ForwardPath" /etc/mail/sendmail.cf  
  
If the entry contains a file path, this is a finding.  
  
Search for any .forward in users home directories on the system by:  
  
# for pwline in `cut -d: -f1,6 /etc/passwd`; do homedir=`echo ${pwline}|cut -d: -f2`;username=`echo ${pwline} | cut -d: -f1`;echo $username `stat -c %n $homedir/.forward 2>null`; done|egrep "\.forward"  
  
If any users have a .forward file in their home directory, this is a finding.   
  
  
  
**Fix Text:**Disable forwarding for sendmail and remove .forward files from the system  
  
Procedure:  
Edit the /etc/mail/sendmail.mc file to change the ForwardPath entry to a null path by adding the line  
define(`confFORWARD\_PATH`,`')  
rebuild the sendmail.cf file.  
  
Remove all .forward files on the system  
# find / -name .forward -delete  
  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4689  
**Group Title:** GEN004600  
**Rule ID:** SV-37507r1\_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.  
  
Procedure:  
#rpm -q sendmail  
RedHat sendmail 8.13.8-8 is the latest required version.  
If the RedHat sendmail is installed and the version is not at least 8.13.8-8, this is a finding.  
  
#rpm -q postfix  
RedHat postfix-2.5.1-0.4.rhel5 is the latest required version.  
If the postfix is installed and the version is not at least 2-5.1-0.4, this is a finding.  
  
  
  
**Fix Text:**Obtain and install a newer version of the SMTP service software (sendmail or Postfix) from RedHat.     
  
**CCI:**CCI-001230  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4690  
**Group Title:** GEN004620  
**Rule ID:** SV-37508r1\_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" or a 550 error code of "access denied", this is a finding.  
  
The RHEL distribution ships with sendmail Version 8.13.8 which is not vulnerable. This should never be a finding.  
  
**Fix Text:**Obtain and install a newer version of the SMTP service software (sendmail or Postfix) from RedHat.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4691  
**Group Title:** GEN004640  
**Rule ID:** SV-37509r1\_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) is to include 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 the decode or the 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.  
  
  
  
**Fix Text:**Disable mail aliases for decode and uudecode. If the /etc/aliases or /usr/lib/aliases (mail alias) file contains entries for these programs, remove them or disable them by placing "#" at the beginning of the line, and then executing the new aliases command. For more information on mail aliases, refer to the man page for aliases. Disabled aliases would be similar to these examples:  
# decode: |/usr/bin/uudecode  
# uudecode: |/usr/bin/uuencode -d     
  
**CCI:**CCI-001230  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4692  
**Group Title:** GEN004660  
**Rule ID:** SV-37510r1\_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 a false positive is suspected, check the log file for the response from the server.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
This vulnerability is applicable only to sendmail. If Postfix is the SMTP service for the system this will never be a finding.  
  
Procedure:  
Determine if EXPN is disabled.  
# grep -v "^#" /etc/mail/sendmail.cf |grep -i PrivacyOptions  
  
If nothing is returned or the returned line does not contain "noexpn", this is a finding.  
  
**Fix Text:**Rebuild /etc/mail/sendmail.cf with the "noexpn" Privacy Flag set.  
  
Procedure:  
Edit /etc/mail/sendmail.mc resetting the Privacy Flags to the default:  
  
define('confPRIVACYFLAGS', 'authwarnings,novrfy,noexpn,restrictqrun')dnl  
  
Rebuild the sendmail.cf file with:  
# make -C /etc/mail  
  
Restart the sendmail service.  
# service sendmail restart  
  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4693  
**Group Title:** GEN004680  
**Rule ID:** SV-37511r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004680  
**Rule Title:**The SMTP service must not have the Verify (VRFY) feature active.  
  
  
**Vulnerability Discussion:**  The VRFY 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:  
# grep -v "^#" /etc/mail/sendmail.cf |grep -i vrfy  
  
Verify the VRFY command is disabled with an entry in the sendmail.cf file. The entry could be any one of "Opnovrfy", "novrfy", or "goaway", which could also have other options included, such as "noexpn". The "goaway" argument encompasses many things, such as "novrfy" and "noexpn".  
  
If no setting to disable VRFY is found, this is a finding.  
  
**Fix Text:**Add the "novrfy" flag to your sendmail in /etc/mail/sendmail.cf.   
  
Procedure:  
Edit the definition of "confPRIVACY\_FLAGS" in /etc/mail/sendmail.mc to include "novrfy".  
  
Rebuild the sendmail.cf file with:  
# make -C /etc/mail  
  
Restart the sendmail service.  
# service sendmail restart  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4694  
**Group Title:** GEN004700  
**Rule ID:** SV-37513r1\_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:**    
Log into the sendmail server with telnet and test the "wiz" command.  
  
Procedure:  
# telnet localhost 25  
  
Trying 127.0.0.1...  
Connected to locahost.localdomain (127.0.0.1).  
Escape character ...  
  
Once the telnet greeting is complete type:  
wiz  
  
If you do not get a "Command unrecognized: " message, this is a finding.  
  
  
  
**Fix Text:**If the WIZ command exists on sendmail then the version of sendmail is archaic and should be replaced with the latest version from RedHat.  
WIZ is not available on any sendmail distribution of RHEL. However, if the WIZ command is enabled on sendmail, it should be disabled by adding this line to the sendmail.cf configuration file (note that 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-37514r1\_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 examine the configuration files.   
Determine if sendmail only binds to loopback addresses by examining the "DaemonPortOptions" configuration options.  
  
Procedure:  
# grep -i "O DaemonPortOptions" /etc/mail/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:  
# grep -i promiscuous\_relay /etc/mail/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, and 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-37515r1\_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 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:  
  
# chkconfig --list gssftp  
# chkconfig --list vsftpd  
  
If any of these services are found, ask the SA if these services are encrypted. If they are not, this is a finding.  
  
**Fix Text:**Disable the FTP daemons.  
  
Procedure:  
# chkconfig gssftp off  
# chkconfig vsftpd off     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-846  
**Group Title:** GEN004820  
**Rule ID:** SV-37526r1\_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 not recommended. If anonymous FTP must be used on a system, the requirement must be authorized and approved in the system accreditation package.  
  
**Documentable:** YES   
**Responsibility:**  Information Assurance Officer  
**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 and the use of anonymous ftp has not been documented and approved by the IAO, 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-37528r1\_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:**  System Administrator  
**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:**Remove anonymous ftp capability or move the system to a DMZ network.     
  
**CCI:**CCI-000787  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-840  
**Group Title:** GEN004880  
**Rule ID:** SV-37530r1\_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.  
  
Procedure:  
For gssftp:  
# ls -l /etc/ftpusers  
  
For vsftp:  
# ls -l /etc/vsftpd.ftpusers  
or  
# ls -l /etc/vsftpd/ftpusers  
  
If the appropriate ftpusers file for the running FTP service does not exist, this is a finding.  
  
  
  
**Fix Text:**Create an ftpusers file appropriate for the running FTP service.  
For gssftp:  
Create an /etc/ftpusers file containing a list of accounts not authorized for FTP.  
  
For vsftp:  
Create an /etc/vfsftpd.ftpusers or /etc/vfsftpd/ftpusers (as appropriate) file containing a list of accounts not authorized for FTP.  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-841  
**Group Title:** GEN004900  
**Rule ID:** SV-37532r1\_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 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.   
For gssftp:  
# more /etc/ftpusers  
  
For vsftp:  
# more /etc/vsftpd.ftpusers /etc/vfsftpd/ftpusers  
If the system has accounts not allowed to use FTP and not listed in the ftpusers file, this is a finding.  
  
**Fix Text:**For gssftp:  
Add accounts not allowed to use FTP to the /etc/ftpusers file.  
For vsftp:  
Add accounts not allowed to use FTP to the /etc/vfsftpd.ftpusers or /etc/vfsftpd/ftpusers file (as appropriate).   
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-842  
**Group Title:** GEN004920  
**Rule ID:** SV-37537r1\_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.  
  
Procedure:  
For gssftp:  
# ls -l /etc/ftpusers  
  
For vsftp:  
# ls -l /etc/vsftpd.ftpusers /etc/vsftpd/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.  
For gssftp:  
# chown root /etc/ftpusers  
  
For vsftp:  
# chown root /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22444  
**Group Title:** GEN004930  
**Rule ID:** SV-37538r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004930  
**Rule Title:**The ftpusers file must be group-owned by root, bin, sys, or system.  
  
  
**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/ftpusers /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers  
  
If the file is not group-owned by root, bin, sys, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group owner of the ftpusers file.  
  
Procedure:  
# chgrp root /etc/ftpusers /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-843  
**Group Title:** GEN004940  
**Rule ID:** SV-37542r1\_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.  
  
Procedure:  
For gssftp:  
# ls -l /etc/ftpusers  
  
For vsftp:  
# ls -l /etc/vsftpd.ftpusers /etc/vsftpd/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.  
  
Procedure:  
For gssftp:  
# chmod 0640 /etc/ftpusers  
  
For vsftp:  
# chmod 0640 /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22445  
**Group Title:** GEN004950  
**Rule ID:** SV-37544r1\_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/ftpusers file.   
# ls -lL /etc/ftpusers /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/ftpusers /etc/vsftpd.ftpusers /etc/vsftpd/ftpusers     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-845  
**Group Title:** GEN004980  
**Rule ID:** SV-37547r1\_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:**    
Find if logging is applied to the ftp daemon. The procedure depends on the implementation of ftpd used by the system.   
  
Procedures:  
  
For vsftpd:   
If vsftpd is started by xinetd:  
  
#grep vsftpd /etc/xinetd.d/\*  
This will indicate the xinetd.d startup file  
  
#grep server\_args <vsftpd xinetd.d startup file>  
This will indicate the vsftpd config file used when starting through xinetd.   
If the line is missing then "/etc/vsftpd/vsftpd.conf", the default config file, is used.  
  
#grep xferlog\_enable <vsftpd config file>  
If "xferlog\_enable" is missing or is not set to "yes", this is a finding.  
  
If vsftp is not started by xinetd:  
#grep xferlog\_enable /etc/vsftpd/vsftpd.conf  
If "xferlog\_enable" is missing or is not set to "yes", this is a finding.  
  
  
For gssftp:  
Find if the -l option will be applied when xinetd starts gssftp  
# grep server\_args /etc/xinetd.d/gssftp  
If the line is missing or does not contain at least one -l, this is a finding.  
  
  
  
**Fix Text:**Enable logging by changing ftpd startup or config files.  
  
Procedure:  
The procedure depends on the implementation of ftpd used by the system.   
  
For vsftpd:   
  
Ensure the server settings in "/etc/vsftpd.conf" (or other configuration file specified by the vaftpd xinetd.d startup file) contains:  
  
xferlog\_enable = yes  
  
For gssftp:  
If the "disable" server setting is missing or set to "no" in "/etc/xinetd.d/gssftp" then  
ensure the server settings in "/etc/xinetd.d/gssftp" contains:  
  
server\_args = -l   
  
The -l option may be added up to three times. Each -l will provide increasing verbosity on the log. Refer to the main page for ftpd for more information.  
  
For both if started using xinetd:  
If the "disable" server setting is missing or set to "no" in the /etc/xinetd.d startup file then  
ensure the server settings contains:  
  
log\_on\_success += DURATION USERID  
This will log the startup and shutdown of the daemon.  
  
log\_on\_failure += HOST USERID     
  
**CCI:**CCI-000130  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4387  
**Group Title:** GEN005000  
**Rule ID:** SV-37549r1\_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-12011  
**Group Title:** GEN005040  
**Rule ID:** SV-37555r1\_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 zero (0).  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the umask setting for FTP users.  
  
Procedure:  
  
For gssftp:  
Assuming an anonymous ftp user has been defined with no user initialization script invoked to change the umask  
# ftp localhost  
Name: (localhost:root): anonymous  
Password: anything  
ftp>umask  
  
If the umask value returned is not 077, this is a finding.  
or:  
# grep "server\_args" /etc/xinetd.d/gssftp  
  
The default umask for FTP is "023" if the server \_args entry does not contain "-u 077" this is a finding.  
  
  
For vsftp:  
# grep "\_mask" /etc/vsftpd/vsftpd.conf  
The default "local\_umask" setting is 077. If this has been changed, or the "anon\_umask" setting is not 077, this is a finding.  
  
**Fix Text:**Edit the initialization files for the ftp user and set the umask to 077.  
  
Procedure:  
  
For gssftp:  
Modify the /etc/xinetd.d/gssftp file adding "-u 077" to the server\_args entry.  
  
For vsftp:  
Modify the "/etc/vsftpd/vsftpd.conf" setting "local\_umask" and "anon\_umask" to 077.  
  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-847  
**Group Title:** GEN005080  
**Rule ID:** SV-37560r1\_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:**    
# grep server\_args /etc/xinetd.d/tftp  
If the "-s" parameter is not specified, this is a finding.  
  
  
  
**Fix Text:**Edit /etc/xinetd.d/tftp file and specify the "-s" parameter in server\_args.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-848  
**Group Title:** GEN005100  
**Rule ID:** SV-37564r1\_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:  
# grep "server " /etc/xinetd.d/tftp  
# ls -lL <in.tftpd binary>   
  
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 <in.tftpd binary>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-849  
**Group Title:** GEN005120  
**Rule ID:** SV-37674r1\_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 someone could log on to the TFTP account and compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/passwd file to determine if TFTP is configured properly.  
  
Procedure:  
Check if TFTP if used.  
# grep disable /etc/xinetd.d/tftp  
If the file does not exist or the returned line indicates "yes", then this is not a finding.  
Otherwise, if the returned line indicates "no" then TFTP is enabled and must use a dedicated "tftp" user.  
  
# grep user /etc/xinetd.d/tftp  
If the returned line indicates a user other than the dedicated "tftp" user, this is a finding.  
  
# 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:**Configure TFTP to use a dedicated "tftp" user.  
  
Procedure:  
Create a dedicated "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.  
Edit /etc/xinetd.d/tftp to have "tftp" as the value of the "user" parameter.  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4695  
**Group Title:** GEN005140  
**Rule ID:** SV-37676r1\_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.  
# chkconfig --list | grep tftp  
  
If TFTP is found enabled ("on") and not documented using site-defined procedures, it is a finding.  
  
**Fix Text:**Document or Disable the TFTP daemon.  
  
If the TFTP daemon is necessary on the system, document and justify its usage for approval from the IAO.  
  
If the TFTP daemon is not necessary on the system, turn it off.  
  
# chkconfig tftp off  
# service xinetd restart     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-850  
**Group Title:** GEN005160  
**Rule ID:** SV-37678r1\_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 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 or .xauth files being utilized by looking for such files in the home directory of a user.  
  
Procedure:  
Verify Xwindows is used on the system.   
# egrep "^x:5.\*X11" /etc/inittab  
If no line is returned the boot process does not start Xwindows. If Xwindows is not configured to run, this rule is not applicable.   
  
Look for xauthority files in user home directory.  
# cd ~someuser  
# ls -la|egrep "(\.Xauthority|\.xauth)"  
  
If the .Xauthority or .xauth (followed by apparently random characters) files do not exist, ask the SA if the user is using Xwindows. If the user is utilizing Xwindows and none of these files 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 writing the .Xauthority file is uncommented.     
  
**CCI:**CCI-000297  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12014  
**Group Title:** GEN005180  
**Rule ID:** SV-37679r1\_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 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.  
  
Procedure:  
# ls -la |egrep "(\.Xauthority|\.xauth)"  
  
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-37682r1\_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 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. These files will be located in user home directories.  
  
Procedure:  
# ls -la ~username |egrep "(\.Xauthority|\.xauth)"  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all .Xauthority     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4697  
**Group Title:** GEN005200  
**Rule ID:** SV-37683r1\_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 Xwindows 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 able to 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-37684r1\_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 file, where "\*" is a display number 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 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-37685r1\_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-37686r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005260  
**Rule Title:**X Window System connections 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 Xorg  
  
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-37688r1\_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 e-mail 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:**    
# service uucp status  
if UUCP is "running", this is a finding.  
  
  
**Fix Text:**# chkconfig uucp off  
# service uucp stop  
# service xinetd restart     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-993  
**Group Title:** GEN005300  
**Rule ID:** SV-37689r1\_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.  
  
Procedure:  
Examine the default install location /etc/snmp/snmpd.conf  
or:  
# find / -name snmpd.conf   
# more <snmpd.conf file>   
  
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", or "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 file snmpd.conf. Edit the file. Locate the line system-group-read-community which has a default password of "public" and make the password something more secure and less guessable. Do the same for the lines reading 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-37692r1\_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:**    
Check the SNMP daemon is not configured to use the v1 or v2c security models.  
  
Procedure:  
Examine the default install location /etc/snmpd.conf  
or:  
# find / -name snmpd.conf   
  
# grep -E '(v1|v2c|community|com2sec)' <snmp.conf file> | grep -v '^#'  
If any configuration is found, this is a finding.  
  
**Fix Text:**Edit /etc/snmpd.conf and remove references to the "v1", "v2c", "community", or "com2sec".   
Restart the SNMP service.  
# service snmpd restart     
  
**CCI:**CCI-001435  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22448  
**Group Title:** GEN005306  
**Rule ID:** SV-37693r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005306  
**Rule Title:**The SNMP service must require the use of a FIPS 140-2 approved cryptographic hash algorithm as part of its authentication and integrity methods.  
  
  
**Vulnerability Discussion:**  The SNMP service must use SHA-1 or a FIPS 140-2 approved successor for authentication and integrity.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Verify the SNMP daemon uses SHA for SNMPv3 users.  
  
Procedure:  
Examine the default install location /etc/snmp/snmpd.conf  
or:  
# find / -name snmpd.conf   
  
# grep -v '^#' <snmpd.conf file> | grep -i createuser | grep -vi SHA  
If any line is present this is a finding.  
  
**Fix Text:**Edit /etc/snmp/snmpd.conf and add the SHA keyword for any create user statement without one.  
Restart the SNMP service.  
# service snmpd restart     
  
**CCI:**CCI-001453  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22449  
**Group Title:** GEN005307  
**Rule ID:** SV-37695r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005307  
**Rule Title:**The SNMP service must require the use of a FIPS 140-2 approved encryption algorithm for protecting the privacy of SNMP messages.  
  
  
**Vulnerability Discussion:**  The SNMP service must use AES or a FIPS 140-2 approved successor algorithm for protecting the privacy of communications.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Verify the SNMP daemon uses AES for SNMPv3 users.  
  
Procedure:  
Examine the default install location /etc/snmp/snmpd.conf  
or:  
# find / -name snmpd.conf   
  
  
# grep -v '^#' <snmpd.conf file> | grep -i createuser | grep -vi AES  
If any line is present this is a finding.  
  
  
**Fix Text:**Edit /etc/snmp/snmpd.conf and add the AES keyword for any create user statement without one.  
Restart the SNMP service.  
# service snmpd restart     
  
**CCI:**CCI-000068  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-994  
**Group Title:** GEN005320  
**Rule ID:** SV-37696r1\_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 file.  
  
Procedure:  
  
Examine the default install location /etc/snmp/snmpd.conf  
or:  
# find / -name snmpd.conf  
  
# ls -lL <snmpd.conf file>  
If the snmpd.conf file has 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-37698r1\_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.  
  
Procedure:  
# find / -name \*.mib   
# ls -lL <mib file>  
  
Any file returned with a mode 0640 or less permissive 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-37700r1\_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 file permissions for the MIB files.  
# find / -name \*.mib   
# ls -lL <mib file>  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all <mib file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12019  
**Group Title:** GEN005360  
**Rule ID:** SV-37703r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005360  
**Rule Title:**The snmpd.conf file must be owned by root.  
  
  
**Vulnerability Discussion:**  The snmpd.conf file contains authenticators and must be protected from unauthorized access and modification. If the file is not owned by root, it 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 file.  
  
Procedure:  
Find the snmpd.conf file. The default install location is /etc/snmp/snmpd.conf but may be different depending on the SNMP agent installed.  
  
# find / -name snmpd.conf   
# ls -lL <snmpd.conf>  
  
If the snmpd.conf file is 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-37704r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005365  
**Rule Title:**The snmpd.conf file must be group-owned by root, bin, sys, or system.  
  
  
**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 file.  
  
Procedure:  
Examine the default install location /etc/snmp/snmpd.conf  
or:  
# find / -name snmpd.conf   
  
# ls -lL <snmpd.conf>  
  
If the file is not group-owned by root, bin, sys, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group ownership of the SNMP configuration file.  
  
Procedure:  
# chgrp root <snmpd.conf>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22452  
**Group Title:** GEN005375  
**Rule ID:** SV-37706r1\_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 file.  
  
Procedure:  
Examine the default install location /etc/snmp/snmpd.conf  
or:  
# find / -name snmpd.conf   
  
# ls -lL <snmpd.conf>  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all <snmpd.conf file>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4392  
**Group Title:** GEN005380  
**Rule ID:** SV-37708r1\_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-37709r1\_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-37710r1\_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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/syslog.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4393  
**Group Title:** GEN005400  
**Rule ID:** SV-37707r1\_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-37711r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005420  
**Rule Title:**The /etc/syslog.conf file must be group-owned by root, bin, sys, or system.  
  
  
**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, bin, or system, this is a finding.  
  
  
  
**Fix Text:**Procedure:  
# chgrp root /etc/syslog.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12020  
**Group Title:** GEN005440  
**Rule ID:** SV-37810r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005440  
**Rule Title:**The system must not be used as a syslog server (loghost) for systems external to the enclave.  
  
  
**Vulnerability Discussion:**  Syslog messages are typically unencrypted, may contain sensitive information, and are restricted to the enclave.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Ask the SA if the loghost 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-37811r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005450  
**Rule Title:**The system must use a remote syslog server (loghost).  
  
  
**Vulnerability Discussion:**  A syslog server (loghost) 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-37812r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005460  
**Rule Title:**The system must only use remote syslog servers (log hosts) that is 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 "loghost", 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 or document the referenced undocumented log host.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12021  
**Group Title:** GEN005480  
**Rule ID:** SV-37813r1\_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:**    
Ask the SA if the system is an authorized syslog server. If the system is an authorized syslog server, this is not applicable.  
  
Determine if the system's syslog service is configured to accept remote messages.  
  
# ps -ef | grep syslogd  
  
If the '-r' option is present, the system is configured to accept remote syslog messages, and this is a finding.  
  
**Fix Text:**Edit /etc/sysconfig/syslog to removing the '-r' in SYSLOGD\_OPTIONS. Restart the syslogd service.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4295  
**Group Title:** GEN005500  
**Rule ID:** SV-37818r1\_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:**    
Locate the sshd\_config file:   
# more /etc/ssh/sshd\_config  
  
Examine the file. If the variables 'Protocol 2,1' or 'Protocol 1' are defined on a line without a leading comment, this is a finding.  
  
If the SSH server is F-Secure, the variable name for SSH 1 compatibility is 'Ssh1Compatibility', not 'protocol'. If the variable 'Ssh1Compatiblity' is set to 'yes', then this is a finding.   
  
  
**Fix Text:**Edit the sshd\_config file and set the "Protocol" setting to "2". If using the F-Secure SSH server, set the "Ssh1Compatibility" setting to "no".     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22456  
**Group Title:** GEN005501  
**Rule ID:** SV-37820r1\_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 not allowing versions less than 2.     
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22457  
**Group Title:** GEN005504  
**Rule ID:** SV-37823r1\_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:**    
Ask the SA to identify which interfaces on the system are designated for management traffic. If all interfaces on the system are authorized for management traffic, this is not applicable.  
  
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-37824r1\_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 the SSH daemon configuration and remove any ciphers not starting with "3des" or "aes" and remove any ciphers ending with "cbc". If necessary, add a "Ciphers" line.       
  
**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-37826r1\_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-37828r1\_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, or the returned ciphers list contains any cipher not starting with "3des" or "aes", this is a finding.  
  
  
  
**Fix Text:**Edit the SSH client configuration and remove any ciphers not starting with "3des" or "aes" and remove any ciphers ending with "cbc". If necessary, add a "Ciphers" line.       
  
**CCI:**CCI-000068  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22462  
**Group Title:** GEN005511  
**Rule ID:** SV-37830r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005511  
**Rule Title:**The SSH client must be configured to not use Cipher-Block Chaining (CBC)-based ciphers.  
  
  
**Vulnerability Discussion:**  The (CBC) mode of encryption as implemented in the SSHv2 protocol is vulnerable to chosen-plaintext 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 the SSH client configuration and remove any ciphers not starting with "3des" or "aes" and remove any ciphers ending with "cbc". If necessary, add a "Ciphers" line.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22463  
**Group Title:** GEN005512  
**Rule ID:** SV-37836r1\_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-37843r1\_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:**    
There are two ways in which access to SSH may restrict users or groups.  
  
Check if /etc/pam.d/sshd is configured to require daemon style login control.  
# grep pam\_access.so /etc/pam.d/sshd|grep "required"|grep "account"| grep -v '^#'   
If no lines are returned, sshd is not configured to use pam\_access.  
  
Check the SSH daemon configuration for the AllowGroups setting.  
# egrep -i "AllowGroups|AllowUsers" /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, sshd is not configured to limit access to users/groups.  
  
If sshd is not configured to limit access either through pam\_access or the use "AllowUsers" or "Allowgroups", this is a finding.  
  
  
  
**Fix Text:**Edit the SSH daemon configuration and add an "AllowGroups" or "AllowUsers" directive specifying the groups and users allowed to have access.  
  
Alternatively, modify the /etc/pam.d/sshd file to include the line   
  
account required pam\_access.so accessfile=<path to access.conf for sshd>  
  
If the "accessfile" option is not specified the default "access.conf" file will be used. The "access.conf" file must contain the user restriction definitions.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22471  
**Group Title:** GEN005522  
**Rule ID:** SV-37844r1\_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-37863r1\_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-37866r1\_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 GSSAPIAuthentication 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-37868r1\_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:**    
The default setting for GSSAPIAuthentication is "no" . Check for a change from the default.  
# grep -i GSSAPIAuthentication /etc/ssh/ssh\_config | grep -v '^#'  
If the setting is "yes" this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and set the GSSAPIAuthentication" directive set to "no".       
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22475  
**Group Title:** GEN005526  
**Rule ID:** SV-37872r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005526  
**Rule Title:**The SSH daemon must not permit Kerberos authentication unless needed.  
  
  
**Vulnerability Discussion:**  Kerberos authentication for SSH is often implemented using GSSAPI. If Kerberos is enabled through SSH, the SSH daemon provides a means of access to the system's Kerberos implementation. Vulnerabilities in the system's Kerberos implementation may then be subject to exploitation. To reduce the attack surface of the system, the Kerberos authentication mechanism within SSH must be disabled for systems not using this capability.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Ask the SA if Kerberos authentication is used by the system. If it is, this is not applicable.  
  
Check the SSH daemon configuration for the KerberosAuthentication setting.  
# grep -i KerberosAuthentication /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) the "KerberosAuthentication" directive set to "no".     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22485  
**Group Title:** GEN005536  
**Rule ID:** SV-37900r1\_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 not present, or not set to "yes", this is a finding.  
  
  
  
**Fix Text:**Edit the SSH daemon configuration and add or edit the "StrictModes" setting value to "yes".     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22486  
**Group Title:** GEN005537  
**Rule ID:** SV-37904r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005537  
**Rule Title:**The SSH daemon must use privilege separation.  
  
  
**Vulnerability Discussion:**  SSH daemon privilege separation causes the SSH process to drop root privileges when not needed, which would decrease the impact of software vulnerabilities in the unprivileged section.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the SSH daemon configuration for the UsePrivilegeSeparation setting.  
# grep -i UsePrivilegeSeparation /etc/ssh/sshd\_config | grep -v '^#'   
If the setting is not present, or not set to "yes", this is a finding.  
  
  
  
**Fix Text:**Edit the SSH daemon configuration and add or edit the "UsePrivilegeSeparation" setting value to "yes".     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22487  
**Group Title:** GEN005538  
**Rule ID:** SV-37905r1\_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 add or edit the "RhostsRSAAuthentication" setting value to "no".     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22488  
**Group Title:** GEN005539  
**Rule ID:** SV-37908r1\_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 | egrep "no|delayed"  
If the setting is missing or is commented out, this is a finding.  
If the setting is present but is not set to "no" or "delayed", 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-37913r1\_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:  
# grep sshd /etc/hosts.deny  
# grep sshd /etc/hosts.allow  
  
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-37915r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005550  
**Rule Title:**The SSH daemon must be configured with the Department of Defense (DoD) logon 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 either through the SSH configuration or a wrapper program such as TCP\_WRAPPERS.  
  
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.  
Procedure:  
  
An exact match is required to have a valid warning banner. Check for the following login banner.  
  
  
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.  
  
  
  
**Fix Text:**Edit /etc/issue and the DoD login 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.  
  
  
Find the location of the banner file for sshd and examine the content:  
  
# grep -i banner /etc/ssh/sshd\_config | grep -v '^#'  
# cat  
  
Edit the SSH daemon configuration and add or edit a "Banner" setting referencing a file containing a logon warning banner.     
  
**CCI:**CCI-000048  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4397  
**Group Title:** GEN005560  
**Rule ID:** SV-37918r1\_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. If the system is a VM host and acts as a router solely for the benefit of its client systems, then this rule is not applicable.  
  
Procedure:  
# netstat -r |grep default  
  
If a default route is not defined, this is a finding.  
  
  
  
**Fix Text:**Set a default gateway for IPv4.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22490  
**Group Title:** GEN005570  
**Rule ID:** SV-37921r1\_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. If the system is a VM host and acts as a router solely for the benefit of its client systems, then this rule is not applicable.  
  
# ip -6 route list | grep default  
If the system uses IPv6, and no results are returned, this is a finding.  
  
  
  
**Fix Text:**Add a default route for IPv6.  
Edit /etc/sysconfig/network-scripts/ifcfg-eth0 (substitute interface as appropriate).  
Add an IPV6\_DEFAULTGW=<gateway> configuration setting.  
Restart the interface.  
# ifdown eth0; ifup eth0     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4398  
**Group Title:** GEN005580  
**Rule ID:** SV-37924r1\_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:**    
If the system is a VM host and acts as a router solely for the benefit of its client systems, then this rule is not applicable.  
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-37926r1\_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. If the system is a VM host and acts as a router solely for the benefits of its client systems, then this rule is not applicable.  
  
# chkconfig --list |grep :on|egrep '(ospf|route|bgp|zebra|quagga)'  
If any routing protocol daemons are listed, this is a finding.  
  
**Fix Text:**Disable any routing protocol daemons.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12023  
**Group Title:** GEN005600  
**Rule ID:** SV-37929r1\_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:**    
Check if the system is configured for IPv4 forwarding. If the system is a VM host and acts as a router solely for the benefits of its client systems, then this rule is not applicable.  
  
Procedure:  
# cat /proc/sys/net/ipv4/ip\_forward  
  
If the value is set to "1", IPv4 forwarding is enabled this is a finding.  
  
  
  
**Fix Text:**Edit "/etc/sysctl.conf" and set net.ipv4.ip\_forward to "0". Restart the system or run "sysctl -p" to make the change take effect.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22491  
**Group Title:** GEN005610  
**Rule ID:** SV-37930r1\_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.  
  
# grep [01] /proc/sys/net/ipv6/conf/\*/forwarding|egrep "default|all"  
  
If all of the resulting lines do not end with 0, this is a finding.  
  
  
  
**Fix Text:**Disable IPv6 forwarding.  
  
Edit /etc/sysctl.conf and add a setting for "net.ipv6.conf.all.forwarding=0" and "net.ipv6.conf.default.forwarding=0".  
  
Reload the sysctls.  
Procedure:  
# sysctl -p     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-928  
**Group Title:** GEN005740  
**Rule ID:** SV-37936r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005740  
**Rule Title:**The Network File System (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 owner of the exports file.  
  
Example:  
# ls -lL /etc/exports  
  
If the export configuration file is not owned by root, this is a finding.  
  
  
  
**Fix Text:**Change the owner of the exports file to root.  
  
Example:  
# chown root /etc/exports     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22492  
**Group Title:** GEN005750  
**Rule ID:** SV-37940r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005750  
**Rule Title:**The Network File System (NFS) export configuration file must be group-owned by root, bin, sys, or system.  
  
  
**Vulnerability Discussion:**  Failure to give group-ownership of the NFS export configuration file to root or a system group 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/exports  
  
If the file is not group-owned by root, bin, sys, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group ownership of the NFS export configuration file.  
  
Procedure:  
# chgrp root /etc/exports     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-929  
**Group Title:** GEN005760  
**Rule ID:** SV-37943r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005760  
**Rule Title:**The Network File System (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/exports  
If the file has a mode more permissive than 0644, this is a finding.  
  
  
  
**Fix Text:**# chmod 0644 /etc/exports     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22493  
**Group Title:** GEN005770  
**Rule ID:** SV-37947r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005770  
**Rule Title:**The Network File System (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 permissions of the NFS export configuration file.  
# ls -lL /etc/exports  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/exports     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-931  
**Group Title:** GEN005800  
**Rule ID:** SV-37849r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005800  
**Rule Title:**All Network File System (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:  
# cat /etc/exports  
For each file system displayed, check the ownership.  
  
# 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-37851r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005810  
**Rule Title:**All Network File System (NFS) exported system files and system directories must be group-owned by root, bin, sys, or system.  
  
  
**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/exports  
For each file system displayed, check the ownership.  
  
# ls -ldL <exported file system path>  
  
If the directory is not group-owned by root, bin, sys, or system, 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-37854r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005820  
**Rule Title:**The Network File System (NFS) anonymous UID and GID must be configured to values without 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 'anonuid' and 'anongid' options are set correctly for exported file systems.  
List exported filesystems:  
# exportfs -v   
  
Each of the exported file systems should include an entry for the 'anonuid=' and 'anongid=' options set to "-1" or an equivalent (60001, 65534, or 65535). If appropriate values for 'anonuid' or 'anongid' are not set, this is a finding.  
  
**Fix Text:**Edit "/etc/exports" and set the "anonuid=-1" and "anongid=-1" options for exports lacking it. Re-export the filesystems.     
  
**CCI:**CCI-000062  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-933  
**Group Title:** GEN005840  
**Rule ID:** SV-37857r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005840  
**Rule Title:**The Network File System (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  
  
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/exports 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-935  
**Group Title:** GEN005880  
**Rule ID:** SV-37859r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005880  
**Rule Title:**The Network File System (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:**    
List the exports.  
# cat /etc/exports  
If any export contains "no\_root\_squash" or does not contain "root\_squash" or "all\_squash", this is a finding.  
  
  
  
**Fix Text:**Edit the "/etc/exports" file and add "root\_squash" (or "all\_squash") and remove "no\_root\_squash".  
    
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-936  
**Group Title:** GEN005900  
**Rule ID:** SV-37860r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005900  
**Rule Title:**The "nosuid" option must be enabled on all Network File System (NFS) client mounts.  
  
  
**Vulnerability Discussion:**  Enabling the nosuid mount option prevents the system from granting owner or group-owner privileges to programs with the suid or sgid 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 suid or sgid 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 " | egrep -v "nosuid"  
  
If the mounted file systems do not have the "nosuid" option, this is a finding.  
  
  
  
**Fix Text:**Edit "/etc/fstab" 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-37862r1\_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 (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 e-mail 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 use 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-37865r1\_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  
-BitTorrent  
  
**Responsibility:**  System Administrator  
**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  
- 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-37867r1\_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 samba package should also be removed or not installed if there is no functional requirement.  
  
Procedure:  
rpm -qa |grep samba  
  
This will show whether "samba" or "samba3x" is installed. To remove:  
  
rpm --erase samba  
or  
rpm --erase samba3x  
    
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1026  
**Group Title:** GEN006080  
**Rule ID:** SV-37870r1\_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. It modifies Samba configuration, which can impact system security, and 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:**    
SWAT is a tool for configuring Samba and should only be found on a system with a requirement for Samba. If SWAT is used, it must be utilized with SSL to ensure a secure connection between the client and the server.  
  
Procedure:  
  
# grep -H "bin/swat" /etc/xinetd.d/\*|cut -d: -f1 |xargs grep "only\_from"  
  
If the value of the "only\_from" line in the "xinetd.d" file which starts "/usr/sbin/swat" is not "localhost" or the equivalent, this is a finding.  
  
**Fix Text:**Disable SWAT or require SWAT is only accessed via SSH.  
  
Procedure:  
If SWAT is not needed for operation of the system remove the SWAT package:  
# rpm -qa|grep swat  
  
Remove "samba-swat" or "samba3x-swat" depending on which one is installed  
# rpm --erase samba-swat  
or  
# rpm --erase samba3x-swat  
  
If SWAT is required but not at all times disable it when it is not needed.  
Modify the /etc/xinetd.d file for "swat" to contain a "disable = yes" line.  
  
To access using SSH:  
Follow vendor configuration documentation to create an stunnel for SWAT.  
  
    
  
**CCI:**CCI-001436  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1027  
**Group Title:** GEN006100  
**Rule ID:** SV-37871r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006100  
**Rule Title:**The /etc/smb.conf file must be owned by root.  
  
  
**Vulnerability Discussion:**  The /etc/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/samba/smb.conf file.  
  
Procedure:  
# ls -l /etc/samba/smb.conf  
If an 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 smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1056  
**Group Title:** GEN006120  
**Rule ID:** SV-37873r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006120  
**Rule Title:**The /etc/smb.conf file must be group-owned by root, bin, sys, or system.  
  
  
**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 -lL /etc/samba/smb.conf  
  
If the "smb.conf" file is not group-owned by root, bin, sys, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group owner of the smb.conf file.  
  
Procedure:  
# chgrp root smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1028  
**Group Title:** GEN006140  
**Rule ID:** SV-37875r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006140  
**Rule Title:**The /etc/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/samba/smb.conf  
  
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 smb.conf.     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22497  
**Group Title:** GEN006150  
**Rule ID:** SV-37877r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006150  
**Rule Title:**The /etc/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 permissions of the Samba configuration file.  
# ls -lL /etc/samba/smb.conf  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/samba/smb.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1029  
**Group Title:** GEN006160  
**Rule ID:** SV-37879r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006160  
**Rule Title:**The /etc/smbpasswd file must be owned by root.  
  
  
**Vulnerability Discussion:**  If the "smbpasswd" file is not owned by root, it 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 -l /etc/samba/passdb.tdb /etc/samba/secrets.tdb  
  
If the "smbpasswd" file is not owned by root, this is a finding.  
  
  
  
**Fix Text:**Use the chown command to configure the files maintained by smbpasswd.  
For instance:  
# chown root /etc/samba/passdb.tdb /etc/samba/secrets.tdb     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1058  
**Group Title:** GEN006180  
**Rule ID:** SV-41574r1\_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/samba/passdb.tdb /etc/samba/secrets.tdb  
  
If the "smbpasswd" file is not group-owned by root, this is a finding.  
  
**Fix Text:**Use the chgrp command to ensure that the group owner of the smbpasswd file is root.  
  
For instance:  
  
# chgrp root /etc/samba/passdb.tdb /etc/samba/secrets.tdb     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1059  
**Group Title:** GEN006200  
**Rule ID:** SV-41575r1\_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 the mode of files maintained using "smbpasswd".  
  
Procedure:  
# ls -lL /etc/samba/passdb.tdb /etc/samba/secrets.tdb  
  
If a "smbpasswd" maintained file has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the files maintained through smbpasswd to 0600.  
  
Procedure:  
# chmod 0600 /etc/samba/passdb.tdb /etc/samba/secrets.tdb     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22498  
**Group Title:** GEN006210  
**Rule ID:** SV-37884r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006210  
**Rule Title:**The /etc/smbpasswd file must not have an extended ACL.  
  
  
**Vulnerability Discussion:**  If the permissions of the "smbpasswd" file are too permissive, it may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the Samba password files.  
  
Procedure:  
# ls -lL /etc/samba/passdb.tdb /etc/samba/secrets.tdb  
  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/samba/passdb.tdb /etc/samba/secrets.tdb     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1030  
**Group Title:** GEN006220  
**Rule ID:** SV-37887r1\_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/samba/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 "/etc/samba/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-37891r1\_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/samba/smb.conf   
If the security mode is "share", this is a finding.  
  
  
**Fix Text:**Edit the "/etc/samba/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-37894r1\_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 Samba.  
# grep -i 'encrypt passwords' /etc/samba/smb.conf   
If the setting is not present, or not set to 'yes', this is a finding.  
  
  
  
**Fix Text:**Edit the "/etc/samba/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-37896r1\_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 access to shares for Samba.  
# grep -i 'guest ok' /etc/samba/smb.conf   
If the setting exists and is set to 'yes', this is a finding.  
  
  
  
**Fix Text:**Edit the "/etc/samba/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-37899r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006240  
**Rule Title:**The system must not run an Internet Network News (INN) server.  
  
  
**Vulnerability Discussion:**  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:**  Information Assurance Officer  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# ps -ef | egrep "innd|nntpd"  
  
If an Internet Network News 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-37901r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006260  
**Rule Title:**The /etc/news/incoming.conf (or equivalent) must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the "incoming.conf" 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:**    
RHEL uses the InternetNewsDaemon (innd) news server. The file corresponding to "/etc/news/hosts.nntp" is "/etc/news/incoming.conf". Check the permissions for "/etc/news/incoming.conf".  
  
# ls -lL /etc/news/incoming.conf  
  
If "/etc/news/incoming.conf" has a mode more permissive than 0600, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the "/etc/news/incoming.conf" file to 0600.  
  
# chmod 0600 /etc/news/incoming.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22502  
**Group Title:** GEN006270  
**Rule ID:** SV-37902r1\_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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/news/hosts.nntp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4274  
**Group Title:** GEN006280  
**Rule ID:** SV-37712r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006280  
**Rule Title:**The /etc/news/infeed.conf (or equivalent) must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the "" 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:**    
RHEL uses the InternetNewsDaemon (innd) news server. The file that corresponds to "/etc/news/hosts.nntp.nolimit" is "/etc/news/infeed.conf". Check the permissions for "/etc/news/infeed.conf".  
  
# ls -lL /etc/news/infeed.conf  
  
If "/etc/news/infeed.conf" has a mode more permissive than 0600, this is a finding.  
  
  
  
**Fix Text:**Change the mode of "/etc/news/infeed.conf" to 0600.  
# chmod 0600 /etc/news/infeed.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22503  
**Group Title:** GEN006290  
**Rule ID:** SV-37713r1\_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 for "/etc/news/hosts.nntp.nolimit".  
  
# ls -lL /etc/news/hosts.nntp.nolimit  
If the permissions include a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/news/hosts.nntp.nolimit     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4275  
**Group Title:** GEN006300  
**Rule ID:** SV-37714r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006300  
**Rule Title:**The /etc/news/readers.conf (or equivalent) must have mode 0600 or less permissive.  
  
  
**Vulnerability Discussion:**  Excessive permissions on the readers.conf 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 for "/etc/news/readers.conf".  
  
# ls -lL /etc/news/readers.conf  
  
If /etc/news/readers.conf has a mode more permissive than 0600, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the /etc/news/readers.conf file to 0600.  
# chmod 0600 /etc/news/readers.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22504  
**Group Title:** GEN006310  
**Rule ID:** SV-37730r1\_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. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/news/nnrp.access     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4276  
**Group Title:** GEN006320  
**Rule ID:** SV-37731r1\_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-37733r1\_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 mode includes a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the file.  
# setfacl --remove-all /etc/news/passwd.nntp     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4277  
**Group Title:** GEN006340  
**Rule ID:** SV-37735r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006340  
**Rule Title:**Files in /etc/news must be owned by root or news.  
  
  
**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 any files are not owned by root or news, this is a finding.  
  
  
  
**Fix Text:**Change the ownership of the files in "/etc/news" to root or news.  
  
Procedure:  
# chown root /etc/news/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4278  
**Group Title:** GEN006360  
**Rule ID:** SV-37737r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006360  
**Rule Title:**The files in /etc/news must be group-owned by root or news.  
  
  
**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" files group ownership:  
  
Procedure:  
# ls -al /etc/news  
  
If "/etc/news" files are not group-owned by root or news, this is a finding.  
  
  
  
**Fix Text:**Change the group-owner of the files in "/etc/news" to root or news.  
  
Procedure:  
# chgrp root /etc/news/\*     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4399  
**Group Title:** GEN006380  
**Rule ID:** SV-37739r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN006380  
**Rule Title:**The system must not use UDP for NIS/NIS+.  
  
  
**Vulnerability Discussion:**  Implementing Network Information Service (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-37742r1\_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 | grep ypbind  
  
If NIS is found active on the system, this is a finding.  
  
  
**Fix Text:**Disable the use of NIS/NIS+. Use as a replacement Kerberos or LDAP.     
  
**CCI:**CCI-001435  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12026  
**Group Title:** GEN006420  
**Rule ID:** SV-37743r1\_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.  
  
If the system does not use NIS, this is not applicable.  
  
**Fix Text:**Change the NIS domainname to a value difficult to guess. Consult vendor documentation for the required procedure.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-782  
**Group Title:** GEN006480  
**Rule ID:** SV-37746r1\_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:**    
Ask the SA or IAO if a host-based intrusion detection application is loaded on the system. The preferred intrusion detection system is McAfee HBSS available through Cybercom.   
  
Procedure:  
Examine the system to see if the Host Intrusion Prevention System (HIPS) is installed  
  
#rpm -qa | grep MFEhiplsm  
  
If the MFEhiplsm package is installed, HBSS is being used on the system.  
  
If another host-based intrusion detection system is loaded on the system  
  
# find / -name <daemon name>   
  
Where <daemon name> is the name of the primary application daemon to determine if the application is loaded on the system.   
  
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-37747r1\_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 e-mail or paging) should be employed consistent with the site’s established operations management systems and procedures.  
  
**Responsibility:**  System Administrator  
**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-37751r1\_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) and the global crontabs in "/etc/crontab", "/etc/cron.\*" for the presence of an rpm verification command such as:  
rpm -qVa | awk '$2!="c" {print $0}'  
If no such cron job is found, this is a finding.  
If the result of the cron job indicates packages which do not pass verification exist, this is a finding.  
  
  
  
**Fix Text:**Add a cron job to run an rpm verification command such as:  
rpm -qVa | awk '$2!="c" {print $0}'  
  
For packages which failed verification:  
If the package is not necessary for operations, remove it from the system.  
  
If the package is necessary for operations, re-install the package.     
  
**CCI:**CCI-000366  
  
  
**CCI:**CCI-000698  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22507  
**Group Title:** GEN006570  
**Rule ID:** SV-37752r1\_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 an Advanced Intrusion Detection Environment (AIDE), verify that the configuration contains the "ACL" option for all monitored files and directories.  
  
Procedure:  
Check for the default location /etc/aide/aide.conf  
or:  
# find / -name aide.conf  
  
# egrep "[+]?acl" <aide.conf file>  
If the 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-37753r1\_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 an Advanced Intrusion Detection Environment (AIDE), verify the configuration contains the "xattrs" option for all monitored files and directories.  
  
Procedure:  
Check for the default location /etc/aide/aide.conf  
or:  
# find / -name aide.conf  
  
# egrep "[+]?xattrs" <aide.conf file>  
If the 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-37754r1\_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 an Advanced Intrusion Detection Environment (AIDE), verify the configuration contains the "sha256" or "sha512" options for all monitored files and directories.  
  
Procedure:  
Check for the default location /etc/aide/aide.conf  
or:  
# find / -name aide.conf  
  
# egrep "[+]?(sha256|sha512)" <aide.conf file>  
If the option is not present. This is a finding.  
If one of these options 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 "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-37756r1\_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:**    
The tcp\_wrappers package is provided with the RHEL distribution. Other access control programs may be available but will need to be checked manually.   
  
Determine if tcp\_wrappers is installed.  
# rpm -qa | grep tcp\_wrappers  
If no package is listed, this is a finding.  
  
  
  
**Fix Text:**Install and configure the tcp\_wrappers package.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-941  
**Group Title:** GEN006600  
**Rule ID:** SV-37757r1\_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:**    
The tcp\_wrappers package is provided with the RHEL distribution. Other access control programs may be available but will need to be checked manually.  
  
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  
authpriv.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 this is a finding.  
  
If an alternate access control program is used and it does not provide logging of access attempts, 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 recorded to 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-37758r1\_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 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.all" and "/etc/hosts.deny" files to configure access restrictions.  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12765  
**Group Title:** GEN006640  
**Rule ID:** SV-37760r1\_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.   
  
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 a cron job to execute the McAfee command line scan tool (uvscan) daily. Other tools may be available but will have to be manually reviewed if they are installed. In addition, the definitions files should not be older than 7 days.   
  
Check if uvscan scheduled to run:  
# grep uvscan /var/spool/cron/\*  
# grep uvscan /etc/cron.d/\*  
# grep uvscan /etc/cron.daily/\*  
# grep uvscan /etc/cron.hourly/\*  
# grep uvscan /etc/cron.monthly/\*  
# grep uvscan /etc/cron.weekly/\*  
  
If a virus scanner is not being run daily and an exception has not been documented with the IAO, this is a finding.  
  
Perform the following command to ensure the virus definition signature files are not older than 7 days.  
The default uvscan install directory is /usr/local/uvscan.  
  
# cd <uvscan install directory>  
# ls -la avvscan.dat avvnames.dat avvclean.dat  
  
If the virus definitions are older than 7 days, this is a finding.  
  
  
  
**Fix Text:**Install McAfee command line virus scan tool, or an appropriate alternative. Ensure the virus signature definition files are no older than 7 days. Configure the system to run a virus scan on altered files dynamically or daily. If daily scans impede operations, justify, document, and obtain IAO approval for alternate scheduling.     
  
**CCI:**CCI-001668  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22511  
**Group Title:** GEN007020  
**Rule ID:** SV-37761r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007020  
**Rule Title:**The Stream Control Transmission Protocol (SCTP) must be disabled unless required.  
  
  
**Vulnerability Discussion:**  The Stream Control Transmission Protocol (SCTP) is an Internet Engineering Task Force (IETF)-standardized transport layer protocol. This protocol is not yet widely used. 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:**    
Verify the SCTP protocol handler is prevented from dynamic loading.  
# grep 'install sctp /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no result is returned, this is a finding.  
  
  
  
**Fix Text:**Prevent the SCTP protocol handler for dynamic loading.  
# echo "install sctp /bin/true" >> /etc/modprobe.conf     
  
**CCI:**CCI-000382  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22514  
**Group Title:** GEN007080  
**Rule ID:** SV-37763r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007080  
**Rule Title:**The Datagram Congestion Control Protocol (DCCP) must be disabled unless required.  
  
  
**Vulnerability Discussion:**  The DCCP is a proposed transport layer protocol. This protocol is not yet widely used. 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:**    
Verify the DCCP protocol handler is prevented from dynamic loading.  
# grep 'install dccp /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no result is returned, this is a finding.  
# grep 'install dccp\_ipv4 /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no result is returned, this is a finding.  
# grep 'install dccp\_ipv6 /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no result is returned, this is a finding.  
  
  
  
**Fix Text:**Prevent the DCCP protocol handler for dynamic loading.  
# echo "install dccp /bin/true" >> /etc/modprobe.conf  
# echo "install dccp\_ipv4 /bin/true" >> /etc/modprobe.conf  
# echo "install dccp\_ipv6 /bin/true" >> /etc/modprobe.conf     
  
**CCI:**CCI-000382  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22524  
**Group Title:** GEN007260  
**Rule ID:** SV-26887r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007260  
**Rule Title:**The AppleTalk protocol must be disabled or not installed.  
  
  
**Vulnerability Discussion:**  The AppleTalk suite of protocols is no longer in common use. 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:**    
Verify the AppleTalk protocol handler is prevented from dynamic loading.  
# grep 'install appletalk' /etc/modprobe.conf /etc/modprobe.d/\*  
If anything is returned check that appletalk is disabled by having the executable set to '/bin/true'. If an uncommented line containing "appletalk" is found which has not been disabled, this is a finding.  
  
**Fix Text:**Prevent the AppleTalk protocol handler for dynamic loading.  
# echo "install appletalk /bin/true" >> /etc/modprobe.conf     
  
**CCI:**CCI-000382  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22530  
**Group Title:** GEN007480  
**Rule ID:** SV-37603r1\_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 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 prevented from dynamic loading.  
# grep 'install rds /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no result is returned, this is a finding.  
  
  
  
**Fix Text:**Prevent the RDS protocol handler for dynamic loading.  
# echo "install rds /bin/true" >> /etc/modprobe.conf     
  
**CCI:**CCI-000382  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22533  
**Group Title:** GEN007540  
**Rule ID:** SV-37604r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007540  
**Rule Title:**The Transparent Inter-Process Communication (TIPC) protocol must be disabled or uninstalled.  
  
  
**Vulnerability Discussion:**  The 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 system 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 is prevented from dynamic loading.  
# grep 'install tipc /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no result is returned, this is a finding.  
  
  
**Fix Text:**Prevent the TIPC protocol handler for dynamic loading.  
# echo "install tipc /bin/true" >> /etc/modprobe.conf     
  
**CCI:**CCI-000382  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22539  
**Group Title:** GEN007660  
**Rule ID:** SV-37605r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007660  
**Rule Title:**The Bluetooth protocol handler must be disabled or not installed.  
  
  
**Vulnerability Discussion:**  Bluetooth is a Personal Area Network (PAN) technology. 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 Bluetooth protocol handler is prevented from dynamic loading.  
# grep 'install bluetooth /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no result is returned, this is a finding.  
  
  
  
**Fix Text:**Prevent the Bluetooth protocol handler for dynamic loading.  
# echo "install bluetooth /bin/true" >> /etc/modprobe.conf     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22541  
**Group Title:** GEN007700  
**Rule ID:** SV-37606r1\_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:**    
If the IPv6 protocol handler is bound to the network stack, and the system does not need IPv6, this is a finding.  
  
# grep NETWORKING\_IPV6 /etc/sysconfig/network  
If the line is set to "yes", this is a finding.  
  
**Fix Text:**Remove the capability to use IPv6 protocol handler.  
  
Procedure:  
Edit /etc/sysconfig/network and change  
NETWORKING\_IPV6=yes  
to  
NETWORKING\_IPV6=no  
  
Edit /etc/modprobe.conf and add these lines (if they are not in it):  
alias net-pf-10 off  
alias ipv6 off  
  
Stop the ipv6tables service by typing:  
service ip6tables stop  
  
Disable the ipv6tables service by typing:  
chkconfig ip6tables off  
  
Remove the ipv6 kernel module  
# rmmod ipv6  
  
Reboot  
    
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22542  
**Group Title:** GEN007720  
**Rule ID:** SV-37609r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007720  
**Rule Title:**The IPv6 protocol handler must be prevented from dynamic loading unless needed.  
  
  
**Vulnerability Discussion:**  IPv6 is the next generation of the Internet protocol. 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:**    
If this system uses IPv6, this is not applicable.  
  
Verify the IPv6 protocol handler is prevented from dynamic loading.  
# grep 'install ipv6 /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no result is returned, this is a finding.  
  
  
  
**Fix Text:**Prevent the IPv6 protocol handler for dynamic loading.  
# echo "install ipv6 /bin/true" >> /etc/modprobe.conf     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22545  
**Group Title:** GEN007780  
**Rule ID:** SV-37610r1\_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 involving 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:**    
Check the system for any active 6to4 tunnels without specific remote addresses.  
# ip tun list | grep "remote any" | grep "ipv6/ip"  
If any results are returned the "tunnel" is the first field.  
If any results are returned, this is a finding.  
  
  
  
**Fix Text:**Disable the active 6to4 tunnel.  
# ip link set <tunnel> down  
Add this command to a startup script, or remove the configuration creating the tunnel.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22546  
**Group Title:** GEN007800  
**Rule ID:** SV-37611r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007800  
**Rule Title:**The system must not have Teredo enabled.  
  
  
**Vulnerability Discussion:**  Teredo is an IPv6 transition mechanism involving tunneling IPv6 packets encapsulated in IPv4 packets. Unauthorized tunneling may circumvent network security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the Miredo service is not running.  
# ps ax | grep miredo | grep -v grep  
If the miredo process is running, this is a finding.  
  
  
  
**Fix Text:**Edit startup scripts to prevent the service from running on startup.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22547  
**Group Title:** GEN007820  
**Rule ID:** SV-37613r1\_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.  
# ip tun list  
# ip -6 tun list  
If any tunnels are listed, this is a finding.  
  
  
  
**Fix Text:**Remove the tunnels.  
# ip tun del <tunnel>  
Edit system startup scripts to prevent tunnel creation on startup.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22548  
**Group Title:** GEN007840  
**Rule ID:** SV-37615r1\_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.  
# grep -i bootproto=dhcp /etc/sysconfig/network-scripts/ifcfg-\*  
If any configuration is found, this is a finding.  
  
  
  
**Fix Text:**Edit the "/etc/sysconfig/network-scripts/ifcfg-\*" file(s) and change the "bootproto" setting to "static".     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22549  
**Group Title:** GEN007850  
**Rule ID:** SV-26933r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007850  
**Rule Title:**The DHCP client must not send dynamic DNS updates.  
  
  
**Vulnerability Discussion:**  Dynamic DNS updates transmit unencrypted information about a system including its name and address and should not be used unless needed.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the DHCP client is configured to not send dynamic DNS updates.  
  
Procedure:  
# grep do-forward-updates /etc/dhclient.conf  
  
If the file is not present, does not contain this configuration, or has the setting set to "true", this is a finding.  
  
**Fix Text:**Edit or add the "/etc/dhclient.conf" file and add or edit the "do-forward-updates" setting to false.  
  
Procedure:  
# echo "do-forward-updates false;" >> /etc/dhclient.conf     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22550  
**Group Title:** GEN007860  
**Rule ID:** SV-37616r1\_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.  
# cat /proc/sys/net/ipv6/conf/all/accept\_redirects  
If the returned value is not "0", this is a finding.  
  
  
  
**Fix Text:**Configure the system to ignore IPv6 ICMP redirect messages.  
Edit "/etc/sysctl.conf" and add a settings for "net.ipv6.conf.default.accept\_redirects=0" and "net.ipv6.conf.all.accept\_redirects=0".   
Restart the system for the setting to take effect.     
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22553  
**Group Title:** GEN007920  
**Rule ID:** SV-37618r1\_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:**    
Determine if the system is configured to forward IPv6 source-routed packets.  
  
Procedure:  
# egrep "net.ipv6.conf.\*forwarding" /etc/sysctl.conf  
If there are no entries found or the value of the entries is not = "0", this is a finding.  
  
  
  
**Fix Text:**Configure the system to not forward IPv6 source-routed packets.  
  
Procedure:  
Edit the /etc/sysctl.conf file to include:  
net.ipv6.conf.all.forwarding = 0  
net.ipv6.conf.default.forwarding = 0  
  
Reload the kernel parameters:  
# sysctl -p  
  
    
  
**CCI:**CCI-001551  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23972  
**Group Title:** GEN007950  
**Rule ID:** SV-29788r1\_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:**    
Check for an iptables rule that drops inbound IPv6 ICMP ECHO\_REQUESTs sent to the all-hosts multicast address.  
  
Procedure:  
# less /etc/sysconfig/ip6tables  
  
Check for a rule in, or referenced by, the INPUT chain such as:  
-A INPUT -p icmpv6 -d ff02::1 --icmpv6-type 128 -j DROP  
  
If such a rule does not exist, this is a finding.  
  
**Fix Text:**Add an iptables rule that drops inbound IPv6 ICMP ECHO\_REQUESTs sent to the all-hosts multicast address.  
  
Edit /etc/sysconfig/ip6tables and add a rule in, or referenced by, the INPUT chain such as:  
-A INPUT -p icmpv6 -d ff02::1 --icmpv6-type 128 -j DROP  
  
Reload the iptables rules.  
Procedure:  
# service ip6tables restart     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23953  
**Group Title:** GEN007960  
**Rule ID:** SV-37621r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007960  
**Rule Title:**The 'ldd' command must be disabled unless it protects against the execution of untrusted files.  
  
  
**Vulnerability Discussion:**  The 'ldd' command provides a list of dependent libraries needed by a given binary, which is useful for troubleshooting software. Instead of parsing the binary file, some 'ldd' implementations invoke the program with a special environment variable set, which causes the system dynamic linker to display the list of libraries. Specially crafted binaries can specify an alternate dynamic linker which may cause a program to be executed instead of examined. If the program is from an untrusted source, such as in a user home directory, or a file suspected of involvement in a system compromise, unauthorized software may be executed with the rights of the user running 'ldd'.   
  
Some 'ldd' implementations include protections that prevent the execution of untrusted files. If such protections exist, this requirement is not applicable.  
  
An acceptable method of disabling 'ldd' is changing its mode to 0000. The SA may conduct troubleshooting by temporarily changing the mode to allow execution and running the 'ldd' command as an unprivileged user upon trusted system binaries.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for the 'ldd' executable.  
  
Procedure:  
# ls -lL /usr/bin/ldd  
  
If the returned line is set to "yes", this is a finding.  
  
  
**Fix Text:**Remove the execute permissions from the 'ldd' executable.  
  
Procedure:  
# chmod a-x /usr/bin/ldd     
  
**CCI:**CCI-000305  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22555  
**Group Title:** GEN007980  
**Rule ID:** SV-37627r1\_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.  
Check if NSS LDAP is using TLS.  
# grep '^ssl start\_tls' /etc/ldap.conf  
If no lines are returned, this is a finding.  
Check if NSS LDAP TLS is using only FIPS 140-2 approved cryptographic algorithms.  
# grep '^tls\_ciphers' /etc/ldap.conf  
If the line is not present, or contains ciphers not approved by FIPS 140-2, this is a finding. FIPS approved ciphers include 3DES and AES. FIPS approved hashes include the SHA hash family.  
  
**Fix Text:**Edit "/etc/ldap.conf" and add a "ssl start\_tls" and "tls\_ciphers" options with only FIPS 140-2 approved ciphers.     
  
**CCI:**CCI-001453  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22556  
**Group Title:** GEN008000  
**Rule ID:** SV-37631r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008000  
**Rule Title:**If the system is using LDAP for authentication or account information, certificates used to authenticate to the LDAP server must be provided from DoD PKI or a DoD-approved external PKI.  
  
  
**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 authentication.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Verify the source of the LDAP certificates  
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 with the SA that the system is connected to the GIG.  
If the system part of a stand alone network which is not connected to the GIG this vulnerability is not applicable.  
  
Verify a certificate is used for client authentication to the server.  
# grep -i '^tls\_cert' /etc/ldap.conf  
If no line is found, this is a finding.  
  
List the certificate issuer.  
# openssl x509 -text -in <cert>  
If the certificate is not issued by DoD PKI or a DoD-approved external PKI, this is a finding.  
  
  
  
**Fix Text:**Edit "/etc/ldap.conf" and add or edit the 'tls\_cert' setting to reference a file containing a client certificate issued by DoD PKI or a DoD-approved external PKI.     
  
**CCI:**CCI-000185  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22557  
**Group Title:** GEN008020  
**Rule ID:** SV-37632r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008020  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP TLS connection must require the server provide a certificate with a valid trust path to a trusted CA.  
  
  
**Vulnerability Discussion:**  The NSS LDAP service provides user mappings which are a vital component of system security. Communication between an LDAP server and a host using LDAP for NSS require authentication.  
  
**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 a server certificate is required and verified by the NSS LDAP configuration.  
# grep -i '^tls\_checkpeer' /etc/ldap.conf  
If no line is returned, or the value is not "yes", this is a finding.  
  
  
  
**Fix Text:**Edit "/etc/ldap.conf" and add or set the "tls\_checkpeer" setting to "yes".     
  
**CCI:**CCI-000185  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22558  
**Group Title:** GEN008040  
**Rule ID:** SV-37634r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008040  
**Rule Title:**If the system is using LDAP for authentication or account information, the system must verify the LDAP server's certificate has not been revoked.  
  
  
**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 authentication.  
  
**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 the NSS LDAP client is configured to check certificates against a certificate revocation list.  
# grep -i '^tls\_crlcheck' /etc/ldap.conf  
If the setting does not exist, or the value is not "all", this is a finding.  
  
  
  
**Fix Text:**Edit "/etc/ldap.conf" and add or set the "tls\_crlcheck" setting to "all".     
  
**CCI:**CCI-000185  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24384  
**Group Title:** GEN008050  
**Rule ID:** SV-37643r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008050  
**Rule Title:**If the system is using LDAP for authentication or account information, the /etc/ldap.conf file (or equivalent) must not contain passwords.  
  
  
**Vulnerability Discussion:**  The authentication of automated LDAP connections between systems must not use passwords since more secure methods are available, such as PKI and Kerberos. Additionally, the storage of unencrypted passwords on the system is not permitted.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check for the "bindpw" option being used in the "/etc/ldap.conf" file.  
  
# grep bindpw /etc/ldap.conf  
If an uncommented "bindpw" option is returned then a cleartext password is in the file, this is a finding.  
  
  
  
**Fix Text:**Edit the "/etc/ldap.conf" file to use anonymous binding by removing the "bindpw" option.     
  
**CCI:**CCI-000196  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22559  
**Group Title:** GEN008060  
**Rule ID:** SV-37951r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008060  
**Rule Title:**If the system is using LDAP for authentication or account information the /etc/ldap.conf (or equivalent) file must have mode 0644 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 the permissions of the file.  
# ls -lL /etc/ldap.conf  
If the mode of the file is more permissive than 0644, this is a finding.  
  
  
**Fix Text:**Change the permissions of the file.  
# chmod 0644 /etc/ldap.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22560  
**Group Title:** GEN008080  
**Rule ID:** SV-37953r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008080  
**Rule Title:**If the system is using LDAP for authentication or account information, the /etc/ldap.conf (or equivalent) 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:**    
Check the ownership of the file.  
# ls -lL /etc/ldap.conf  
If the file is not owned by root, this is a finding.  
  
  
  
**Fix Text:**Change the owner of the file.  
# chown root /etc/ldap.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22561  
**Group Title:** GEN008100  
**Rule ID:** SV-37955r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008100  
**Rule Title:**If the system is using LDAP for authentication or account information, the /etc/ldap.conf (or equivalent) file must be group-owned by root, bin, sys, or system.  
  
  
**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 file.  
  
Procedure:  
# ls -lL /etc/ldap.conf  
  
If the file is not group-owned by root, bin, sys, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group owner of the file to root, bin, sys, or system.  
  
Procedure:  
# chgrp root /etc/ldap.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22562  
**Group Title:** GEN008120  
**Rule ID:** SV-37956r1\_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:**    
Check the permissions of the file.  
# ls -lL /etc/ldap.conf  
If the mode includes a '+', the file has an extended ACL. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the "/etc/ldap.conf" file.  
# setfacl --remove-all /etc/ldap.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22563  
**Group Title:** GEN008140  
**Rule ID:** SV-37959r1\_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:**    
Determine if LDAP is used for account information on the system.  
# grep -i ldap /etc/nsswitch.conf  
If no un-commented reference to "ldap" is identified, LDAP is not used for account information on the system and this is not applicable.  
  
Determine the certificate authority file and/or directory.  
# grep -i '^tls\_cacert' /etc/ldap.conf  
  
For each file or directory returned, check the ownership.  
# ls -lLd <certpath>  
  
If the owner of any file or directory is not root, this is a finding.  
  
  
**Fix Text:**Change the ownership of the file or directory.  
# chown root <certpath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22564  
**Group Title:** GEN008160  
**Rule ID:** SV-37961r1\_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, sys, or system.  
  
  
**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:**    
Determine the certificate authority file and/or directory.  
# grep -i '^tls\_cacert' /etc/ldap.conf  
For each file or directory returned, check the group ownership.  
# ls -lLd <certpath>  
If the group-owner of any file or directory is not root, bin, sys, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group ownership of the file or directory.  
# chgrp root <certpath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22565  
**Group Title:** GEN008180  
**Rule ID:** SV-37962r1\_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:**    
Determine the certificate authority file and/or directory.  
  
Procedure:  
# grep -i '^tls\_cacert' /etc/ldap.conf  
For each file or directory returned, check the permissions.  
  
Procedure:  
# ls -lLd <certpath>  
  
If the mode of the file is more permissive than 0644 (or 0755 for directories), this is a finding.  
  
  
  
**Fix Text:**Change the mode of the file or directory.  
  
File Procedure:  
# chmod 0644 <certpath>   
  
Directory Procedure:  
# chmod 0755 <certpath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22566  
**Group Title:** GEN008200  
**Rule ID:** SV-37964r1\_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:**    
Determine the certificate authority file and/or directory.  
# grep -i '^tls\_cacert' /etc/ldap.conf  
For each file or directory returned, check the permissions.  
# ls -lLd <certpath>  
If the mode of the file or directory contains a '+', an extended ACL is present. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the certificate file.  
  
Procedure:  
For each certificate file found remove all extended permissions  
  
# setfacl --remove-all <certpath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22567  
**Group Title:** GEN008220  
**Rule ID:** SV-37965r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008220  
**Rule Title:**For systems using NSS LDAP, the TLS certificate file must be owned by root.  
  
  
**Vulnerability Discussion:**  The NSS LDAP service provides user mappings which are a vital component of system security. Its configuration must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine the certificate file.  
# grep -i '^tls\_cert' /etc/ldap.conf  
Check the ownership.  
# ls -lL <certpath>  
If the owner of the file is not root, this is a finding.  
  
  
  
**Fix Text:**Change the ownership of the file.  
# chown root <certpath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22568  
**Group Title:** GEN008240  
**Rule ID:** SV-37967r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008240  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP TLS certificate file must be group-owned by root, bin, sys, or system.  
  
  
**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:**    
Determine the certificate file.  
Procedure:  
# grep -i '^tls\_cert' /etc/ldap.conf  
  
Check the group ownership.  
Procedure:  
# ls -lL <certpath>  
  
If the group owner of the file is not root, bin, sys, or system, this is a finding.  
  
  
  
**Fix Text:**Change the group ownership of the file.  
  
Procedure:  
# chgrp root <certpath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22569  
**Group Title:** GEN008260  
**Rule ID:** SV-37966r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008260  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP TLS certificate file must have mode 0644 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:**    
Determine the certificate file.  
# grep -i '^tls\_cacert' /etc/ldap.conf  
Check the permissions.  
# ls -lL <certpath>  
If the mode of the file is more permissive than 0644, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the file.  
# chmod 0644 <certpath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22570  
**Group Title:** GEN008280  
**Rule ID:** SV-37968r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008280  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP TLS certificate 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:**    
Determine the certificate file.  
# grep -i '^tls\_cert' /etc/ldap.conf  
Check the permissions.  
# ls -lL <certpath>  
If the mode of the file contains a '+', an extended ACL is present. This is a finding.  
  
  
  
**Fix Text:**Remove the extended ACL from the certificate file.  
  
Procedure:  
For each certificate file found remove all extended permissions.  
  
# setfacl --remove-all <certpath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22571  
**Group Title:** GEN008300  
**Rule ID:** SV-37969r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008300  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP TLS key 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:**    
Determine the key file.  
# grep -i '^tls\_key' /etc/ldap.conf  
Check the ownership.  
# ls -lL <keypath>  
If the owner of the file is not root, this is a finding.  
  
  
  
**Fix Text:**Change the ownership of the file.  
# chown root <keypath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22572  
**Group Title:** GEN008320  
**Rule ID:** SV-37971r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008320  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP TLS key 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:**    
Determine the key file.  
# grep -i '^tls\_key' /etc/ldap.conf  
Check the group ownership.  
# ls -lL <keypath>  
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.  
# chgrp root <keypath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22573  
**Group Title:** GEN008340  
**Rule ID:** SV-37973r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008340  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP TLS key 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.  
  
Note: Depending on the particular implementation, group and other read permission may be necessary for unprivileged users to successfully resolve account information using LDAP. This will still be a finding, as these permissions provide users with access to system authenticators.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine the key file.  
# grep -i '^tls\_key' /etc/ldap.conf  
Check the permissions.  
# ls -lL <keypath>  
If the mode of the file is more permissive than 0600, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the file.  
# chmod 0600 <keypath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22574  
**Group Title:** GEN008360  
**Rule ID:** SV-37977r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008360  
**Rule Title:**If the system is using LDAP for authentication or account information, the LDAP TLS key 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:**    
Determine the key file.  
# grep -i '^tls\_key' /etc/ldap.conf  
Check the permissions.  
# ls -lL <keypath>  
If the permissions of the file contains a '+', an extended ACL is present. If the file has an extended ACL and it has not been documented with the IAO, this is a finding.  
  
  
  
  
**Fix Text:**Remove the extended ACL from the key file.  
  
Procedure:  
For each key file found remove all extended permissions.  
  
# setfacl --remove-all <keypath>     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22575  
**Group Title:** GEN008380  
**Rule ID:** SV-37978r1\_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-22576  
**Group Title:** GEN008420  
**Rule ID:** SV-37979r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008420  
**Rule Title:**The system must use available memory address randomization techniques.  
  
  
**Vulnerability Discussion:**  Successful exploitation of buffer overflow vulnerabilities relies in some measure to having a predictable address structure of the executing program. Address randomization techniques reduce the probability of a successful exploit.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify exec-shield is enabled if present.  
# cat /proc/sys/kernel/exec-shield  
If the file is present and contains a value of "0", this is a finding.  
  
  
  
**Fix Text:**Edit the kernel boot parameters, or "/etc/sysctl.conf", and set exec-shield to "1". Reboot the system.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22577  
**Group Title:** GEN008440  
**Rule ID:** SV-37980r1\_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.  
# service autofs status  
If the service is running, this is a finding.  
  
  
  
**Fix Text:**Stop and disable the autofs service.  
# service autofs stop  
# chkconfig autofs off  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22578  
**Group Title:** GEN008460  
**Rule ID:** SV-37981r1\_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 with the potential 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.  
Check if the directory "/proc/bus/usb" exists. If so, this is a finding.  
  
  
  
**Fix Text:**Edit the grub bootloader file "/boot/grub/grub.conf" or "/boot/grub/menu.lst" by appending the "nousb" parameter to the kernel boot line.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22579  
**Group Title:** GEN008480  
**Rule ID:** SV-37982r1\_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 with the potential 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.  
Check if usb-storage is prevented from loading.  
# grep 'install usb-storage /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no results are returned, this is a finding.  
  
  
  
**Fix Text:**Prevent the usb-storage module from loading.  
# echo 'install usb-storage /bin/true' >> /etc/modprobe.conf     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22580  
**Group Title:** GEN008500  
**Rule ID:** SV-37983r1\_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 with the potential 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 'install ieee1394 /bin/true' /etc/modprobe.conf /etc/modprobe.d/\*  
If no results are returned, this is a finding.  
  
  
  
**Fix Text:**Prevent the system from loading the firewire module.  
# echo 'install ieee1394 /bin/true' >> /etc/modprobe.conf  
    
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22582  
**Group Title:** GEN008520  
**Rule ID:** SV-37984r1\_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.  
# chkconfig --list iptables  
If the service is not "on" in the standard runlevel (ordinarily 3 or 5), this is a finding.  
  
  
  
**Fix Text:**Enable the system's local firewall.  
# chkconfig iptables on  
# service iptables start  
    
  
**CCI:**CCI-001118  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22583  
**Group Title:** GEN008540  
**Rule ID:** SV-37985r1\_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.  
  
# iptables --list  
  
Example of a rule meeting this criteria:  
REJECT all -- anywhere anywhere reject-with icmp-host-prohibited  
  
A rule using DROP is also acceptable. The default rule should be the last rule of a table and match all traffic.  
  
If there is no default deny rule, this is a finding.  
  
**Fix Text:**Edit "/etc/sysconfig/iptables" and add a default deny rule.  
  
An example of a default deny rule:  
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited  
  
Restart the iptable service.  
# service iptables restart   
    
  
**CCI:**CCI-001109  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1013  
**Group Title:** GEN008600  
**Rule ID:** SV-37986r1\_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 with the potential to compromise or damage 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.  
  
  
  
**Fix Text:**Configure the system to only boot from system startup media.  
  
Procedure:  
On systems with a BIOS or system controller use the BIOS interface at startup to remove all but the proper boot device from the boot device list.     
  
**CCI:**CCI-000366  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4246  
**Group Title:** GEN008620  
**Rule ID:** SV-37925r1\_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.  
  
**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-42186r1\_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 that can provide authentication for access to the system or boot loader.  
  
**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/grub.conf  
  
If no grub.conf file exists, and the bootloader on the system has not been authorized, justified, and documented, this is a finding.  
  
**Fix Text:**Configure the system to use the GRUB bootloader or document, justify, and authorize the alternate 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-37933r1\_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:**    
Check the "/boot/grub/grub.conf" or "/boot/grub/menu.lst" files.  
# more /boot/grub/menu.lst  
  
Check for a password configuration line, such as:  
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.  
  
For any bootloader other than GRUB which has been authorized, justified and documented for use on the system refer to the vendor documentation on password support. If the bootloader does not support encrypted passwords, 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/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-37938r1\_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 GRUB for password configuration.  
  
Procedure:  
Check the /boot/grub/grub.conf or /boot/grub/menu.lst files.  
# grep "password" /boot/grub/grub.conf /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:**Consult vendor documentation for procedures concerning the system's boot loader. Configure the boot loader to hash boot loader passwords using MD5 or a stronger hash.     
  
**CCI:**CCI-000213  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4250  
**Group Title:** GEN008720  
**Rule ID:** SV-37942r1\_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 /boot/grub/grub.conf permissions:  
  
# ls -lL /boot/grub/grub.conf  
  
If /boot/grub/grub.conf has a mode more permissive than 0600, then this is a finding.  
  
For any bootloader other than GRUB which has been authorized, justified and documented for use on the system refer to the vendor documentation for the location of the configuration file. If the bootloader configuration file 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 /boot/grub/grub.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22585  
**Group Title:** GEN008740  
**Rule ID:** SV-26984r1\_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 -lL /boot/grub/grub.conf  
  
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.  
# setfacl --remove-all /etc/grub.conf     
  
**CCI:**CCI-000225  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22586  
**Group Title:** GEN008760  
**Rule ID:** SV-26986r1\_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-26988r1\_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, bin, sys, or system 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-26990r1\_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 RPM signature validation is not disabled.  
# grep nosignature /etc/rpmrc /usr/lib/rpm/rpmrc /usr/lib/rpm/redhat/rpmrc ~root/.rpmrc  
If any configuration is found, this is a finding.  
  
Verify YUM signature validation is not disabled.  
# grep gpgcheck /etc/yum.conf /etc/yum.repos.d/\*  
If any "gpgcheck" setting is returned that is not equal to "1", this is a finding.  
  
**Fix Text:**Edit the RPM configuration file containing the "nosignature" option and remove the option.  
Edit the YUM configuration containing "gpgcheck=0" and set the value to "1".     
  
**CCI:**CCI-000351  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22589  
**Group Title:** GEN008820  
**Rule ID:** SV-26992r1\_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 of malicious packages being introduced.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the YUM service is enabled.  
# service yum-updatesd status  
If the service is enabled, this is a finding.  
  
**Fix Text:**Disable the yum service.  
# chkconfig yum-updatesd off ; service yum-updatesd stop     
  
**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**