**UNCLASSIFIED**

**Draft AIX Security Technical Implementation Guide**

**Version: 1**

**Release: 0.1**

**17 Aug 2011**

**Sort Order:** Rule Version (STIG-ID), ascending   
**Description:** The AIX Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) AIX 5.3 and 6.1 information systems. Comments or proposed revisions to this document should be sent via e-mail to the following address: fso\_spt@disa.mil.  
  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
**Group ID (Vulid):** V-969  
**Group Title:** GEN000000-AIX00020  
**Rule ID:** SV-969r5\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX00020  
**Rule Title:**AIX Trusted Computing Base (TCB) software must be implemented.  
  
**Vulnerability Discussion:**  The AIX Trusted Computing Base (TCB) software provides protection from the unauthorized modification of core system files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Perform:  
  
      # /bin/tcbck  
  
If TCB is not installed, the output will show an error code of 3001-101 and/or a text message indicating TCB is not installed. This will result in a finding.  
  
  
**Fix Text:**Ensure the Trusted Computing Base (TCB) software is implemented. TCB can only be installed at OS installation time.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4284  
**Group Title:** GEN000000-AIX00040  
**Rule ID:** SV-4284r5\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX00040  
**Rule Title:**The securetcpip command must be used.  
  
**Vulnerability Discussion:**  The AIX securetcpip command disables insecure network utilities such as rcp, rlogin, rlogind, rsh, rshd, tftp, tftpd and trpt/d. These services increase the attack surface of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
The securetcpip command is in /etc. If it is not there, this is a finding.   
Perform:  
  
      more /etc/security/config  
  
If the stanza below is not there, then is a finding.  
  
tcpip:  
netrc = ftp, rexec  
  
The stanza indicates the securetcpip command, which disables all the unsafe tcpip commands, (e.g., rsh, rlogin, tftp)has been executed.  
  
  
**Fix Text:**Ensure secure tcp/ip has been invoked before allowing operations on the system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4287  
**Group Title:** GEN000000-AIX00060  
**Rule ID:** SV-4287r5\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX00060  
**Rule Title:**The integrity of AIX files with the TCB bit set must be checked weekly.  
  
**Vulnerability Discussion:**  If the integrity of files with the TCB bit set is not checked weekly, a system compromise may not be detected.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Perform the following command with no parameters to ensure the system is in trusted mode:  
  
      #       /bin/tcbck  
  
If TCB is not installed, the output will show an error code of 3001-101 and/or a text message indicating TCB is not installed. If the output from the command indicates it is not in trusted mode, mark this item not reviewed. Otherwise, check the root crontab to verify tcbck is executed weekly. If it is not in the crontab, ask the SA if the check is run manually and to see the results of the check.  
  
  
**Fix Text:**Add tcbck command as a weekly cronjob with the output sent to the SA.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12035  
**Group Title:** GEN000000-AIX00080  
**Rule ID:** SV-12536r3\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN000000-AIX00080  
**Rule Title:**The SYSTEM attribute must not be set to NONE for any account.   
  
**Vulnerability Discussion:**  The SYSTEM attribute in /etc/security/user defines the mechanisms used to authenticate specific user accounts. If the value is set to NONE, other attributes will be used to determine the authentication mechanisms, but if these attributes are not present, no authentication will be performed. To ensure authentication is always used for the system's accounts, the SYSTEM attribute must always be set to a valid setting other than NONE.  
  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Examine the /etc/security/user file:  
  
      #       grep SYSTEM /etc/security/user  
  
If the line contains SYSTEM=NONE then this is a finding.  
  
  
**Fix Text:**Edit /etc/security/user and change any SYSTEM=NONE settings to a valid authentication setting.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29491  
**Group Title:** GEN000000-AIX0085  
**Rule ID:** SV-38695r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0085  
**Rule Title:**The /etc/netsvc.conf file must be root owned  
  
**Vulnerability Discussion:**  The /etc/netsvc.conf file is used to specify the ordering of name resolution for the sendmail command, alias resolution for the sendmail command, and host name resolution routines. Malicious changes could prevent the system from functioning correctly or compromise system security.  
  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the /etc/netsvc.conf file is owned by root.   
# ls -l /etc/netsvc.conf   
If the file is not owned by root, this is a finding.   
  
**Fix Text:**Change the owner of the /etc/netsvc.conf file to root.   
  
# chown root /etc/netscv.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29492  
**Group Title:** GEN000000-AIX0090  
**Rule ID:** SV-38696r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0090  
**Rule Title:**The /etc/netsvc.conf file must be group-owned by root, bin, sys, or system.  
  
**Vulnerability Discussion:**  The /etc/netsvc.conf file is used to specify the ordering of name resolution for the sendmail command, alias resolution for the sendmail command, and host name resolution routines. Malicious changes could prevent the system from functioning correctly or compromise system security.  
  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the /etc/netcsvc.conf file.  
  
Procedure:  
# ls -lL /etc/netsvc.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 /etc/netsvc.conf file to root, bin, sys, or system.  
  
Procedure:  
# chgrp system /etc/netsvc.conf  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29493  
**Group Title:** GEN000000-AIX0100  
**Rule ID:** SV-38697r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0100  
**Rule Title:**The /etc/netsvc.conf file must have mode 0644 or less permissive.  
  
**Vulnerability Discussion:**  The /etc/netsvc.conf file is used to specify the ordering of name resolution for the sendmail command, alias resolution for the sendmail command, and host name resolution routines. Malicious changes could prevent the system from functioning correctly or compromise system security.  
  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/netsvc.conf file.  
# ls -l /etc/netsvc.conf  
If the file mode is more permissive than 0644, this is a finding.  
  
  
**Fix Text:**Change the mode of the /etc/netsvc.conf file to 0644 or less permissive.  
# chmod 0644 /etc/netsvc.conf  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29494  
**Group Title:** GEN000000-AIX0110  
**Rule ID:** SV-38698r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0110  
**Rule Title:**The /etc/netsvc.conf file must not have an extended ACL.  
  
**Vulnerability Discussion:**  The /etc/netsvc.conf file is used to specify the ordering of name resolution for the sendmail command, alias resolution for the sendmail command, and host name resolution routines. Malicious changes could prevent the system from functioning correctly or compromise system security.  
  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check there is no extended ACL on the /etc/netsvc.conf file.  
# aclget /etc/netsvc.conf   
If extended permissions are enabled, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the /etc/nsswitch.conf file.   
  
#acledit /etc/netsvc.conf and disable extended permissions.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29495  
**Group Title:** GEN000000-AIX0200  
**Rule ID:** SV-38699r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0200  
**Rule Title:**The system must not allow directed broadcasts to gateway.  
  
**Vulnerability Discussion:**  Disabling directed\_broadcast prevents packets directed to a gateway to be broadcasted on a remote network.  
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the directed\_broacast option.  
# /usr/sbin/no –o directed\_broadcast  
If the value returned is not 0, this is a finding.  
  
  
**Fix Text:**Configure directed\_broadcast to 0.  
  
# /usr/sbin/no –p –o directed\_broadcast=0   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29496  
**Group Title:** GEN000000-AIX0210  
**Rule ID:** SV-38700r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0210  
**Rule Title:**The system must provide protection from Internet Control Message Protocol (ICMP) attacks on TCP connections.  
  
**Vulnerability Discussion:**  The ICMP attacks may be of the form of ICMP source quench attacks and Path MTU Discovery (PMTUD) attacks. If this network option tcp\_icmpsecure is turned on, the system does not react to ICMP source quench messages. This will protect against ICMP source quench attacks. The payload of the ICMP message is tested to determine if the sequence number of the TCP header portion of the payload is within the range of acceptable sequence numbers. This will mitigate PMTUD attacks to a large extent.   
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the value of the tcp\_icmpsecure parameter.  
  
# /usr/sbin/no –o tcp\_icmpsecure  
If the value returned is not 1, this is a finding.  
  
  
**Fix Text:**Set the tcp\_icmpsecure parameter to 1.  
  
# /usr/sbin/no –p-o tcp\_icmpsecure=1   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29497  
**Group Title:** GEN000000-AIX0220  
**Rule ID:** SV-38701r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0220  
**Rule Title:**System must provide protection for the TCP stack against connection resets, SYN and data injection attacks.  
  
**Vulnerability Discussion:**  The tcp\_tcpsecure parameter provides protection for TCP connections from fake SYN's, fake RST, and data injections on established connections. The first vulnerability involves sending a fake SYN to an established connection to abort the connection. The second vulnerability involves sending a fake RST to an established connection to abort the connection. The third vulnerability involves injecting fake data in an established TCP connection.  
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the value of the tcp\_tcpsecure parameter.  
  
# /usr/sbin/no –o tcp\_tcpsecure  
If the value returned is not 7, this is a finding.  
  
  
**Fix Text:**Set the tcp\_tcpsecure parameter to 7.  
  
# /usr/sbin/no –p –o tcp\_tcpsecure=7   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29498  
**Group Title:** GEN000000-AIX0230  
**Rule ID:** SV-38702r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0230  
**Rule Title:**The system must provide protection against IP fragmentation attacks.  
  
**Vulnerability Discussion:**  The parameter ip\_nfrag provides an additional layer of protection against IP fragmentation attacks. The value the ip\_nfrag specifies is the maximum number of fragments of an IP packet that can be kept in the IP reassembly queue at any time. The default value of this network option is 200. This is a reasonable value for most environments and offers protection from IP fragmentation attacks.   
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the value of the ip\_nfrag parameter.  
  
# /usr/sbin/no –o ip\_nfrag  
If the result retuned is less than 199, this is a finding.  
  
  
**Fix Text:**Set the ip\_nfrag parameter to 200.  
  
# /usr/sbin/no –p –o ip\_nfrag=200   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29499  
**Group Title:** GEN000000-AIX0300  
**Rule ID:** SV-38703r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0300  
**Rule Title:**The system must not have the bootp service active.  
  
**Vulnerability Discussion:**  The bootp service is used for Network Installation Management (NIM) and remote booting of systems. The bootp service should not be active unless it is needed for NIM servers or booting remote systems. Running unnecessary services increases the attack vector of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active bootp service.  
  
# grep bootp /etc/inetd.conf |grep -v \#  
  
If the bootp service is not disabled, this is a finding.  
  
  
**Fix Text:**Disable the bootp service from /etc/inetd.conf.  
  
Edit /etc/inetd.conf and comment out bootp service line.   
  
Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29519  
**Group Title:** GEN000000-AIX0310  
**Rule ID:** SV-38750r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0310  
**Rule Title:**The /etc/ftpaccess.ctl file must exist.  
  
**Vulnerability Discussion:**  The ftpaccess.ctl file contains options for the ftp daemon such as herald, motd, user access, and permissions to files and directories. If the ftpaccess.ctl file does not exist, the ftpd process will not display any warning banners, and permissions will only be enforced using basic UNIX permissions.   
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for the existence of the /etc/ftpaccess.ctl file.  
  
# ls -l /etc/ftpaccess.ctl  
  
If the ftpaccess.ctl file does not exist, this is a finding.  
  
  
**Fix Text:**Create a /etc/ftpaccess.ctl file.  
#touch /etc/ftpaccess.ctl  
  
Add at least the herald: /path to login banner to the /etc/ftpaccess.ctl file.  
  
#vi /etc/ftpaccess.ctl  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29520  
**Group Title:** GEN000000-AIX0320  
**Rule ID:** SV-38751r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0320  
**Rule Title:**The /etc/ftpaccess.ctl file must be owned by root.  
  
**Vulnerability Discussion:**  If the ftpaccess.ctl file is not owned by root, an unauthorized user may modify the file to allow unauthorized access to change the file. Unauthorized modification could result in Denial of Service to authorized FTP users or permit unauthorized access to system information.  
  
  
  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the /etc/ftpaccess.ctl file.  
  
# ls -l /etc/ftpaccess.ctl  
  
If the ftpaccess.ctl file is not owned by root, this is a finding.  
  
  
**Fix Text:**Change the owner of the ftpaccess.ctl file to root.  
  
# chown root /etc/ftpaccess.ctl  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29521  
**Group Title:** GEN000000-AIX0330  
**Rule ID:** SV-38752r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0330  
**Rule Title:**The /etc/ftpaccess.ctl file must be group-owned by root, bin, sys, or system.  
  
**Vulnerability Discussion:**  If the ftpaccess.ctl file is not group-owned by root or a system group, an unauthorized user may modify the file to allow unauthorized access to modify the file. Unauthorized modification could result in Denial of Service to authorized FTP users or permit unauthorized access to system information.  
  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the ftpaccess.ctl file.  
  
# ls -lL /etc/ftpaccess.ctl  
  
If the /etc/ftpaccess.ctl file is not group-owned by root, bin, sys, or system, this is a finding.  
  
  
**Fix Text:**Change the group owner of the /etc/ftpaccess.ctl file.  
  
# chgrp system /etc/ftpaccess.ctl  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29522  
**Group Title:** GEN000000-AIX0340  
**Rule ID:** SV-38753r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0340  
**Rule Title:**The /etc/ftpaccess.ctl file must have mode 0640 or less permissive.  
  
**Vulnerability Discussion:**  Excessive permissions on the ftpaccess.ctl file could permit unauthorized modification. Unauthorized modification could result in Denial of Service to authorized FTP users or permit unauthorized access to system information.  
  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the /etc/ftpaccess.ctl file.  
  
# ls -l /etc/ftpaccess.ctl  
  
If the ftpaccess.ctl file has a mode more permissive than 0640, this is a finding.  
  
  
**Fix Text:**Change the mode of the /etc/ftpaccess.ctl file to 0640.  
  
# chmod 0640 /etc/ftpaccess.ctl  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29523  
**Group Title:** GEN000000-AIX0350  
**Rule ID:** SV-38754r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000000-AIX0350  
**Rule Title:**The /etc/ftpaccess.ctl file must not have an extended ACL.  
  
**Vulnerability Discussion:**  Excessive permissions on the ftpaccess.ctl file could permit unauthorized modification. Unauthorized modification could result in Denial of Service to authorized FTP users or permit unauthorized access to system information.  
  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the /etc/ftpaccess.ctl file.  
  
#aclget /etc/ftpaccess.ctl   
Check if extended permissions are disabled.  
  
If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the /etc/ftpaccess.ctl file.   
  
#acledit /etc/ftpaccess.ctl   
Disable extended permissions.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-756  
**Group Title:** GEN000020  
**Rule ID:** SV-27039r1\_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 a valid root password 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:**    
Ensure the root account for any bootable partitions has a password assigned in the /etc/security/passwd file.  
  
  
**Fix Text:**Assign a root account password for any bootable partition.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11940  
**Group Title:** GEN000100  
**Rule ID:** SV-27052r1\_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.  
  
**Security Override Guidance:**   
If an extended support agreement providing 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:**    
# oslevel  
Vendor supported versions are 5.3 and later at the time of writing.  
  
AIX 5.3 End of support 30 April 2012  
AIX 5.2 End of support 30 April 2009  
AIX 5.1 End of support 1 April 2006  
  
If the release is not supported, this is a finding.  
  
  
**Fix Text:**Upgrade to a supported version of the operating system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-783  
**Group Title:** GEN000120  
**Rule ID:** SV-27060r1\_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 patches from IBM.  
Verify the available patches and service packs have been installed on the system.  
Check the currently running TL (Technology Levels and Service Packs)  
#oslevel -s  
  
Perform the following to obtain a list of installed patches:  
# /usr/sbin/instfix -i  
  
If there are patches available and applicable for the system that have not been installed, this is a finding.   
  
**Fix Text:**Use a web browser to access the vendor's support website. Download the service packs and patches. Use SMIT to apply the updates.   
  
#smitty update\_all   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11941  
**Group Title:** Create and Maintain System Baseline  
**Rule ID:** SV-38784r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000140  
**Rule Title:**A file integrity baseline must be created and maintained.  
  
**Vulnerability Discussion:**  A file integrity baseline is a collection of file metadata which is to evaluate the integrity of the system. A minimal baseline must contain metadata for all device files, setuid files, setgid files, system libraries, system binaries, and system configuration files. The minimal metadata must consist of the mode, owner, group owner, and modification times. For regular files, metadata must also include file size and a cryptographic hash of the file’s contents.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSW-1  
  
**Check Content:**    
Determine if a file integrity baseline, which includes cryptographic hashes, has been created and maintained for the system. If no file integrity baseline exists for the system, this is a finding. If the file integrity baseline contains no cryptographic hashes, this is a finding. If the file integrity baseline is not maintained (that is, the baseline has not been updated to be consistent with the latest approved system configuration changes), this is a finding.  
  
**Fix Text:**Create a file integrity baseline, including cryptographic hashes, for the system.   
  
# find / -depth –print | tee Baseline  
  
Open the above file and either manually execute md5sum, csum, or the chksum command on each file. Alternatively, write a script to perform the above. NOTE: For security purposes, “md5sum” is preferred over “chksum” The md5sum command can be loaded from the Linux tool kit for AIX.   
Alternatively, OpenSSL can be used to create hashes.  
#openssl dgst –md5 <file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11945  
**Group Title:** Baseline for System Libraries and Binaries Check  
**Rule ID:** SV-30005r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000220  
**Rule Title:**A file integrity tool must be used at least daily 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: This requirement only applies to MAC I systems.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
This will virtually always be a manual review. Determine if there is an automated job, scheduled to run daily or more frequently, to run the file integrity tool to check for unauthorized system libraries or binaries, or unauthorized modification to authorized system libraries or binaries. If there is not, this is a finding.  
  
**Fix Text:**Establish an automated job, scheduled to run daily or more frequently, to run the file integrity tool to check for unauthorized system libraries or binaries, or unauthorized modification to authorized system libraries or binaries.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4301  
**Group Title:** GEN000240  
**Rule ID:** SV-38666r1\_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 synchronizing with upstream authoritative sources. Specific requirements for the upstream synchronization of Network Time Protocol (NTP) servers are covered in the Network Other Devices STIG.  
  
For systems located on isolated or closed networks, it is not necessary to synchronize with a global authoritative time source. If a global authoritative time source is not available to systems on an isolated network, a local authoritative time source must be established on this network and used by the systems connected to this network. This is necessary to provide the ability to correlate events and allow for the correct operation of time-dependent protocols between systems on the isolated network.  
  
If the system is completely isolated (no connections to networks or other systems), time synchronization is not required as no correlation of events between systems will be necessary. If the system is completely isolated, this requirement is not applicable.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check if NTP running:  
#lssrc –s xntpd or  
# ps -ef | egrep "xntpd|ntpd" or  
# ntpq -–p  
  
Check if xntpd is started at boot time and scheduled to run:  
#grep xntpd /etc/rc.tcpip | grep –v \#  
  
If NTP is running:  
# more /etc/ntp.conf and   
# ntpq -p  
  
Confirm the servers and peers or multicastclient (as applicable) are local or an authoritative U.S. DoD source.  
  
If a non-local/non-authoritative (U.S. DoD source) time-server is used, this is a finding.  
  
  
  
**Fix Text:**Use a local authoritative time server that synchronizes to an authorized DoD time source. Ensure all systems in the facility feed from one or more local time servers that feed from the authoritative time server.   
  
View the (x)ntp/(x)ntpd man page(s):  
  
# man xntpd  
  
Create/edit the /etc/ntp.conf file, delete any non-local and/or non-US/DoD sources and insert the local or an authoritative U.S. DoD source.  
  
Start or restart the NTP service.  
# refresh –s xntpd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22290  
**Group Title:** GEN000241  
**Rule ID:** SV-39091r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000241  
**Rule Title:**The system clock must be synchronized continuously, or at least daily.   
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. Internal system clocks tend to drift and require periodic resynchronization to ensure their accuracy. Software, such as ntpd, can be used to continuously synchronize the system clock with authoritative sources. Alternatively, the system may be synchronized periodically, with a maximum of one day between synchronizations.  
  
If the system is completely isolated (no connections to networks or other systems), time synchronization is not required as no correlation of events or operation of time-dependent protocols between systems will be necessary. If the system is completely isolated, this requirement is not applicable.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the root crontab for ntpdate jobs running at least daily. # crontab -l | grep ntpdate columns 3, 4, and 5 must be an asterisk (\*) for the job to be run daily. If this job exists, this is not a finding. OR Verify the auto-startup of xntpd in /etc/rc.tcpip.  
# cat /etc/rc.tcpip | grep –v “^#”   
  
Check the system for a running NTP daemon, which is the preferred method. # ps -ef | grep ntp If an (x)ntpd process exists, this is not a finding. Otherwise, this is a finding.   
  
**Fix Text:**Enable the NTP daemon for continuous synchronization. Edit /etc/rc.tcpip and enable xntpd daemon. Edit /etc/ntp.conf and add the ntp server entry. Then: # startsrc -s xntpd OR Add a daily or more frequent cronjob to perform synchronization using ntpdate. NOTE: While it is possible to run ntpdate from a cron script, it is important to mention that ntpdate with contrived cron scripts is no substitute for the NTP daemon, which uses sophisticated algorithms to maximize accuracy and reliability while minimizing resource use. Finally, since ntpdate polling does not discipline the host clock frequency as does xntpd, the accuracy using ntpdate is limited. The process of passively listening for NTP broadcasts (i.e., placing the line broadcastclient yes in the /etc/ntp.conf file) is preferred over any procedural form of direct server polling for a large network with many nodes needing to be time-synchronized. This method is preferred because it significantly reduces the network traffic load related to NTP.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22291  
**Group Title:** GEN000242  
**Rule ID:** SV-39092r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000242  
**Rule Title:**The system must use at least two time sources for clock synchronization.  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. For redundancy, two time sources are required so synchronization continues to function if one source fails.   
  
If the system is completely isolated (no connections to networks or other systems), time synchronization is not required as no correlation of events or operation of time-dependent protocols between systems will be necessary. If the system is completely isolated, this requirement is not applicable.  
  
NOTE: For the Network Time Protocol (NTP), the requirement is two servers, but it is recommended to configure at least four distinct time servers which allow NTP to effectively exclude a time source not consistent with the others. The system's local clock must be excluded from the count of time sources.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for a running NTP daemon.   
# ps -ef | grep ntp   
Verify the auto-startup of xntpd in /etc/rc.tcpip.  
# cat /etc/rc.tcpip | grep –v “^#”   
Verify at least two external NTP servers are listed in the /etc/ntp.conf file.   
# cat /etc/ntp.conf | grep –v “^#” | grep –i server | \ egrep –v “127.127.1.1|127.127.1.0” If xntpd is not invoked with at least two external NTP servers listed (127.127.1.0 or 127.127.1.1 are local clock references and therefore not allowed), this is a finding.   
  
**Fix Text:**If auto-starting xntpd, add (when necessary) the correct number of (at least two) external servers to the /etc/ntp.conf file. If using ntpdate, add additional NTP servers (at least two are required) to the cron job running ntpdate.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22292  
**Group Title:** GEN000244  
**Rule ID:** SV-28718r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000244  
**Rule Title:**The system must use time sources local to the enclave.  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. The network architecture should provide multiple time servers within an enclave that provide local service to the enclave and synchronize with time sources outside of the enclave.  
  
If this server is an enclave time server, this requirement is not applicable.  
  
If the system is completely isolated (no connections to networks or other systems), time synchronization is not required as no correlation of events or operation of time-dependent protocols between systems will be necessary. If the system is completely isolated, this requirement is not applicable.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the root crontab for ntpdate entries.  
# crontab -l | grep ntpdate  
If the ntpdate command is invoked with NTP servers outside of the enclave, this is a finding.  
  
Check the NTP daemon configuration.  
# grep ^server ntp.conf  
If an NTP server is listed outside of the enclave, this is a finding.  
  
**Fix Text:**If using ntpdate, remove NTP servers external to the enclave from the cron job running ntpdate.  
  
If using the NTP daemon, remove the server line from ntp.conf for each NTP server external to the enclave.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22293  
**Group Title:** GEN000246  
**Rule ID:** SV-28719r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000246  
**Rule Title:**The system time synchronization method must use cryptographic algorithms to verify the authenticity and integrity of the time data.  
  
**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.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the root crontab for ntpdate entries.  
# crontab -l | grep ntpdate  
If the ntpdate command is not invoked with the -a parameter, this is a finding.  
  
Check the NTP daemon configuration.  
# grep ^server ntp.conf | grep -v '( key | autokey )'  
If server lines are present without key or autokey options, this is a finding.  
  
**Fix Text:** If using ntpdate, add the -a option with a key to the cron job running ntpdate.  
  
If using the NTP daemon, add the key or autokey options, as appropriate, to each server line in ntp.conf for each NTP server not configured for authentication.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22294  
**Group Title:** GEN000250  
**Rule ID:** SV-28720r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000250  
**Rule Title:**The time synchronization configuration file (such as /etc/ntp.conf) must be owned by root.  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. If an illicit time source is used for synchronization, the integrity of system logs and the security of the system could be compromised. If the configuration files controlling time synchronization are not owned by a system account, unauthorized modifications could result in the failure of time synchronization.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Run ls -l ntp.conf to display the owner of the NTP configuration file. If the owner is not root, this is a finding.  
  
**Fix Text:**Change the owner of the NTP configuration file to root.  
# chown root ntp.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22295  
**Group Title:** GEN000251  
**Rule ID:** SV-39093r1\_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, sys, or system.  
  
**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, sys, or system, this is a finding.  
  
**Fix Text:**Change the group owner of the NTP configuration file.  
  
Procedure:  
# chgrp system /etc/ntp.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22296  
**Group Title:** GEN000252  
**Rule ID:** SV-28722r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000252  
**Rule Title:**The time synchronization configuration file (such as /etc/ntp.conf) must have mode 0640 or less permissive.  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. If an illicit time source is used for synchronization, the integrity of system logs and the security of the system could be compromised. If the configuration files controlling time synchronization are not protected, unauthorized modifications could result in the failure of time synchronization.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the mode for the NTP configuration file is not more permissive than 0640.  
# ls -l ntp.conf  
  
If the mode is more permissive than 0640, this is a finding.  
  
**Fix Text:**Change the mode of the NTP configuration file to 0640 or less permissive.  
# chmod 0640 ntp.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22297  
**Group Title:** GEN000253  
**Rule ID:** SV-38667r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000253  
**Rule Title:**The time synchronization configuration file (such as /etc/ntp.conf) must not have an extended ACL.  
  
**Vulnerability Discussion:**  A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. If an illicit time source is used for synchronization, the integrity of system logs and the security of the system could be compromised. If the configuration files controlling time synchronization are not protected, unauthorized modifications could result in the failure of time synchronization.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check for an extended ACL on the NTP configuration file.  
# –aclget /etc/ntp.conf  
If extended permissions are not disabled this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the ntp.conf file.  
#acledit /etc/ntp.conf  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-760  
**Group Title:** A shared, i.e., default, application, or utility -  
**Rule ID:** SV-38668r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000280  
**Rule Title:**Direct logins must not be permitted to shared, default, application, or utility accounts.  
  
**IAControls:**  IAIA-1  
  
**Check Content:**    
Use the last command to check for multiple accesses to an account from different workstations/IP addresses. If users log directly onto accounts, rather than using the su command from their own named account to access them, this is a finding (such as logging directly on to Oracle). Also, ask the SA or the IAO if shared accounts are logged into directly or if users log on to an individual account and switch user to the shared account.  
  
# last <unix account>  
  
Shared or Application accounts can have direct login disabled by setting the rlogin parameter to false in the user's stanza of the /etc/security/user file.   
#lsuser –a rlogin < user\_id >  
  
If users log directly on to shared accounts, this is a finding.  
  
**Fix Text:**Use the switch user (su) command from a named account login to access shared accounts. Maintain audit trails to identify the actual user of that account name. Document requirements and procedures for users/administrators to log into their own accounts first and then switch user (su) to the account that must be shared.   
  
Direct login to shared or application accounts can be prevented by setting the rlogin = false in the accounts stanza of the /etc/security/user file. Additional hardening of the shared/application accounts can be done with the sugroups = in the accounts stanza of the /etc/security/user file.  
#chuser rlogin=false < user id >  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4269  
**Group Title:** GEN000290  
**Rule ID:** SV-38767r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000290  
**Rule Title:**The system must not have unnecessary accounts.  
  
**Vulnerability Discussion:**  Accounts providing no operational purpose provide additional opportunities for system compromise. Unnecessary accounts include user accounts for individuals not requiring access to the system and application accounts for applications not installed on the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAAC-1  
  
**Check Content:**    
Check the system for unnecessary user accounts.  
  
Procedure:  
# more /etc/passwd  
  
Some examples of unnecessary accounts includes guest, uucp, games, news, gopher, ftp, and lp. If any unnecessary accounts are found, this is a finding.  
  
  
**Fix Text:** Remove all unnecessary accounts, such as games, from the /etc/passwd file before connecting a system to the network. Other accounts, such as news and gopher that are associated with a service not in use should also be removed.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-761  
**Group Title:** Accounts have the same user or account name.  
**Rule ID:** SV-27064r1\_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:**    
Perform the following to ensure there are no duplicate account names:  
# usrck -n ALL  
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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-762  
**Group Title:** Accounts have been assigned the same User Id  
**Rule ID:** SV-27067r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000320  
**Rule Title:**All accounts must be assigned unique User Identification Numbers (UIDs).  
  
**Vulnerability Discussion:**  Accounts that share 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:  
# usrck -n ALL  
If any duplicate UIDs are found, this is a finding.  
  
**Fix Text:**Edit user accounts to provide unique UIDs for each account.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11946  
**Group Title:** GEN000340  
**Rule ID:** SV-38669r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000340  
**Rule Title:**UIDs reserved for system accounts must not be assigned to non-system accounts.  
  
**Vulnerability Discussion:**  Reserved UIDs are typically used by system software packages. If non-system accounts have UIDs in this range, they may conflict with system software, possibly leading to the user having permissions to modify system files.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the UID assignments of all accounts.  
# more /etc/passwd   
Confirm all accounts with a UID of 128 and below are used by a system account. If a UID reserved for system accounts (0-128) is used by a non-system account, this is a finding.  
  
  
**Fix Text:**Using the passwd command, change the UID numbers for non-system accounts with reserved UIDs (those less or equal to 128).   
  
Alternatively, smit can be used for this same purpose.   
#smitty users   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-780  
**Group Title:** GEN000360  
**Rule ID:** SV-39094r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000360  
**Rule Title:**Group Identifiers (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:**    
# more /etc/passwd  
  
Confirm all accounts with a GID of 99 and below (499 and below for Linux) are used by a system account.  
  
If a GID reserved for system accounts, 0 – 99 (0 – 499 for Linux), is used by a non-system account, then this is a finding.  
  
**Fix Text:**Change the primary group GID numbers for non-system accounts with reserved primary group GIDs (those less or equal to 99 in general, or 499 for Linux).  
  
# smitty chuser   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-781  
**Group Title:** GEN000380  
**Rule ID:** SV-27071r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000380  
**Rule Title:**All Group Identifiers (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 that does not exist on the system, and a group with that 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:  
# usrck -n ALL  
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.   
  
# smitty mkgroup   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-763  
**Group Title:** GEN000400  
**Rule ID:** SV-38932r1\_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/security/login.cfg and assign the herald value for the default and /dev/console stanzas to one of the DoD login banners (based on the character limitations imposed by the system).  
  
#chsec –f /etc/security/login.cfg –s default –a herald=”<DoD Login Banner>”  
  
OR  
  
#vi /etc/security/login.cfg and add a herald = <DoD Login Banner> statement to the default stanza  
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."   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24331  
**Group Title:** GEN000402  
**Rule ID:** SV-38933r1\_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 login. 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 the Xresources file to configure the system to display one of the DoD login banners (based on the character limitations imposed by the system) prior to, or as part of, the graphical desktop environment login process.   
  
For Dt login, change the variable Dtlogin\*greeting.labelString: in Xresources file.  
#cp /usr/dt/config/C/Xresoruces /etc/dt/config/C/Xresources  
#vi /etc/dt/config/C/Xresources  
  
For XDM login, change the variable Xlogin\*greeting in the Xresources file.  
#vi /usr/lpp/X11/lib/X11/xdm/Xresources.  
  
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."   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23732  
**Group Title:** GEN000410  
**Rule ID:** SV-38934r1\_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 and should be used in place of FTP. SFTP is implemented by the SSH service and uses its banner configuration.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECWM-1  
  
**Check Content:**    
FTP to the system.  
# ftp localhost  
Check for either of the following login banners based on the character limitations imposed by the system. An exact match is required. If one of these banners is not displayed, this is a finding. If the system does not run the FTP service, this is not applicable.  
  
DoD Login Banners:  
  
"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.  
  
By using this IS (which includes any device attached to this IS), you consent to the following conditions:  
  
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.  
  
-At any time, the USG may inspect and seize data stored on this IS.  
  
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.  
  
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.  
  
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."  
  
OR  
  
"I've read & consent to terms in IS user agreem't."  
  
**Fix Text:**Configure the system to display one of the DoD login banners (based on the character limitations imposed by the system) prior to any FTP login attempt.  
  
Add a banner file to the system with the DoD login banner.  
  
#vi /etc/herald  
<Add DoD banner to file>  
#chmod 644 /etc/herald  
#chown root:system /etc/herald  
  
Add a herald line to the /etc/ftpaccess.ctl file.  
#vi /etc/ftpaccess.ctl  
<add/update line in /etc/ftpasccess.ctl> herald: /etc/herald  
#chown root:system /etc/ftpaccess.ctl  
#chmod 640 /etc/ftpaccess.ctl  
  
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."   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-765  
**Group Title:** GEN000440  
**Rule ID:** SV-38935r1\_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:**    
Check the system logs for successful and unsuccessful logins. If these events are not present in the logs, this is a finding.  
  
**Check Content:**    
To determine if successful logons are being logged, perform the following:  
# last | more   
To determine if unsuccessful logons are being logged, perform the following:   
# last -f /etc/security/failedlogin | more  
If the commands do not return successful and unsuccessful logins, this is a finding.  
  
**Fix Text:**Edit /etc/syslog.conf and add local log destinations for auth.\* or both auth.notice and auth.info.   
  
“auth.info /var/log/authlog”  
  
Verify service startup scripts for syslog and utmp (if present) are enabled.   
  
# vi /etc/rc.tcpip  
Check the syslogd service is not commented out.  
  
Refresh syslogd  
#refresh –s syslogd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22298  
**Group Title:** GEN000450  
**Rule ID:** SV-38670r1\_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:**    
#grep maxlogins /etc/security/login.cfg | grep -v \\*  
  
If no values are returned, or the value returned is greater than 10, this is a finding.  
  
**Fix Text:**Configure the system to limit the number of simultaneous logins for user accounts with the chsec command.   
  
#chsec –f /etc/security/login.cfg –s usw –a maxlogins=10  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22299  
**Group Title:** GEN000452  
**Rule ID:** SV-39095r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000452  
**Rule Title:**The system must display the date and time of the last successful account login upon login.  
  
**Vulnerability Discussion:**  Providing users with feedback on when account accesses last occurred facilitates user recognition and reporting of unauthorized account use.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system displays the date and time of the last successful login upon logging in. This can be accomplished by logging into the system and verifying whether or not the necessary information is displayed. If the system does not provide this information upon login, this is a finding.  
  
Verify the SSH daemon is configured to display last login information. # cat /etc/ssh/etc/sshd\_config | grep -i PrintLastLog  
  
If PrintLastLog is disabled, this is a finding.   
  
**Fix Text:**Configure the system to display the date and time of the last successful login upon logging in. Consult OS documentation for the configuration procedure.  
  
Enable PrintLastLog in the SSH daemon. To enable PrintLastLog in the SSH daemon, remove any comment disabling this option from /etc/ssh/etc/sshd\_config. The line should look like: PrintLastLog yes   
  
Restart sshd  
# kill -1 <PID of sshd>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22300  
**Group Title:** GEN000454  
**Rule ID:** SV-25947r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000454  
**Rule Title:**The system must display the number of unsuccessful login attempts since the last successful login for a user account upon logging in.  
  
**Vulnerability Discussion:**  Providing users with feedback on recent login failures facilitates user recognition and reporting of attempted unauthorized account use.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system displays the number of failed login attempts upon logging in. Attempt to log into the system once using an invalid password or other authenticator, then log into the system using the same account with a valid authenticator. If the system does not display a message indicating there was a failed login attempt, this is a finding.  
  
**Fix Text:**Configure the system to display the number of failed logins upon logging in. Consult OS documentation for the necessary procedure.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-766  
**Group Title:** After three consecutive unsuccessful login attempt  
**Rule ID:** SV-38671r1\_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:**    
# /usr/sbin/lsuser -a loginretries ALL | more   
Check all active accounts on the system for the maximum number of tries before the system will lock the account. If a user has values set to 0 or greater then 3, this is a finding.  
  
  
**Fix Text:**Use the chsec command to configure the number of unsuccessful logins resulting in account lockout.   
  
#chsec –f /etc/security/user –s default –a loginretries=3   
#chsec -f /etc/security/user -s <user id> -a loginretries=3   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-768  
**Group Title:** GEN000480  
**Rule ID:** SV-38839r1\_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 logindelay parameter.  
# more /etc/security/login.cfg   
OR  
#grep logindelay /etc/security/login.cfg | grep –v \\*  
  
Verify the value of the logindelay variable is four or more in each stanza. If the value of logindelay is not four or more, this is a finding.  
  
  
**Fix Text:**Use vi or the chsec command to change the login delay time period.  
  
#chsec –f /etc/security/login.cfg –s default –a logindelay=4   
  
OR  
  
# vi /etc/security/login.cfg   
Add logindelay = 4 to the default stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4083  
**Group Title:** GEN000500  
**Rule ID:** SV-39096r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000500  
**Rule Title:**Graphical desktop environments provided by the system must automatically lock after 15 minutes of inactivity and the system must require users to re-authenticate to unlock the environment.  
  
**Vulnerability Discussion:**  If graphical desktop sessions do not lock the session after 15 minutes of inactivity, requiring re-authentication to resume operations, the system or individual data could be compromised by an alert intruder who could exploit the oversight. This requirement applies to graphical desktop environments provided by the system to locally attached displays and input devices as well as to graphical desktop environments provided to remote systems, including thin clients.  
  
**Responsibility:**  System Administrator  
**IAControls:**  PESL-1  
  
**Check Content:**    
Log into a graphical desktop environment provided by the system. Allow the session to remain idle for 15 minutes. If the desktop session is not automatically locked after 15 minutes, or does not require re-authentication to resume operations, this is a finding.  
  
**Fix Text:**Consult vendor documentation to determine the settings required for the system to lock graphical desktop environments. Configure the system to lock graphical desktop environments after 15 minutes of inactivity and require re-authentication to resume operations.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22301  
**Group Title:** GEN000510  
**Rule ID:** SV-25948r1\_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 (such as a blank screen). This requirement applies to graphical desktop environments provided by the system to locally attached displays and input devices as well as to graphical desktop environments provided to remote systems using remote access protocols.  
  
**Responsibility:**  System Administrator  
**IAControls:**  PESL-1  
  
**Check Content:**    
Determine if a publicly-viewable pattern is displayed during a session lock. If the session lock pattern is not publicly-viewable, this is a finding.  
  
**Fix Text:**Configure the system to display a publicly-viewable pattern during a session lock.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-769  
**Group Title:** GEN000520  
**Rule ID:** SV-769r7\_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 that is continuously in use (such as a network monitoring application), ask the SA what the name of the application is. 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 requiring a continuous screen display, such as a network management display, is not root. Ensure the display is also located in a secure, controlled access area. Document and justify this requirement. Ensure the terminal and keyboard for the display (or workstation) are secure from all but authorized personnel by maintaining them in a secure area, in a locked cabinet where a swipe card, or other positive forms of identification, must be used to gain entry.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1032  
**Group Title:** GEN000540  
**Rule ID:** SV-38768r1\_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 minage field for each user.  
# /usr/sbin/lsuser -a minage ALL  
If the minage field is less than 1 for any user, this is a finding.  
  
  
**Fix Text:**Use SMIT or the chsec command to set the minimum password age to 1 week.  
  
# chsec –f /etc/security/user –s default –a minage=1   
# chsec -f /etc/security/user -s <user id> -a minage=1  
  
OR  
  
# smitty chuser   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-770  
**Group Title:** An account on the system is not password protected  
**Rule ID:** SV-27107r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN000560  
**Rule Title:**The system must not have accounts configured with blank or null passwords.  
  
**Vulnerability Discussion:**  If an account is configured for password authentication but does not have an assigned password, it may be possible to log into the account without authentication. If the root user is configured without a password, the entire system may be compromised. For user accounts not using password authentication, the account must be configured with a password lock value instead of a blank or null value.   
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Verify no accounts have blank passwords.  
# pwdck -n ALL  
If any account with a blank password is found, this is a finding.  
  
**Fix Text:**Remove or configure a password for any account with a blank password.   
  
# passwd <user id>  
# smitty passwd  
  
To remove an account with a blank password.  
# smitty rmuser   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11947  
**Group Title:** GEN000580  
**Rule ID:** SV-38936r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000580  
**Rule Title:**The system must require passwords to 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.  
# /usr/sbin/lsuser -a minlen ALL  
If minlen is not set to 14 or more, this is a finding.  
  
**Fix Text:**Change the minimum password length to 14 or more.   
#chsec –f /etc/security/user –s default –a minlen=14  
#chuser minlen=14 <user id>  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22302  
**Group Title:** GEN000585  
**Rule ID:** SV-38769r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000585  
**Rule Title:**The system must enforce the correctness of the entire password during authentication.  
  
**Vulnerability Discussion:**  Some common password hashing schemes only process the first eight characters of a user's password, which reduces the effective strength of the password.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Verify no password hashes in /etc/password.  
# cat /etc/passwd | cut -f2,2 -d":"  
If there are password hashes present, this is a finding.  
  
Verify no password hashes in the /etc/security/passwd file  
begins with the characters other than (ssha256) or (ssha512)  
  
#cat etc/security/passwd | grep password  
If there are password hashes that do not begin with (ssha256) or (ssha512), this is a finding.  
  
**Fix Text:**Configure the system to enforce the correctness of the entire password during authentication.  
  
Configure the system to use sha password hashing.  
#chsec -f /etc/security/login.cfg -s usw -a pwd\_algorithm=ssha256   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23825  
**Group Title:** GEN000588  
**Rule ID:** SV-38937r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000588  
**Rule Title:**The system must use a FIPS 140-2 validated cryptographic module (operating in FIPS mode) for generating system password hashes.  
  
**Vulnerability Discussion:**  Cryptographic modules used by the system must be validated by the NIST CVMP as compliant with FIPS 140-2. Cryptography performed by modules that are not validated is viewed by NIST as providing no protection for the data.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Determine if the system uses a FIPS 140-2 validated cryptographic module (operating in FIPS mode) for generating system password hashes. The NIST CVMP web site provides a list of validated modules and the required security policies for the compliant use of such modules. Verify the module is on this list and configured in accordance with the validated security policy.  
  
If the system does not use a FIPS 140-2 validated cryptographic module (operating in FIPS mode) for generating system password hashes, this is a finding.  
  
**Fix Text:**Configure the system to use a FIPS 140-2 validated cryptographic module (operating in FIPS mode) for generating system password hashes.   
#chsec –f /etc/security/login.cfg –s usw –a pwd\_algorithm=ssha256  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22303  
**Group Title:** GEN000590  
**Rule ID:** SV-38938r1\_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 that are more vulnerable to compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1, IAIA-1, IAIA-2  
  
**Check Content:**    
Determine if the system creates password hashes using a FIPS 140-2 approved cryptographic hashing algorithm. Consult OS documentation to determine the necessary configuration settings. If the system is not configured to generate password hashes using a FIPS 140-2 approved algorithm, this is a finding.  
  
**Fix Text:**Configure the system to use a FIPS 140-2 approved cryptographic hash algorithm for creating password hashes.   
#chsec –f /etc/security/login.cfg –s usw –a pwd\_algorithm=ssha256   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22304  
**Group Title:** GEN000595  
**Rule ID:** SV-38672r1\_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 that are more vulnerable to compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1, IAIA-1, IAIA-2  
  
**Check Content:**    
Verify all password hashes in /etc/security/passwd begin with {ssha256} or {ssha512}.  
  
Procedure:  
# cat /etc/passwd | cut -f2,2 -d “:”  
  
# cat /etc/security/passwd | grep   
passwd  
  
If any password hashes are present not beginning with (ssha256) or {ssha512}, this is a finding.  
  
  
  
**Fix Text:**Change the passwords for all accounts using non-compliant password hashes.   
  
# passwd account  
OR  
# smitty passwd  
  
(This requires that GEN000590 is already met.)   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11948  
**Group Title:** GEN000600  
**Rule ID:** SV-38673r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000600  
**Rule Title:**The system must require passwords to contain at least one uppercase alphabetic character.  
  
**Vulnerability Discussion:**  To enforce the use of complex passwords, minimum numbers of characters of different classes are mandated. The use of complex passwords reduces the ability of attackers to successfully obtain valid passwords using guessing or exhaustive search techniques. Complexity requirements increase the password search space by requiring users to construct passwords from a larger character set than they may otherwise use.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the minalpha setting.  
  
Procedure:  
  
# grep minalpha /etc/security/user   
OR  
#lsuser –a minalpha ALL  
If minalpha is not set to 1 or more, this is a finding.  
  
**Fix Text:**Use the chsec command to set minalpha to at least 1.   
#chsec –f /etc/security/user –s default –a minalpha=1  
#chuser minalpha=1 < user id >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22305  
**Group Title:** GEN000610  
**Rule ID:** SV-38771r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000610  
**Rule Title:**The system must require passwords to 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:**    
NOTE: This will always require a manual review. More importantly, AIX by default does not currently support enforcement of upper and lower case characters in passwords. This is considered a local, written policies check. Consult site documentation for the local policy specifying non-use of mixed case characters in passwords. If it does not, this is a finding.   
  
**Fix Text:**No Fix. AIX does not provide this functionality out of the box.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11972  
**Group Title:** GEN000620  
**Rule ID:** SV-38674r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000620  
**Rule Title:**The system must require passwords to contain at least one numeric character.  
  
**Vulnerability Discussion:**  To enforce the use of complex passwords, minimum numbers of characters of different classes are mandated. The use of complex passwords reduces the ability of attackers to successfully obtain valid passwords using guessing or exhaustive search techniques. Complexity requirements increase the password search space by requiring users to construct passwords from a larger character set than they may otherwise use.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the minother setting.  
  
Procedure:  
# grep minother /etc/security/user  
#lsuser -a minother ALL  
If the minother setting is less than 1, this is a finding.  
  
  
**Fix Text:**Use the chsec command to set the minother setting to 1.  
#chsec –f /etc/security/user –s default –a minother=1  
  
#chuser minother=1 < user id >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11973  
**Group Title:** GEN000640  
**Rule ID:** SV-39503r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000640  
**Rule Title:**The system must require that 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 minother setting.  
  
Procedure:  
# grep minother /etc/security/user  
#lsuser -a minother ALL  
If the minother setting is less than 1, this is a finding.  
  
**Fix Text:**Use the chsec command to set the minother setting to 1.  
#chsec –f /etc/security/user –s default –a minother=1  
  
#chuser minother=1 < user id >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11975  
**Group Title:** GEN000680  
**Rule ID:** SV-38675r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000680  
**Rule Title:**The system must require passwords to contain no more than three consecutive repeating characters.  
  
**Vulnerability Discussion:**  To enforce the use of complex passwords, the number of consecutive repeating characters is limited. Passwords with excessive repeated characters may be more vulnerable to password-guessing attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the maxrepeats setting.  
  
Procedure:  
  
# grep -i maxrepeats /etc/security/user  
#lsuser –a maxrepeats ALL  
If the maxrepeats setting is greater than 3, this is a finding.  
  
**Fix Text:**Use the chsec command to set maxrepeats to 3.  
#chsec –f /etc/security/user –s default –a maxrepeats=3  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11976  
**Group Title:** GEN000700  
**Rule ID:** SV-38939r1\_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 maxage field for each user. The field represents the number of weeks a password is valid.  
  
Procedure:  
# /usr/sbin/lsuser -a maxage ALL  
If the maxage field is 0 or greater than 8 for any user, this is a finding.  
  
**Fix Text:**Use the chsec command to set the maxage field to 7 for each user.  
#chsec –f /etc/security/user –s default –a maxage=7   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11977  
**Group Title:** GEN000740  
**Rule ID:** SV-38676r1\_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:**    
NOTE: This will always require a manual review. This is a local policy issue/question. Ask the SA if there are any automated processing accounts on the system. If there are automated processing accounts on the system, ask the SA if the passwords for those automated accounts are changed at least once a year. If the SA indicates passwords for automated processing accounts are not changed once per year, this is a finding.  
  
Procedure:  
Get the last password change date for the system account.  
#grep –p <account\_name> /etc/security/passwd | grep lastupdate  
To examine the time a password was last changed, the following perl script has been provided. Put the lastupdate value in the <lastupdate>.  
#perl –e ‘use POSIX; print strftime(“%c\n” , localtime(<lastupdate>));’  
  
**Fix Text:**Implement or establish procedures to change the passwords of automated processing accounts at least once per year.   
#passwd account   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22306  
**Group Title:** GEN000750  
**Rule ID:** SV-38677r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000750  
**Rule Title:**The system must require at least four characters be changed between the old and new passwords during a password change.  
  
**Vulnerability Discussion:**  To ensure password changes are effective in their goals, the system must ensure old and new passwords have significant differences. Without significant changes, new passwords may be easily guessed based on the value of a previously compromised password.  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the value of the mindiff parameter.  
Procedure:  
#lsuser –a mindiff ALL  
If any users mindiff is less than 4, this is a finding.  
  
**Fix Text:** Use the chsec command to change mindiff to 4.  
#chsec –f /etc/security/user –s default –a mindiff=4.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-918  
**Group Title:** GEN000760  
**Rule ID:** SV-38840r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000760  
**Rule Title:**Accounts must be locked upon 35 days of inactivity.  
  
**Vulnerability Discussion:**  On some systems, accounts with disabled passwords still allow access using rcp, remsh, or rlogin through equivalent remote hosts. All that is required is the remote host name and the user name match an entry in a hosts.equiv file and have a .rhosts file in the user directory. Using a shell called /bin/false or /dev/null (or an equivalent) will add a layered defense.  
  
Non-interactive accounts on the system, such as application accounts, may be documented exceptions.  
  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  IAAC-1  
  
**Check Content:**    
Indications of inactive accounts are those without entries in the last log. Check the date in the last log to verify it is within the last 35 days. If an inactive account is not disabled via an invalid login shell /bin/false entry in the shell field of the /etc/passwd file or account\_locked = true in /etc/security/user file, this is a finding.  
  
**Fix Text:**All inactive accounts will have /bin/false, /usr/bin/false, or /dev/null as the default shell in the /etc/passwd file and have the password disabled. Disable the inactive accounts. Examine the inactive accounts using the last command. NOTR: The date of last login for each account. If any (other than system and application accounts) exceed 35 days, then disable them by placing a shell of /bin/false or /dev/null in the shell field of the passwd file entry for that account. An alternative, and preferable method, is to disable the account using SMIT or the chsec command.   
  
Change the accounts login shell  
#chsh <account> /bin/false  
  
Lock the account in /etc/security/user file   
#chuser account\_locked=true < user id >  
OR  
# smitty chuser  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22307  
**Group Title:** GEN000790  
**Rule ID:** SV-38678r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000790  
**Rule Title:**The system must prevent the use of dictionary words for passwords.  
  
**Vulnerability Discussion:**  An easily guessable password provides an open door to any external or internal malicious intruder. Many computer compromises occur as the result of account name and password guessing. This is generally done by someone with an automated script using repeated logon attempts until the correct account and password pair is guessed. Utilities, such as cracklib, can be used to validate that passwords are not dictionary words and meet other criteria during password changes.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Procedure:  
#lsuser –a dictionlist ALL  
  
If the dictionlist is blank or not listed the system is not checking against a dictionary of words that are not to be used for passwords. This is a finding.  
  
  
**Fix Text:**Install the default dictionary of words from the ‘bos.data’ fileset with smitty or installp.  
# smitty installp  
#installp bos.data   
  
Customize or modify the dictionary in /usr/share/dict/words as necessary.  
#vi /usr/share/dict/words  
  
Add a dictionary list to /etc/security/user file with the chsec command.  
#chsec –f /etc/security/user –s default –a dictionlist=/usr/share/dict/words   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4084  
**Group Title:** GEN000800  
**Rule ID:** SV-38679r1\_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:**    
Procedure:  
#lsuser –a histsize ALL  
If the returned histsize for any user is less than 5, this is a finding.  
  
  
**Fix Text:**Use the chsec command to configure the system to prohibit the reuse of passwords within five iterations.   
#chsec –f /etc/security/user –s default –a histsize=5  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22308  
**Group Title:** GEN000850  
**Rule ID:** SV-38680r1\_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:**    
Examine the sugroups of the root user. Generally only users in the adm group should have su – to root capacity,  
  
Procedure:  
#lsuser –a sugroups root  
If this is blank or ALL, this is a finding.  
  
  
**Fix Text:**Use the chsec command to only allow users in the adm group to su to root.  
#chsec –f /etc/security/user –s root –a sugroups=adm  
  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-773  
**Group Title:** An account other than root has a UID of 0.  
**Rule ID:** SV-773r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000880  
**Rule Title:**The root account must be the only account having an UID of 0.  
  
**Vulnerability Discussion:**  If an account has an UID of 0, it has root authority. Multiple accounts with an UID of 0 afford more opportunity for potential intruders to guess a password for a privileged account.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the system for duplicate UID 0 assignments by listing all accounts assigned UID 0.  
  
Procedure:  
# grep ":0:" /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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-774  
**Group Title:** GEN000900  
**Rule ID:** SV-38940r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN000900  
**Rule Title:**The root user's home directory must not be the root directory (/).  
  
**Vulnerability Discussion:**  Changing the root home directory to something other than / and assigning it a 0700 protection makes it more difficult for intruders to manipulate the system by reading the files that root places in its default directory. It also gives root the same discretionary access control for root's home directory as for the other plain user home directories.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Determine if root is assigned a home directory other than / by listing its home directory.  
  
Procedure:  
# grep "^root" /etc/passwd | awk -F":" '{print $6}'  
  
If the root user home directory is /, this is a finding.  
  
**Fix Text:**The root home directory should be something other than / (such as /root).  
  
Procedure:  
# mkdir /root  
# chown root /root  
# chgrp root /root  
# chmod 700 /root  
# cp -r /.??\* /root/.  
  
Then, edit the passwd file and change the root home directory to /root. The cp –r /.??\* command copies all files and subdirectories of file names that begin with “.” into the new root directory, which preserves the previous root environment. Ensure you are in the “/” directory when executing the “cp” command.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-775  
**Group Title:** GEN000920  
**Rule ID:** SV-38941r1\_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 is not applicable.  
  
**Fix Text:**The root home directory will have permissions of 0700. Do not change the protections of the / directory. Use the following command to change protections for the root home directory:   
# chmod 0700 /root.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22309  
**Group Title:** GEN000930  
**Rule ID:** SV-38690r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000930  
**Rule Title:**The root account's home directory must not have an extended ACL.  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the root account's home directory has no extended ACL.  
  
Procedure:  
# aclget ~root  
If extended permissions are enabled, the directory has an extended ACL, and this is a finding.   
  
**Fix Text:**Remove the extended ACL from the root account's home directory.  
#acledit ~/root   
Change extended attributes to disabled.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-776  
**Group Title:** GEN000940  
**Rule ID:** SV-776r7\_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:**  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. 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22310  
**Group Title:** GEN000945  
**Rule ID:** SV-38770r1\_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) contains a list of directories for the dynamic linker to search to find libraries. If this path includes the current working directory or other relative paths, libraries in these directories may be loaded instead of system libraries. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon or two consecutive colons, this is interpreted as the current working directory. Entries starting with a slash (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the LIBPATH and LD\_LIBRARY\_PATH variables are empty or not defined for the root user.  
  
# echo $LD\_LIBRARY\_PATH  
# echo $LIBPATH  
  
If a path list is returned, this is a finding.  
  
**Fix Text:**Edit the root user's initialization files and remove any definition of LD\_LIBRARY\_PATH and LIBPATH.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22311  
**Group Title:** GEN000950  
**Rule ID:** SV-38772r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000950  
**Rule Title:**The root account's list of preloaded libraries must be empty.  
  
**Vulnerability Discussion:**  The library preload list environment variable contains a list of libraries for the dynamic linker to load before loading the libraries required by the binary. If this list contains paths to libraries relative to the current working directory, unintended libraries may be preloaded. This variable is formatted as a space-separated list of libraries. Paths starting with (/) are absolute paths.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Verify the LDR\_PRELOAD environment variable is empty or not defined for the root user.  
  
# env | grep LDR\_PRELOAD  
  
If a path is returned, this is a finding.  
  
**Fix Text:**Edit the root users initialization files and remove any definition of LDR\_PRELOAD.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-777  
**Group Title:** GEN000960  
**Rule ID:** SV-777r7\_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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-778  
**Group Title:** GEN000980  
**Rule ID:** SV-38683r1\_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  
  
**Check Content:**    
Check the remote login ability of the root account.  
  
Procedure:  
# lsuser –a rlogin root  
If the rlogin value is not false, this is a finding.  
  
**Fix Text:**The root account can be protected from non-console device logins by setting rlogin = false in the root: stanza of the /etc/security/user file.  
  
#chsec –f /etc/security/user –s root rlogin=false   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4298  
**Group Title:** GEN001000  
**Rule ID:** SV-27149r1\_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/security/login.cfg  
# more /etc/security/login.cfg  
If an alternate console is defined, this is a finding.  
  
**Fix Text:**Edit /etc/security/login.cfg and remove the alternate console definition.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11979  
**Group Title:** Direct Root Login  
**Rule ID:** SV-12480r5\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001020  
**Rule Title:**The root account must not be used for direct logins.  
  
**Vulnerability Discussion:**  Direct login with the root account prevents individual user accountability. Acceptable non-routine uses of the root account for direct login are limited to emergency maintenance, the use of single-user mode for maintenance, and situations where individual administrator accounts are not available.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Check if the root is used for direct logins.  
  
Procedure:  
# last root | grep –v reboot  
  
If the last command is not available, consult vendor documentation to determine an appropriate method for obtaining a list of root account logins.  
  
If any direct login records for root exist, 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 (using su, for example).   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11980  
**Group Title:** GEN001060  
**Rule ID:** SV-27154r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001060  
**Rule Title:**The system must log successful and unsuccessful access to the root account.  
  
**Vulnerability Discussion:**  If successful and unsuccessful logins and logouts are not monitored or recorded, access attempts cannot be tracked. Without this logging, it may be impossible to track unauthorized access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the following log files to determine if access to the root account is being logged. Try to su - and enter an incorrect password.  
  
# more /var/adm/sulog  
  
If root login accounts are not being logged, this is a finding.  
  
**Fix Text:**Troubleshoot the system logging configuration to provide for logging of root account login attempts.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1062  
**Group Title:** GEN001080  
**Rule ID:** SV-38773r1\_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 /usr has a dedicated file system.  
  
Procedure:  
# grep /usr: /etc/filesystems  
  
If /usr is on a dedicated file system, check the location of root's default shell.  
  
Find the location of the root users shell.  
# grep "^root" /etc/passwd|cut -d: -f7|cut -d/ -f2   
  
If the root shell is found to be on a /usr 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1046  
**Group Title:** GEN001100  
**Rule ID:** SV-39097r1\_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:**  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:**Install OpenSSH from AIX installation media or AIX Expansion Pack.   
#smitty installp  
  
Enable SSH on the system and use it for all remote connections used to attain root access.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1047  
**Group Title:** Encrypting Root Access  
**Rule ID:** SV-38684r1\_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:  
# find / -name sshd\_config – ls# grep –v “^#” <sshd\_config path and file> | grep –i permitrootlogin  
  
If the PermitRootLogin entry is not found or is not set to no, this is a finding.  
  
**Fix Text:**Edit the /etc/ssh/sshd\_config file and set the PermitRootLogin option to no and refresh sshd.   
#kill -1 <pid of sshd>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-784  
**Group Title:** GEN001140  
**Rule ID:** SV-784r6\_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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-785  
**Group Title:** GEN001160  
**Rule ID:** SV-38942r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001160  
**Rule Title:**All files and directories must have a valid owner.  
  
**Vulnerability Discussion:**  Unowned files and directories may be unintentionally inherited if a user is assigned the same UID as the UID of the unowned files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the system for files with no assigned owner.  
  
Procedure:  
# find / -nouser -print  
  
If any files have no assigned owner, this is a finding.  
  
**Fix Text:**: All directories and files (executable and data) will have an identifiable owner and group name. Either trace files to an authorized user, change the file’s owner to root, or delete them. Determine the legitimate owner of the files and use the chown command to set the owner and group to the correct value. If the legitimate owner cannot be determined, change the owner to root (but make sure none of the changed files remain executable because they could be Trojan horses or other malicious code). Examine the files to determine their origin and the reason for their lack of an owner/group.   
#chown <a-valid-user> <directory>/<file>  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22312  
**Group Title:** GEN001170  
**Rule ID:** SV-25959r1\_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:**    
Determine if any file on the system does not have a valid group owner. If any such 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   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-786  
**Group Title:** GEN001180  
**Rule ID:** SV-38774r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001180  
**Rule Title:**All network services daemon files must have mode 0755 or less permissive.  
  
**Vulnerability Discussion:**  Restricting permission on daemons will protect them from unauthorized modification and possible system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of network services daemons.  
# ls -la /usr/sbin /usr/bin   
If the mode of a network services daemon is more permissive than 0755, this is a finding.  
NOTE: Network daemons that may not reside 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 0755 <path>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22313  
**Group Title:** GEN001190  
**Rule ID:** SV-38685r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001190  
**Rule Title:**All network services daemon files must not have extended ACLs.  
  
**Vulnerability Discussion:**  Restricting permission on daemons will protect them from unauthorized modification and possible system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify network services daemon files have no extended ACLs.   
# aclget <directory>/<network service daemon>   
NOTE: Network daemons that may not reside in these directories (such as httpd or sshd) must also be checked for extended ACLs.  
If any of the service daemons have extended attributes enabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL(s) from the network service daemon file(s).  
#acledit < directory >/< network service daemon >  
Disable extended permissions.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-794  
**Group Title:** GEN001200  
**Rule ID:** SV-794r7\_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.  
  
**Security 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:  
# ls -lL /etc /bin /usr/bin /usr/lbin /usr/usb /sbin /usr/sbin  
  
If any file listed has a mode more permissive than 0755, this is a finding.  
  
NOTE: Elevate to Severity Code I if any file listed world-writable.  
  
**Fix Text:**Change the mode for system command files to 0755 or less permissive.  
  
Procedure:  
# chmod 0755 <filename>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22314  
**Group Title:** GEN001210  
**Rule ID:** SV-38686r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001210  
**Rule Title:**All system command files must not have extended ACLs.  
  
**Vulnerability Discussion:**  Restricting permissions will protect system command files from unauthorized modification. System command files include files present in directories used by the operating system for storing default system executables and files present in directories included in the system's default executable search paths.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify all system command files have no extended ACLs.  
  
# aclget /etc  
# aclget /bin   
# aclget /usr/bin   
# aclget /usr/lbin   
# aclget /usr/usb  
# aclget /sbin   
# aclget /usr/sbin  
  
If any of the command files have extended permissions enabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL(s) from the system command file(s) and set the extended permissions to disabled.  
  
#acledit < command path >/< command file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-795  
**Group Title:** GEN001220  
**Rule ID:** SV-795r7\_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.)   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-796  
**Group Title:** GEN001240  
**Rule ID:** SV-39098r1\_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 sys /path/to/system/file (System groups other than sys may be used.)   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-787  
**Group Title:** GEN001260  
**Rule ID:** SV-787r9\_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  
  
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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22315  
**Group Title:** GEN001270  
**Rule ID:** SV-38687r1\_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:**    
Determine if any system log file has an extended ACL. If an extended ACL exists, verify with the SA if the ACL is required to support authorized software and provides the minimum necessary permissions. If an extended ACL exists that provides access beyond the needs of authorized software, this is a finding.  
  
Check to see if extended permissions are disabled.  
#aclget <directory>/<file>  
  
**Fix Text:**Remove the extended ACL(s) from the system log file(s) and disable extended permissions,  
  
# acledit < directory >/< file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-792  
**Group Title:** GEN001280  
**Rule ID:** SV-792r7\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001280  
**Rule Title:**Manual page files must have mode 0644 or less permissive.  
  
**Vulnerability Discussion:**  If manual pages are compromised, misleading information could be inserted, causing actions that may compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the mode of the manual page files.  
  
Procedure:  
# ls –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>/<manpage>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22316  
**Group Title:** GEN001290  
**Rule ID:** SV-38688r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001290  
**Rule Title:**All manual page files must not have extended ACLs.  
  
**Vulnerability Discussion:**  If manual pages are compromised, misleading information could be inserted, causing actions that may compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine if any manual page files on the system have extended ACLs.  
  
Check to see if extended permissions are disabled.  
#aclget < directory >/< file >   
If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACLs from system manual page file(s) and disable extended permissions.  
  
#acledit < directory >/< file >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-793  
**Group Title:** GEN001300  
**Rule ID:** SV-38943r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001300  
**Rule Title:**Library files must have mode 0755 or less permissive.  
  
**Vulnerability Discussion:**  Unauthorized access could destroy the integrity of the library files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Check the mode of library files.  
  
Procedure:  
# ls –lLR /usr/lib /lib  
  
If any of the library files have a mode more permissive than 0755, this is a finding.  
  
**Fix Text:**Change the mode of library files to 0755 or less permissive.  
  
Procedure (example):  
# chmod 0755 <path>/<library-file>  
  
NOTE: Library files should have an extension of .a or a .so (a=archive, so=shared object) extension, possibly followed by a version.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22317  
**Group Title:** GEN001310  
**Rule ID:** SV-38689r1\_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:**    
Determine if any system library file has an extended ACL. If so, this is a finding.  
  
Check to see if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
#aclget < directory >/< file >   
  
**Fix Text:**Remove the extended ACL(s) from the system library file(s) and disable extended permissions.  
  
#acledit < directory >/< file >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-789  
**Group Title:** GEN001320  
**Rule ID:** SV-38775r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001320  
**Rule Title:**NIS/NIS+/yp files must be owned by root, sys, or bin.  
  
**Vulnerability Discussion:**  NIS/NIS+/yp files are part of the system's identification and authentication processes and are, therefore, critical to system security. Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Perform the following to check NIS file ownership:  
# ls -la /var/nis or /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, bin, or system. Consult vendor documentation to determine the location of the files.  
  
Procedure (example):  
# chown root <filename>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-790  
**Group Title:** GEN001340  
**Rule ID:** SV-38776r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001340  
**Rule Title:**NIS/NIS+/yp files must be group-owned by root, sys, bin, other, or system.  
  
**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:**    
Check the group ownership of the NIS files.  
  
Procedure:  
# ls /var/nis or /var/yp  
  
If the file group-owner is not root, sys, bin, or system, this is a finding.  
  
  
**Fix Text:**Change the group owner of the NIS files to root, sys, bin, system, or other.   
Procedure:  
# chgrp system < directory>/< file >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-791  
**Group Title:** GEN001360  
**Rule ID:** SV-38781r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001360  
**Rule Title:**The NIS/NIS+/yp command files must have mode 0755 or less permissive.  
  
**Vulnerability Discussion:**  NIS/NIS+/yp files are part of the system's identification and authentication processes and are, therefore, critical to system security. Unauthorized modification of these files could compromise these processes and the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Perform the following to check NIS file mode:  
# ls -la /var/nis or /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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22318  
**Group Title:** GEN001361  
**Rule ID:** SV-38691r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001361  
**Rule Title:**NIS/NIS+/yp command files must not have extended ACLs.  
  
**Vulnerability Discussion:**  NIS/NIS+/yp files are part of the system's identification and authentication processes and are, therefore, critical to system security. ACLs on these files could result in unauthorized modification, which could compromise these processes and the system.   
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine if any NIS/NIS+/yp command files have an extended ACL. Check if extended permissions are disabled.  
  
Procedure:  
  
# aclget /var/nis   
# aclget /var/yp   
If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the NS/NIS+/yp command file(s) and disable extended permissions.  
  
#acledit < directory >/< file >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22319  
**Group Title:** GEN001362  
**Rule ID:** SV-26395r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001362  
**Rule Title:**The /etc/resolv.conf file must be owned by root.  
  
**Vulnerability Discussion:**  The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions such as time synchronization, centralized authentication, and remote system logging.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the /etc/resolv.conf file is owned by root.  
  
Procedure:  
# ls -l /etc/resolv.conf  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/resolv.conf file to root.  
# chown root /etc/resolv.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22320  
**Group Title:** GEN001363  
**Rule ID:** SV-39099r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001363  
**Rule Title:**The /etc/resolv.conf file must be group-owned by root, bin, sys, or system.  
  
**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, sys, or system, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/resolv.conf file to root, bin, sys, or system.  
  
Procedure:  
# chgrp system /etc/resolv.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22321  
**Group Title:** GEN001364  
**Rule ID:** SV-26397r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001364  
**Rule Title:**The /etc/resolv.conf file must have mode 0644 or less permissive.   
  
**Vulnerability Discussion:**  The resolv.conf (or equivalent) file configures the system's DNS resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions such as time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/resolv.conf file.  
  
Procedure:  
# ls -l /etc/resolv.conf  
If the file mode is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/resolv.conf file to 0644 or less permissive.  
  
# chmod 0644 /etc/resolv.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22322  
**Group Title:** GEN001365  
**Rule ID:** SV-38692r1\_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.  
Check if extended permissions are disabled.  
  
Procedure:  
  
#aclget /etc/resolv.conf   
If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from /etc/resolv.conf file and disable extended permissions.  
  
#acledit /etc/resolv.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22323  
**Group Title:** GEN001366  
**Rule ID:** SV-26410r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001366  
**Rule Title:**The /etc/hosts file must be owned by root.  
  
**Vulnerability Discussion:**  The /etc/hosts file (or equivalent) configures local host name to IP address mappings that typically take precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the /etc/hosts file is owned by root.  
  
Procedure:  
# ls -l /etc/hosts  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/hosts file to root.  
  
# chown root /etc/hosts   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22324  
**Group Title:** GEN001367  
**Rule ID:** SV-39100r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001367  
**Rule Title:**The /etc/hosts file must be group-owned by root, bin, sys, or system.  
  
**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, sys, or system, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/hosts file to root, sys, bin, or system.  
  
Procedure:  
# chgrp system /etc/hosts   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22325  
**Group Title:** GEN001368  
**Rule ID:** SV-26412r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001368  
**Rule Title:**The /etc/hosts file must have mode 0644 or less permissive.  
  
**Vulnerability Discussion:**  The /etc/hosts file (or equivalent) configures local host name to IP address mappings that typically take precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/hosts file.  
  
Procedure:  
# ls -l /etc/hosts  
If the file mode is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/hosts file to 0644 or less permissive.  
  
# chmod 0644 /etc/hosts   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22326  
**Group Title:** GEN001369  
**Rule ID:** SV-38693r1\_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.  
Check if extended permissions are disabled.  
Procedure:  
  
#aclget /etc/hosts   
If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the /etc/hosts file and disable extended permissions.   
  
#acledit /etc/hosts   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22327  
**Group Title:** GEN001371  
**Rule ID:** SV-39330r1\_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.  
  
AIX does not use the /etc/nsswitch.conf file. This check is not applicable.  
  
Procedure:  
# ls -l /etc/nsswitch.conf  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/nsswitch.conf file to root.  
  
# chown root /etc/nsswitch.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22328  
**Group Title:** GEN001372  
**Rule ID:** SV-39101r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001372  
**Rule Title:**The /etc/nsswitch.conf file must be group-owned by root, bin, sys, or system.  
  
**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.  
  
AIX does not use the /etc/nsswitch.conf file. This check is not applicable.  
  
Procedure:  
# ls -lL /etc/nsswitch.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 /etc/nsswitch.conf file to root, bin, sys, or system.  
  
Procedure:  
# chgrp system /etc/nsswitch.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22329  
**Group Title:** GEN001373  
**Rule ID:** SV-39332r1\_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.  
  
AIX does not use the /etc/nsswitch.conf file. This check is not applicable.  
  
Procedure:  
# ls -l /etc/nsswitch.conf  
If the file mode is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/nsswitch.conf file to 0644 or less permissive.  
  
# chmod 0644 /etc/nsswitch.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22330  
**Group Title:** GEN001374  
**Rule ID:** SV-39334r1\_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.   
  
AIX does not use the /etc/nsswitch.conf file. This check is not applicable.  
  
Procedure:   
# aclget /etc/nsswitch.conf   
If extended permissions are enabled, this is a finding.   
  
**Fix Text:**Remove the extended ACL from the /etc/nsswitch.conf file.   
  
# acledit /etc/nsswitch.conf  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22331  
**Group Title:** GEN001375  
**Rule ID:** SV-38877r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001375  
**Rule Title:**For systems using DNS resolution, at least two name servers must be configured.  
  
**Vulnerability Discussion:**  To provide availability for name resolution services, multiple redundant name servers are mandated. A failure in name resolution could lead to the failure of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if DNS is enabled on the system.  
  
# grep ^hosts= /etc/netsvc.conf | grep bind  
  
If no line is returned, or any returned line is commented out, the system does not use DNS, and this is not applicable.  
  
Determine the name servers used by the system.  
# grep nameserver /etc/resolv.conf  
If less than two lines are returned not commented out, this is a finding.  
  
**Fix Text:**Edit /etc/resolv.conf and add additional nameserver lines until at least two are present.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22332  
**Group Title:** GEN001378  
**Rule ID:** SV-26425r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001378  
**Rule Title:**The /etc/passwd file must be owned by root.  
  
**Vulnerability Discussion:**  The /etc/passwd file contains the list of local system accounts. It is vital to system security and must be protected from unauthorized modification.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the /etc/passwd file is owned by root.  
  
Procedure:  
# ls -l /etc/passwd  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/passwd file to root.  
  
# chown root /etc/passwd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22333  
**Group Title:** GEN001379  
**Rule ID:** SV-38723r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001379  
**Rule Title:**The /etc/passwd file must be group-owned by root, bin, security, sys, or system.  
  
**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 security, root, bin, sys, or system, this is a finding.  
  
  
**Fix Text:**Change the group-owner of the /etc/passwd file to security, root, bin, sys, or system.  
  
Procedure:  
# chgrp security /etc/passwd   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-798  
**Group Title:** /etc/passwd File Permissions  
**Rule ID:** SV-798r7\_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  
  
Document all changes.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22334  
**Group Title:** GEN001390  
**Rule ID:** SV-38724r1\_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 the /etc/passwd file has no extended ACL.  
  
Procedure:  
#aclget /etc/passwd   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the /etc/passwd file. and disable extended permissions.  
  
#acledit /etc/passwd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22335  
**Group Title:** GEN001391  
**Rule ID:** SV-26431r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001391  
**Rule Title:**The /etc/group file must be owned by root.  
  
**Vulnerability Discussion:**  The /etc/group file is critical to system security and must be owned by a privileged user. The group file contains a list of system groups and associated information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Verify the /etc/group file is owned by root.  
  
Procedure:  
# ls -l /etc/group  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/group file to root.  
  
# chown root /etc/group   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22336  
**Group Title:** GEN001392  
**Rule ID:** SV-38725r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001392  
**Rule Title:**The /etc/group file must be group-owned by root, bin, sys, or system.  
  
**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 security, root, bin, sys, or system, this is a finding.  
  
  
**Fix Text:**Change the group owner of the /etc/group file.  
  
# chgrp security /etc/group  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22337  
**Group Title:** GEN001393  
**Rule ID:** SV-26433r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001393  
**Rule Title:**The /etc/group file must have mode 0644 or less permissive.  
  
**Vulnerability Discussion:**  The /etc/group file is critical to system security and must be protected from unauthorized modification. The group file contains a list of system groups and associated information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the /etc/group file.  
  
Procedure:  
# ls -l /etc/group  
If the file mode is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/group file to 0644 or less permissive.  
# chmod 0644 /etc/group   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22338  
**Group Title:** GEN001394  
**Rule ID:** SV-38726r1\_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 the /etc/group file has no extended ACL.  
  
Procedure:  
  
#aclget /etc/group   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the /etc/group file and disable extended permissions.  
  
#acledit /etc/group   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-797  
**Group Title:** /etc/passwd and/or /etc/shadow File Ownership  
**Rule ID:** SV-38944r1\_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/security/passwd file.  
Procedure:  
# ls -lL /etc/security/passwd  
If the owner of this file is not root, this is a finding.  
  
**Fix Text:**Change the ownership of the /etc/security/passwd file.  
# chown root /etc/security/passwd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22339  
**Group Title:** GEN001410  
**Rule ID:** SV-38727r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001410  
**Rule Title:**The /etc/shadow file (or equivalent) must be group-owned by root, bin, sys, or system.  
  
**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/security/passwd file.  
  
Procedure:  
# ls -lL   
/etc/security/passwd  
  
If the file is not group-owned by security, root, bin, sys, or system, this is a finding.  
  
**Fix Text:**Change the group-owner of the /etc/security/passwd file.  
  
Procedure:  
# chgrp security /etc/security/passwd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-800  
**Group Title:** /etc/shadow File Permissions  
**Rule ID:** SV-38728r1\_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/security/passwd file.  
Procedure:  
# ls -lL /etc/security/passwd  
If the mode of this file is more permissive than 0400, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the /etc/shadow (or equivalent) file.  
# chmod 0400/etc/security/passwd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22340  
**Group Title:** GEN001430  
**Rule ID:** SV-38729r1\_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 the /etc/security/passwd file has no extended ACL and check if extended permissions are disabled.  
Procedure:   
#aclget /etc/security/passwd  
If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the /etc/security/passwd file   
and disable extended permissions.  
  
#acledit /etc/security/passwd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-899  
**Group Title:** Assign Home Directories  
**Rule ID:** SV-27186r1\_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 usrck to verify home directory assignments are present.  
Procedure:  
# usrck -n ALL  
If any user is not assigned a home directory, this is a finding.  
  
  
**Fix Text:**Assign a home directory to any user without one.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-900  
**Group Title:** Assigned Home Directories Exist  
**Rule ID:** SV-27194r1\_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 check that assigned home directories exist.  
Procedure:  
# usrck -n ALL  
If any user's assigned home directory does not exist, this is a finding.  
  
**Fix Text:**If a user has no home directory, determine why. If possible, delete accounts that have no home directory. If the account is valid, then create the home directory using the appropriate system administration utility or manually.  
For instance: mkdir directoryname; copy the skeleton files into the directory; chown accountname for the new directory and the skeleton files. Document all changes.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22347  
**Group Title:** GEN001470  
**Rule ID:** SV-38841r1\_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:**    
AIX Does not store password hashes in the world read-able /etc/passwd file, so this check does not apply. Mark this as 'not a finding'.  
  
**Fix Text:**No fix, AIX is compliant.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22348  
**Group Title:** GEN001475  
**Rule ID:** SV-26447r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001475  
**Rule Title:**The /etc/group file must not contain any group password hashes.  
  
**Vulnerability Discussion:**  Group passwords are typically shared and should not be used. Additionally, if password hashes are readable by non-administrators, the passwords are subject to attack through lookup tables or cryptographic weaknesses in the hashes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the /etc/group file for password hashes.  
Procedure:  
# cut -d : -f 2 /etc/group | egrep -v '^(x|!)$'  
If any password hashes are returned, this is a finding.  
  
**Fix Text:**Edit /etc/group and change the password field to an exclamation point (!) to lock the group password.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-901  
**Group Title:** GEN001480  
**Rule ID:** SV-901r8\_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:  
# ls -ld `awk -F":" '{print $6}' /etc/passwd` | more  
  
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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22350  
**Group Title:** GEN001490  
**Rule ID:** SV-38730r1\_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.  
Procedure:  
# cat /etc/passwd | cut –f 6,6 –d “:” | xargs -n1 aclget  
Check if extended permissions are disabled.  
If extended permissions are not disabled, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the user home directory and disable extended permissions.  
  
#acledit <directory>/<file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-902  
**Group Title:** GEN001500  
**Rule ID:** SV-902r7\_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:  
# ls –lLd <user home directory>  
  
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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-903  
**Group Title:** GEN001520  
**Rule ID:** SV-903r7\_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 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:  
# ls –lLd <user home directory>  
  
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:  
# chgrp groupname directoryname  
  
(Replace examples with appropriate group and home directory.)  
  
Document all changes.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-914  
**Group Title:** GEN001540  
**Rule ID:** SV-914r7\_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 /<usershomedirecotory> ! –fstype nfs ! –user <username> ! /( –name .login –o –name .cshrc –o –name .logout –o –name .profile –o –name .bash\_profile –o –name .bbashrc –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   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22351  
**Group Title:** GEN001550  
**Rule ID:** SV-26453r1\_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 associated with the user's account.  
# 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 [user's primary group] [file with bad group ownership]   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-915  
**Group Title:** GEN001560  
**Rule ID:** SV-915r6\_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:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
For each user in the /etc/passwd file, check for files and directories with a mode more permissive than 0750.  
  
Procedure:  
# find /<usershomedirecotory> ! –fstype nfs ! /( –name .login –o –name .cshrc –o –name .logout –o –name .profile –o –name .bash\_profile –o –name .bbashrc –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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22352  
**Group Title:** GEN001570  
**Rule ID:** SV-38731r1\_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.  
Procedure:  
# cat /etc/passwd | cut -f 6,6 –d “:” | xargs -n1 -IDIR –aclget DIR  
OR  
#aclget <directory>/<file>   
Check if extended permissions are disabled.  
If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL(s) from the files and directories in user home directories and disable extended permissions.  
  
#acledit <directory>/<file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-906  
**Group Title:** GEN001580  
**Rule ID:** SV-38732r1\_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\*  
#find rc\* -ls   
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, 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 startupfile   
Document all changes.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22353  
**Group Title:** GEN001590  
**Rule ID:** SV-38733r1\_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.  
Check if extended permissions are disabled.  
# ls -l /etc/rc\*  
# aclget /etc/rc\*   
# aclget /etc/init.d  
If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the run control script(s) and disable extended permissions.  
  
#acledit <directory>/<file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-907  
**Group Title:** GEN001600  
**Rule ID:** SV-907r7\_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.  
Procedure:  
# 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, and this is a finding.  
  
  
  
**Fix Text:**Edit the run control script and remove the relative path entry from the executable search path variable.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22354  
**Group Title:** GEN001605  
**Rule ID:** SV-38879r1\_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) contains 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.   
Procedure:  
# grep -r LIB /etc/rc\* /etc/init.d  
  
The variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/), this is a relative path, and this is a finding.  
  
  
**Fix Text:**Edit run control scripts' library search path variables. Remove empty entries or entries that are not absolute paths.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22355  
**Group Title:** GEN001610  
**Rule ID:** SV-38881r1\_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. This variable is formatted as a colon-separated list of paths. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/), this is a relative path, and this is a finding.  
# grep -r LDR\_PRELOAD /etc/rc\* /etc/init.d  
  
  
**Fix Text:**Edit the run control scripts' library preload list and remove relative paths.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-910  
**Group Title:** GEN001640  
**Rule ID:** SV-910r6\_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.  
  
Procedure:  
# more <startup script>  
# ls -lL <script or executable referenced by startup script>  
  
Alternatively, obtain a list of all world-writable files on the system and check system startup scripts to determine if any are referenced.  
  
Procedure:  
# find / -perm -002 -type f > wwlist  
  
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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4089  
**Group Title:** GEN001660  
**Rule ID:** SV-27209r1\_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 the run control scripts' ownership.  
Procedure:  
# ls -lL /etc/rc\*   
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.  
# chown root <run control script>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4090  
**Group Title:** GEN001680  
**Rule ID:** SV-27216r1\_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\*   
  
If any run control script is not group-owned by root, sys, bin, other, or system, 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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4091  
**Group Title:** GEN001700  
**Rule ID:** SV-27221r1\_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 indicate the system may have been compromised.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Check the ownership of any files executed from system startup scripts. If any of these files are not owned by root, bin, sys, or other, 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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11981  
**Group Title:** GEN001720  
**Rule ID:** SV-38882r1\_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 the ownership of global initialization files.  
  
Procedure:  
# ls -lL /etc/.login /etc/profile /etc/bashrc /etc/environment /etc/security/environ /etc/security/.profile  
  
If any global initialization file is not owned by root, this is a finding.  
  
  
**Fix Text:**Change the mode of the global initialization file(s) to 0644.  
# chmod 0644 <global initialization file>  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22356  
**Group Title:** GEN001730  
**Rule ID:** SV-38734r1\_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.  
Procedure:  
#aclget /etc/profile /etc/bashrc /etc/csh.login /etc/csh.cshrc /etc/environment /etc/.login /etc/security/environ /etc/security/.profile  
  
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the global initialization file(s) and disable extended permissions.  
  
#acledit <directory>/<file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11982  
**Group Title:** GEN001740  
**Rule ID:** SV-38884r1\_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/.login /etc/profile /etc/bashrc /etc/environment /etc/security/environ /etc/security/.profile  
  
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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11983  
**Group Title:** GEN001760  
**Rule ID:** SV-38892r1\_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, security, 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/.login /etc/profile /etc/bashrc /etc/environment /etc/security/environ /etc/security/.profile  
  
If any global initialization file is not group-owned by root, sys, bin, other, system, security, 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 system <global initialization file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-825  
**Group Title:** GEN001780  
**Rule ID:** SV-38893r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001780  
**Rule Title:**Global initialization files must contain the mesg -n or mesg n commands.  
  
**Vulnerability Discussion:**  If the mesg -n or mesg n command is not placed into the system profile, messaging can be used to cause a Denial of Service attack.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check global initialization files for the presence of mesg -n or mesg n.  
  
Procedure:  
# grep "mesg” /etc/.login /etc/profile /etc/bashrc /etc/environment /etc/security/environ /etc/security/.profile  
  
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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-788  
**Group Title:** Default/Skeleton Dot Files Permissions  
**Rule ID:** SV-38735r1\_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.  
Procedure:  
# ls -l /etc/security/.profile  
  
If a skeleton file has a mode more permissive than 0644, this is a finding.  
Check the mkuser.sys file. The /etc/security/mkuser.sys is a script containing items used in creation of users ~/.profile files. This script needs to be both protected from unauthorized modification, but also needs to be executable, therefore the permissions need to be at the mode of 755.  
#ls –l /etc/security/mkuser.sys  
If the mkuser.sys file has a mode more permissive than 0755, this is a finding.  
  
  
**Fix Text:**Change the mode of skeleton files with incorrect mode:  
# chmod 0644 /etc/security/.profile   
#chmod 0755 /etc/security/mkuser.sys  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22357  
**Group Title:** GEN001810  
**Rule ID:** SV-38736r1\_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.  
Procedure:  
#aclget /etc/security/.profile   
#aclget /etc/security/mkuser.sys  
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the skeleton file(s) and disable extended permissions.  
  
#acledit /etc/security/.profile   
#acledit /etc/security/mkuser.sys   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11984  
**Group Title:** Default/Skeleton Dot Files Ownership  
**Rule ID:** SV-38737r1\_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.  
Procedure:  
# ls -l /etc/security/.profile /etc/security/mkuser.sys  
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 /etc/security/,profile /etc/security/mkuser.sys  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22358  
**Group Title:** GEN001830  
**Rule ID:** SV-38738r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001830  
**Rule Title:**All skeleton files (typically in /etc/skel) must be group-owned by security, 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/security/.profile /etc/security/mkuser.sys  
  
If a skeleton file is not group-owned by root, this is a finding.  
  
  
**Fix Text:**Change the group-owner of the skeleton file to root, bin, sys, system, security, or other.  
  
Procedure:  
# chgrp security /etc/security/.profile /etc/security/mkuser.sys  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11985  
**Group Title:** GEN001840  
**Rule ID:** SV-12486r5\_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/profile /etc/bashrc /etc/csh.login /etc/csh.cshrc /etc/environment /etc/.login /etc/security/environ  
This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/), this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the global initialization file(s) with PATH variables containing relative paths. Edit the file and remove the relative path from the PATH variable.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22359  
**Group Title:** GEN001845  
**Rule ID:** SV-38842r1\_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.   
  
#egrep '(LD\_LIBRARY\_PATH|LIBPATH)' /etc/profile /etc/bashrc /etc/security/.login /etc/environment /etc/security/environ  
  
The LIBPATH or LD\_LIBRARY\_PATH variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/), this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the global initialization files /etc/profile /etc/bashrc /etc/security/.login /etc/environment /etc/security/environ and remove relative entries from the library search path variables.  
  
#vi /etc/profile /etc/bashrc /etc/security/.login /etc/environment /etc/security/environ   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22360  
**Group Title:** GEN001850  
**Rule ID:** SV-38843r1\_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 LDR\_PRELOAD /etc/profile /etc/bashrc /etc/security/.login /etc/environment /etc/security/environ  
  
This variable is formatted as a colon-separated list of paths. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/), this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the global initialization files and remove the relative path entry from the library preload list variable 'LDR\_PRELOAD'.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-904  
**Group Title:** GEN001860  
**Rule ID:** SV-904r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001860  
**Rule Title:**All local initialization files must be owned by the user or root.  
  
**Vulnerability Discussion:**  Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of local initialization files.  
  
Procedure:  
# ls –al /<usershomedirectory>/.login  
# ls –al /<usershomedirectory>/.cschrc  
# 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22361  
**Group Title:** GEN001870  
**Rule ID:** SV-26481r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001870  
**Rule Title:**Local initialization files must be group-owned by the user's primary group or root.  
  
**Vulnerability Discussion:**  Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check user home directories for local initialization files group-owned by a group other than the user's primary group or root.  
  
1. List user accounts and their primary GID.  
# cut -d : -f 1,4 /etc/passwd   
  
2. Check local initialization files for each user.  
# ls -alL ~USER/.login ~USER/.cschrc ~USER/.logout ~USER/.profile ~USER/.bash\_profile ~USER/.bashrc ~USER/.bash\_logout ~USER/.env ~USER/.dtprofile ~USER/.dispatch ~USER/.emacs ~USER/.exrc  
  
3. If any file is not group-owned by root or the user's primary GID, this is a finding.  
  
**Fix Text:**Change the group-owner of the local initialization file to the user's primary group, or root.  
# chgrp [USER's primary GID] ~USER/[local initialization file]   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-905  
**Group Title:** GEN001880  
**Rule ID:** SV-905r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001880  
**Rule Title:**All local initialization files must have mode 0740 or less permissive.  
  
**Vulnerability Discussion:**  Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the modes of local initialization files.  
  
Procedure:  
# ls –al /<usershomedirectory>/.login  
# ls –al /<usershomedirectory>/.cschrc  
# ls –al /<usershomedirectory>/.logout  
# ls –al /<usershomedirectory>/.profile  
# ls –al /<usershomedirectory>/.bash\_profile  
# ls –al /<usershomedirectory>/.bashrc  
# ls –al /<usershomedirectory>/.bash\_logout  
# ls –al /<usershomedirectory>/.env  
# ls –al /<usershomedirectory>/.dtprofile (permissions should be 0755)  
# ls –al /<usershomedirectory>/.dispatch  
# ls –al /<usershomedirectory>/.emacs  
# ls –al /<usershomedirectory>/.exrc  
# find /<usershomedirecotory>/.dt ! –fstype nfs \( -perm –0002 –o –perm –0020 \) -exec ls -ld {} \; (permissions not to be more   
permissive than 0755)  
  
If local initialization files are more permissive than 0740, the .dt directory 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22362  
**Group Title:** GEN001890  
**Rule ID:** SV-38739r1\_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.  
Procedure:  
# cat /etc/passwd | cut -f 6,6 –d “:” | xargs -n1 -IDIR ls -le DIR/.login DIR/.cschrc DIR/.logout DIR/.profile DIR/.bash\_profile DIR/.bashrc DIR/.bash\_logout DIR/.env DIR/.dtprofile DIR/.dispatch DIR/.emacs DIR/.exrc  
  
Procedure:  
#aclget <directory>/<file> and check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the local initialization file(s) and disable extended permissions.  
  
#acledit <directory>/<file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11986  
**Group Title:** Local Initialization Files PATH Variable  
**Rule ID:** SV-12487r5\_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.  
Procedure:  
# cut -d : -f 1 /etc/passwd | xargs -n1 -IUSER sh -c 'grep -l PATH ~USER/.\*'  
This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/), this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the local initialization file and remove the relative path entry from the executable search path variable.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22363  
**Group Title:** GEN001901  
**Rule ID:** SV-38844r1\_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.  
  
# cat /etc/passwd | cut -f 1,1 –d “:” | xargs -n1 -IUSER sh -c 'grep -l LIB ~USER/.\*'  
  
The LIBPATH and LD\_LIBRARY\_PATH variables are formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding. If an entry begins with a character other than a slash (/), this is a relative path, and this is a finding.  
  
**Fix Text:**Edit the local initialization file(s) and remove the relative path entry from the library search path.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22364  
**Group Title:** GEN001902  
**Rule ID:** SV-39102r1\_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:  
# cat /etc/passwd | cut -f 1,1 –d “:” | xargs -n1 -IUSER sh -c “grep -l LDR\_PRELOAD ~USER/.\*”  
This variable is formatted as a colon-separated list of paths. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is a finding.  
If an entry begins with a character other than a slash (/), this is a finding.   
  
**Fix Text:**Edit the local initialization file and remove the relative path entry from the library preload variable LDR\_PRELOAD.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4087  
**Group Title:** GEN001940  
**Rule ID:** SV-4087r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN001940  
**Rule Title:**User start-up files must not execute world-writable programs.  
  
**Vulnerability Discussion:**  If start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to become trojans destroying user files or otherwise compromising the system at the user, or higher, level. If the system is compromised at the user level, it is much easier to eventually compromise the system at the root and network level.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSW-1  
  
**Check Content:**    
Check local initialization files for any executed world-writable programs or scripts.  
  
Procedure:  
# more /<usershomedirectory>/.\*   
# ls -al <program or script>  
  
If any local initialization file executes a world-writable program or script, this is a finding.  
  
**Fix Text:**Remove the world-writable permission of files referenced by local initialization scripts, or remove the references to these files in the local initialization scripts.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4088  
**Group Title:** Local Initialization files mesg -y  
**Rule ID:** SV-4088r7\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN001960  
**Rule Title:**User start-up files must not contain the mesg -y or mesg y command.  
  
**Vulnerability Discussion:**  The mesg -y or mesg y command turns on terminal messaging. On systems that do not default to mesg -n, the system profile (or equivalent) provides it. If the user changes this setting, write access may be provided to the terminal screen which could disrupt processing or cause enough confusion to result in damage to sensitive files. Educate users about the danger of having terminal messaging set on.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# grep “mesg” /<usershomedirectory>/.\*   
  
If local initialization files contain the mesg –y or mesg y command, this is a finding.  
  
**Fix Text:**Edit the local initialization file(s) and remove the mesg -y command.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11987  
**Group Title:** GEN001980  
**Rule ID:** SV-38740r1\_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  
# cat /<directorylocation>/.rhosts | grep –v “^#” | grep “\+”  
  
# find / -name .shosts  
# cat /<directorylocation>/.shosts | grep –v “^#” | grep “\+”  
  
# find / -name hosts.equiv  
# cat /<directorylocation>/hosts.equiv | grep –v “^#” | grep “\+”  
  
# find / -name shosts.equiv  
# cat /<directorylocation>/shosts.equiv | grep –v “^#” | grep “\+”  
  
# cat /etc/passwd | grep –v “^#” | grep “\+”  
# cat /etc/security/passwd | grep –v “^#” | grep “\+”   
# cat /etc/group | grep –v “^#” | grep “\+”  
  
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/security/passwd, and/or /etc/group files and remove entries containing a plus (+).   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-913  
**Group Title:** A .netrc file exists  
**Rule ID:** SV-913r8\_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:**  IAIA-1, IAIA-2  
  
**Check Content:**    
Check the system for the existence of any .netrc files.  
  
Procedure:  
# find / -name .netrc   
  
If any .netrc file exists, this is a finding.  
  
**Fix Text:**Remove the .netrc file(s).  
  
Procedure:  
# rm .netrc   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4427  
**Group Title:** Access Control Files Host Pairs  
**Rule ID:** SV-4427r8\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002020  
**Rule Title:**All .rhosts, .shosts, or host.equiv files must only contain trusted host-user pairs.  
  
**Vulnerability Discussion:**  If these files are not properly configured, they could allow malicious access by unknown malicious users from untrusted hosts who could compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Locate and examine all .rhosts, .shosts, hosts.equiv, and shosts.equiv files.  
  
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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11988  
**Group Title:** Access Control Files Documentation  
**Rule ID:** SV-12489r5\_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, this is a finding.  
  
  
  
  
**Fix Text:**Remove the .rhosts, .shosts, hosts.equiv, and/or shosts.equiv files.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4428  
**Group Title:** Access Control Files Accessibility  
**Rule ID:** SV-39502r1\_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:**    
# find / -type f -name .rhosts  
# ls -alL /<directorylocation>/.rhosts  
  
# find / -type f -name .shosts  
# ls -alL /<directorylocation>/.shosts  
  
# find / -type f -name hosts.equiv  
# ls -lL /<directorylocation>/hosts.equiv  
  
# find / -type f -name shosts.equiv  
# ls -lL /<directorylocation>/shosts.equiv  
  
If the .rhosts, .shosts, hosts.equiv, or shosts.equiv files have permissions greater than 700, this is a finding.  
  
  
**Fix Text:**Ensure the permission for these files is set at 700 or less and the owner is the owner of the home directory that it is in. These files, outside of home directories (other than hosts.equiv which is in /etc and owned by root), have no meaning.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11989  
**Group Title:** GEN002100  
**Rule ID:** SV-38845r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002100  
**Rule Title:**The .rhosts file must not be supported in PAM.  
  
**Vulnerability Discussion:**  The .rhosts files are used to specify a list of hosts permitted remote access to a particular account without authenticating. The use of such a mechanism defeats strong identification and authentication requirements.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the PAM configuration for rhosts\_auth. Procedure:   
  
# grep rhosts\_auth /etc/pam.conf |grep -v \#  
  
If a rhosts\_auth entry is found, this is a finding.   
  
  
**Fix Text:**Edit /etc/pam.conf and remove the reference(s) to the rhosts\_auth module.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-916  
**Group Title:** GEN002120  
**Rule ID:** SV-38741r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002120  
**Rule Title:**The /etc/shells (or equivalent) file must exist.  
  
**Vulnerability Discussion:**  The shells file (or equivalent) lists approved default shells. It helps provide layered defense to the security approach by ensuring users cannot change their default shell to an unauthorized shell that may not be secure.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check /etc/security/login.cfg for a shells stanza.  
Procedure:  
#grep –p usw: | grep “shells =” stanza. If no such stanza exists, this is a finding.  
  
Check the /etc/shells file.  
Procedure:  
#more /etc/shells         
If the /etc/shells file does not exist, this is a finding.  
  
**Fix Text:**Edit the /etc/security/login.cfg file and add a shells stanza containing a list of valid shells.  
#chsec –f /etc/security/login.cfg –s usw -a shells=<list of approved shells>  
  
Create the /etc/shells file.  
#vi /etc/shells   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-917  
**Group Title:** GEN002140  
**Rule ID:** SV-38742r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002140  
**Rule Title:**All shells referenced in /etc/passwd must be listed in the /etc/shells file, except any shells specified for the purpose of preventing logins.  
  
**Vulnerability Discussion:**  The shells file lists approved default shells. It helps provide layered defense to the security approach by ensuring users cannot change their default shell to an unauthorized shell that may not be secure.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Confirm the login shells referenced in the /etc/passwd file are listed in the /etc/security/login.cfg file's shells =variable in the usw stanza.  
  
# more /etc/security/login.cfg   
# more /etc/shells  
  
The /usr/bin/false, /bin/false, /dev/null, /sbin/nologin, (and equivalents), and sdshell will be considered valid shells for use in the /etc/passwd file, but will not be listed in the shells stanza. If a shell referenced in /etc/passwd is not listed in the shells stanza, excluding the above mentioned shells, then 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.   
  
Alternatively, use the SMIT to change the /etc/passwd shell entry.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-921  
**Group Title:** GEN002200  
**Rule ID:** SV-38847r1\_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:**    
Obtain a list of system shells from /etc/security/login.cfg and check the ownership of these shells.  
Procedure:  
#grep shells /etc/security/login.cfg | grep –v \\* | cut –f 2 –d = | sed s/,/\ /g | xargs –n1 ls –l  
If any shell is not owned by root or bin, this is a finding.  
  
Obtain a list of system shells from /etc/shells and check the ownership of these shells.  
Procedure:  
#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 >   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22365  
**Group Title:** GEN002210  
**Rule ID:** SV-38848r1\_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:**    
Check the group ownership of each shell referenced.  
  
Procedure:  
# cat /etc/shells | xargs -n1 ls -l  
If any shell is not group owned by root, bin, sys, or system, this is a finding.  
  
#grep shells /etc/security/login.cfg | grep –v \\* | cut –f 2 –d = | sed s/,/\ /g | xargs –n1 ls –l  
If any shell is not group owned by root, bin, sys, or system, this is a finding.  
  
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.  
  
# chgrp system < shell >   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-922  
**Group Title:** GEN002220  
**Rule ID:** SV-38846r1\_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:**    
Obtain a list of system shells from /etc/security/login.cfg and check the permissions of these shells.  
Procedure:  
#grep shells /etc/security/login.cfg | grep –v \\* | cut –f 2 –d = | sed s/,/\ /g | xargs –n1 ls –l  
If any shell has a mode more permissive than 0755, this is a finding.  
  
Obtain a list of system shells from /etc/shells and check the ownership of these shells.  
Procedure:  
#cat /etc/shells | xargs –n1 ls -l  
  
If any shell has a mode more permissive than 0755, this is a finding.  
  
**Fix Text:**Change the mode of the shell.  
# chmod 0755 < shell >  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22366  
**Group Title:** GEN002230  
**Rule ID:** SV-38744r1\_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:**    
Check the permissions of each shell referenced in /etc/shells.  
Procedure:  
# cat /etc/shells   
  
For each shell listed, run aclget <shell path>  
#aclget <shell>  
  
Check the permissions of each shell referenced in /etc/security/login.cfg.  
Procedure:  
#grep shells /etc/security/login.cfg  
For each shell listed, run aclget <shell path>  
# aclget <shell>  
  
Otherwise, check any shells found on the system.  
# find / -name "\*sh  
  
#aclget <directory>/<file>   
  
If extended permissions are enabled on any shell, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the shell file(s) and disable extended permissions.  
  
#acledit <directory>/<file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-923  
**Group Title:** GEN002260  
**Rule ID:** SV-923r7\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002260  
**Rule Title:**The system must be checked for extraneous device files at least weekly.  
  
**Vulnerability Discussion:**  If an unauthorized device is allowed to exist on the system, there is the possibility the system may perform unauthorized operations.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for an automated job, or check with the SA, to determine if the system is checked for extraneous device files on a weekly basis. If no automated or manual process is in place, this is a finding.  
  
  
  
**Fix Text:**Establish a weekly automated or manual process to create a list of device files on the system and determine if any files have been added, moved, or deleted since the last list was generated. A list of device files can be generated with this command:  
# find / -type b -o -type c > device-file-list   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-924  
**Group Title:** Device Files Directories Permissions  
**Rule ID:** SV-924r6\_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:**  ECLP-1  
  
**Check Content:**    
Find all device files existing anywhere on the system.  
  
Procedure:  
# find / -type b -print > devicelist  
# find / -type c -print >> devicelist  
  
Check the permissions on the directories above subdirectories containing device files. If any of the device files or their parent directories 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-925  
**Group Title:** Device Files Ownership  
**Rule ID:** SV-38745r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002300  
**Rule Title:**Device files used for backup must only be readable and/or writable by root or the backup user.  
  
**Vulnerability Discussion:**  System backups could be accidentally or maliciously overwritten and destroy the ability to recover the system if a compromise should occur. Unauthorized users could also copy system files.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check the system for world-writable device files.  
  
Procedure:  
# find / -perm -2 -a \( -type b -o -type c \) -exec ls -ld {} \;  
  
If any device file(s) used for backup are writable by users other than root, this is a finding (Typical backup devices for tape are/dev/rmt\* and cd/dvd writers are /dev/cd\*).  
  
  
**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.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1048  
**Group Title:** An audio device is more permissive than 644.  
**Rule ID:** SV-27243r1\_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 to a bugging device.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of audio devices.  
# /usr/sbin/lsdev -C | grep -i audio   
# ls -lL /dev/\*aud0   
If the mode of audio devices are more permissive than 0660, this is a finding.  
  
**Fix Text:**Change the mode of audio devices.  
# chmod 0660 <audio device>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22367  
**Group Title:** GEN002330  
**Rule ID:** SV-38743r1\_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:**    
Determine the audio device files for the system.  
Procedure:  
# /usr/sbin/lsdev -C | grep -i audio   
  
#aclget /dev/\*aud0   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the audio device file(s) and disable extended permissions.  
  
#acledit <directory>/<file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1049  
**Group Title:** Audio device ownership.  
**Rule ID:** SV-27248r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002340  
**Rule Title:**Audio devices must be owned by root.  
  
**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 to a bugging device.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the owner of audio devices.  
Procedure:  
# /usr/sbin/lsdev -C | grep -i audio   
# ls -lL /dev/\*aud0   
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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1061  
**Group Title:** Audio device group ownership.  
**Rule ID:** SV-27253r1\_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:  
# /usr/sbin/lsdev -C | grep -i audio   
# ls -lL /dev/\*aud0   
  
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 system <audio device>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-801  
**Group Title:** GEN002380  
**Rule ID:** SV-801r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002380  
**Rule Title:**The owner, group owner, mode, ACL, and location of files with the setuid bit set must be documented using site-defined procedures.  
  
**Vulnerability Discussion:**  All files with the setuid bit set will allow anyone running these files to be temporarily assigned the UID of the file. While many system files depend on these attributes for proper operation, security problems can result if setuid is assigned to programs that allow reading and writing of files, or shell escapes. Only default vendor-supplied executables should have the setuid bit set.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Files with the setuid bit set will allow anyone running these files to be temporarily assigned the user or group ID of the file. If an executable with setuid allows shell escapes, the user can operate on the system with the effective permission rights of the user or group owner.  
  
List all setuid files on the system.  
Procedure:  
# find / -perm -4000 -exec ls –l {} \; | more   
  
NOTE: Executing these commands may result in large listings of files; the output may be redirected to a file for easier analysis.  
  
Ask the SA or IAO if files with the suid bit set have been documented. If any undocumented file has its suid bit set, this is a finding.  
  
**Fix Text:**Document the files with the suid bit set or unset the suid bit on the executable.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-803  
**Group Title:** GEN002400  
**Rule ID:** SV-803r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002400  
**Rule Title:**The system must be checked weekly for unauthorized setuid files as well as unauthorized modification to authorized setuid files.  
  
**Vulnerability Discussion:**  Files with the setuid bit set will allow anyone running these files to be temporarily assigned the UID of the file. While many system files depend on these attributes for proper operation, security problems can result if setuid is assigned to programs that allow reading and writing of files, or shell escapes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Determine if a weekly automated or manual process is used to generate a list of suid 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 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   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-805  
**Group Title:** File systems mounted with nosuid  
**Rule ID:** SV-38746r1\_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/filesystems 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.  
  
Each file system stanza must contain a device special file and may additionally contain all of the following fields  
type = , options = , and check = .  
  
# more /etc/filesystems  
# lsfs  
  
If any of these files systems do not mount with the nosuid option, it is a finding.  
  
**Fix Text:**Edit /etc/filesystems and add the options = nosuid to the stanza of file system mounted from removable media or network shares, and any file system not containing approved setuid or setgid files.  
  
OR  
Add the nosuid option with the chfs command.  
#chfs –a options=nosuid <filesystem>  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22368  
**Group Title:** GEN002430  
**Rule ID:** SV-38747r1\_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:**    
If the system does not support a nodev option, this is not applicable.  
  
Check /etc/filesystems and verify the nodev mount option (options = ) is used on any file systems mounted from removable media or network shares, or file systems not containing any approved device files. If any such file system is not using the nodev option, this is a finding.  
  
**Fix Text:**Edit /etc/filesystems and add the options = nodev to all entries for remote or removable media file systems, and file systems containing no approved device files.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-802  
**Group Title:** GEN002440  
**Rule ID:** SV-38945r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002440  
**Rule Title:**The owner, group owner, mode, ACL, and location of files with the setgid bit set must be documented using site-defined procedures.  
  
**Vulnerability Discussion:**  All files with the setgid bit set will allow anyone running these files to be temporarily assigned the GID of the file. While many system files depend on these attributes for proper operation, security problems can result if setgid is assigned to programs that allow reading and writing of files, or shell escapes.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Locate all setgid files on the system.  
  
Procedure:  
# find / -perm -2000  
  
If the ownership, permissions, location, and ACLs of all files with the setgid bit set are not documented, this is a finding.  
  
**Fix Text:**All files with the sgid bit set will be documented in the system baseline and authorized by the Information Systems Security Officer. Locate all sgid files with the following command:   
  
#find / -perm –2000 –exec ls –lL {} \;  
# find / -perm -2000 –exec aclget {} \;  
  
Ensure sgid files are part of the operating system software, documented application software, documented utility software, or documented locally developed software. Ensure none are text files or shell programs.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-804  
**Group Title:** GEN002460  
**Rule ID:** SV-804r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002460  
**Rule Title:**The system must be checked weekly for unauthorized setgid files as well as unauthorized modification to authorized setgid files.  
  
**Vulnerability Discussion:**  Files with the setgid bit set will allow anyone running these files to be temporarily assigned the group id of the file. While many system files depend on these attributes for proper operation, security problems can result if setgid is assigned to programs that allow reading and writing of files, or shell escapes.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Determine if a weekly automated or manual process is used to generate a list of sgid 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 sgid files on the system and compare it with the prior list. To create a list of sgid files use the following command:  
# find / -perm -2000 > suid-file-list   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1010  
**Group Title:** GEN002480  
**Rule ID:** SV-1010r7\_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 that is not required to be world-writable.  
  
Procedure:  
# chmod o-w <file>  
  
Document all changes.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-806  
**Group Title:** GEN002500  
**Rule ID:** SV-806r7\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002500  
**Rule Title:**The sticky bit must be set on all public directories.  
  
**Vulnerability Discussion:**  Failing to set the sticky bit on the public directories allows unauthorized users to delete files in the directory structure.  
  
The only authorized public directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage (e.g., /tmp) and for directories requiring global read/write access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Verify all world-writable directories have the sticky bit set.  
  
Procedure:  
# find / -type d -perm -002 ! -perm -1000 > wwlist  
  
If the sticky bit is not set on a world-writable directory, this is a finding.  
  
**Fix Text:**Set the sticky bit on all public directories.   
  
Procedure:  
# chmod 1777 /tmp  
  
(Replace /tmp with the public directory missing the sticky bit, if necessary.)   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-807  
**Group Title:** GEN002520  
**Rule ID:** SV-807r6\_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.)   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11990  
**Group Title:** GEN002540  
**Rule ID:** SV-12491r4\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002540  
**Rule Title:**All public directories must be group-owned by root or an application group.  
  
**Vulnerability Discussion:**  If a public directory has the sticky bit set and is not group-owned by a 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 directories 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.)   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-808  
**Group Title:** Default umask  
**Rule ID:** SV-39501r1\_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   
**Security 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:   
# grep umask /userhomedirectory/.\*   
  
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 (CAT I) finding.  
  
**Fix Text:**Edit local and global initialization files that contain "umask" and change them to use 077 instead of the current value.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-810  
**Group Title:** Disabled default system accounts  
**Rule ID:** SV-38897r1\_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 guest, sys, bin, uucp, nuucp, daemon, smtp) have been disabled.  
Procedure:  
# grep account\_locked /etc/security/user  
If there are any unlocked default system accounts, this is a finding.  
  
**Fix Text:**Lock the default system account(s).  
# chuser account\_locked=true <user>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-811  
**Group Title:** Configure and implement auditing  
**Rule ID:** SV-38946r1\_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.  
# /usr/sbin/audit query | head -1  
If the response Auditing On is not returned, this is a finding.  
  
**Fix Text:**Use SMIT or command line to enable auditing on the system.   
#audit start  
  
Additionally, make sure auditing subsystem starts on system startup.  
#mkitab -i cron "audit:2:once:/usr/sbin/audit start 2>&1 >   
/dev/console"   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Rule ID:** SV-28610r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN000220  
**Rule Title:**A file integrity tool must be used at least weekly to check for unauthorized file changes, particularly the addition of unauthorized system libraries or binaries, or for unauthorized modification to authorized system libraries or binaries.  
  
**Vulnerability Discussion:**  Changes in system libraries and binaries can indicate compromise or significant system events such as patching needing to be checked by automated processes and the results reviewed by the SA.  
  
NOTE: This requirement only applies to MAC II and III systems.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Determine if there is a cron job, scheduled to run weekly or more frequently, to run the file integrity tool to check for unauthorized system libraries or binaries, or unauthorized modification to authorized system libraries or binaries.   
  
Procedure:  
# crontab -l  
  
If there is no cron job meeting these requirements, this is a finding.  
  
**Fix Text:**Create a cron job, scheduled to run weekly or more frequently, to run the file integrity tool to check for unauthorized system libraries or binaries, or unauthorized modification to authorized system libraries or binaries.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-812  
**Group Title:** Audit logs accessibility  
**Rule ID:** SV-38900r1\_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 -p bin: /etc/security/audit/config  
Directories to search will be listed under the bin stanza.  
# ls -la <audit directories>  
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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22702  
**Group Title:** GEN002690  
**Rule ID:** SV-38902r1\_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:**    
Procedure:  
# grep -p bin: /etc/security/audit/config  
Directories to search will be listed under the bin stanza.  
  
# ls -la <audit directories>  
  
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 system < audit log file >   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-813  
**Group Title:** Audit logs permissions  
**Rule ID:** SV-38904r1\_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 -p bin: /etc/security/audit/config  
Directories to search will be listed under the bin stanza.  
# ls -la <audit directories>  
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 file(s).  
# chmod 0640 <audit log file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22369  
**Group Title:** GEN002710  
**Rule ID:** SV-38748r1\_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:**    
Procedure:  
# grep -p bin: /etc/security/audit/config  
Directories and files to search will be listed under the bin stanza.  
#aclget <directory>/<file>   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the system audit file(s) and disable extended permissions.  
  
#acledit <directory>/<file> and disable extended permissions  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22370  
**Group Title:** GEN002715  
**Rule ID:** SV-38749r1\_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:**    
Determine if the system audit tool executables are owned by root. Audit tools include, but are not limited to audit, auditcat, auditconv, auditpr, auditselect, auditstream, auditbin and auditmerge.  
  
Procedure:  
ls -lL `which <audit tool executable>'  
  
If any system audit tool executable is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the system audit tool executables to root.   
#chown root <system audit tool executable>  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22371  
**Group Title:** GEN002716  
**Rule ID:** SV-38906r1\_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:**    
Determine the group ownership of system audit tool executables. Audit tools include, but are not limited to audit, auditcat, auditconv, auditpr, auditselect, auditstream, auditbin, and auditmerge.  
  
Procedure:  
# ls -lL `which <audit tool executable>`  
  
If any system audit tool executable is not group-owned by root, bin, sys, or system, this is a finding.  
  
  
**Fix Text:**Change the group owner of system audit tool executables to root, bin, sys, or system.  
  
Procedure:  
# chgrp system < system audit tool executable>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22372  
**Group Title:** GEN002717  
**Rule ID:** SV-38778r1\_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:**    
Determine if system audit tool executables have a mode more permissive than 0750. If any do, this is a finding. Audit tools include, but are not limited to audit, auditcat, auditconv, auditpr, auditselect, auditstream, auditbin and auditmerge.  
  
**Fix Text:**Many audit tools have SUID bit set. Before changing permissions on system audit tool executables, check the file permissions for SUID bits. Change the mode of system audit tool executables to 0750.   
#chmod 0750 or 4750 <system audit tool executable>  
Document all changes made.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22373  
**Group Title:** GEN002718  
**Rule ID:** SV-38779r1\_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:**    
Determine if system audit tool executables have extended ACLs Audit tools include, but are not limited to audit, auditcat, auditconv, auditpr, auditselect, auditstream, auditbin, and auditmerge.  
Procedure:  
#aclget <system audit tool executable>   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the system audit tool executable(s) and disable extended permissions.  
  
#acledit <system audit tool executable>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22374  
**Group Title:** GEN002719  
**Rule ID:** SV-38849r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN002719  
**Rule Title:**The audit system must alert the SA in the event of an audit processing failure.  
  
**Vulnerability Discussion:**  An accurate and current audit trail is essential for maintaining a record of system activity. If the system fails, the SA must be notified and must take prompt action to correct the problem.  
  
Minimally, the system must log this event and the SA will receive this notification during the   
daily system log review. If feasible, active alerting (such as email or paging) should be employed consistent with the site’s established operations management systems and procedures.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Determine if the audit system is configured to alert the SA in the event of an audit processing failure. If it is not, this is a finding.  
  
Check the binmode auditing parameter.  
Procedure:  
#more /etc/security/audit/config  
If the binmode = parameter in file /etc/security/audit/config is set to panic, this effectively stops the system causing a Denial of Service if auditing fails, this is a finding.  
  
**Fix Text:**Configure the audit system to alert the SA in the event of an audit processing failure.   
  
Set the binmode = to a value other than panic in the /etc/security/audit/config file.   
Restart the auditing subsystem.  
#audit shutdown  
#audit start  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-814  
**Group Title:** Audit failed file and program access attempts  
**Rule ID:** SV-38850r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002720  
**Rule Title:**The audit system must be configured to audit failed attempts to access files and programs.  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the system audit configuration to determine if failed attempts to access files and programs are audited.   
Check system activities (events) to audit are listed in the /etc/security/audit/events file.  
Procedure:  
# more /etc/security/audit/events  
If the FILE\_Open event is not configured, this is a finding.  
  
Check the FILE\_Open audit event is defined in the audit classes stanza classes: of the /etc/security/audit/config file.  
Procedure:  
#more /etc/security/audit/config  
Make note of the audit class(es) that the FILE\_Open event is associated with.  
If the FILE\_Open event is not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify the audit class is associated with the default user and all other user ids listed in the users: stanza of the /etc/security/audit/config file.  
Procedure:  
#more /etc/security/audit/config  
If the class(es) the FILE\_Open event is(/are) not associated with the default user and all the system users in the users: stanza, this is a finding.  
  
Supplementary Information:  
Successful setup of AIX auditing requires several files and stanza’s to be correctly configured.  
1.       The /etc/security/audit/events must have the system call defined.  
2.       The /etc/security/audit/config has 2 stanza’s that need to be configured  
a.       “classes:” stanza. Each entry in this stanza defines two things. The first is the name of a class to group the events to be audited on. The class is linked to users of the system for auditing. The second is the event(s) to be audited in this class:  
Example:  
classes:  
DISA\_CLASS = FILE\_Open, File\_Unlink, FS\_Rmdir   
  
b.       “users:” stanza. There are two options of specifying what users audit on. The first is to explicitly spell out user names.  
EXAMPLE:  
users:  
root = DISA\_CLASS  
  
The second is to specify a default catching all uses not listed else where in the users: stanza  
EXAMPLE  
users:  
root = DISA\_CLASS  
default = DISA\_CLASS  
3.       An approach to setup auditing to meet STIG requirements would be to create class stanza with all audit events that are required. The users: stanza would then be populated with the root user, any other user ids with special requirements and finally a default user.  
4.       The /usr/lib/security/mkuser.default file can have under the users: stanza an entry   
auditclasses = <class(es) of events to be audited for each new user added to the system.  
  
**Fix Text:**Edit /etc/security/audit/events and add the FILE\_Open event to the list of audited events.  
  
Edit /etc/security/audit/config and add .the FILE\_Open audit event to an audit class in the classes: stanza.  
  
Edit the /etc/security/audit/config and assign the audit classes that have the FILE\_Open event to the users listed in the users: stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22375  
**Group Title:** GEN002730  
**Rule ID:** SV-26022r1\_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:**  ECAT-1  
  
**Check Content:**    
Determine if the audit system is configured to alert the SA when the audit storage volume approaches capacity. If it does not, this is a finding.  
  
**Fix Text:**Configure the audit system to alert the SA when the audit storage volume approaches capacity.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-815  
**Group Title:** Audit file and program deletion  
**Rule ID:** SV-27294r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002740  
**Rule Title:**The audit system must be configured to audit file deletions.  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the system audit configuration to determine if failed attempts to access files and programs are audited.  
# more /etc/security/audit/events  
If auditing of the FILE\_Unlink or FS\_Rmdir events is not configured, this is a finding.  
If no results are returned, this is a finding.  
  
Check the FILE\_Unlink and FS\_Rmdir audit event(s) are defined in the audit classes stanza classes: of the /etc/security/audit/config file.  
  
#more /etc/security/audit/config  
Make note of the audit class(es) that the File\_Unlink and FS\_Rmdir events are associated with.  
If the FILE\_Unlink and FS\_Rmdir events are not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify the audit class is associated with the default user and all other user ids listed in the users: stanza of the /etc/security/audit/config file.  
#more /etc/security/audit/config  
If the class(es) that the FILE\_Unkink and FS\_Rmdir events are not associated with the default user and all the system users in the users: stanza, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit/events and add the FILE\_Unlink or FS\_Rmdir events to the list of audited events.  
  
Edit /etc/security/audit/config and add the FILE\_Unkink and FS\_Rmdir audit events to an audit class in the classes: stanza.  
  
Edit the /etc/security/audit/config and assign the audit classes containing the FILE\_Unkink and FS\_Rmdir events to the all users listed in the users: stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22376  
**Group Title:** GEN002750  
**Rule ID:** SV-38851r1\_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 the audit system is configured to audit account creation.   
  
Procedure:  
# more /etc/security/audit/events  
If auditing of the USER\_Create event is not configured, check the USER\_Create audit event is defined in the audit classes' stanza of the /etc/security/audit/config file.  
  
Procedure:  
#more /etc/security/audit/config  
Make note of the audit class the USER\_Create event is associated with.  
If the USER\_Create event is not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify the audit class is associated with the default user and all other user ids listed in the users: stanza of the /etc/security/audit/config file.  
Procedure:  
#more /etc/security/audit/config  
If the class(es) the USER\_Create event is not associated with the default user and all the system users in the ‘users’: stanza, this is a finding.  
  
**Fix Text:**Configure the audit system to audit account creation.   
  
Edit /etc/security/audit/events and add the User\_Create event to the list of audited events.  
  
Edit /etc/security/audit/config and add the USER\_Create audit event to an audit class in the classes: stanza.  
  
Edit the /etc/security/audit/config and assign the audit classes with the USER\_Create event to the all users listed in the users: stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22377  
**Group Title:** GEN002751  
**Rule ID:** SV-38852r1\_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 the audit system is configured to audit account modification.  
Procedure:   
# more /etc/security/audit/events  
If auditing of the USER\_Change event is not configured, this is a finding.  
  
Verify the USER\_Change audit event is defined in the audit classes stanza classes: of the /etc/security/audit/config file.  
Procedure:  
#more /etc/security/audit/config  
Make note of the audit class(es) the USER\_Change event is associated with.  
If the USER\_Change event is not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify the audit class is associated with the default user and all other user ids listed in the users: stanza of the /etc/security/audit/config file.  
Procedure:  
#more /etc/security/audit/config  
If the class(es) the USER\_Change event is not associated with the default user and all the system users in the users: stanza, this is a finding.  
  
**Fix Text:**Configure the system to audit account modification.   
  
Edit /etc/security/audit/events and add the USER\_Change event to the list of audited events.  
  
Edit /etc/security/audit/config and add the USER\_Change audit event to an audit class in the classes: stanza.  
  
Edit /etc/security/audit/config and assign the audit classes with the USER\_Change event to the all users listed in the users: stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22378  
**Group Title:** GEN002752  
**Rule ID:** SV-38853r1\_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 the system is configured to audit account disabling.   
Procedure:  
# more /etc/security/audit/events  
If auditing of the USER\_Change and USER\_Locked events are not configured, this is a finding.  
  
Check the USER\_Change and USER\_Locked audit event(s) are defined in the audit classes stanza classes: of the /etc/security/audit/config file.  
Procedure:  
#more /etc/security/audit/config  
Make note of the audit class(es) the USER\_Change and USER\_Locked events are associated with.  
If the USER\_Change and USER\_Locked events are not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify the audit class is associated with the default user and all other user ids listed in the users: stanza of the /etc/security/audit/config file.  
  
Procedure:  
#more /etc/security/audit/config  
If the class(es) the USER\_Change and USER\_Locked events are not associated with the default user and all the system users in the users: stanza, this is a finding.  
  
**Fix Text:**Configure the system to audit account disabling.   
  
Edit /etc/security/audit/events and add the USER\_Change and USER\_Locked events to the list of audited events.  
  
Edit /etc/security/audit/config and add the USER\_Change and USER\_Locked audits event to an audit class in the classes: stanza.  
  
Edit the /etc/security/audit/config and assign the audit classes with the USER\_Change and USER\_Locked events to the all users listed in the users: stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22382  
**Group Title:** GEN002753  
**Rule ID:** SV-38854r1\_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 the system is configured to audit account termination.  
  
Procedure:  
# more /etc/security/audit/events  
If auditing of the USER\_Remove event is not configured, this is a finding.  
  
Verify the USER\_Remove audit event is defined in the audit classes stanza classes: of the /etc/security/audit/config file.  
  
Procedure:  
#more /etc/security/audit/config  
Make note of the audit class(es) the USER\_Remove event is associated with.  
If the USER\_Remove event is not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify that the audit class is associated with the default user and all other user ids listed in the ‘users:’ stanza of the /etc/security/audit/config file.  
Procedure:  
#more /etc/security/audit/config  
If the class(es) that the USER\_Remove event is not associated with the default user and all the system users in the users: stanza, this is a finding.  
  
**Fix Text:**Configure the system to audit account termination.   
  
Edit /etc/security/audit/events and add the USER\_Remove event to the list of audited events  
  
Edit /etc/security/audit/config and add the USER\_Remove audit event to an audit class in the classes: stanza.  
  
Edit the /etc/security/audit/config and assign the audit classes with the USER\_Remove event to the all users listed in the users: stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-816  
**Group Title:** Audit administrative, privileged, security actions  
**Rule ID:** SV-38855r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002760  
**Rule Title:**The audit system must be configured to audit all administrative, privileged, and security actions.  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises, and damages incurred during a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the auditing configuration of the system.  
# more /etc/security/audit/events  
  
verify the following events are configured:  
ACCT\_Disable, ACCT\_Enable, AUD\_it, BACKUP\_Export, DEV\_Change, DEV\_Configure, DEV\_Create, FILE\_Chpriv, FILE\_Fchpriv, FILE\_Mknod, FILE\_Owner, FS\_Chroot, FS\_Mount, FS\_Umount, PASSWORD\_Check, PROC\_Adjtime,PROC\_Kill, PROC\_Privilege, PROC\_Setpgid, PROC\_SetUserIDs, RESTORE\_Import, TCBCK\_Delete, USER\_Change, USER\_Create, USER\_Reboot, USER\_Remove, and USER\_SetEnv  
  
If any of these events are missing from the configuration, this is a finding.  
  
Check the ACCT\_Disable, ACCT\_Enable, AUD\_it, BACKUP\_Export, DEV\_Change, DEV\_Configure, DEV\_Create, FILE\_Chpriv, FILE\_Fchpriv, FILE\_Mknod, FILE\_Owner, FS\_Chroot, FS\_Mount, FS\_Umount, PASSWORD\_Check, PROC\_Adjtime,PROC\_Kill, PROC\_Privilege, PROC\_Setpgid, PROC\_SetUserIDs, RESTORE\_Import, TCBCK\_Delete, USER\_Change, USER\_Create, USER\_Reboot, USER\_Remove, and USER\_SetEnv audit events are defined in the audit classes stanza ‘classes:’ of the /etc/security/audit/config file.  
  
#more /etc/security/audit/config  
Make note of the audit class(es) that the ACCT\_Disable, ACCT\_Enable, AUD\_it, BACKUP\_Export, DEV\_Change, DEV\_Configure, DEV\_Create, FILE\_Chpriv, FILE\_Fchpriv, FILE\_Mknod, FILE\_Owner, FS\_Chroot, FS\_Mount, FS\_Umount, PASSWORD\_Check, PROC\_Adjtime,PROC\_Kill, PROC\_Privilege, PROC\_Setpgid, PROC\_SetUserIDs, RESTORE\_Import, TCBCK\_Delete, USER\_Change, USER\_Create, USER\_Reboot, USER\_Remove, and USER\_SetEnv events are associated with.  
If the ACCT\_Disable, ACCT\_Enable, AUD\_it, BACKUP\_Export, DEV\_Change, DEV\_Configure, DEV\_Create, FILE\_Chpriv, FILE\_Fchpriv, FILE\_Mknod, FILE\_Owner, FS\_Chroot, FS\_Mount, FS\_Umount, PASSWORD\_Check, PROC\_Adjtime,PROC\_Kill, PROC\_Privilege, PROC\_Setpgid, PROC\_SetUserIDs, RESTORE\_Import, TCBCK\_Delete, USER\_Change, USER\_Create, USER\_Reboot, USER\_Remove, and USER\_SetEnv events are not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify the audit class is associated with the default user and all other user ids listed in the users: stanza of the /etc/security/audit/config file.  
#more /etc/security/audit/config  
If the class(es) that the ACCT\_Disable, ACCT\_Enable, AUD\_it, BACKUP\_Export, DEV\_Change, DEV\_Configure, DEV\_Create, FILE\_Chpriv, FILE\_Fchpriv, FILE\_Mknod, FILE\_Owner, FS\_Chroot, FS\_Mount, FS\_Umount, PASSWORD\_Check, PROC\_Adjtime,PROC\_Kill, PROC\_Privilege, PROC\_Setpgid, PROC\_SetUserIds, RESTORE\_Import, TCBCK\_Delete, USER\_Change, USER\_Create, USER\_Reboot, USER\_Remove, and USER\_SetEnv events are not associated with the default user and all the system users in the ‘users’: stanza, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit/events and add the following events to the list of audited events:  
ACCT\_Disable, ACCT\_Enable, AUD\_it, BACKUP\_Export, DEV\_Change, DEV\_Configure, DEV\_Create, FILE\_Chpriv, FILE\_Fchpriv, FILE\_Mknod, FILE\_Owner, FS\_Chroot, FS\_Mount, FS\_Umount, PASSWORD\_Check, PROC\_Adjtime,PROC\_Kill, PROC\_Privilege, PROC\_Setpgid, PROC\_SetUserIDs, RESTORE\_Import, TCBCK\_Delete, USER\_Change, USER\_Create, USER\_Reboot, USER\_Remove, and USER\_SetEnv.   
  
Edit /etc/security/audit/config and add the ACCT\_Disable, ACCT\_Enable, AUD\_it, BACKUP\_Export, DEV\_Change, DEV\_Configure, DEV\_Create, FILE\_Chpriv, FILE\_Fchpriv, FILE\_Mknod, FILE\_Owner, FS\_Chroot, FS\_Mount, FS\_Umount, PASSWORD\_Check, PROC\_Adjtime,PROC\_Kill, PROC\_Privilege, PROC\_Setpgid, PROC\_SetUserIDs, RESTORE\_Import, TCBCK\_Delete, USER\_Change, USER\_Create, USER\_Reboot, USER\_Remove, and USER\_SetEnv audit events to an audit class in the classes: stanza.  
  
Edit the /etc/security/audit/config and assign the audit classes with the ACCT\_Disable, ACCT\_Enable, AUD\_it, BACKUP\_Export, DEV\_Change, DEV\_Configure, DEV\_Create, FILE\_Chpriv, FILE\_Fchpriv, FILE\_Mknod, FILE\_Owner, FS\_Chroot, FS\_Mount, FS\_Umount, PASSWORD\_Check, PROC\_Adjtime,PROC\_Kill, PROC\_Privilege, PROC\_Setpgid, PROC\_SetUserIDs, RESTORE\_Import, TCBCK\_Delete, USER\_Change, USER\_Create, USER\_Reboot, USER\_Remove, and USER\_SetEnv events to the all users listed in the users: stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-818  
**Group Title:** Audit login, logout, and session initiation  
**Rule ID:** SV-38856r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002800  
**Rule Title:**The audit system must be configured to audit login, logout, and session initiation.  
  
**Vulnerability Discussion:**  If the system is not configured to audit certain activities and write them to an audit log, it is more difficult to detect and track system compromises and damages incurred during a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
Check the system's audit configuration.  
# more /etc/security/audit/events  
Confirm the following events are configured:  
USER\_Login, USER\_Logout, INIT\_Start, INIT\_End and USER\_SU.  
If any of these events are not present, this is a finding.  
  
Check the USER\_Login, USER\_Logout, INIT\_Start, INIT\_End, and USER\_SU audit events are defined in the audit classes stanza ‘classes:’ of the /etc/security/audit/config file.  
#more /etc/security/audit/config  
Make note of the audit class(es) the USER\_Login, USER\_Logout, INIT\_Start, INIT\_End, and USER\_SU events are associated with.  
If the USER\_Login, USER\_Logout, INIT\_Start, INIT\_End, and USER\_SU events are not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify the audit class is associated with the default user and all other user ids listed in the users: stanza of the /etc/security/audit/config file.  
#more /etc/security/audit/config  
If the class(es) the USER\_Login, USER\_Logout, INIT\_Start, INIT\_End, and USER\_SU events are not associated with the default user and all the system users in the users: stanza, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit/events and add the USER\_Login, USER\_Logout, INIT\_Start, INIT\_End, and USER\_SU events to the list of audited events.   
  
Edit /etc/security/audit/config and add the USER\_Login, USER\_Logout, INIT\_Start, INIT\_End, and USER\_SU audit events to an audit class in the classes: stanza.  
  
Edit the /etc/security/audit/config and assign the audit classes with the USER\_Login, USER\_Logout, INIT\_Start, INIT\_End, and USER\_SU events to the all users listed in the users: stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-819  
**Group Title:** Audit discretionary access control permission   
**Rule ID:** SV-38857r1\_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.  
# more /etc/security/audit/events  
Confirm the following events are configured:  
FILE\_Acl, FILE\_Fchmod, FILE\_Fchown, FILE\_Mode, and   
FILE\_Owner  
If any of these events are not configured, this is a finding.  
  
Check the FILE\_Acl, FILE\_Fchmod, FILE\_Fchown, FILE\_Mode, and FILE\_Owner audit events are defined in the audit classes stanza classes: of the /etc/security/audit/config file.  
#more /etc/security/audit/config  
Make note of the audit class(es) the FILE\_Acl, FILE\_Fchmod, FILE\_Fchown, FILE\_Mode, and   
FILE\_Owner events are associated with.  
  
If the FILE\_Acl, FILE\_Fchmod, FILE\_Fchown, FILE\_Mode, and   
FILE\_Owner events are not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify the audit class is associated with the default user and all other user ids listed in the users: stanza of the /etc/security/audit/config file.  
  
If the class(es) the FILE\_Acl, FILE\_Fchmod, FILE\_Fchown, FILE\_Mode, and FILE\_Owner events are not associated with the default user and all the system users in the users: stanza, this is a finding.  
  
**Fix Text:**Edit /etc/security/audit/events and add the FILE\_Acl, FILE\_Fchmod, FILE\_Fchown, FILE\_Mode, and FILE\_Owner events to the list of audited events.   
  
Edit /etc/security/audit/config and add the FILE\_Acl, FILE\_Fchmod, FILE\_Fchown, FILE\_Mode, and FILE\_Owner audit events to an audit class in the classes: stanza.  
  
Edit the /etc/security/audit/config and assign the audit classes with the FILE\_Acl, FILE\_Fchmod, FILE\_Fchown, FILE\_Mode, and FILE\_Owner events to the all users listed in the users: stanza.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22383  
**Group Title:** GEN002825  
**Rule ID:** SV-38858r1\_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 system is configured to audit the loading and unloading of dynamic kernel modules.   
  
Check the system's audit configuration.  
# more /etc/security/audit/events  
Confirm the following events are configured:  
DEV\_Create, FILE\_Mknod, DEV\_Configure, DEV\_Stop, DEV\_Unconfigure, and DEV\_Remove.  
If any of these events are not configured, this is a finding.  
  
Check the File DEV\_Create, FILE\_Mknod, DEV\_Configure, DEV\_Stop, DEV\_Unconfigure, and DEV\_Remove. Audit events are defined in the audit classes stanza classes: of the /etc/security/audit/config file.  
#more /etc/security/audit/config  
Make note of the audit class(es) the DEV\_Create, FILE\_Mknod, DEV\_Configure, DEV\_Stop, DEV\_Unconfigure, and DEV\_Remove events are associated with.  
  
If the DEV\_Create, FILE\_Mknod, DEV\_Configure, DEV\_Stop, DEV\_Unconfigure, and DEV\_Remove events are not associated with any audit classes in the classes: stanza this is a finding.  
  
Verify the audit class is associated with the default user and all other user ids listed in the users: stanza of the /etc/security/audit/config file.  
  
#more /etc/security/audit/config  
If the class(es) that the DEV\_Create, FILE\_Mknod, DEV\_Configure, DEV\_Stop, DEV\_Unconfigure, and DEV\_Remove events are not associated with the default user and all the system users in the users: stanza, this is a finding.  
  
**Fix Text:**Configure the system to audit the loading and unloading of dynamic kernel modules.  
  
Edit /etc/security/audit/events and add the DEV\_Create, FILE\_Mknod, DEV\_Configure, DEV\_Stop, DEV\_Unconfigure, and DEV\_Remove events to the list of audited events.  
  
Edit /etc/security/audit/config and add the DEV\_Create, FILE\_Mknod, DEV\_Configure, DEV\_Stop, DEV\_Unconfigure, and DEV\_Remove audit events to an audit class in the classes: stanza.  
  
  
Edit the /etc/security/audit/config and assign the audit classes that has the DEV\_Create, FILE\_Mknod, DEV\_Configure, DEV\_Stop, DEV\_Unconfigure and DEV\_Remove events to the all users listed in the ‘users:’ stanza.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4357  
**Group Title:** Audit Logs Rotation  
**Rule ID:** SV-4357r7\_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 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 that automatically rotates audit logs, this is not a finding. If the SA manually rotates audit logs, this is still a finding, because if the SA is not there, it will not be accomplished. If the audit output is not archived daily, to tape or disk, this is a finding. This can be ascertained by looking at the audit log directory and, if more than one file is there, or if the file does not have today’s date, this is a finding.  
  
  
  
**Fix Text:**Configure a cron job or other automated process to rotate the audit logs on a daily basis.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24357  
**Group Title:** GEN002870  
**Rule ID:** SV-38859r1\_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:**    
Consult vendor documentation to determine the settings required for the audit system for sending audit records to a remote system or via syslog.  
  
Remote audit logging can be done with the syslog (logger) facility or a third party tool. If the system is not configured to send audit logs to a remote system, this is a finding.  
  
**Fix Text:**Configure the system to send audit records to a remote system.   
  
Enable stream mode by editing the /etc/security/audit/config and set streammode = on.  
  
Edit /etc/security/audit/streamcmds to send stream logs to the syslog facility with an entry such as:  
/usr/sbin/auditstream | auditpr –v | /usr/bin/logger –p local7.info &  
  
Edit the /etc/syslog.conf file to configure syslog to send local7.info to a remote server with an entry such as:  
Local7.info @logserver   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-974  
**Group Title:** Cron Utility Accessibility  
**Rule ID:** SV-27318r1\_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 /var/adm/cron/cron.allow  
# ls -lL /var/adm/cron/cron.deny  
If neither file exists, this is a finding.  
  
**Fix Text:**Create /var/adm/cron/cron.allow and/or /var/adm/cron/cron.deny with appropriate content.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-975  
**Group Title:** GEN002980  
**Rule ID:** SV-27324r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002980  
**Rule Title:**The cron.allow file must have mode 0600 or less permissive.  
  
**Vulnerability Discussion:**  A cron.allow file that is readable and/or writable by other than root could allow potential intruders and malicious users to use the file contents to help discern information, such as who is allowed to execute cron programs, which could be harmful to overall system and network security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check mode of the cron.allow file.  
  
Procedure:  
# ls -lL /var/adm/cron/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 /var/adm/cron/cron.allow  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22384  
**Group Title:** GEN002990  
**Rule ID:** SV-38780r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN002990  
**Rule Title:**The cron.allow file must not have an extended ACL.  
  
**Vulnerability Discussion:**  A cron.allow file that is readable and/or writable by other than root could allow potential intruders and malicious users to use the file contents to help discern information, such as who is allowed to execute cron programs, which could be harmful to overall system and network security.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the cron.allow file.  
  
#aclget /var/adm/cron/cron.allow  
Verify if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the cron.allow file and disable extended permissions.  
  
#acledit /var/adm/cron/cron.allow   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-976  
**Group Title:** Cron Executes World Writable Programs  
**Rule ID:** SV-27329r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003000  
**Rule Title:**Cron must not execute group-writable or world-writable programs.  
  
**Vulnerability Discussion:**  If cron executes group-writable or world-writable programs, there is a possibility that unauthorized users could manipulate the programs with malicious intent. This could compromise system and network security.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List all cronjobs on the system.   
Procedure:   
# ls /var/spool/cron/crontabs/  
  
If cron jobs exist under any of the above directories, search for programs executed by cron.  
Procedure:  
# more <cron job file>  
  
Determine if the file is group-writable or world-writable.  
Procedure:  
# ls -la <cron program file>  
  
If cron executes group-writable or world-writable files, this is a finding.  
  
**Fix Text:**Remove the world-writable and group-writable permissions from the cron program file(s) identified.  
# chmod go-w <cron program file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-977  
**Group Title:** Cron Executes Programs in World Writable Dirs  
**Rule ID:** SV-38947r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003020  
**Rule Title:**Cron must not execute programs in, or subordinate to, world-writable directories.  
  
**Vulnerability Discussion:**  If cron programs are located in or subordinate to world-writable directories, they become vulnerable to removal and replacement by malicious users or system intruders.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List all cronjobs on the system.  
Procedure:  
# ls /var/spool/cron/crontabs/  
  
If cron jobs exist under any of the above directories search for programs executed by cron.  
Procedure:  
# more <cron job file>  
  
Determine if the directory containing programs executed from cron is world-writable.  
Procedure:  
# ls -ld <cron program directory>  
  
If cron executes programs in world-writable directories, this is a finding.  
  
**Fix Text:**Remove the world-writable permission from the cron program directories identified.  
  
Procedure:  
# chmod o-w <cron program directory>   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11994  
**Group Title:** Crontabs Ownership  
**Rule ID:** SV-27333r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003040  
**Rule Title:**Crontabs must be owned by root or the crontab creator.  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and prevent malicious modification to these jobs, crontab files must be secured.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List all crontabs on the system.   
# ls -lL /var/spool/cron/crontabs/  
  
If any crontab is not owned by root or the creating user, this is a finding.  
  
**Fix Text:**Change the crontab owner to root or the crontab creator.  
# chown root <crontab file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22385  
**Group Title:** GEN003050  
**Rule ID:** SV-26531r1\_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.  
# ls -lL /var/spool/cron/crontabs/  
If the group owner is not root, cron, 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]   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11995  
**Group Title:** Default System Accounts and Cron  
**Rule ID:** SV-27336r1\_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 /var/adm/cron/cron.allow  
# more /var/adm/cron/cron.deny  
  
If a default system account (such as bin, sys, adm, or others) is listed in the cron.allow file, or not listed in the cron.deny file if no cron.allow file exists, this is a finding.  
  
  
**Fix Text:**Remove default system accounts (such as bin, sys, adm, or others) from the cron.allow file if it exists, or add those accounts to the cron.deny file.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-978  
**Group Title:** Crontab files permissions  
**Rule ID:** SV-27340r1\_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/crontabs/  
If any crontab file has a mode more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the crontab files.  
# chmod 0600 /var/spool/cron/crontabs/\*   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22386  
**Group Title:** GEN003090  
**Rule ID:** SV-38782r1\_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.  
Get a listing of crontab files.  
#ls /var/spool/cron/crontabs  
  
Check all of the crontabls listed for an extended ACL.  
#aclget <directory>/<file>   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the crontab file(s) and disable extended permissions.  
  
#acledit <directory>/<file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-979  
**Group Title:** Cron and Crontab Directories Permissions  
**Rule ID:** SV-27342r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003100  
**Rule Title:**Cron and crontab directories must have mode 0755 or less permissive.  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and to prevent malicious modification to these jobs, crontab files must be secured.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the crontab directory.  
# ls -ld /var/spool/cron/crontabs  
If the mode of the crontab directory is more permissive than 0755, this is a finding.  
  
  
**Fix Text:**Change the mode of the crontab directory.  
# chmod 0755 /var/spool/cron/crontabs   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22387  
**Group Title:** GEN003110  
**Rule ID:** SV-39103r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003110  
**Rule Title:**Cron and crontab directories must not have extended ACLs.  
  
**Vulnerability Discussion:**  To protect the integrity of scheduled system jobs and to prevent malicious modification to these jobs, crontab files must be secured. ACLs on cron and crontab directories may provide unauthorized access to these directories. Unauthorized modifications to these directories or their contents may result in the addition of unauthorized cron jobs or deny service to authorized cron jobs.  
  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the crontab directories.  
  
# ls -lL /var/spool/cron/crontabs  
# aclget < crontab >  
# aclget /var/spool/cron  
  
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the crontab file(s) and disable extended permissions.   
  
#acledit <directory>/<file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-980  
**Group Title:** Cron and Crontab Directories Ownership  
**Rule ID:** SV-27345r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003120  
**Rule Title:**Cron and crontab directories must be owned by root or bin.  
  
**Vulnerability Discussion:**  Incorrect ownership of the cron or crontab directories could permit unauthorized users the ability to alter cron jobs and run automated jobs as privileged users. Failure to give ownership of cron or crontab directories to root or to bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the owner of the crontab directory.  
# ls -ld /var/spool/cron/crontabs  
If the owner of the crontab directory is not root or bin, this is a finding.  
  
  
**Fix Text:**Change the mode of the crontab directory.  
# chown root /var/spool/cron/crontabs   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-981  
**Group Title:** Cron and Crontab Directories Group Ownership  
**Rule ID:** SV-39104r1\_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/crontabs  
  
If a cron or crontab directory is not group-owned by root, sys, system, bin, or cron, this is a finding.   
  
**Fix Text:**Change the group owner of the crontab directories to root, sys, system, bin, or cron.   
Procedure: #   
chown system /var/spool/cron/crontabs   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-982  
**Group Title:** Cron Logging  
**Rule ID:** SV-27350r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003160  
**Rule Title:**Cron logging must be implemented.  
  
**Vulnerability Discussion:**  Cron logging can be used to trace the successful or unsuccessful execution of cron jobs. It can also be used to spot intrusions into the use of the cron facility by unauthorized and malicious users.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-1, ECAR-2, ECAR-3  
  
**Check Content:**    
# ls -lL /var/adm/cron/log  
If this file does not exist or is older than the last cron job, this is a finding.  
  
**Fix Text:**Enable cron logging on the system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-983  
**Group Title:** Cronlog Permissions  
**Rule ID:** SV-27355r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003180  
**Rule Title:**The cronlog file must have mode 0600 or less permissive.  
  
**Vulnerability Discussion:**  Cron logs contain reports of scheduled system activities and must be protected from unauthorized access or manipulation.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1, ECTP-1  
  
**Check Content:**    
Check the mode of the cron log file.  
# ls -lL /var/adm/cron/log  
If the mode is more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the cron log file.  
# chmod 0600 /var/adm/cron/log  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22388  
**Group Title:** GEN003190  
**Rule ID:** SV-38783r1\_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:**    
#aclget /var/adm/cron/log   
Verify if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the cronlog file and disable extended permissions.  
  
#acledit /var/adm/cron/log   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4358  
**Group Title:** cron.deny permissions  
**Rule ID:** SV-27360r1\_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 /var/adm/cron/cron.deny  
  
If the cron.deny file is more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the cron.deny file.  
# chmod 0600 /var/adm/cron/cron.deny   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22389  
**Group Title:** GEN003210  
**Rule ID:** SV-38785r1\_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:**    
#aclget /var/adm/cron/cron.deny  
  
Verify if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the cron.deny file and disable extended permissions.  
  
#acledit /var/adm/cron/cron.deny   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4360  
**Group Title:** Cron programs umask  
**Rule ID:** SV-27364r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003220  
**Rule Title:**Cron programs must not set the umask to a value less restrictive than 077.  
  
**Vulnerability Discussion:**  The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask is often represented as a 4-digit octal number, the first digit representing special access modes is typically ignored or required to be 0.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Determine if there are any crontabs by viewing a long listing of the directory. If there are crontabs, examine them to determine what cron jobs exist. Check for any programs specifying an umask.  
  
# ls -lL /var/spool/cron/crontabs  
# cat <crontab file>  
# grep umask <cron program>  
  
If there are no cron jobs present, this vulnerability is not applicable. If any cron job contains an umask value more permissive than 077, this is a finding.  
  
**Fix Text:**Edit cron script files and modify the umask to 077.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4361  
**Group Title:** cron.allow ownership.  
**Rule ID:** SV-27367r1\_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 /var/adm/cron/cron.allow  
  
If the cron.allow file is not owned by root, sys, or bin, this is a finding.  
  
**Fix Text:**# chown root /var/adm/cron/cron.allow   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22390  
**Group Title:** GEN003245  
**Rule ID:** SV-38786r1\_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:**    
#aclget /var/adm/cron/at.allow  
Verify if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the at.allow file and disable extended permissions.  
  
#acledit /var/adm/cron/at.allow   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22391  
**Group Title:** GEN003250  
**Rule ID:** SV-39346r1\_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:**    
Determine the group owner of the cron.allow file.   
Procedure:   
# ls -lL /var/adm/cron/cron.allow   
If the group owner is not root, bin, sys, system, or cron, this is a finding.   
  
**Fix Text:**Change the group owner of the cron.allow file to root, bin, sys, system, or cron.   
Procedure:   
# chgrp system /var/adm/cron/cron.allow   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22392  
**Group Title:** GEN003252  
**Rule ID:** SV-38787r1\_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:**    
Determine the mode of the at.deny file.  
# ls -lL /var/adm/cron/at.deny  
If the mode of the at.deny file is more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the at.deny file to 0600.  
# chmod 0600 /var/adm/cron/at.deny   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22393  
**Group Title:** GEN003255  
**Rule ID:** SV-38788r1\_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:**    
Determine if the at.deny file has an extended ACL.  
  
#aclget /var/adm/cron/at.deny  
Verify if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the at.deny file and disable extended permissions.  
#acledit /var/adm/cron/at.deny   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4430  
**Group Title:** cron.deny ownership  
**Rule ID:** SV-27372r1\_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 /var/adm/cron/cron.deny  
  
If the cron.deny file is not owned by root, sys, or bin, this is a finding.  
  
  
**Fix Text:**# chown root /var/adm/cron/cron.deny   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22394  
**Group Title:** GEN003270  
**Rule ID:** SV-38789r1\_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:**    
Determine the cron.deny file's group owner.  
  
Procedure:  
# ls -lL /var/adm/cron/cron.deny  
  
If the file is not group-owned by root, bin, sys, or cron, this is a finding.  
  
  
**Fix Text:**Change the group owner of the cron.deny file to root, sys, system, bin, or cron.  
  
Procedure:  
# chgrp system /var/adm/cron/cron.deny  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-984  
**Group Title:** At Utility Accessibility  
**Rule ID:** SV-27377r1\_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 /var/adm/cron/at.allow  
# ls -lL /var/adm/cron/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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-985  
**Group Title:** GEN003300  
**Rule ID:** SV-27381r1\_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 /var/adm/cron/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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-986  
**Group Title:** Default System Accounts and At  
**Rule ID:** SV-27385r1\_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 /var/adm/cron/at.allow  
If default accounts (such as bin, sys, adm, and others) are listed in the at.allow file, this is a finding.  
  
**Fix Text:**Remove the default accounts (such as bin, sys, adm, and others) from the at.allow file.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-987  
**Group Title:** at.allow and at.deny permissions  
**Rule ID:** SV-27389r1\_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 /var/adm/cron/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 /var/adm/cron/at.allow   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-988  
**Group Title:** At Executes World Writable Programs  
**Rule ID:** SV-988r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003360  
**Rule Title:**The at daemon must not execute group-writable or world-writable programs.  
  
**Vulnerability Discussion:**  If the at facility executes world-writable or group-writable programs, it is possible for the programs to be accidentally or maliciously changed or replaced without the owner's intent or knowledge. This would cause a system security breach.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List the at jobs on the system.  
Procedure:  
# ls -la /var/spool/cron/atjobs /var/spool/atjobs  
  
For each at job file, determine which programs are executed.  
Procedure:  
# more <at job file>  
  
Check each program executed by at for group- or world-writable permissions.  
Procedure:  
# ls –la <at program file>  
  
If at executes group- or world-writable programs, this is a finding.  
  
**Fix Text:**Remove group-write and world-write permissions from files executed by at jobs.  
Procedure:  
# chmod go-w <file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-989  
**Group Title:** At Executes Programs in World Writable Directories  
**Rule ID:** SV-989r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003380  
**Rule Title:**The at daemon must not execute programs in, or subordinate to, world-writable directories.  
  
**Vulnerability Discussion:**  If at programs are located in, or subordinate, to world-writable directories, they become vulnerable to removal and replacement by malicious users or system intruders.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
List any at jobs on the system.  
Procedure:  
# ls /var/spool/cron/atjobs /var/spool/atjobs  
  
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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4364  
**Group Title:** GEN003400  
**Rule ID:** SV-38907r1\_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.  
# ls –lLd /var/spool/cron/atjobs   
  
If the directory mode is more permissive than 0755, this is a finding.  
  
**Fix Text:**Change the mode of the at directory to 0755.  
  
Procedure:  
# chmod 0755 < at directory >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22395  
**Group Title:** GEN003410  
**Rule ID:** SV-38790r1\_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 file.  
#aclget /var/spool/cron/atjobs   
Verify if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the at directory and disable extended permissions.  
  
#acledit /var/spool/cron/atjobs   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4365  
**Group Title:** GEN003420  
**Rule ID:** SV-39350r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003420  
**Rule Title:**The at directory must be owned by root, bin, or sys.  
  
**Vulnerability Discussion:**  If the owner of the at directory is not root, bin, or sys, unauthorized users could be allowed to view or edit files containing sensitive information within the directory.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the at directory.   
Procedure:   
# ls –ld /var/spool/cron/atjobs  
  
If the directory is not owned by root, sys, bin, daemon, or cron, this is a finding.  
  
**Fix Text:**Change the owner of the at directory to root, bin, sys, or system.   
Procedure:   
# chown root /var/spool/cron/atjobs   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22396  
**Group Title:** GEN003430  
**Rule ID:** SV-39352r1\_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/cron/atjobs   
  
If the file is not group-owned by root, bin, sys, system, or cron, this is a finding.  
  
**Fix Text:**Change the group ownership of the file to root, bin, sys, system, or cron.  
  
Procedure:  
# chgrp root /var/spool/cron/atjobs /var/spool/atjobs   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4366  
**Group Title:** At programs umask  
**Rule ID:** SV-4366r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003440  
**Rule Title:**At jobs must not set the umask to a value less restrictive than 077.  
  
**Vulnerability Discussion:**  The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask is often represented as a 4-digit number, the first digit representing special access modes is typically ignored or required to be 0.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Determine what at jobs exist on the system.  
Procedure:  
# ls /var/spool/cron/atjobs /var/spool/atjobs  
  
If there are no at jobs present, this is not applicable.  
  
Determine if any of the at jobs or any scripts referenced execute the umask command. Check for any umask setting more permissive than 077.  
  
# grep umask <at job or referenced script>  
  
If any at job or referenced script sets umask to a value more permissive than 077, this is a finding.  
  
**Fix Text:**Edit at jobs or referenced scripts to remove umask commands that set umask to a value less restrictive than 077.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4367  
**Group Title:** at.allow ownership  
**Rule ID:** SV-27393r1\_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 /var/adm/cron/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 /var/adm/cron/at.allow   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22397  
**Group Title:** GEN003470  
**Rule ID:** SV-39354r1\_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:**    
Determine the group owner of the at.allow file.   
Procedure:   
# ls -lL /var/adm/cron/at.allow   
If the group-owner is not root, bin, sys, system, or cron, this is a finding.   
  
**Fix Text:**Change the group owner of the at.allow file to root, sys, system, bin, or cron.   
Procedure:   
# chgrp system /var/adm/cron/at.allow   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4368  
**Group Title:** at.deny ownership  
**Rule ID:** SV-27397r1\_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 /var/adm/cron/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 /var/adm/cron/at.deny   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22398  
**Group Title:** GEN003490  
**Rule ID:** SV-39356r1\_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:**    
Determine the group-owner of the at.deny file.   
Procedure:  
# ls -lL /var/adm/cron/at.deny   
If the group-owner is not root, bin, sys, system, or cron, this is a finding.   
  
**Fix Text:**Change the group owner of the at.deny file to root, bin, sys, system, or cron.  
Procedure:   
# chgrp root /var/adm/cron/at.deny   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11996  
**Group Title:** Disable Core Dumps  
**Rule ID:** SV-27402r1\_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:**    
lsuer –a core ALL  
  
If any user does not have a value of core = 0, this is a finding.  
  
  
**Fix Text:**#chsec -f /etc/security/limits –s default –a core=0   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22399  
**Group Title:** GEN003501  
**Rule ID:** SV-38791r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003501  
**Rule Title:**The system must be configured to store any process core dumps in a specific, centralized directory.  
  
**Vulnerability Discussion:**  Specifying a centralized location for core file creation allows for the centralized protection of core files. Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If process core dump creation is not configured to use a centralized directory, core dumps may be created in a directory without appropriate ownership or permissions configured, which could result in unauthorized access to the core dumps.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
#more /etc/security/user  
Look for both core\_path = on and core\_pathname = in the default: stanza. If these are blank or not existent, this is a finding.  
  
  
**Fix Text:**Configure the system to create process core dumps only in a specific, centralized location.   
#chsec –f /etc/security/user –s default –a core\_path=on  
#chsec –f /etc/security/user –s default –a core\_pathname=< directory path to process coredumps>  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22400  
**Group Title:** GEN003502  
**Rule ID:** SV-38792r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003502  
**Rule Title:**The centralized process core dump data directory must be owned by root.  
  
**Vulnerability Discussion:**  Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the centralized process core dump data directory is not owned by root, the core dumps contained in the directory may be subject to unauthorized access.  
  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine the owner of the centralized process core dump directory.  
#grep core\_pathname /etc/security/user  
# ls -lLd < process core dump directory>  
If the owner is not root, this is a finding.  
  
  
**Fix Text:**Change the owner of the centralized process core dump directory to root.  
# chown root < process core dump directory>   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22401  
**Group Title:** GEN003503  
**Rule ID:** SV-38793r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003503  
**Rule Title:**The centralized process core dump data directory must be group-owned by root, bin, sys, or system.  
  
**Vulnerability Discussion:**  Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the centralized process core dump data directory is not group-owned by a system group, the core dumps contained in the directory may be subject to unauthorized access  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine the group-owner of the centralized process core dump directory.  
#grep core\_pathname /etc/security/user  
# ls -lLd < process core dump directory >  
If the group owner is not root, bin, sys, or system, this is a finding.  
  
  
**Fix Text:**Change the group-owner of the centralized process core dump data directory to root, bin, sys, or system.  
# chgrp root <process core dump directory>   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22402  
**Group Title:** GEN003504  
**Rule ID:** SV-38794r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003504  
**Rule Title:**The centralized process core dump data directory must have mode 0700 or less permissive.  
  
**Vulnerability Discussion:**  Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the process core dump data directory has a mode more permissive than 0700, unauthorized users may be able to view or to modify sensitive information contained any process core dumps in the directory.  
  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine the mode of the centralized process core dump data directory.  
  
Procedure:  
#grep core\_pathname /etc/security/user  
# ls -lLd <process core dump directory>  
  
If the mode is more permissive than 0700, this is a finding.  
  
  
**Fix Text:**Change the mode of the centralized process core dump directory to 0700.  
Procedure:  
# chmod 0700 <process core dump directory>   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22403  
**Group Title:** GEN003505  
**Rule ID:** SV-38795r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003505  
**Rule Title:**The centralized process core dump data directory must not have an extended ACL.  
  
**Vulnerability Discussion:**  Process core dumps contain the memory in use by the process when it crashed. Any data the process was handling may be contained in the core file, and it must be protected accordingly. If the process core dump data directory has an extended ACL, unauthorized users may be able to view or to modify sensitive information contained any process core dumps in the directory.  
  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Determine if the centralized process core dump data directory has an extended ACL.  
#grep core\_pathname /etc/security/user  
  
#aclget <process core dump directory>   
Verify if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the centralized process core dump data directory and disable extended permissions.  
  
#acledit <process core dump directory>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22404  
**Group Title:** GEN003510  
**Rule ID:** SV-38860r1\_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:**    
Determine if kernel core dumps are enabled on the system.   
  
#sysdumpdev –l  
  
Look at both the primary and secondary dump devices. If either the primary or secondary dump device is not /dev/sysdumpnull, this is a finding.  
  
  
**Fix Text:**Disable kernel core dumps on the system by setting primary and secondary dump devices to sysdumpnull.   
  
#sysdumpdev –P –p /dev/sysdumpnull  
  
#sysdumpdev –P –s /dev/sysdumpnull  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11997  
**Group Title:** Core Dump Directory Ownership and Permissions  
**Rule ID:** SV-38861r1\_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:**    
Determine the core file copy location.  
#sysdumpdev –l | grep –i”core dir”  
  
Check the ownership of the kernel core dump data directory.  
# ls -ld < dump file location >  
If the kernel core dump data directory is not owned by root, this is a finding.  
  
Supplementary Information: The location of the kernel dump area should be moved out of /var/adm/ras. This directory may be world read/writeable. A suggestion would be to create /var/adm/kcore; chown root:sys /var/adm/kcore; chmod 700 /var/adm/kcore.   
Change where the system copies its kernel core files to.  
sysdumpdev –d /var/adm/kcore  
  
  
**Fix Text:**Change the owner of the kernel core dump data directory to root.   
  
# chown root /var/adm/ras  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22405  
**Group Title:** GEN003521  
**Rule ID:** SV-38862r1\_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 core file copy location.  
#sysdumpdev –l | grep –i”core dir”  
  
Determine the group-owner of the kernel core dump data directory.  
# ls -lLd < directory >  
If the group-owner is not root, bin, sys, or system, this is a finding.  
  
**Fix Text:**Change the group-owner of the kernel core dump data directory to root, bin, sys, or system.  
# chgrp root < directory >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22406  
**Group Title:** GEN003522  
**Rule ID:** SV-38863r1\_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 core file copy location.  
  
#sysdumpdev –l |grep –I ”core dir”   
  
Determine the mode of the kernel core dump data directory.  
# ls -lLd < directory >  
  
If the mode is more permissive than 0700, this is a finding.  
  
  
  
**Fix Text:**Change the mode of the kernel core dump data directory to 0700.  
  
# chmod 0700 < directory >  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22407  
**Group Title:** GEN003523  
**Rule ID:** SV-38864r1\_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 core file copy location from the sysdumpdev command  
  
#sysdumpdev –l | grep –I “core dir”  
  
Determine if the kernel core dump data directory has an extended ACL.  
  
#aclget < directory >   
Verify if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the kernel core dump data directory and disable extended permissions.  
  
#acledit < directory >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-11999  
**Group Title:** Disable Executable Stack  
**Rule ID:** SV-39504r1\_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:**  ECSC-1  
  
**Check Content:**    
Determine if the system implements non-executable program stacks. If the system does not implement non-executable program stacks, this is a finding.  
  
**Fix Text:**Enable non-executable program stacks on the system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12001  
**Group Title:** GEN003580  
**Rule ID:** SV-38838r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003580  
**Rule Title:**The system must use initial TCP sequence numbers most resistant to sequence number guessing attacks.  
  
**Vulnerability Discussion:**  One use of initial TCP sequence numbers is to verify bidirectional communication between two hosts, which provides some protection against spoofed source addresses being used by the connection originator. If the initial TCP sequence numbers for a host can be determined by an attacker, it may be possible to establish a TCP connection from a spoofed source address without bidirectional communication.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# instfix -ik iy55950, this applies to AIX 4.3 and AIX 5.1.  
# instfix -ik iy55949 , this applies to AIX 5.2.  
# instfix -ik iy62006, this applies to AIX 5.3.  
If the above patches (or successors) are not applied, this is a finding.  
  
**Fix Text:**Install these patches (or successors): iy55950, iy55949, iy62006. Keep OS patches / TL(Technology Levels) and SP (Service Packs) current. Use a web browser to check the vendor's website for Patches, Technology Levels, and Service Packs.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22408  
**Group Title:** GEN003581  
**Rule ID:** SV-38865r1\_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:**    
Determine if any network interfaces on the system are configured to allow user control.   
  
AIX does not allow non-root user to configure network interfaces. Mark this as not a finding.  
  
  
**Fix Text:**No fix needed.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12002  
**Group Title:** GEN003600  
**Rule ID:** SV-38948r1\_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:**    
# /usr/sbin/no -o ipsrcrouteforward  
If the returned value is not 0, this is a finding.  
  
**Fix Text:**# /usr/sbin/no -po "ipsrcrouteforward=0"   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23741  
**Group Title:** GEN003601  
**Rule ID:** SV-38796r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003601  
**Rule Title:**TCP backlog queue sizes must be set appropriately.  
  
**Vulnerability Discussion:**  To provide some mitigation to TCP DoS attacks, the clear\_partial\_conns parameter must be enabled.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# /usr/sbin/no –o clean\_partial\_conns  
If the value returned is 0, this is a finding.  
  
**Fix Text:**  
# /usr/sbin/no –po clean\_partial\_conns=1   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22409  
**Group Title:** GEN003602  
**Rule ID:** SV-38866r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003602  
**Rule Title:**The system must not process ICMP timestamp requests.  
  
**Vulnerability Discussion:**  The processing of Internet Control Message Protocol (ICMP) timestamp requests increases the attack surface of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system is configured to respond to ICMP Timestamp requests.   
  
#lsfit  
  
If there is no rule blocking ICMP packet type of 13 and ICMP packet type of 14, this is a finding.  
  
  
**Fix Text:**Use SMIT or genfilt commands to configure the system firewall to block ICMP packet types 13, and 14.  
  
#smitty ipsec4  
  
# genfilt  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22410  
**Group Title:** GEN003603  
**Rule ID:** SV-38797r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003603  
**Rule Title:**The system must not respond to ICMPv4 echoes sent to a broadcast address.  
  
**Vulnerability Discussion:**  Responding to broadcast Internet Control Message Protocol (ICMP) echoes facilitates network mapping and provides a vector for amplification attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# /usr/sbin/no –o icmpaddressmask  
If the value returned is not 0, this is a finding.  
  
  
**Fix Text:**Configure the system to ignore ICMP ECHO\_REQUESTs sent to broadcast addresses.   
#no –po icmpaddressmask=0  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22411  
**Group Title:** GEN003604  
**Rule ID:** SV-38798r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003604  
**Rule Title:**The system must not respond to ICMP timestamp requests sent to a broadcast address.  
  
**Vulnerability Discussion:**  The processing of Internet Control Message Protocol (ICMP) timestamp requests increases the attack surface of the system. Responding to broadcast ICMP timestamp requests facilitates network mapping and provides a vector for amplification attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# /usr/sbin/no –o bcastping  
If the value returned is not 0, this is a finding.  
  
  
**Fix Text:**Configure the system to ignore ICMP Timestamp requests sent to broadcast addresses.   
#no –po bcastping=0  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22412  
**Group Title:** GEN003605  
**Rule ID:** SV-38799r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003605  
**Rule Title:**The system must not apply reversed source routing to TCP responses.  
  
**Vulnerability Discussion:**  Source-routed packets allow the source of the packet to suggest routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system is configured to apply reverse source routing to TCP responses to source-routed packets#/usr/sbin/no –p nolocsroute  
If the value is not 0, this is a finding.  
  
  
**Fix Text:**Configure the system to not apply reverse source routing to TCP responses to source-routed packets.   
#/usr/sbin/no –po nolocsroute=0  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22413  
**Group Title:** GEN003606  
**Rule ID:** SV-38949r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003606  
**Rule Title:**The system must prevent local applications from generating source-routed packets.  
  
**Vulnerability Discussion:**  Source-routed packets allow the source of the packet to suggest routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# /usr/sbin/no -o ipsrcroutesend  
If the result is not 0, this is a finding.  
  
**Fix Text:**# /usr/sbin/no -po "ipsrcroutesend=0"   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22414  
**Group Title:** GEN003607  
**Rule ID:** SV-38800r1\_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, such as when IPv4 forwarding is enabled and the system is functioning as a router  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# /usr/sbin/no –o ipsrcrouterecv   
If the result is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not accept source-routed IPv4 packets.   
#/usr/sbin/no –p –o ipsrcrouterecv=0   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22415  
**Group Title:** GEN003608  
**Rule ID:** SV-38867r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003608  
**Rule Title:**Proxy ARP must not be enabled on the system.  
  
**Vulnerability Discussion:**  Proxy ARP allows a system to respond to ARP requests on one interface on behalf of hosts connected to another interface. If this function is enabled when not required, addressing information may be leaked between the attached network segments.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system has proxy ARP enabled.  
  
Check Content:   
Check the system for non-local published ARP entries.  
# arp –a  
If any entries are listed as published, this is a finding.  
  
  
  
**Fix Text:**Remove any non-local published ARP entries.  
# arp -d < host >  
  
Check system initialization scripts for any commands configuring published ARP entries (such as "arp -s <host> <addr> pub") and remove them.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22416  
**Group Title:** GEN003609  
**Rule ID:** SV-38801r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003609  
**Rule Title:**The system must ignore IPv4 ICMP redirect messages.  
  
**Vulnerability Discussion:**  ICMP redirect messages are used by routers to inform hosts 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:**    
# /usr/sbin/no –o ipignoreredirects  
If the value returned is not 1, this is a finding.  
  
**Fix Text:**Configure the system to ignore IPv4 ICMP redirect messages.   
#/usr/sbin/no –p –o ipignoreredirects = 1  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22417  
**Group Title:** GEN003610  
**Rule ID:** SV-38802r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003610  
**Rule Title:**The system must not send IPv4 ICMP redirects.  
  
**Vulnerability Discussion:**  ICMP redirect messages are used by routers to inform hosts 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:**    
# /usr/sbin/no –o ipsendredirects  
If the value is not 0, this is a finding.  
  
**Fix Text:**  
#/usr/sbin/no -p –o ipsendredirects=0   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22418  
**Group Title:** GEN003611  
**Rule ID:** SV-38868r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003611  
**Rule Title:**The system must log martian packets.  
  
**Vulnerability Discussion:**  Martian packets are packets containing addresses known by the system to be invalid. Logging these messages allows the SA to identify misconfigurations or attacks in progress.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Determine if the system is configured to log martian packets. Examine the IPF rules on the system.  
  
# lsfilt -a  
  
There must be rules to log inbound traffic containing invalid source addresses, which minimally include the system's own addresses and broadcast addresses for attached subnets. If no such rules exist, this is a finding.  
  
**Fix Text:**Configure the system to log martian packets.  
  
Add rules to log inbound traffic containing invalid source addresses, which minimally include the system's own addresses and broadcast addresses for attached subnets.  
  
For example, consider a system with a single network connection having IP address 192.168.1.10 with a local subnet broadcast address of 192.168.1.255.   
Packets with source addresses of 192.168.1.10 and 192.168.1.255 must be logged if received by the system from the network connection.  
Use the smit utility or genfilt command to add logging of martian packets (packets with a source address of 192.168.1.10 and 192.168.1.255).  
  
#smitty ipsec4  
  
OR  
  
#genfilt –v4 –a P –s 192.168.1.10 –m 0.0.0.0 –d 0.0.0.0 –M -0.0.0.0 –c all –o any –O any –p 0 –P 0 –w I –l y –a en0   
#genfilt –v4 –a P –s 192.168.1.255 –m 0.0.0.0 –d 0.0.0.0 –M -0.0.0.0 –c all –o any –O any –p 0 –P 0 –w I –l y –a en0   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22419  
**Group Title:** GEN003612  
**Rule ID:** SV-38803r1\_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 not track a connection until 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:**    
# /usr/sbin/no –o clean\_partial\_conns  
If the value returned is not 1, this is a finding.  
  
**Fix Text:**  
#/usr/sbin/no –p –o clean\_partial\_conns=1   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22420  
**Group Title:** GEN003613  
**Rule ID:** SV-38869r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003613  
**Rule Title:**The system must use a reverse-path filter for IPv4 network traffic when possible.  
  
**Vulnerability Discussion:**  Reverse-path filtering provides protection against spoofed source addresses by causing the system to discard packets with source addresses for which the system has no route or if the route does not point towards the interface on which the packet arrived. Reverse-path filtering should be used whenever possible. Depending on the role of the system, reverse-path filtering may cause legitimate traffic to be discarded and, therefore, should be used in a more permissive mode or not at all.   
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system is configured to use reverse-path filtering.   
Examine the IPSec rules on the system.  
# lsfilt -a  
  
All systems must block inbound traffic destined to the loopback address.   
  
Additionally, if the system is multihomed and the attached networks are isolated or perform symmetric routing, traffic with source addresses expected on one interface must be blocked when received on another interface.  
  
If this filtering is not configured on the system, this is a finding.  
  
**Fix Text:**Configure the system to use reverse-path filtering.   
  
Add a rule to block traffic with loopback network source addresses from being received on interfaces other than the loopback.  
Use smitty or genfilt command to block loopback address from network interfaces.  
#smitty ipsec4  
  
#genfilt –v4 –a D –s 127.0.0.0 –m 255.0.0 –d 0.0.0.0 –M 0.0.0.0 –c all –O any –w I –l y –a en0  
        
If the system is multihomed and the attached networks are isolated or perform symmetric routing, add rules to block traffic with source addresses expected on one interface when received on another interface.  
  
For example, consider a system with two network interfaces, one attached to an isolated management network with address 10.0.0.55/24 and the other attached to a production network with address 192.168.1.2/24 and a default route. Traffic with a source address on the 10.0.0.0/24 network must be the only traffic accepted on the management interface and must not be accepted on the production interface. This can be accomplished with IPF rules such as:  
  
#smitty ipsec4  
#genfilt –v4 –a D –s 10.0.0.0 –m 255.255.255.0 –d 0.0.0.0 –M 0.0.0.0 –c all –O any –w I –l y –a (prod en{x})  
#genfilt –v4 –a D –s 192.168.1.0 –m 255.255.255.0 –d 0.0.0.0 –M 0.0.0.0 –c all –O any –w I –l y –a (mgmt en{x})   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22421  
**Group Title:** GEN003619  
**Rule ID:** SV-38804r1\_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:**    
Not applicable (NA) for AIX.  
  
**Fix Text:**None required.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12003  
**Group Title:** GEN003620  
**Rule ID:** SV-38870r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003620  
**Rule Title:**A separate file system must be used for user home directories (such as /home or equivalent).  
  
**Vulnerability Discussion:**  The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the /home path is a separate file system.  
  
#df –k /home  
  
If /home is not on its own file system, this is a finding.  
  
**Fix Text:**Migrate the /home (or equivalent) path onto a separate file system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23736  
**Group Title:** GEN003621  
**Rule ID:** SV-38871r1\_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 file system.   
# df –k /var  
If /var is not on its own file system, this is a finding.  
  
**Fix Text:**Migrate the /var path onto a separate file system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23738  
**Group Title:** GEN003623  
**Rule ID:** SV-38872r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003623  
**Rule Title:**The system must use a separate file system for the system audit data path.  
  
**Vulnerability Discussion:**  The use of separate file systems for different paths can protect the system from failures resulting from a file system becoming full or failing.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine the location of the audit data path.  
  
#more /etc/security/audit/config  
Make note of the binfile and trail location.  
(The best practice is to have the audit data and trails sent to /audit.)  
  
# cd < audit path >  
#df –k .  
  
If the system audit data path is not on a separate file system, this is a finding.  
  
**Fix Text:**Migrate the system audit data path onto a separate file system.   
  
Update the /etc/security/audit/config file as necessary to reflect the location of the audit data.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23739  
**Group Title:** GEN003624  
**Rule ID:** SV-39505r1\_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 file system.  
  
#df –k /tmp  
  
If ‘/tmp’ is not own its own file system, this is a finding.  
  
  
**Fix Text:**Migrate the /tmp path onto a separate file system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4304  
**Group Title:** GEN003640  
**Rule ID:** SV-38909r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003640  
**Rule Title:**The root file system must employ journaling or another mechanism ensuring file system consistency.  
  
**Vulnerability Discussion:**  File system journaling, or logging, can allow reconstruction of file system data after a system crash, thus, preserving the integrity of data that may have otherwise been lost. Journaling file systems typically do not require consistency checks upon booting after a crash, which can improve system availability. Some file systems employ other mechanisms to ensure consistency which also satisfy this requirement.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Logging should be enabled for those types of files systems that do not turn on logging by default.   
  
Procedure:  
# mount  
#lsfs  
  
JFS,JFS2, 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 system types, if the root file system does not have the logging option, this is a finding. If the nolog option or the log=NULL option is set on the root file system, this is a finding.  
  
**Fix Text:**Implement file system journaling for the root file system, or use a file system using other mechanisms to ensure consistency. If the root file system supports journaling, enable it. If the file system does not support journaling or another mechanism to ensure consistency, a migration to a different file system will be necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22422  
**Group Title:** GEN003650  
**Rule ID:** SV-39105r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003650  
**Rule Title:**All local file systems must employ journaling or another mechanism ensuring file system consistency.  
  
**Vulnerability Discussion:**  File system journaling, or logging, can allow reconstruction of file system data after a system crash, thus preserving the integrity of data that may have otherwise been lost. Journaling file systems typically do not require consistency checks upon booting after a crash, which can improve system availability. Some file systems employ other mechanisms to ensure consistency which also satisfy this requirement.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the local file systems employ journaling or another mechanism ensuring file system consistency.  
  
Procedure:  
List all local file system mount points.  
#df -l  
#lsfs < each file system returned>  
  
If any file systems are not jfs or jfs2, this is a finding.   
  
**Fix Text:**Convert local file systems to use journaling or another mechanism ensuring file system consistency.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12004  
**Group Title:** Authentication Data Logging  
**Rule ID:** SV-12505r5\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003660  
**Rule Title:**The system must log authentication informational data.  
  
**Vulnerability Discussion:**  Monitoring and recording successful and unsuccessful logins assists in tracking unauthorized access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAR-2, ECAR-3  
  
**Check Content:**    
Check /etc/syslog.conf and verify the auth facility is logging both the notice and info level messages by:  
  
# grep “auth.notice” /etc/syslog.conf  
# grep “auth.info” /etc/syslog.conf  
OR  
# grep 'auth.\*' /etc/syslog.conf  
  
If auth.\* is not found, and either auth.notice or auth.info is not found, this is a finding.  
  
**Fix Text:**Edit /etc/syslog.conf and add local log destinations for auth.\* or both auth.notice and auth.info.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12005  
**Group Title:** Disable inetd/xinetd   
**Rule ID:** SV-12506r4\_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:**    
First, determine if inetd/xinetd is running.  
# ps -ef |grep inetd  
If inetd is not running, this check is not a finding.  
# grep -v "^#" /etc/inetd.conf  
If no active services are found, yet the inetd daemon is running, this is a finding.  
  
**Fix Text:**Remove or disable the inetd startup scripts and kill the service.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-821  
**Group Title:** GEN003720  
**Rule ID:** SV-821r6\_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 which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of inetd.conf file.  
  
Procedure:  
# ls -lL /etc/inetd.conf  
  
This is a finding if any of the above files or directories are not owned by root or bin.  
  
**Fix Text:**Change the ownership of the inetd.conf file to root or bin.   
  
Procedure:  
# chown root /etc/inetd.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22423  
**Group Title:** GEN003730  
**Rule ID:** SV-26650r1\_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 which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the inetd and xinetd configuration files, and xinetd directory.  
  
Procedure:  
# ls -alL /etc/inetd.conf /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 ownership of the inetd configuration file.  
# chgrp root /etc/inetd.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-822  
**Group Title:** GEN003740  
**Rule ID:** SV-822r7\_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 inetd.conf file by:  
# ls -lL /etc/inetd.conf  
If the mode of the file(s) is more permissive than 0440, this is a finding.  
  
  
**Fix Text:**Change the mode of the inetd.conf file.  
# chmod 0440 /etc/inetd.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22424  
**Group Title:** GEN003745  
**Rule ID:** SV-38805r1\_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 inetd configuration file.  
#aclget /etc/inetd.conf   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the /etc/inetd.conf file and disable extended permissions.   
  
#acledit /etc/inetd.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22425  
**Group Title:** GEN003750  
**Rule ID:** SV-39106r1\_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:**    
AIX does not use the xinetd.conf file or directory. Mark this as not a finding.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22426  
**Group Title:** GEN003755  
**Rule ID:** SV-38873r1\_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:**    
AIX does not use the xinetd.conf file or directory. Mark this as not a finding.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-823  
**Group Title:** GEN003760  
**Rule ID:** SV-823r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003760  
**Rule Title:**The services file must be owned by root or bin.  
  
**Vulnerability Discussion:**  Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the services file.  
  
Procedure:  
# ls -lL /etc/services  
  
If the services file is not owned by root or bin, this is a finding.  
  
**Fix Text:**Change the ownership of the services file to root or bin.  
  
Procedure:  
# chown root /etc/services   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22427  
**Group Title:** GEN003770  
**Rule ID:** SV-39112r1\_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 which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the services file.  
  
Procedure:  
# ls -lL /etc/services  
  
If the file is not group-owned by root, bin, sys, or system, this is a finding.  
  
  
**Fix Text:**Change the group owner of the services file.  
  
Procedure:  
# chgrp system /etc/services   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-824  
**Group Title:** GEN003780  
**Rule ID:** SV-824r7\_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   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22428  
**Group Title:** GEN003790  
**Rule ID:** SV-38950r1\_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.  
  
#aclget /etc/services  
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the services file and disable extended permissions.  
  
#acledit /etc/services   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1011  
**Group Title:** GEN003800  
**Rule ID:** SV-38951r1\_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 that are connecting to their machines and to observe what network services are being sought. This provides valuable information when trying to find the source of malicious users and potential malicious users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if inetd or xinetd has logging or tracing enabled.   
  
# ps -ef |grep inetd |grep "-d"   
  
If no results are returned, this is a finding.  
  
**Fix Text:**Edit the inetd startup script to contain the "-d" parameter for the inetd process.  
  
#vi /etc/rc.tcpip  
  
# chssys -s inetd -a '-d'   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22429  
**Group Title:** GEN003810  
**Rule ID:** SV-38874r1\_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:**    
If the portmap service is required for system operations, this is not a finding.  
  
Determine if the portmap service is running.  
#ps –ef|grep portmap  
If portmap is running, this is a finding.  
  
  
**Fix Text:**Disable the portmap service from auto starting by commenting out portmap from /etc/rc.tcpip.  
  
# vi /etc/rc.tcpip  
  
Shutdown the portmap service  
#ps –ef|grep portmap  
#kill <pid of portmap>  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22430  
**Group Title:** GEN003815  
**Rule ID:** SV-38952r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003815  
**Rule Title:**The portmap or rpcbind service must not be installed unless needed.  
  
**Vulnerability Discussion:**  The portmap and rpcbind services increase the attack surface of the system and should only be used when needed. The portmap or rpcbind services are used by a variety of services using Remote Procedure Calls (RPCs).  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system needs the portmap service to operate, this is not applicable. Consult vendor documentation to determine the name and location of the portmap service.   
  
The portmap executable is part of fileset bos.net.tcp.client and is not removable, so this will always be a finding.  
  
**Fix Text:**If the portmap or rpcbind service is part of a removable package, consult vendor documentation for the procedure to remove the package. If the service cannot be removed, prevent service activation by removing all permissions from the executable.   
  
Procedure:  
# chmod 0000 /usr/sbin/portmap   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4687  
**Group Title:** GEN003820  
**Rule ID:** SV-27434r1\_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:**    
# grep -v "^#" /etc/inetd.conf |grep rshd  
If rshd is found to be enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the rshd service. Restart the inetd service.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22431  
**Group Title:** GEN003825  
**Rule ID:** SV-38806r1\_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:**    
Determine if the rshd service is installed. If so, this is a finding. The rshd is part of the bos.net.tcp.client fileset and is not removable.   
  
**Fix Text:**#chmod 000 /usr/sbin/rshd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22432  
**Group Title:** GEN003830  
**Rule ID:** SV-38876r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003830  
**Rule Title:**The rlogind service must not be running.  
  
**Vulnerability Discussion:**  The rlogind process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1  
  
**Check Content:**    
Determine if the rlogind service is running. If it is, this is a finding.  
# grep -v "^#" /etc/inetd.conf |grep rlogin  
If any results are returned, this is a finding  
  
  
  
**Fix Text:**Disable the rlogind service out of the ‘/etc/inetd.conf’ file.  
#vi /etc/inetd.conf   
Comment out the rlogind service. Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22433  
**Group Title:** GEN003835  
**Rule ID:** SV-38910r1\_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:**    
Determine if the rlogind service is installed. If so, this is a finding.   
  
The rlogind is part of the bos.net.tcp.client fileset and is not removable.   
  
**Fix Text:**#chmod 000 /usr/bin/rlogind   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4688  
**Group Title:** GEN003840  
**Rule ID:** SV-38878r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN003840  
**Rule Title:**The rexec daemon must not be running.  
  
**Vulnerability Discussion:**  The rexecd process provides a typically unencrypted, host-authenticated remote access service. SSH should be used in place of this service.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# grep -v "^#" /etc/inetd.conf |grep rexec  
  
If any results are returned, this is a finding.  
  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the line for the rexec service.   
Refresh the inetd daemon.  
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22434  
**Group Title:** GEN003845  
**Rule ID:** SV-38911r1\_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:**    
Determine if the rexecd service is installed. If it is, this is a finding.   
  
# ls -l `which rexecd`  
  
The rexecd is part of the bos.net.tcp.client fileset and is not removable.   
  
**Fix Text:**#chmod 000 /usr/sbin/rexecd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24386  
**Group Title:** GEN003850  
**Rule ID:** SV-38953r1\_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.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1  
  
**Check Content:**    
Consult vendor documentation to determine the method for determining if the telnet daemon is running. If the system uses inetd, use the following procedure:  
# grep -v '^#' /etc/inetd.conf | grep telnet  
If an entry is returned, the telnet daemon is running.  
  
If the telnet daemon is running, this is a finding.  
  
**Fix Text:**Edit the /etc/inetd.conf file and comment out the telnet line.  
  
Reload the inetd process.   
#refresh –s inetd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4701  
**Group Title:** GEN003860  
**Rule ID:** SV-27440r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN003860  
**Rule Title:**The system must not have the finger service active.  
  
**Vulnerability Discussion:**  The finger service provides information about the system's users to network clients. This information could expose information that could be used in subsequent attacks.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPP-1  
  
**Check Content:**    
# grep -v "^#" /etc/inetd.conf |grep finger  
If the finger service is not disabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the finger service line. Restart the inetd service.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12049  
**Group Title:** GEN003865  
**Rule ID:** SV-38880r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003865  
**Rule Title:**Network analysis tools must not be installed.  
  
**Vulnerability Discussion:**  Network analysis tools allow for the capture of network traffic visible to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCPA-1  
  
**Check Content:**    
Determine if any network analysis tools are installed.  
  
Procedure:  
# find / -name ethereal  
# find / -name wireshark  
# find / -name tshark  
# find / -name netcat  
# find / -name tcpdump  
# find / -name snoop  
  
If any network analysis tools are found, this is a finding.  
  
Additional Information: The binary tcpdump is provided in the bos.net.tcp.server fileset and this fileset can not be uninstalled.  
  
  
**Fix Text:**Remove the network analysis tool binary from the system.   
  
Procedure:  
# rm /usr/sbin/tcpdump   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-827  
**Group Title:** GEN003900  
**Rule ID:** SV-38883r1\_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:**    
Look for the presence of a print service configuration file.  
  
Procedure:  
# find /etc -name hosts.lpd -print  
# find /etc -name Systems -print   
# find /etc -name printers.conf  
  
If none of the files are found, this check should be marked not applicable.   
  
Otherwise, examine the configuration file.  
  
Procedure:  
# more <print service file>  
  
Check for entries containing a "+" character by itself on any line. If any are found, this is a finding.  
  
**Fix Text:**Remove the "+" entries from the hosts.lpd (or equivalent) file.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-828  
**Group Title:** GEN003920  
**Rule ID:** SV-828r6\_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:**    
Locate any print service configuration file on the system. Consult vendor documentation to verify the names and locations of print service configuration files on the system.  
  
Procedure:  
# find /etc -name hosts.lpd -print  
# find /etc -name Systems -print   
  
If no print service configuration file is found, this is not applicable.  
  
Check the ownership of the print service configuration file(s).  
  
Procedure:  
# ls –lL <print service file>  
  
If the owner of the file is not root, sys, bin, or lp, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/hosts.lpd file (or equivalent, such as /etc/lp/Systems) to root, lp, or another privileged UID. Consult vendor documentation to determine the name and location of print service configuration files.  
  
Procedure:  
# chown root /etc/hosts.lpd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22435  
**Group Title:** GEN003930  
**Rule ID:** SV-26675r1\_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/hosts.lpd file.  
  
Procedure:  
# ls -lL /etc/hosts.lpd  
  
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 hosts.lpd file.  
  
Procedure:  
# chgrp root /etc/hosts.lpd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-829  
**Group Title:** GEN003940  
**Rule ID:** SV-829r7\_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:**    
Locate any print service configuration file on the system. Consult vendor documentation for the name and location of print service configuration files.  
  
Procedure:  
# find /etc -name hosts.lpd -print  
# find /etc -name Systems -print   
  
If no print service configuration file is found, this is not applicable.  
  
Check the mode of the print service configuration file.  
  
Procedure:  
# ls -lL <print service file>  
  
If the mode of the print service configuration file is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/hosts.lpd file (or equivalent, such as /etc/lp/Systems) to 0644 or less permissive. Consult vendor documentation for the name and location of print service configuration files.  
  
Procedure:  
# chmod 0644 /etc/hosts.lpd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22436  
**Group Title:** GEN003950  
**Rule ID:** SV-38807r1\_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/hosts.lpd file.  
#aclget /etc/hosts.lpd   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the hosts.lpd file and disable extended permissions.  
  
#acledit /etc/hosts.lpd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4369  
**Group Title:** GEN003960  
**Rule ID:** SV-28393r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN003960  
**Rule Title:**The traceroute command owner must be root.  
  
**Vulnerability Discussion:**  If the traceroute command owner has not been set to root, an unauthorized user could use this command to obtain knowledge of the network topology inside the firewall. This information may allow an attacker to determine trusted routers and other network information possibly leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /usr/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 /usr/bin/traceroute   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4370  
**Group Title:** GEN003980  
**Rule ID:** SV-28397r1\_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 possibly leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the traceroute file.  
  
Procedure:  
# ls -lL /usr/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, sys, bin, or system.  
  
Procedure:  
# chgrp system /usr/bin/traceroute   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4371  
**Group Title:** GEN004000  
**Rule ID:** SV-28400r1\_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 possibly leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
# ls -lL /usr/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 /usr/bin/traceroute  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22437  
**Group Title:** GEN004010  
**Rule ID:** SV-38808r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004010  
**Rule Title:**The traceroute file must not have an extended ACL.  
  
**Vulnerability Discussion:**  If an extended ACL exists on the traceroute executable file, it may provide unauthorized users with access to the file. Malicious code could be inserted by an attacker and triggered whenever the traceroute command is executed by authorized users. Additionally, if an unauthorized user is granted executable permissions to the traceroute command, it could be used to gain information about the network topology behind the firewall. This information may allow an attacker to determine trusted routers and other network information possibly leading to system and network compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the /usr/sbin/traceroute file.  
#aclget /usr/sbin/traceroute   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the traceroute file and disable extended permissions.  
  
#acledit /usr/sbin/traceroute   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4382  
**Group Title:** GEN004220  
**Rule ID:** SV-4382r6\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN004220  
**Rule Title:**Administrative accounts must not run a web browser, except as needed for local service administration.  
  
**Vulnerability Discussion:**  If a web browser flaw is exploited while running as a privileged user, the entire system could be compromised.  
  
Specific exceptions for local service administration should be documented in site-defined policy. These exceptions may include HTTP(S)-based tools used for the administration of the local system, services, or attached devices. Examples of possible exceptions are HP’s System Management Homepage (SMH), the CUPS administrative interface, and Sun's StorageTek Common Array Manager (CAM) when these services are running on the local system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Look in the root account home directory for a .netscape or a .mozilla directory. If none exists, mark this check as not a finding. If there is one, verify with the root users and the IAO what the intent of the browsing is. Some evidence may be obtained by using the browser to view cached pages under the .netscape directory.  
  
**Fix Text:**Enforce policy requiring administrative accounts use web browsers only for local service administration.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-831  
**Group Title:** aliases ownership  
**Rule ID:** SV-831r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004360  
**Rule Title:**The alias file must be owned by root.  
  
**Vulnerability Discussion:**  If the alias file is not owned by root, an unauthorized user may modify the file to add aliases to run malicious code or redirect email.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the aliases file on the system.  
  
Procedure:  
# find / -name aliases –depth –print  
  
Check the ownership of the alias file.  
  
Procedure:  
# ls –lL <alias location>  
  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/mail/aliases file (or equivalent, such as /usr/lib/aliases) to root.  
  
Procedure:  
# chown root /etc/mail/aliases   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22438  
**Group Title:** GEN004370  
**Rule ID:** SV-26684r1\_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 to add aliases to run malicious code or redirect email.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the /etc/mail/aliases file.  
  
Procedure:  
# ls -lL /etc/mail/aliases  
  
If the file is not group-owned by root, sys, bin, or system, this is a finding.  
  
**Fix Text:**Change the group-owner of the /etc/mail/aliases file.  
  
Procedure:  
# chgrp root /etc/mail/aliases   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-832  
**Group Title:** aliases permissions  
**Rule ID:** SV-832r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004380  
**Rule Title:**The alias file must have mode 0644 or less permissive.  
  
**Vulnerability Discussion:**  Excessive permissions on the aliases file may permit unauthorized modification. If the alias file is modified by an unauthorized user, they may modify the file to run malicious code or redirect email.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the aliases file on the system.  
Procedure:  
# find / -name aliases -depth -print  
  
Check the mode of the alias file.  
Procedure:  
# ls –lL <alias location>  
  
If the alias file has a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the /etc/mail/aliases file (or equivalent, such as /usr/lib/aliases) to 0644.   
  
Procedure:  
# chmod 0644 /etc/aliases   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22439  
**Group Title:** GEN004390  
**Rule ID:** SV-38809r1\_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 /etc/mail/aliases file.  
  
#aclget /etc/mail/aliases   
  
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the alias file and disable extended permissions.  
  
#acledit /etc/mail/aliases   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-833  
**Group Title:** File Executed Through Aliases Accessibility  
**Rule ID:** SV-39506r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN004400  
**Rule Title:**Files executed through a mail aliases file must be owned by root and must reside within a directory owned and writable only by root.  
  
**Vulnerability Discussion:**  If a file executed through a mail aliases file is not owned and writable only by root, it may be subject to unauthorized modification. Unauthorized modification of files executed through aliases may allow unauthorized users to attain root privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the aliases file on the system.  
  
Procedure:  
# find / -name aliases –depth –print  
# more < aliases file location >  
  
Examine the aliases file for any directories or paths that may be utilized.  
  
Procedure:  
# ls –lL < path >  
  
Check if the file or parent directory is owned by root. If not, this is a finding.  
  
**Fix Text:**Edit the /etc/mail/aliases file (alternatively, /usr/lib/sendmail.cf). Locate the entries that execute a program. They will appear similar to the following line:  
  
Aliasname: : /usr/local/bin/ls (or some other program name)  
  
Ensure root owns the programs and the directory(ies) they reside in by using the chown command to change owner to root.  
Procedure:  
# chown root filename   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22440  
**Group Title:** GEN004410  
**Rule ID:** SV-26689r1\_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/mail/aliases file.  
For each file referenced, check the group ownership of the file.  
  
Procedure:  
# ls -lL <file referenced from aliases>  
  
If the group owner of any file is not root, bin, sys, or system, this is a finding.  
  
**Fix Text:**Change the group ownership of the file referenced from /etc/mail/aliases.  
  
Procedure:  
# chgrp root <file referenced from aliases>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-834  
**Group Title:** File Executed Through Aliases Permissions  
**Rule ID:** SV-834r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004420  
**Rule Title:**Files executed through a mail aliases file must have mode 0755 or less permissive.  
  
**Vulnerability Discussion:**  If a file executed through a mail alias file has permissions greater than 0755, it can be modified by an unauthorized user and may contain malicious code or instructions possibly compromising the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Find the aliases file on the system.  
Procedure:  
# find / -name aliases -depth -print  
  
Examine the aliases file for any directories or paths that may be utilized.  
Procedure:  
# more <aliases file location>  
  
Check the permissions for any paths referenced.  
Procedure:  
# ls -lL <path>  
  
If any file referenced from the aliases file has a mode more permissive than 0755, this is a finding.  
  
  
**Fix Text:**Use the chmod command to change the access permissions for files executed from the alias file.  
For example:  
  
# chmod 0755 < filename >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22441  
**Group Title:** GEN004430  
**Rule ID:** SV-38810r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004430  
**Rule Title:**Files executed through a mail aliases file must not have extended ACLs.  
  
**Vulnerability Discussion:**  Excessive permissions on files executed through a mail alias file could result in modification by an unauthorized user, execution of malicious code, and/or system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Examine the contents of the /etc/mail/aliases file.  
For each file referenced, check the permissions of the file.  
  
  
#aclget [File references from alias]   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the file(s) referenced from the aliases file and disable extended permissions.  
  
#acledit [File referenced from aliases]   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-835  
**Group Title:** GEN004440  
**Rule ID:** SV-38916r1\_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:  
# grep “O L” /etc/mail/sendmail.cf  
  
OR  
  
# grep LogLevel /etc/mail/sendmail.cf  
  
If logging is set to less than 9, this is a finding.  
  
**Fix Text:**Edit the sendmail.conf file, locate the "O L" or LogLevel entry and change it to 9.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-836  
**Group Title:** Critical Level Sendmail Messages Logging  
**Rule ID:** SV-39155r1\_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:**  ECSC-1  
  
**Check Content:**    
Check the syslog configuration file for mail.crit logging configuration. The syslog.conf file critical mail logging option line will typically appear as one of the following examples: mail.crit /var/log/syslog \*.crit /var/log/syslog mail.\* /var/log/syslog.  
  
Procedure:   
# more /etc/syslog.conf   
  
If syslog is not configured to log critical Sendmail messages, this is a finding.   
  
**Fix Text:**Edit the syslog.conf file and add a configuration line specifying an appropriate destination for mail.crit syslogs.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-837  
**Group Title:** Critical Sendmail Log File Ownership  
**Rule ID:** SV-837r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004480  
**Rule Title:**The SMTP service log file must be owned by root.  
  
**Vulnerability Discussion:**  If the SMTP service log file is not owned by root, then unauthorized personnel may modify or delete the file to hide a system compromise.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Locate any mail log files by checking the syslog configuration file.  
  
Procedure:  
# more /etc/syslog.conf  
  
Identify any log files configured for the "mail" service at any severity level, or those configured for all services. Check the ownership of these log files.  
  
Procedure:  
# ls -lL <file location>  
  
If any mail log file is not owned by root, this is a finding.  
  
**Fix Text:**Change the ownership of the Sendmail log file.  
# chown root <sendmail log file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-838  
**Group Title:** Critical Sendmail Log File Permissions  
**Rule ID:** SV-838r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004500  
**Rule Title:**The SMTP service log file must have mode 0644 or less permissive.  
  
**Vulnerability Discussion:**  If the SMTP service log file is more permissive than 0644, unauthorized users may be allowed to change the log file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the mode of the SMTP service log file.  
  
Procedure:  
# more /etc/syslog.conf  
  
Check the configuration to determine which log files contain logs for mail.crit, mail.debug, or \*.crit.  
  
Procedure:  
# ls -lL <file location>  
  
If the log file permissions are greater than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the SMTP service log file.  
  
Procedure:  
# chmod 0644 <sendmail log file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22442  
**Group Title:** GEN004510  
**Rule ID:** SV-38811r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004510  
**Rule Title:**The SMTP service log file must not have an extended ACL.  
  
**Vulnerability Discussion:**  If the SMTP service log file has an extended ACL, unauthorized users may be allowed to access or to modify the log file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Examine /etc/syslog.conf and determine the log file(s) receiving logs for mail.crit, mail.debug, mail.\*, or \*.crit.  
Check the permissions on these log files.  
#aclget [log file]   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the SMTP service log file and disable extended permissions.  
  
#acledit [ log file ]   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12006  
**Group Title:** GEN004540  
**Rule ID:** SV-38885r1\_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 to see if help is disabled in Sendmail.  
  
Procedure:  
# telnet <host> 25  
help  
  
If the help command returns any Sendmail version information, this is a finding.  
  
**Fix Text:**To disable the SMTP HELP command create an empty Sendmail help file.  
  
# > /etc/mail/help   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4384  
**Group Title:** GEN004560  
**Rule ID:** SV-39164r1\_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:**    
Check for the Sendmail version being displayed in the greeting:   
# telnet localhost 25   
If a version number is displayed, this is a finding.   
  
**Fix Text:**Ensure Sendmail or its equivalent has been configured to mask the version information. If necessary, change the O SmtpGreetingMessage line in the /etc/sendmail.cf file.  
  
O SmtpGreetingMessage=$j Sendmail $v/$Z; $b  
  
Change it to:   
  
O SmtpGreetingMessage= Mail Server Ready ; $b   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4385  
**Group Title:** .forward files  
**Rule ID:** SV-4385r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004580  
**Rule Title:**The system must not use .forward files.  
  
**Vulnerability Discussion:**  The .forward file allows users to automatically forward mail to another system. Use of .forward files could allow the unauthorized forwarding of mail and could potentially create mail loops which could degrade system performance.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Search for any .forward files on the system.  
  
# find / -name .forward -print  
  
This is considered a finding if any .forward files are found on the system.  
  
**Fix Text:**Remove .forward files from the system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4689  
**Group Title:** GEN004600  
**Rule ID:** SV-38917r1\_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.  
  
Locate the sendmail daemon.  
Procedure:  
# find / -name sendmail   
  
Obtain version information for the Sendmail daemon.  
Procedure:  
# what <file location>   
OR  
# strings <file location> | grep version   
  
Version 8.14.5 is the latest released version.  
  
If the Sendmail version is not at least 8.14.5 or the vendor's latest version, this is a finding.  
  
**Fix Text:**Obtain and install a newer version of Sendmail from the operating system vendor or from http://www.sendmail.org or ftp://ftp.cs.berkeley.edu/ucb/sendmail.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4690  
**Group Title:** GEN004620  
**Rule ID:** SV-4690r6\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN004620  
**Rule Title:**The Sendmail server must have the debug feature disabled.  
  
**Vulnerability Discussion:**  Debug mode is a feature present in older versions of Sendmail which, if not disabled, may allow an attacker to gain access to a system through the Sendmail service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for an enabled "debug" command provided by the SMTP service.  
  
Procedure:  
# telnet localhost 25  
debug  
  
If the command does not return a 500 error code of command unrecognized, this is a finding.  
  
**Fix Text:**Obtain and install a more recent version of Sendmail, which does not implement the DEBUG feature.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4691  
**Group Title:** GEN004640  
**Rule ID:** SV-4691r6\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN004640  
**Rule Title:**The SMTP service must not have a uudecode alias active.  
  
**Vulnerability Discussion:**  A common configuration for older Mail Transfer Agents (MTAs) includes an alias for the decode user. All mail sent to this user is sent to the uudecode program, which automatically converts and stores files. By sending mail to the decode or the uudecode aliases that are 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 newaliases 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   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4692  
**Group Title:** GEN004660  
**Rule ID:** SV-28402r1\_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:**    
Perform the following to determine if EXPN is disabled:  
  
# telnet localhost 25  
expn root  
  
If the command does not return a 500 error code of command unrecognized, this is a finding.  
  
OR  
  
Locate the sendmail.cf configuration file by:  
  
# find / -name sendmail.cf -print  
# grep -v "^#" <sendmail.cf location> |grep -i privacyoptions  
  
The O PrivacyOptions should have the noexpn or the goaway option (covering both noexpn and novrfy).  
If the EXPN command is not disabled, this is a finding.  
  
**Fix Text:**Edit the sendmail.cf file and add or edit the following line:  
O PrivacyOptions=goaway  
Restart the Sendmail service.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4693  
**Group Title:** GEN004680  
**Rule ID:** SV-39171r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004680  
**Rule Title:**The SMTP service must not have the VRFY feature active.  
  
**Vulnerability Discussion:**  The VRFY (Verify) command allows an attacker to determine if an account exists on a system, providing significant assistance to a brute force attack on user accounts. VRFY may provide additional information about users on the system, such as the full names of account owners.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if VRFY is disabled.   
Procedure: # telnet localhost 25   
vrfy root  
If the command does not return a 500 error code of command unrecognized, this is a finding.  
  
OR  
  
Locate the sendmail.cf configuration file.   
Procedure:  
# find / -name sendmail.cf –print # grep –v “^#” |grep –i vrfy   
  
Ensure 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:**If you are running Sendmail, add the line Opnovrfy to your Sendmail configuration file, usually located in /etc/sendmail.cf. For other mail servers, contact the vendor for information on how to disable the verify command. Newer versions of Sendmail are available at http://www.sendmail.org or from ftp://ftp.cs.berkeley.edu/ucb/sendmail.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4694  
**Group Title:** GEN004700  
**Rule ID:** SV-4694r7\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN004700  
**Rule Title:**The Sendmail service must not have the wizard backdoor active.  
  
**Vulnerability Discussion:**  Very old installations of the Sendmail mailing system contained a feature whereby a remote user connecting to the SMTP port can enter the WIZ command and be given an interactive shell with root privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Locate the sendmail.cf configuration file and check for wiz configuration.  
  
Procedure:  
# find / -name sendmail.cf –print  
# grep -v “^#” <sendmail.cf location> |grep -i wiz  
  
If an entry is found for wiz, this is a finding.  
  
**Fix Text:**If the WIZ command is enabled on Sendmail, it should be disabled by adding this line to the sendmail.cf configuration file (it must be typed in uppercase):  
  
OW\*  
  
For the change to take effect, kill the Sendmail process, refreeze the sendmail.cf file, and restart the Sendmail process.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23952  
**Group Title:** GEN004710  
**Rule ID:** SV-38919r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004710  
**Rule Title:**Mail relaying must be restricted.  
  
**Vulnerability Discussion:**  If unrestricted mail relaying is permitted, unauthorized senders could use this host as a mail relay for the purpose of sending SPAM or other unauthorized activity.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system uses Sendmail, locate the sendmail.cf file.  
Procedure:  
# find / -name sendmail.cf  
  
Determine if Sendmail only binds to loopback addresses by examining the DaemonPortOptions configuration options.  
Procedure:  
# grep -i “O DaemonPortOptions” /etc/mail/sendmai.cf  
  
If there are uncommented DaemonPortOptions lines, and all such lines specify system loopback addresses, this is not a finding.  
  
Otherwise, determine if Sendmail is configured to allow open relay operation.  
Procedure:  
# find / -name sendmail.mc  
# grep -i promiscuous\_relay </path/to/sendmail.mc>  
  
If the promiscuous relay feature is enabled, this is a finding.  
  
If the system uses Postfix, locate the main.cf file.  
Procedure:  
# find / -name main.cf  
  
Determine if Postfix only binds to loopback addresses by examining the inet\_interfaces line.  
Procedure:  
# grep inet\_interfaces </path/to/main.cf>  
  
If inet\_interfaces is set to loopback-only or contains only loopback addresses such as 127.0.0.1 and [::1], Postfix is not listening on external network interfaces, 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 that 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12010  
**Group Title:** GEN004800  
**Rule ID:** SV-39176r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004800  
**Rule Title:**Unencrypted FTP must not be used on the system.  
  
**Vulnerability Discussion:**  FTP is typically unencrypted and, therefore, presents confidentiality and integrity risks. FTP may be protected by encryption in certain cases, such as when used in a Kerberos environment. SFTP and FTPS are encrypted alternatives to FTP.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if unencrypted ftp or telnet are enabled.  
  
Procedure:  
# grep ftp /etc/inetd.conf   
# grep telnet /etc/inetd.conf  
  
If either of these services are found, and are active, ask the SA if both of these services are encrypted. If they are not, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out or remove the ftp and telnet service lines.   
  
# vi /etc/inetd.conf  
  
Restart the inetd service.  
  
# refresh -s inetd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-846  
**Group Title:** Anonymous FTP  
**Rule ID:** SV-846r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004820  
**Rule Title:**Anonymous FTP must not be active on the system unless authorized.  
  
**Vulnerability Discussion:**  Due to the numerous vulnerabilities inherent in anonymous FTP, it is recommended that it not be used. If anonymous FTP must be used on a system, the requirement must be authorized and approved in the system accreditation package.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Attempt to log into this host with a user name of anonymous and a password of guest (also try the password of guest@mail.com). If the logon is successful, this is a finding.  
  
Procedure:  
# ftp localhost  
Name: anonymous  
530 Guest login not allowed on this machine.  
  
  
**Fix Text:**Configure the FTP service to not permit anonymous logins.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4702  
**Group Title:** Anonymous FTP Segregation into DMZ  
**Rule ID:** SV-4702r6\_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:**  ECSC-1  
  
**Check Content:**    
Use the command ftp to connect the system's FTP service. Attempt to log into this host with a user name of anonymous and a password of guest (also try the password of guest@mail.com). If the logon is not successful, this check is not applicable.  
  
Ask the SA if the system is located on a DMZ network. If the system is not located on a DMZ network, this is a finding.  
  
**Fix Text:**Move the system to a DMZ network.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-840  
**Group Title:** GEN004880  
**Rule ID:** SV-28403r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004880  
**Rule Title:**The ftpusers file must exist.  
  
**Vulnerability Discussion:**  The ftpusers file contains a list of accounts not allowed to use FTP to transfer files. If this file does not exist, then unauthorized accounts can utilize FTP.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check for the existence of the ftpusers file.  
# ls -l /etc/ftpusers  
If the ftpusers file does not exist, this is a finding.  
  
**Fix Text:**Create a /etc/ftpusers file containing a list of accounts not authorized for FTP.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-841  
**Group Title:** GEN004900  
**Rule ID:** SV-28406r1\_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. If the system has accounts not allowed to use FTP and are not listed in the ftpusers file, this is a finding.  
# more /etc/ftpusers  
  
**Fix Text:**Add accounts not allowed to use FTP to the /etc/ftpusers file.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-842  
**Group Title:** GEN004920  
**Rule ID:** SV-28409r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004920  
**Rule Title:**The ftpusers file must be owned by root.  
  
**Vulnerability Discussion:**  If the file ftpusers is not owned by root, an unauthorized user may modify the file to allow unauthorized accounts to use FTP.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the ftpusers file.  
# ls -l /etc/ftpusers  
If the ftpusers file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the ftpusers file to root.  
# chown root /etc/ftpusers   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22444  
**Group Title:** GEN004930  
**Rule ID:** SV-39180r1\_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   
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 system /etc/ftpusers   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-843  
**Group Title:** GEN004940  
**Rule ID:** SV-28412r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN004940  
**Rule Title:**The ftpusers file must have mode 0640 or less permissive.  
  
**Vulnerability Discussion:**  Excessive permissions on the ftpusers file could permit unauthorized modification. Unauthorized modification could result in Denial of Service to authorized FTP users or permit unauthorized users to access the FTP service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the ftpusers file.  
# ls -l /etc/ftpusers  
If the ftpusers file has a mode more permissive than 0640, this is a finding.  
  
**Fix Text:**Change the mode of the ftpusers file to 0640.  
# chmod 0640 /etc/ftpusers   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22445  
**Group Title:** GEN004950  
**Rule ID:** SV-38812r1\_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.  
#aclget /etc/ftpusers   
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the ftpusers file and disable extended permissions.   
  
#acledit /etc/ftpusers   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-845  
**Group Title:** FTP Daemon Logging  
**Rule ID:** SV-38991r1\_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 logging of connections. 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:**    
Perform:  
  
# grep ftpd /etc/inetd.conf,   
  
Check the line for ftpd to check if the –l argument. If the ftpd is invoked without the -l argument, this is a finding.  
  
Check the /etc/syslog.conf file for daemon.info or \*.info.   
# more /etc/syslog.conf  
If daemon.info or \*.info is not being logged, this is a finding.  
  
**Fix Text:**Edit the /etc/inetd.conf file and add the -l argument to the ftpd service line.  
  
# vi /etc/inetd.conf  
  
Restart inetd.conf  
  
# refresh -s inetd  
  
Add daemon.info or \*.info to the /etc/syslog.conf file.  
  
#vi /etc/syslog.conf  
\*.info /var/log/syslog  
  
Restart the syslog daemon.  
  
# refresh -s syslogd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4387  
**Group Title:** Anonymous FTP Account Shell  
**Rule ID:** SV-4387r8\_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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4388  
**Group Title:** Anonymous FTP Configuration  
**Rule ID:** SV-38887r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005020  
**Rule Title:**The anonymous FTP account must be configured to use chroot or a similarly isolated environment.  
  
**Vulnerability Discussion:**  If an anonymous FTP account does not use a chroot or similarly isolated environment, the system may be more vulnerable to exploits against the FTP service. Such exploits could allow an attacker to gain shell access to the system and view, edit, or remove sensitive files.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Consult vendor documentation for the anonymous FTP service to determine the necessary configuration for operating the service in a chroot environment. If the system is not configured to operate the anonymous FTP service in a chroot environment, this is a finding.  
  
**Fix Text:**Configure the anonymous FTP service to operate in a chroot environment.   
  
Consult the following resources for setting up anonymous ftp.  
  
# more /usr/samples/tcpip/anon.users.ftp  
  
Web link:  
http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/HT\_security\_anonymous\_ftp.htm   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12011  
**Group Title:** FTP User’s umask  
**Rule ID:** SV-38813r1\_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 the "ftp" user.  
  
Procedure:  
lsuser –a umask ftp  
  
If the umask value does not return 077 or 77, this is a finding.  
  
Check the default umask that the ftpd daemon is running with  
#grep ftpd /etc/inetd.conf  
If there is not a -u077 argument on the ftpd, this is a finding.  
  
**Fix Text:**Add the arguments –u077 to the ftpd on the /etc/inetd.conf and refresh inetd.  
#vi /etc/inetd.conf  
#refresh –s inetd  
  
Change the umask of the ftp user.  
#chuser umask=077 ftp   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12013  
**Group Title:** FSP Is Enabled  
**Rule ID:** SV-28415r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005060  
**Rule Title:**The system must not have an FSP service enabled.  
  
**Vulnerability Discussion:**  FSP is a UDP-based file transfer protocol that, in the past, was commonly used for file sharing.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# grep -v "^#" /etc/inetd.conf |grep in.fspd  
If any results are returned, this is a finding.  
  
Determine if the fspd process is running.  
# ps -ef | grep fspd  
If the process is running, this is a finding.  
  
  
**Fix Text:**Edit /etc/inetd.conf and comment out or remove any lines referencing in.fspd.  
Kill any running fspd processes and disable any fspd startup scripts.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-847  
**Group Title:** GEN005080  
**Rule ID:** SV-28420r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005080  
**Rule Title:**The TFTP daemon must operate in "secure mode" which provides access only to a single directory on the host file system.  
  
**Vulnerability Discussion:**  Secure mode limits TFTP requests to a specific directory. If TFTP is not running in secure mode, it may be able to write to any file or directory and may seriously impair system integrity, confidentiality, and availability.  
  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if tftpd is running in secure mode.  
# more /etc/tftpaccess.ctl  
If the file does not exist, this is a finding. If the file does not contain an entry restricting access to the tftp user home directory, this is a finding. If other configuration is in the file, this is a finding.  
  
**Fix Text:**Edit /etc/tftpaccess.ctl to only contain an entry restricting access to the tftp user home directory.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-848  
**Group Title:** GEN005100  
**Rule ID:** SV-848r7\_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:  
# find / -name "\*tftpd" -print   
# ls -lL <file location>   
  
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 <tftp server>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-849  
**Group Title:** GEN005120  
**Rule ID:** SV-849r7\_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 that someone could logon 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:  
# grep tftp /etc/passwd  
  
If a tftp user account does not exist and TFTP is active, this is a finding.  
  
Check the user shell for the tftp user. If it is not /bin/false or equivalent, this is a finding.  
  
Check the home directory assigned to the tftp user. If no home directory is set, or the directory specified is not dedicated to the use of the TFTP service, this is a finding.  
  
  
**Fix Text:**Create a "tftp" user account if none exists.  
Assign a non-login shell to the "tftp" user account, such as /bin/false.  
Assign a home directory to the "tftp" user account.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4695  
**Group Title:** GEN005140  
**Rule ID:** SV-39193r1\_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.  
# grep -v "^#" /etc/inetd.conf |grep tftp  
If TFTP is found enabled, it is a finding if it is not documented using site-defined procedures.  
  
**Fix Text:**Disable the TFTP daemon.  
Edit /etc/inetd.conf and comment out the tftp line.   
  
Restart the inetd service.  
# refresh -s inetd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-850  
**Group Title:** .Xauthority Files  
**Rule ID:** SV-850r7\_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 that specific X Windows host. If .Xauthority files are not used, it may be possible to obtain unauthorized access to the X Windows host.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Check for .Xauthority files being utilized by looking for such files in the home directory of a user that uses X.  
  
Procedure:  
# cd ~someuser  
# ls –la .Xauthority  
  
If the .Xauthority file does not exist, ask the SA if the user is using X Windows. If the user is utilizing X Windows and the .Xauthority file does not exist, this is a finding.  
  
**Fix Text:**Ensure the X Windows host is configured to write .Xauthority files into user home directories. Edit the Xaccess file. Ensure the line that writes the .Xauthority file is uncommented.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12014  
**Group Title:** .Xauthority File Permissions  
**Rule ID:** SV-12515r5\_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 that 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 -lL .Xauthority  
  
If the file mode is more permissive than 0600, this is finding.  
  
  
**Fix Text:**Change the mode of the .Xauthority files.  
  
Procedure:  
# chmod 0600 .Xauthority   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22446  
**Group Title:** GEN005190  
**Rule ID:** SV-38814r1\_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 that 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:**    
Get a list of (non-system account) users and the associated home directories.   
# cat /etc/passwd | cut -f 1,6 -d ":"   
Check the file permissions for the user .Xauthority files.  
  
#aclget .Xauthority  
Check if extended permissions are disabled. If extended permissions are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the .Xauthority file(s) and disable extended permissions.  
  
#acledit .Xauthority   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4697  
**Group Title:** GEN005200  
**Rule ID:** SV-4697r6\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005200  
**Rule Title:**X displays must not be exported to the world.  
  
**Vulnerability Discussion:**  Open X displays allow an attacker to capture keystrokes and to execute commands remotely. Many users have their X Server set to xhost +, permitting access to the X Server by anyone, from anywhere.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If X Windows is not used on the system, this is not applicable.  
  
Check the output of the "xhost" command from an X terminal.  
  
Procedure:  
$ xhost  
If the output reports access control is enabled (and possibly lists the hosts that can receive X window logins), this is not a finding. If the xhost command returns a line indicating access control is disabled, this is a finding.  
  
NOTE: It may be necessary to define the display if the command reports it cannot open the display.   
  
Procedure:  
$ DISPLAY=MachineName:0.0; export DISPLAY  
MachineName may be replaced with an Internet Protocol Address. Repeat the check procedure after setting the display.  
  
  
**Fix Text:**If using an xhost-type authentication the "xhost -" command can be used to remove current trusted hosts and then selectively allow only trusted hosts to connect with "xhost +" commands. A cryptographically secure authentication, such as provided by the xauth program, is always preferred. Refer to your X11 server's documentation for further security information.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12016  
**Group Title:** GEN005220  
**Rule ID:** SV-12517r4\_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, the user's X session may be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2  
  
**Check Content:**    
Determine if the X server is running.  
Procedure:  
# ps –ef |grep X  
  
Determine if xauth is being used.  
Procedure:  
# xauth  
xauth> list  
  
If the above command sequence does not show any host other than the localhost, then xauth is not being used.  
  
Search the system for an X\*.hosts files, where \* is a display number that may be used to limit X window connections. If no files are found, X\*.hosts files are not being used. If the X\*.hosts files contain any unauthorized hosts, this is a finding.  
  
If both xauth and X\*.hosts files are not being used, this is a finding.  
  
**Fix Text:**Create an X\*.hosts file, where \* is a display number that may be used to limit X window connections. Add the list of authorized X clients to the file.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12017  
**Group Title:** GEN005240  
**Rule ID:** SV-12518r4\_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, the 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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12018  
**Group Title:** GEN005260  
**Rule ID:** SV-38954r1\_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, the user's X session may be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the X Window system is running.  
  
Procedure:  
# ps –ef |grep X  
  
Ask the SA if the X Window system is an operational requirement. If it is not, this is a finding.  
  
**Fix Text:**Disable the X Windows server on the system.   
Comment out /etc/rc.dt out of /etc/inittab  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4696  
**Group Title:** Disable UUCP  
**Rule ID:** SV-28427r1\_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:**    
# grep uucp /etc/inetd.conf  
If uucp is found enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the uucp service. Restart the inetd service.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-993  
**Group Title:** Changed SNMP Community Strings  
**Rule ID:** SV-38889r1\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN005300  
**Rule Title:**SNMP communities, users, and passphrases must be changed from the default.  
  
**Vulnerability Discussion:**  Whether active or not, default SNMP passwords, users, and passphrases must be changed to maintain security. If the service is running with the default authenticators, then anyone can gather data about the system and the network and use the information to potentially compromise the integrity of the system or network(s).  
  
**Responsibility:**  System Administrator  
**IAControls:**  IAAC-1  
  
**Check Content:**    
Check the SNMP configuration for default passwords.  
  
Locate and examine the SNMP configuration.  
Procedure:  
# find / -name "snmp\*.conf" –print  
# more <snmpd.conf>   
  
Identify any community names or user password configuration. If any community name or password is set to a default value such as public, private, snmp-trap, 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 /etc/snmpd.conf or the file /etc/snmpd3.conf. Edit the file. Locate the line system-group-read-community which has a default password of public and make the password something more random (less guessable). Do the same for the lines that read system-group-write-community, read-community, write-community, trap, and trap-community. Read the information in the file carefully. The trap is defining who to send traps to, for instance, by default. It is not a password, but the name of a host.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22447  
**Group Title:** GEN005305  
**Rule ID:** SV-38816r1\_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:**    
Determine if the system's SNMP service only uses SNMPv3 or its successors. Consult vendor documentation to determine if earlier versions of SNMP are supported and what configuration is necessary to enable or disable the protocols. Snmpd version 1 was the only version available in AIX versions prior to AIX 5.2.  
  
#which snmpd  
#ls –l <path to snmpd>  
If the results are not /usr/sbin/snmpdv3e or /usr/sbin/snpdv3ne this is an earlier version of the protocol used by the service, this is a finding.  
  
**Fix Text:**Configure the system's SNMP service to only use SNMPv3 with encryption or its successors. The snmp version supporting encryption is an installable fileset on the expansion cd as fileset ‘snmp.crypto’.  
  
To enable snmpv3 with encryption:  
  
#snmpv3\_ssw -e   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22448  
**Group Title:** GEN005306  
**Rule ID:** SV-38890r1\_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:**    
NOTE: This will virtually always require a manual review. Determine if the SNMP service uses a FIPS 140-2 approved cryptographic hash algorithm as part of its authentication and integrity methods. The NIST CVMP web site provides a list of validated modules and the required security policies for the compliant use of such modules. Verify the module is on the NIST list and configured in accordance with the validated security policy. If it does not, this is a finding.  
  
**Fix Text:**Configure the SNMP service to use a FIPS 140-2 approved cryptographic hash algorithm as part of its authentication and integrity methods.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22449  
**Group Title:** GEN005307  
**Rule ID:** SV-38891r1\_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:**    
NOTE: This will virtually always require a manual review. Determine if the SNMP service uses a FIPS 140-2 approved cryptographic hash algorithm as part of its authentication and integrity methods. The NIST CVMP web site provides a list of validated modules and the required security policies for the compliant use of such modules. Verify the module is on the NIST list and configured in accordance with the validated security policy. If it does not, this is a finding.  
  
**Fix Text:**Configure the SNMP service to use a FIPS 140-2 approved encryption algorithm for protecting the privacy of SNMP messages.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-994  
**Group Title:** GEN005320  
**Rule ID:** SV-38817r1\_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.  
  
Locate the SNMP daemon configuration file. Consult vendor documentation to verify the name and location of the file.  
Procedure:  
# find / -name “snmpd\*.conf”  
  
Check the mode of the SNMP daemon configuration file.  
Procedure:  
# ls -lL <snmpd conf>  
  
  
**Fix Text:**Change the mode of the SNMP daemon configuration file to 0600.   
  
Procedure:  
# chmod 0600 /etc/snmpd.conf  
# chmod 0600 /etc/snmpdv3.conf  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-995  
**Group Title:** GEN005340  
**Rule ID:** SV-995r7\_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 -print  
# ls -lL <mib file>  
  
If any file is returned that does not have mode 0640 or less permissive, this is a finding.  
  
  
**Fix Text:**Change the mode of MIB files to 0640.  
  
Procedure:  
# chmod 0640 <mib file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22450  
**Group Title:** GEN005350  
**Rule ID:** SV-38818r1\_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 -print  
# aclget [mib file]  
If the extended attributes are not disabled, this is a finding  
  
  
**Fix Text:**Remove the extended ACL from the MIB file(s) and change extended attributes to disabled.  
  
#acledit [mib file]   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12019  
**Group Title:** GEN005360  
**Rule ID:** SV-38920r1\_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. Consult vendor documentation to determine the location and name of the file.   
  
Procedure:  
# 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>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22451  
**Group Title:** GEN005365  
**Rule ID:** SV-38921r1\_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:**    
Determine the group owner of the snmpd.conf file (or equivalent).  
  
Procedure:  
# 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 owner of the snmpd.conf file (or equivalent).   
Procedure:  
# chgrp system /etc/snmpd.conf  
# chgrp system /etc/snmpdv3.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22452  
**Group Title:** GEN005375  
**Rule ID:** SV-38819r1\_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:**    
Determine if the snmpd.conf file or equivalent has an extended ACL.  
  
Procedure:  
  
# find / -name “snmpd\*.conf”  
# aclget < snmpd conf >  
If the extended attributes are not disabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the snmpd.conf file (or equivalent) and change extended attributes to disabled.  
  
#acledit < snmpd conf >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4392  
**Group Title:** Dedicated Hardware for SNMP  
**Rule ID:** SV-4392r6\_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 that has been 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22453  
**Group Title:** GEN005390  
**Rule ID:** SV-26740r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005390  
**Rule Title:**The /etc/syslog.conf file must have mode 0640 or less permissive.  
  
**Vulnerability Discussion:**  Unauthorized users must not be allowed to access or modify the /etc/syslog.conf file.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the syslog configuration file.  
# ls -lL /etc/syslog.conf  
If the mode of the file is more permissive than 0640, this is a finding.  
  
**Fix Text:**Change the permissions of the syslog configuration file.  
# chmod 0640 /etc/syslog.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22454  
**Group Title:** GEN005395  
**Rule ID:** SV-38820r1\_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.  
# aclget /etc/syslog.conf  
If the extended attributes are not disabled, this is a finding  
  
  
**Fix Text:**Remove the extended ACL from the syslog.conf file and change extended attributes to disabled.  
  
#acledit /etc/syslog.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4393  
**Group Title:** /etc/syslog.conf accessibility  
**Rule ID:** SV-4393r8\_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   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4394  
**Group Title:** /etc/syslog.conf group ownership  
**Rule ID:** SV-4394r6\_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:**Change the group-owner of the /etc/syslog.conf file to root, bin, sys, or system.  
  
Procedure:  
# chgrp root /etc/syslog.conf   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12020  
**Group Title:** GEN005440  
**Rule ID:** SV-39205r1\_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 and may contain sensitive information and are, therefore, restricted to the enclave.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
NOTE: This will virtually always require a manual review. 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22455  
**Group Title:** GEN005450  
**Rule ID:** SV-26745r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005450  
**Rule Title:**The system must use a remote syslog server (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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4395  
**Group Title:** GEN005460  
**Rule ID:** SV-4395r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005460  
**Rule Title:**The system must only use remote syslog servers (log hosts) justified and documented using site-defined procedures.  
  
**Vulnerability Discussion:**  If a remote log host is in use and it has not been justified and documented with the IAO, sensitive information could be obtained by unauthorized users without the SA's knowledge. A remote log host is any host to which the system is sending syslog messages over a network.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Examine the syslog.conf file for any references to remote log hosts.  
# grep -v "^#" /etc/syslog.conf | grep '@'  
Destination locations beginning with an '@' represent log hosts. If the log host name is a local alias such as "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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12021  
**Group Title:** GEN005480  
**Rule ID:** SV-38894r1\_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 that accepts 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:**    
#ps -ef | grep syslogd | grep -v grep  
  
If the -R option is not present, this is a finding.  
  
**Fix Text:**Change the syslogd arguments in the src subsystem control and restart the syslogd daemon.  
#chssys –s syslogd –a ‘-R’  
#stopsrc –s syslogd  
#startsrc –s syslogd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23826  
**Group Title:** GEN005490  
**Rule ID:** SV-38895r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005490  
**Rule Title:**The SSH daemon must use a FIPS 140-2 validated cryptographic module (operating in FIPS mode).  
  
**Vulnerability Discussion:**  Cryptographic modules used by the system must be validated by the NIST CVMP as compliant with FIPS 140-2. Cryptography performed by unvalidated modules is viewed by NIST as providing no protection for the data.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
NOTE: This will virtually always require a manual review. Determine if the SSH daemon uses a FIPS 140-2 validated cryptographic module (operating in FIPS mode). The NIST CVMP web site provides a list of validated modules and the required security policies for the compliant use of such modules. Verify the module is on the NIST list and configured in accordance with the validated security policy. If it does not, this is a finding.  
  
**Fix Text:**Configure the SSH daemon to use a FIPS 140-2 validated cryptographic module (operating in FIPS mode).   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23827  
**Group Title:** GEN005495  
**Rule ID:** SV-38896r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005495  
**Rule Title:**The SSH client must use a FIPS 140-2 validated cryptographic module (operating in FIPS mode).  
  
**Vulnerability Discussion:**  Cryptographic modules used by the system must be validated by the NIST CVMP as compliant with FIPS 140-2. Cryptography performed by modules not validated is viewed by NIST as providing no protection for the data.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
NOTE: This will virtually always require a manual review. Determine if the SSH daemon uses a FIPS 140-2 validated cryptographic module (operating in FIPS mode). The NIST CVMP web site provides a list of validated modules and the required security policies for the compliant use of such modules. Verify the module is on the NIST list and configured in accordance with the validated security policy. If it does not, this is a finding.  
  
**Fix Text:**Configure the SSH client to use a FIPS 140-2 validated cryptographic module (operating in FIPS mode).   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4295  
**Group Title:** GEN005500  
**Rule ID:** SV-4295r6\_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  
  
**Check Content:**    
Locate the sshd\_config file.   
# find / -name sshd\_config   
# more <sshd\_config file location>  
  
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, 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22456  
**Group Title:** GEN005501  
**Rule ID:** SV-39209r1\_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 variables Protocol 2,1 or Protocol 1 are defined on a line without a leading comment, this is a finding.   
  
If the SSH client is F-Secure, the variable name for SSH 1 compatibility is Ssh1Compatibility, not protocol. If the variable Ssh1Compatiblity is set to yes, this is a finding.   
  
**Fix Text:**Edit the /etc/ssh/ssh\_config file and add or edit a Protocol configuration line that does not allow versions less than 2.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22457  
**Group Title:** GEN005504  
**Rule ID:** SV-26750r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005504  
**Rule Title:**The SSH daemon must only listen on management network addresses unless authorized for uses other than management.  
  
**Vulnerability Discussion:**  The SSH daemon should only listen on network addresses designated for management traffic. If the system has multiple network interfaces and SSH listens on addresses not designated for management traffic, the SSH service could be subject to unauthorized access. If SSH is used for purposes other than management, such as providing an SFTP service, the list of approved listening addresses may be documented.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for listening network addresses.  
# grep -i Listen /etc/ssh/sshd\_config | grep -v '^#'  
If no configuration is returned, or if a returned Listen configuration contains addresses not designated for management traffic, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration to specify listening network addresses designated for management traffic.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22458  
**Group Title:** GEN005505  
**Rule ID:** SV-26751r1\_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. If necessary, add a Ciphers line.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**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 the SSH daemon configuration and remove any ciphers ending with cbc. If necessary, add a Ciphers line.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22460  
**Group Title:** GEN005507  
**Rule ID:** SV-26753r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005507  
**Rule Title:**The SSH daemon must be configured to only use Message Authentication Codes (MACs) that employ 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22461  
**Group Title:** GEN005510  
**Rule ID:** SV-26754r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005510  
**Rule Title:**The SSH client must be configured to only use FIPS 140-2 approved ciphers.  
  
**Vulnerability Discussion:**  DoD information systems are required to use FIPS 140-2 approved ciphers. SSHv2 ciphers meeting this requirement are 3DES and AES.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Check the SSH client configuration for allowed ciphers.  
# grep -i ciphers /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, the returned ciphers list contains any cipher that does not start 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. If necessary, add a Ciphers line.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22462  
**Group Title:** GEN005511  
**Rule ID:** SV-26755r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005511  
**Rule Title:**The SSH client must be configured to not use CBC-based ciphers.  
  
**Vulnerability Discussion:**  The Cipher-Block Chaining (CBC) mode of encryption as implemented in the SSHv2 protocol is vulnerable to chosen-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 ending with cbc. If necessary, add a Ciphers line.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22463  
**Group Title:** GEN005512  
**Rule ID:** SV-26756r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005512  
**Rule Title:**The SSH client must be configured to only use Message Authentication Codes (MACs) that employ 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22464  
**Group Title:** GEN005515  
**Rule ID:** SV-26757r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005515  
**Rule Title:**The SSH daemon must be configured to not allow TCP connection forwarding.  
  
**Vulnerability Discussion:**  SSH TCP connection forwarding provides a mechanism to establish TCP connections proxied by the SSH server. This function can provide similar convenience to a Virtual Private Network (VPN) with the similar risk of providing a path to circumvent firewalls and network ACLs.  
  
If this function is necessary to support a valid mission requirement, its use must be authorized and approved in the system accreditation package.  
  
**Mitigations:**   
GEN005515  
  
**Mitigation Control:**   
If TCP connection forwarding is required, the risk of unauthorized use of this feature can be mitigated by placing restrictions on which users are permitted to use it. For instance, OpenSSH provides conditional configuration blocks (using the Match keyword) used to limit TCP connection forwarding based on user, group, host, or address.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for the TCP connection forwarding setting.  
# grep -i AllowTCPForwarding /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, or the returned setting has a value evaluating to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and change or add the AllowTCPForwarding setting to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22465  
**Group Title:** GEN005516  
**Rule ID:** SV-26758r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005516  
**Rule Title:**The SSH client must be configured to not allow TCP forwarding.  
  
**Vulnerability Discussion:**  SSH TCP connection forwarding provides a mechanism to establish TCP connections proxied by the SSH server. This function can provide similar convenience to a Virtual Private Network (VPN) with the similar risk of providing a path to circumvent firewalls and network ACLs.  
  
If this function is necessary to support a valid mission requirement, its use must be authorized and approved in the system accreditation package.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH client configuration for the TCP forwarding setting.  
# grep -i AllowTCPForwarding /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, or the returned setting has a value evaluating to yes, this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and change or add the AllowTCPForwarding setting to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22466  
**Group Title:** GEN005517  
**Rule ID:** SV-26759r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005517  
**Rule Title:**The SSH daemon must be configured to not allow gateway ports.  
  
**Vulnerability Discussion:**  SSH TCP connection forwarding provides a mechanism to establish TCP connections proxied by the SSH server. This function can provide similar convenience to a Virtual Private Network (VPN) with the similar risk of providing a path to circumvent firewalls and network ACLs. Gateway ports allow remote forwarded ports to bind to non-loopback addresses on the server.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for the gateway ports setting.  
# grep -i GatewayPorts /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, or the returned setting has a value evaluating to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and change or add the GatewayPorts setting to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22467  
**Group Title:** GEN005518  
**Rule ID:** SV-26760r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005518  
**Rule Title:**The SSH client must be configured to not allow gateway ports.  
  
**Vulnerability Discussion:**  SSH TCP connection forwarding provides a mechanism to establish TCP connections proxied by the SSH server. This function can provide similar convenience to a Virtual Private Network (VPN) with the similar risk of providing a path to circumvent firewalls and network ACLs. Gateway ports allow remote forwarded ports to bind to non-loopback addresses on the server.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH client configuration for the gateway ports setting.  
# grep -i GatewayPorts /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, or the returned setting has a value evaluating to yes, this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and change or add the GatewayPorts setting to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22468  
**Group Title:** GEN005519  
**Rule ID:** SV-26761r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005519  
**Rule Title:**The SSH daemon must be configured to not allow X11 forwarding.  
  
**Vulnerability Discussion:**  X11 forwarding over SSH allows for the secure remote execution of X11-based applications. This feature can increase the attack surface of an SSH connection and should not be enabled unless needed.  
  
If this function is necessary to support a valid mission requirement, its use must be authorized and approved in the system accreditation package.  
  
**Mitigations:**   
GEN005519  
  
**Mitigation Control:**   
If X11 connection forwarding is required, the risk of unauthorized use of this feature can be mitigated by placing restrictions on which users are permitted to use it. For instance, OpenSSH provides conditional configuration blocks (using the Match keyword) used to limit X11 connection forwarding based on user, group, host, or address.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for the X11 forwarding setting.  
# grep -i X11Forwarding /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, or the returned setting has a value evaluating to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and change or add the X11Forwarding setting to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22469  
**Group Title:** GEN005520  
**Rule ID:** SV-26762r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005520  
**Rule Title:**The SSH client must be configured to not allow X11 forwarding.  
  
**Vulnerability Discussion:**  X11 forwarding over SSH allows for the secure remote execution of X11-based applications. This feature can increase the attack surface of an SSH connection and should not be enabled unless needed.  
  
If this function is necessary to support a valid mission requirement, its use must be authorized and approved in the system accreditation package.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH client configuration for the X11 forwarding setting.  
# grep -i X11Forwarding /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, or the returned setting has a value evaluating to yes, this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and change or add the X11Forwarding setting to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22470  
**Group Title:** GEN005521  
**Rule ID:** SV-26763r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005521  
**Rule Title:**The SSH daemon must restrict login ability to specific users and/or groups.  
  
**Vulnerability Discussion:**  Restricting SSH logins to a limited group of users, such as system administrators, prevents password-guessing and other SSH attacks from reaching system accounts and other accounts not authorized for SSH access.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the SSH daemon configuration for the AllowGroups setting.  
# grep -i AllowGroups /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and add an AllowGroups directive.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22471  
**Group Title:** GEN005522  
**Rule ID:** SV-26764r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005522  
**Rule Title:**The SSH public host key files must have mode 0644 or less permissive.  
  
**Vulnerability Discussion:**  If a public host key file is modified by an unauthorized user, the SSH service may be compromised.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions for SSH public host key files.  
# ls -lL /etc/ssh/\*key.pub  
If any file has a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the permissions for the SSH public host key files.  
# chmod 0644 /etc/ssh/\*key.pub   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22472  
**Group Title:** GEN005523  
**Rule ID:** SV-26765r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005523  
**Rule Title:**The SSH private host key files must have mode 0600 or less permissive.  
  
**Vulnerability Discussion:**  If an unauthorized user obtains the private SSH host key file, the host could be impersonated.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions for SSH private host key files.  
# ls -lL /etc/ssh/\*key  
If any file has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the permissions for the SSH private host key files.  
# chmod 0600 /etc/ssh/\*key   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22473  
**Group Title:** GEN005524  
**Rule ID:** SV-26766r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005524  
**Rule Title:**The SSH daemon must not permit GSSAPI authentication unless needed.  
  
**Vulnerability Discussion:**  GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system’s GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Ask the SA if GSSAPI authentication is used for SSH authentication to the system. If so, this is not applicable.  
  
Check the SSH daemon configuration for the GSSAPI authentication setting.  
# grep -i GSSAPIAuthentication /etc/ssh/sshd\_config | grep -v '^#'   
If no lines are returned, or the setting is set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and set (add if necessary) a GSSAPIAuthentication directive set to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22474  
**Group Title:** GEN005525  
**Rule ID:** SV-26767r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005525  
**Rule Title:**The SSH client must not permit GSSAPI authentication unless needed.  
  
**Vulnerability Discussion:**  GSSAPI authentication is used to provide additional authentication mechanisms to applications. Allowing GSSAPI authentication through SSH exposes the system’s GSSAPI to remote hosts, increasing the attack surface of the system. GSSAPI authentication must be disabled unless needed.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH clients configuration for the GSSAPI authentication setting.  
# grep -i GSSAPIAuthentication /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, or the setting is set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and set (add if necessary) a GSSAPIAuthentication directive set to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22475  
**Group Title:** GEN005526  
**Rule ID:** SV-26768r1\_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 Kerberos authentication 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) a KerberosAuthentication directive set to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22476  
**Group Title:** GEN005527  
**Rule ID:** SV-26770r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005527  
**Rule Title:**The SSH client 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 client 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 the system uses Kerberos authentication. If it does, this is not applicable.  
  
Check the SSH clients configuration for the Kerberos authentication setting.  
# grep -i KerberosAuthentication /etc/ssh/ssh\_config | grep -v '^#'   
If no lines are returned, or the setting is set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and set (add if necessary) a KerberosAuthentication directive set to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22477  
**Group Title:** GEN005528  
**Rule ID:** SV-26771r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005528  
**Rule Title:**The SSH daemon must not accept environment variables from the client or must only accept those pertaining to locale.  
  
**Vulnerability Discussion:**  Environment variables can be used to change the behavior of remote sessions and should be limited. Locale environment variables specify the language, character set, and other features modifying the operation of software to match the user's preferences.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for the AcceptEnv setting.  
# grep -i AcceptEnv /etc/ssh/sshd\_config | grep -v '^#'   
If any line is returned other than those permitting LOCALE or LC\_\* environment variables, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and remove or edit the AcceptEnv setting(s) to only accept LOCALE or LC\_\* environment variables.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22478  
**Group Title:** GEN005529  
**Rule ID:** SV-26772r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005529  
**Rule Title:**The SSH client must not send environment variables to the server or must only send those pertaining to locale.  
  
**Vulnerability Discussion:**  Environment variables can be used to change the behavior of remote sessions and should be limited. Locale environment variables specify the language, character set, and other features modifying the operation of software to match the user's preferences.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH client configuration for the SendEnv setting.  
# grep -i SendEnv /etc/ssh/ssh\_config | grep -v '^#'   
If any line is returned other than those permitting LOCALE or LC\_\* environment variables, this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and remove or edit the SendEnv setting(s) to only accept LOCALE or LC\_\* environment variables.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22479  
**Group Title:** GEN005530  
**Rule ID:** SV-26773r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005530  
**Rule Title:**The SSH daemon must not permit user environment settings.  
  
**Vulnerability Discussion:**  SSH may be used to provide limited functions other than an interactive shell session, such as file transfer. If local, user-defined environment settings (such as those configured in ~/.ssh/authorized\_keys or ~/.ssh/environment, or equivalent) are configured by the user and permitted by the SSH daemon, they could be used to alter the behavior of the limited functions, potentially granting unauthorized access to the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the PermitUserEnvironment setting in the SSH daemon configuration.  
  
Procedure:  
# grep -i PermitUserEnvironment sshd\_config  
  
If the setting is not present, or set to a value other than no, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and edit or add the PermitUserEnvironment setting with a value of no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22480  
**Group Title:** GEN005531  
**Rule ID:** SV-26774r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005531  
**Rule Title:**The SSH daemon must not permit tunnels.  
  
**Vulnerability Discussion:**  OpenSSH has the ability to create network tunnels (layer-2 and layer-3) over an SSH connection. This function can provide similar convenience to a Virtual Private Network (VPN) with the similar risk of providing a path to circumvent firewalls and network ACLs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for the PermitTunnel setting.  
# grep -i PermitTunnel /etc/ssh/sshd\_config | grep -v '^#'   
If the setting is not present, or set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and add or edit the PermitTunnel setting value to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22481  
**Group Title:** GEN005532  
**Rule ID:** SV-26775r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005532  
**Rule Title:**The SSH client must not permit tunnels.  
  
**Vulnerability Discussion:**  OpenSSH has the ability to create network tunnels (layer-2 and layer-3) over an SSH connection. This function can provide similar convenience to a Virtual Private Network (VPN) with the similar risk of providing a path to circumvent firewalls and network ACLs.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH client configuration for the PermitTunnel setting.  
# grep -i PermitTunnel /etc/ssh/ssh\_config | grep -v '^#'   
If the setting is not present, or set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH client configuration and add or edit the PermitTunnel setting value to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22482  
**Group Title:** GEN005533  
**Rule ID:** SV-26776r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005533  
**Rule Title:**The SSH daemon must limit connections to a single session.  
  
**Vulnerability Discussion:**  The SSH protocol has the ability to provide multiple sessions over a single connection without reauthentication. A compromised client could use this feature to establish additional sessions to a system without consent or knowledge of the user.  
  
Alternate per-connection session limits may be documented if needed for a valid mission requirement. Greater limits are expected to be necessary in situations where TCP or X11 forwarding are used.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for the MaxSessions setting.  
# grep -i MaxSessions /etc/ssh/sshd\_config | grep -v '^#'   
If the setting is not present, or not set to 1, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and add or edit the MaxSessions setting value to 1.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22485  
**Group Title:** GEN005536  
**Rule ID:** SV-26781r1\_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 PubkeyAuthentication setting value to yes.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22486  
**Group Title:** GEN005537  
**Rule ID:** SV-26782r1\_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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22487  
**Group Title:** GEN005538  
**Rule ID:** SV-26786r1\_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 not present, or not set to no, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and add or edit the RhostsRSAAuthentication setting value to no.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22488  
**Group Title:** GEN005539  
**Rule ID:** SV-26787r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005539  
**Rule Title:**The SSH daemon must not allow compression or must only allow compression after successful authentication.  
  
**Vulnerability Discussion:**  If compression is allowed in an SSH connection prior to authentication, vulnerabilities in the compression software could result in compromise of the system from an unauthenticated connection, potentially with root privileges.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the SSH daemon configuration for the Compression setting.  
# grep -i Compression /etc/ssh/sshd\_config | grep -v '^#'   
If the setting is not present, or set to yes, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and add or edit the Compression setting value to no or delayed.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12022  
**Group Title:** Encrypted Communications IP Filtering and Banners  
**Rule ID:** SV-38955r1\_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  
  
**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.   
TCP Wrappers can be installed using SMIT from the AIX expansion pack as fileset netsec.options.tcpwrappers.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22489  
**Group Title:** GEN005550  
**Rule ID:** SV-26802r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005550  
**Rule Title:**The SSH daemon must be configured with the Department of Defense (DoD) login banner.  
  
**Vulnerability Discussion:**  Failure to display the DoD logon banner prior to a logon attempt will negate legal proceedings resulting from unauthorized access to system resources.  
  
The SSH service must be configured to display the DoD logon warning banner 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.  
# grep -i banner /etc/ssh/sshd\_config | grep -v '^#'  
# cat [banner file]  
Verify the Banner configuration line is present and the file it references contains a login warning banner.  
  
Otherwise, verify TCP\_WRAPPERS are configured for SSH and display a logon warning banner.  
  
If neither the SSH daemon nor TCP\_WRAPPERS is configured to display a logon warning banner, this is a finding.  
  
**Fix Text:**Edit the SSH daemon configuration and add or edit a Banner setting that references a file containing a logon warning banner.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4397  
**Group Title:** Default Gateway  
**Rule ID:** SV-39217r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005560  
**Rule Title:**The system must be configured with a default gateway for IPv4 if the system uses IPv4, unless the system is a router.  
  
**Vulnerability Discussion:**  If a system has no default gateway defined, the system is at increased risk of man-in-the-middle, monitoring, and Denial of Service attacks.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the system for an IPv4 default route.  
  
Procedure:  
# netstat –r |grep default  
  
If a default route is not defined, this is a finding.  
  
**Fix Text:**Set a default gateway for IPv4.   
  
# smitty route  
  
OR  
  
# route add 0 < ip address of gateway >  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22490  
**Group Title:** GEN005570  
**Rule ID:** SV-39215r1\_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:**    
If the system is a router, this is not applicable.  
If the system does not use IPv6, this is not applicable. Determine if the system has a default route configured for IPv6.   
  
# netstat -r | grep default  
If a default route is not defined, this is a finding.  
  
  
**Fix Text:**Configure an IPv6 default route on the system.   
  
# smitty route  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4398  
**Group Title:** Dedicated Hardware for Routing   
**Rule ID:** SV-4398r6\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005580  
**Rule Title:**A system used for routing must not run other network services or applications.  
  
**Vulnerability Discussion:**  Installing extraneous software on a system designated as a dedicated router poses a security threat to the system and the network. Should an attacker gain access to the router through the unauthorized software, the entire network is susceptible to malicious activity.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSP-1  
  
**Check Content:**    
Ask the SA if the system is a designated router. If it is not, this is not applicable.  
  
Check the system for non-routing network services.  
  
Procedure:  
# netstat -a | grep -i listen  
# ps -ef  
  
If non-routing services, including Web servers, file servers, DNS servers, or applications servers, but excluding management services such as SSH and SNMP, are running on the system, this is a finding.  
  
**Fix Text:**Ensure only authorized software is loaded on a designated router. Authorized software will be limited to the most current version of routing protocols and SSH for system administration purposes.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22665  
**Group Title:** GEN005590  
**Rule ID:** SV-38923r1\_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.  
# ps -ef | egrep '(ospf|route|bgp|zebra|quagga|gate)'  
If any routing protocol daemons are listed, this is a finding.  
  
  
**Fix Text:**Disable any routing protocol daemons.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12023  
**Group Title:** Disable IP Forwarding  
**Rule ID:** SV-38821r1\_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:**    
#no –o ipforwarding  
If the value returned is not 0, this is a finding.  
  
**Fix Text:**Disable IPv4 forwarding on the system.  
#no -p –o ipforwarding=0  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22491  
**Group Title:** GEN005610  
**Rule ID:** SV-38822r1\_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:**    
# /usr/sbin/no –o ip6forwarding  
If the value returned is 1, this is a finding.  
  
  
**Fix Text:**Disable IPv6 forwarding on the system.   
# /usr/sbin/no –p –o ip6forwarding=0  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-927  
**Group Title:** NFS Port Monitoring  
**Rule ID:** SV-28441r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005720  
**Rule Title:**NFS servers must only accept NFS requests from privileged ports on client systems.  
  
**Vulnerability Discussion:**  If clients are not required to use privileged ports to get NFS services, then exported file systems may be in danger of mounting by malicious users and intruders that do not have access to privileged ports.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Perform the following command to determine if NFS port monitoring is enabled.  
# nfso -o nfs\_portmon  
OR  
# nfso -o portcheck  
If the returned value is not '1', this is a finding.  
  
**Fix Text:**# nfso -p -o nfs\_portmon=1  
OR  
# nfso -p -o portcheck=1   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-928  
**Group Title:** Export Configuration File Ownership  
**Rule ID:** SV-28445r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005740  
**Rule Title:**The NFS export configuration file must be owned by root.  
  
**Vulnerability Discussion:**  Failure to give ownership of the NFS export configuration file to root provides the designated owner and possible unauthorized users with the potential to change system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the 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   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22492  
**Group Title:** GEN005750  
**Rule ID:** SV-26167r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005750  
**Rule Title:**The 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 <NFS export configuration file>  
  
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 to root, bin, sys, or system.  
Procedure:  
# chgrp root <NFS export file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-929  
**Group Title:** Export Configuration File Permissions  
**Rule ID:** SV-28447r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005760  
**Rule Title:**The NFS export configuration file must have mode 0644 or less permissive.  
  
**Vulnerability Discussion:**  Excessive permissions on the NFS export configuration file could allow unauthorized modification of the file, which could result in Denial of Service to authorized NFS exports and the creation of additional unauthorized exports.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECCD-1, ECCD-2, ECLP-1  
  
**Check Content:**    
# ls -lL /etc/exports  
If the file has a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**# chmod 0644 /etc/exports   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22493  
**Group Title:** GEN005770  
**Rule ID:** SV-38823r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN005770  
**Rule Title:**The NFS exports configuration file must not have an extended ACL.  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files. Excessive permissions on the NFS export configuration file could allow unauthorized modification of the file, which could result in Denial of Service to authorized NFS exports and the creation of additional unauthorized exports.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
  
# aclget /etc/exports  
If the extended attributes are not disabled, this is a finding  
  
  
**Fix Text:**Remove the extended ACL from the NFS export configuration file and change extended attributes to disabled.  
  
#acledit /etc/exports   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-931  
**Group Title:** Exported System Files and Directories Ownership  
**Rule ID:** SV-931r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005800  
**Rule Title:**All NFS-exported system files and system directories must be owned by root.  
  
**Vulnerability Discussion:**  Failure to give ownership of sensitive files or directories to root provides the designated owner and possible unauthorized users with the potential to access sensitive information or change system configuration which could weaken the system's security posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check for NFS exported file systems.  
  
Procedure:  
# exportfs –v  
  
This will display all of the exported file systems. For each file system displayed, check the ownership.  
  
Procedure:  
# ls –lLa <exported file system path>  
  
If the files and directories are not owned by root, this is a finding.  
  
**Fix Text:**Change the ownership of exported file systems not owned by root.  
  
Procedure:  
# chown root <path>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22496  
**Group Title:** GEN005810  
**Rule ID:** SV-26171r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005810  
**Rule Title:**All NFS-exported system files and system directories must be group-owned by root, bin, 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:**    
Determine if the NFS exported directories on the system are group-owned by root. If any are not, this is a finding.  
  
**Fix Text:**Change the group-owner of NFS exported directories to root.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-932  
**Group Title:** Deny NFS Client Access Without Userid  
**Rule ID:** SV-38956r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005820  
**Rule Title:**The 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  
  
**Check Content:**    
Check if the 'anon' option is set correctly for exported file systems.  
  
List exported file systems:  
# exportfs -v   
  
Each of the exported file systems should include an entry for the 'anon=' option set to -1 or an equivalent (60001, 65534, or 65535). If an appropriate 'anon=' setting is not present for an exported file system, this is a finding.  
  
  
  
**Fix Text:**Edit /etc/exports and set the anon=-1 option for exported file systems without it. Re-export the file systems.   
  
# exportfs -a   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-933  
**Group Title:** GEN005840  
**Rule ID:** SV-933r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005840  
**Rule Title:**The NFS server must be configured to restrict file system access to local hosts.  
  
**Vulnerability Discussion:**  The NFS access option limits user access to the specified level. This assists in protecting exported file systems. If access is not restricted, unauthorized hosts may be able to access the system's NFS exports.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the permissions on exported NFS file systems.  
  
Procedure:  
# exportfs -v  
  
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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-935  
**Group Title:** GEN005880  
**Rule ID:** SV-935r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005880  
**Rule Title:**The NFS server must not allow remote root access.  
  
**Vulnerability Discussion:**  If the NFS server allows root access to local file systems from remote hosts, this access could be used to compromise the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  EBRP-1  
  
**Check Content:**    
Determine if the NFS server is exporting with the root access option.  
  
Procedure:  
# exportfs –v | grep “root=”  
  
If an export with the root option is found, this is a finding.  
  
**Fix Text:**Edit /etc/exports and remove the root= option for all exports. Re-export the file systems.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-936  
**Group Title:** GEN005900  
**Rule ID:** SV-38957r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN005900  
**Rule Title:**The nosuid option must be enabled on all NFS client mounts.  
  
**Vulnerability Discussion:**  Enabling the nosuid mount option prevents the system from granting owner or group-owner privileges to programs with the 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:**  System Administrator  
**IAControls:**  ECPA-1  
  
**Check Content:**    
Check the system for NFS mounts not using the nosuid option.   
Procedure:   
# lsfs -v nfs  
If the mounted file systems do not have the nosuid option, this is a finding.   
  
  
**Fix Text:**Edit /etc/filesystems and add the nosuid option for all NFS file systems. Remount the NFS file systems to make the change take effect.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12024  
**Group Title:** GEN006000  
**Rule ID:** SV-12525r4\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006000  
**Rule Title:**The system must not have a public instant messaging (IM) client installed.  
  
**Vulnerability Discussion:**  Public Instant Messaging (IM) systems are not approved for use and may result in the unauthorized distribution of information. IM clients provide a way for a user to send a message to one or more other users in real time. Additional capabilities may include file transfer and support for distributed game playing. Communication between clients and associated directory services are managed through messaging servers. Commercial IM clients include AOL Instant Messenger (AIM), MSN Messenger, and Yahoo! Messenger.  
  
IM clients present a security issue when the clients route messages through public servers. The obvious implication is potentially sensitive information could be intercepted or altered in the course of transmission. This same issue is associated with the use of public 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 used to access internal or DoD-controlled IM services are permitted.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECIM-1  
  
**Check Content:**    
If an IM client is installed, ask the SA if it has access to any public domain IM servers. If it does have access to public servers, this is a finding.  
  
  
  
**Fix Text:**Uninstall the IM client from the system, or configure the client to only connect to DoD-approved IM services.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12025  
**Group Title:** GEN006040  
**Rule ID:** SV-12526r4\_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:**  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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4321  
**Group Title:** GEN006060  
**Rule ID:** SV-4321r5\_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:**  ECSC-1  
  
**Check Content:**    
Check the system for a running Samba server.  
  
Procedure:  
# ps –ef |grep smbd  
  
If the Samba server is running, ask the SA if the Samba server is operationally required. If it is not, this is a finding.  
  
**Fix Text:**If there is no functional need for Samba and the daemon is running, disable the daemon by killing the process ID as noted from the output of ps -ef |grep smbd. The utility should also be removed or not installed if there is no functional requirement.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1026  
**Group Title:** GEN006080  
**Rule ID:** SV-1026r5\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006080  
**Rule Title:**The Samba Web Administration Tool (SWAT) must be restricted to the local host or require SSL.  
  
**Vulnerability Discussion:**  SWAT is a tool used to configure Samba. As it modifies Samba configuration, which can impact system security, it must be protected from unauthorized access. SWAT authentication may involve the root password, which must be protected by encryption when traversing the network.  
  
Restricting access to the local host allows for the use of SSH TCP forwarding, if configured, or administration by a web browser on the local system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  EBRP-1  
  
**Check Content:**    
If SWAT is used, it must be utilized with SSH to ensure a secure connection between the client and the server.   
  
If SWAT is running, ask the SA if SSH port forwarding is used to access it. If not, this is a finding.  
  
**Fix Text:**Disable SWAT or require that SWAT is only accessed via SSH.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1027  
**Group Title:** GEN006100  
**Rule ID:** SV-1027r4\_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/smb.conf file.  
  
Procedure:  
# find / -name smb.conf  
# ls -l <smb.conf file>  
  
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   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1056  
**Group Title:** GEN006120  
**Rule ID:** SV-39231r1\_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:  
# find / -name smb.conf  
# ls -l <smb.conf file>  
  
If an 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 system smb.conf   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1028  
**Group Title:** GEN006140  
**Rule ID:** SV-39229r1\_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:  
# find / -name smb.conf  
# ls –lL <smb.conf file>  
  
If the smb.conf has a mode more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the mode of the smb.conf file to 0644 or less permissive.  
  
Procedure:  
# chmod 0644 smb.conf.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22497  
**Group Title:** GEN006150  
**Rule ID:** SV-38824r1\_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 group ownership of the Samba configuration file.  
# find / -name smb.conf  
# aclget <smb.conf file>  
If the extended attributes are not disabled, this is a finding  
  
  
**Fix Text:**Remove the extended ACL from the /etc/smb.conf file and change extended attributes to disabled.  
  
#acledit < smb.conf file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1029  
**Group Title:** GEN006160  
**Rule ID:** SV-1029r4\_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, the smbpasswd file may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the ownership of the smbpasswd file.  
  
# find / -name smbpasswd  
# ls -l <smbpasswd file>  
  
If an smbpasswd file is not owned by root, this is a finding.  
  
**Fix Text:**Use the chown command to configure the smb passwd file. For instance: chown root /etc/smbpasswd.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1058  
**Group Title:** GEN006180  
**Rule ID:** SV-39235r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006180  
**Rule Title:**The /etc/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.  
# find / -name smbpasswd   
# ls –lL < smbpasswd file>  
If smbpasswd is not group-owned by root, sys, or system, this is a finding.   
  
  
**Fix Text:**Use the chgrp command to change the group owner of the smbpasswd file is root.   
  
# chgrp system < smbpasswd file >   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1059  
**Group Title:** GEN006200  
**Rule ID:** SV-1059r5\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006200  
**Rule Title:**The /etc/smbpasswd file must have mode 0600 or less permissive.  
  
**Vulnerability Discussion:**  If the smbpasswd file has a mode more permissive than 0600, the smbpasswd file may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check smbpasswd mode.  
  
Procedure:  
# find / -name smbpasswd  
# ls –lL <smbpasswd file>  
  
If smbpasswd has a mode more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the smbpasswd file to 0600.  
  
Procedure:  
# chmod 0600 smbpasswd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22498  
**Group Title:** GEN006210  
**Rule ID:** SV-38928r1\_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, the smbpasswd file may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the group ownership of the Samba configuration file.  
# find / -name smbpasswd   
  
# aclget <sbmpasswd file>  
If the extended attributes are not disabled, this is a finding  
  
  
**Fix Text:**Remove the extended ACL from the /etc/smbpasswd file.   
  
# acledit < smbpasswd file >  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1030  
**Group Title:** GEN006220  
**Rule ID:** SV-39237r1\_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.  
  
# find / -name smb.conf  
# more < smb.conf file >  
  
If the hosts option is not present to restrict access to a list of authorized hosts and networks, this is a finding.  
  
**Fix Text:**Edit the smb.conf file and set the hosts option to permit only authorized hosts to access Samba.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22499  
**Group Title:** GEN006225  
**Rule ID:** SV-39239r1\_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.  
# find / -name smb.conf  
# grep -i security < smb.conf file >  
If the security mode is "share", this is a finding.  
  
  
**Fix Text:**Edit the /etc/smb.conf file and change the security setting to user or another valid setting other than share.  
  
# vi < smb.conf file >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22500  
**Group Title:** GEN006230  
**Rule ID:** SV-39241r1\_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 the Samba configuration.  
  
#find / -name smb.conf  
# grep -i 'encrypt passwords' < smb.conf file >  
If the setting is not present, or not set to 'yes', this is a finding.  
  
**Fix Text:**Edit the smb.conf file and change the "encrypt passwords" setting to yes.   
  
# vi < smb.conf file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22501  
**Group Title:** GEN006235  
**Rule ID:** SV-39245r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006235  
**Rule Title:**Samba must be configured to not allow guest access to shares.  
  
**Vulnerability Discussion:**  Guest access to shares permits anonymous access and is not permitted.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the encryption setting the Samba configuration.  
# find / -name smb.conf  
# grep -i 'guest ok' < smb.conf file >  
If the setting exists and is set to 'yes', this is a finding.  
  
**Fix Text:**Edit the smb.conf file and change the "guest ok" setting to no.   
  
# vi < smb.conf file >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1023  
**Group Title:** GEN006240  
**Rule ID:** SV-1023r5\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006240  
**Rule Title:**The system must not run an Internet Network News (INN) server.  
  
**Vulnerability Discussion:**  Internet Network News (INN) servers access Usenet newsfeeds and store newsgroup articles. INN servers use the Network News Transfer Protocol (NNTP) to transfer information from the Usenet to the server and from the server to authorized remote hosts.  
  
If this function is necessary to support a valid mission requirement, its use must be authorized and approved in the system accreditation package.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# ps –ef | egrep “innd|nntpd”  
  
If an Internet Network News server is running, this is a finding.  
  
  
**Fix Text:**Disable the INN server.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4273  
**Group Title:** /etc/news/hosts.nntp permissions  
**Rule ID:** SV-39250r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006260  
**Rule Title:**The /etc/news/hosts.nntp (or equivalent) must have mode 0600 or less permissive.  
  
**Vulnerability Discussion:**  Excessive permissions on the hosts.nntp file may allow unauthorized modification which could lead to Denial of Service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/news/hosts.nntp permissions.  
  
# find / -name hosts.nntp  
# ls –lL < hosts.nntp file >  
  
If /etc/news/hosts.nntp has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the hosts.nntp file to 0600.  
  
# chmod 0600 < hosts.nntp file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22502  
**Group Title:** GEN006270  
**Rule ID:** SV-38898r1\_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 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 hosts.nntp file.  
# find / -type f –name hosts.nntp   
# aclget < hosts.nntp file >  
If extended permissions are enabled, the file has an extended ACL, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the hosts.nntp file.   
#acledit < hosts.nntp file >  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4274  
**Group Title:** /etc/news/hosts.nntp.nolimit permissions  
**Rule ID:** SV-39252r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006280  
**Rule Title:**The /etc/news/hosts.nntp.nolimit (or equivalent) must have mode 0600 or less permissive.  
  
**Vulnerability Discussion:**  Excessive permissions on the hosts.nntp.nolimit file may allow unauthorized modification which could lead to denial of service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/news/hosts.nntp.nolimit permissions.  
  
# find / -name hosts.nntp.nolimit  
  
# ls –lL < hosts.nntp.nolimit file >  
  
If hosts.nntp.nolimit has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of hosts.nntp.nolimit to 0600.  
# chmod 0600 < hosts.nntp.nolimit file>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22503  
**Group Title:** GEN006290  
**Rule ID:** SV-38899r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006290  
**Rule Title:**The /etc/news/hosts.nntp.nolimit file must not have an extended ACL.  
  
**Vulnerability Discussion:**  File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files. Excessive permissions on the hosts.nntp.nolimit file may allow unauthorized modification which could lead to Denial of Service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check the permissions of the file.  
  
# fine / -name hosts.nntp.nolimit  
  
# acelget < hosts.nntp.nolimit >  
If the extended permissions are enabled the file has an extended ACL, this is a finding.  
  
  
**Fix Text:**Remove the extended ACL from the hosts.nntp.nolimit file.   
  
# acledit < hosts.nntp.nolimit >  
  
Set the extended permissions to disabled.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4275  
**Group Title:** /etc/news/nnrp.access permissions  
**Rule ID:** SV-39255r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006300  
**Rule Title:**The /etc/news/nnrp.access (or equivalent) must have mode 0600 or less permissive.  
  
**Vulnerability Discussion:**  Excessive permissions on the nnrp.access file may allow unauthorized modification which could lead to Denial of Service to authorized users or provide access to unauthorized users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECLP-1  
  
**Check Content:**    
Check /etc/news/nnrp.access permissions.  
  
# find / -name nnrp.access  
# ls –lL < nnrp.access >  
  
If /etc/news/nnrp.access has a mode more permissive than 0600, this is a finding.  
  
**Fix Text:**Change the mode of the nnrp.access file to 0600.  
  
# chmod 0600 < nnrp.access >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22504  
**Group Title:** GEN006310  
**Rule ID:** SV-39258r1\_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.  
  
# find / -name nnrp.access  
# ls -lL < nnrp.access >  
If extended permissions are enabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the nnrp.access file.   
  
# acledit < nnrp.access >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4276  
**Group Title:** /etc/news/passwd.nntp permissions  
**Rule ID:** SV-39260r1\_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.  
  
# find / -name passwd.nntp  
  
# ls –lL < passwd.nntp >  
  
If passwd.nntp has a mode more permissive than 0600, this is a finding.  
  
  
**Fix Text:**Change the mode of the passwd.nntp file.  
  
# chmod 0600 < passwd.nntp >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22505  
**Group Title:** GEN006330  
**Rule ID:** SV-39262r1\_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.  
  
# find / -name passwd.nntp  
# ls -lL < passwd.nntp >  
If extended permissions are enabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the passwd.nntp file.  
  
# acledit < passwd.nntp >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4277  
**Group Title:** /etc/news files ownership  
**Rule ID:** SV-4277r4\_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/\*   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4278  
**Group Title:** /etc/news files group ownership  
**Rule ID:** SV-4278r4\_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/\*   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4399  
**Group Title:** GEN006380  
**Rule ID:** SV-4399r6\_rule  
**Severity: CAT I**  
**Rule Version (STIG-ID):** GEN006380  
**Rule Title:**The system must not use UDP for NIS/NIS+.  
  
**Vulnerability Discussion:**  Implementing NIS or NIS+ under UDP may make the system more susceptible to a Denial of Service attack and does not provide the same quality of service as TCP.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system does not use NIS or NIS+, this is not applicable.  
  
Check if NIS or NIS+ is implemented using UDP.  
  
Procedure:  
# rpcinfo -p | grep yp | grep udp  
  
If NIS or NIS+ is implemented using UDP, this is a finding.  
  
**Fix Text:**Configure the system to not use UDP for NIS and NIS+. Consult vendor documentation for the required procedure.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-867  
**Group Title:** GEN006400  
**Rule ID:** SV-867r7\_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. Possible replacements are NIS+ and LDAP.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12026  
**Group Title:** GEN006420  
**Rule ID:** SV-12527r4\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006420  
**Rule Title:**NIS maps must be protected through hard-to-guess domain names.  
  
**Vulnerability Discussion:**  The use of hard-to-guess NIS domain names provides additional protection from unauthorized access to the NIS directory information.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the domain name for NIS maps.  
  
Procedure:  
# domainname  
  
If the name returned is simple to guess, such as the organization name, building or room name, etc., this is a finding.  
  
**Fix Text:**Change the NIS domainname to a value difficult to guess. Consult vendor documentation for the required procedure.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-926  
**Group Title:** GEN006460  
**Rule ID:** SV-926r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006460  
**Rule Title:**Any NIS+ server must be operating at security level 2.  
  
**Vulnerability Discussion:**  If the NIS+ server is not operating in, at least, security level 2, there is no encryption and the system could be penetrated by intruders and/or malicious users.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system is not using NIS+, this is not applicable.  
  
Check the system to determine if NIS+ security level 2 is implemented.  
  
Execute this command:  
# niscat cred.org\_dir   
  
If the second column does not contain DES, the system is not using NIS+ security level 2, and this is a finding.  
  
**Fix Text:**Configure the NIS+ server to use security level 2.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-782  
**Group Title:** GEN006480  
**Rule ID:** SV-782r7\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006480  
**Rule Title:**The system must have a host-based intrusion detection tool installed.  
  
**Vulnerability Discussion:**  Without a host-based intrusion detection tool, there is no system-level defense when an intruder gains access to a system or network. Additionally, a host-based intrusion detection tool can provide methods to immediately lock out detected intrusion attempts.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECID-1  
  
**Check Content:**    
A few applications providing host-based network intrusion protection are:  
  
- Dragon Squire by Enterasys Networks  
- ITA by Symantec  
- Hostsentry by Psionic Software  
- Logcheck by Psionic Software  
- RealSecure agent by ISS  
- Swatch by Stanford University  
  
Ask the SA or IAO if a host-based intrusion detection application is loaded on the system.  
  
Procedure to determine if the application is loaded on the system:  
# find / -name <daemon name> -print   
  
  
  
Determine if the application is active on the system.  
  
Procedure:  
# ps –ef | grep <daemon name>   
  
If no host-based intrusion detection system is installed on the system, this is a finding.  
  
  
**Fix Text:**Install a host-based intrusion detection tool.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12028  
**Group Title:** GEN006560  
**Rule ID:** SV-12529r3\_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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22506  
**Group Title:** GEN006565  
**Rule ID:** SV-38958r1\_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 that do not use package management tools.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
Check the root crontab for a job invoking the system package management tool to verify the integrity of installed packages.   
  
# crontab -l | grep lppchk  
  
If no such job exists, this is a finding.   
  
  
**Fix Text:**Add a job to the root crontab invoking the system package management tool to verify the integrity of installed packages.   
  
# lppchk –c   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22507  
**Group Title:** GEN006570  
**Rule ID:** SV-26858r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN006570  
**Rule Title:**The file integrity tool must be configured to verify ACLs.  
  
**Vulnerability Discussion:**  ACLs can provide permissions beyond those permitted through the file mode and must be verified by file integrity tools.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
If using AIDE, verify the configuration contains the acl option for all monitored files and directories. 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22508  
**Group Title:** GEN006571  
**Rule ID:** SV-26860r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN006571  
**Rule Title:**The file integrity tool must be configured to verify extended attributes.  
  
**Vulnerability Discussion:**  Extended attributes in file systems are used to contain arbitrary data and file metadata with security implications.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECAT-1  
  
**Check Content:**    
If using AIDE, verify the configuration contains the "xattrs" option for all monitored files and directories. 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22509  
**Group Title:** GEN006575  
**Rule ID:** SV-26861r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN006575  
**Rule Title:**The file integrity tool must use FIPS 140-2 approved cryptographic hashes for validating file contents.  
  
**Vulnerability Discussion:**  File integrity tools often use cryptographic hashes for verifying that file contents have not been altered. These hashes must be FIPS 140-2 approved.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If using AIDE, verify the configuration contains the "sha256" or "sha512" options for all monitored files and directories. 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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-940  
**Group Title:** Access Control Program  
**Rule ID:** SV-38959r1\_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:**    
Determine if TCP\_WRAPPERS is being used.  
# grep tcpd /etc/inetd.conf  
If no services are listed, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and use tcpd to wrap services.   
Use SMIT to install TCP Wrappers from the AIX Expansion pack media as fileset netsec.options.tcpwrappers.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-941  
**Group Title:** Access Control Program Logging  
**Rule ID:** SV-941r7\_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-2, ECAR-3  
  
**Check Content:**    
Normally, tcpd logs to the mail facility in /etc/syslog.conf. Determine if syslog is configured to log events by tcpd.  
  
Procedure:  
# more /etc/syslog.conf  
  
Look for entries similar to the following:  
mail.debug                         /var/adm/maillog  
mail.none                               /var/adm/maillog  
mail.\*                               /var/log/mail  
auth.info                               /var/log/messages  
  
The above entries would indicate mail alerts are being logged. If no entries for mail exist, then tcpd is not logging and this is a finding.  
  
**Fix Text:**Configure the access restriction program to log every access attempt. Ensure the implementation instructions for TCP\_WRAPPERS are followed so logging of system access attempts is logged into the system log files. If an alternate application is used, it must support this function.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12030  
**Group Title:** Access Control Program Control System Access  
**Rule ID:** SV-12531r4\_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:**  ECSC-1  
  
**Check Content:**    
Check for the existence of the /etc/hosts.allow and /etc/hosts.deny files.  
  
Procedure:  
# ls –la /etc/hosts.allow  
# ls –la /etc/hosts.deny  
  
If either file does not exist, this is a finding.  
  
Check for the presence of a default deny entry.  
  
Procedure:  
# grep “ALL: ALL” /etc/hosts.deny  
  
If the ‘ALL: ALL’ entry is not present in the /etc/hosts.deny file, any TCP service from a host or network not matching other rules will be allowed access. If the entry is not in /etc/hosts.deny, this is a finding.  
  
**Fix Text:**Edit the /etc/hosts.all and /etc/hosts.deny files to configure access restrictions.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-12765  
**Group Title:** GEN006640  
**Rule ID:** SV-28461r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN006640  
**Rule Title:**The system must use and update a DoD-approved virus scan program.  
  
**Vulnerability Discussion:**  Virus scanning software can be used to protect a system from penetration from computer viruses and to limit their spread through intermediate systems. Virus scanning software is available to DoD on the JTF-GNO website.  
  
The virus scanning software should be configured to perform scans dynamically on accessed files. If this capability is not available, the system must be configured to scan, at a minimum, all altered files on the system on a daily basis.  
  
If the system processes inbound SMTP mail, the virus scanner must be configured to scan all received mail.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECVP-1  
  
**Check Content:**    
Check for the existence of the McAfee command line scan tool to be executed weekly in the cron file. Additional tools specific for each operating system are also available and will have to be manually reviewed if installed. In addition, the definitions file should not be older than 14 days.   
  
Check if uvscan is scheduled to run:  
# grep uvscan /var/spool/cron/crontabs/\*  
  
Perform the following command to ensure the virus definition signature files are not older than 14 days.  
  
# ls -la clean.dat names.dat scan.dat  
  
If a virus scanner is not being run weekly or the virus definitions are older than 14 days, this is a finding.  
  
**Fix Text:**Install McAfee command line virus scan tool, or an appropriate alternative from https://www.jtfgno.mil. Ensure the virus signature definition files are no older than 14 days. Updates are also available from https://www.jtfgno.mil.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22511  
**Group Title:** GEN007020  
**Rule ID:** SV-38960r1\_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 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:**    
If there is no SCTP protocol handler for the system, this is not applicable.  
  
Determine if the system is configured to prevent the dynamic loading of the SCTP protocol handler. If not, this is a finding.  
  
  
  
**Fix Text:**Configure the system to prevent the dynamic loading of the SCTP protocol handler. Unload the SCTP module from the kernel.  
#sctpctl unload  
If SCTP is not needed, use SMIT to uninstall the bos.net.sctp fileset.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22514  
**Group Title:** GEN007080  
**Rule ID:** SV-38901r1\_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 Datagram Congestion Control Protocol (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:**    
If there is no DCCP protocol handler for the system, this is not applicable.  
  
DCCP is not currently available for the AIX 5 and AIX 6 platforms and is therefore not applicable .  
  
**Fix Text:**No fix is necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22517  
**Group Title:** GEN007140  
**Rule ID:** SV-38903r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007140  
**Rule Title:**The Lightweight User Datagram Protocol (UDP-Lite) must be disabled unless required.  
  
**Vulnerability Discussion:**  The Lightweight User Datagram Protocol (UDP-Lite) 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:**    
If there is no UDP-Lite protocol handler available for the system, this is not applicable.  
  
Lightweight User Datagram Protocol is not currently available for AIX 5 and AIX6 therefore it is not applicable.  
  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22520  
**Group Title:** GEN007200  
**Rule ID:** SV-38905r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007200  
**Rule Title:**The Internetwork Packet Exchange (IPX) protocol must be disabled or not installed.  
  
**Vulnerability Discussion:**  The Internetwork Packet Exchange (IPX) protocol is a network-layer protocol that 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:**    
If there is no IPX protocol handler for the system, this is not applicable.  
  
IPX Protocol is not currently available for the AIX 5 and AIX6 and is therefore not applicable.  
  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22524  
**Group Title:** GEN007260  
**Rule ID:** SV-38908r1\_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:**    
If there is no AppleTalk protocol handler for the system, this is not applicable.  
  
AppleTalk Protocol is not currently available for the AIX 5 and AIX6 and is therefore not applicable.  
  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22527  
**Group Title:** GEN007320  
**Rule ID:** SV-38912r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007320  
**Rule Title:**The DECnet protocol must be disabled or not installed.  
  
**Vulnerability Discussion:**  The DECnet 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:**    
If there is no DECnet protocol handler for the system, this is not applicable.  
  
DECnet Protocol is not currently available for the AIX 5 and AIX6 and is therefore not applicable.  
  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22530  
**Group Title:** GEN007480  
**Rule ID:** SV-38913r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007480  
**Rule Title:**The Reliable Datagram Sockets (RDS) protocol must be disabled or not installed unless required.  
  
**Vulnerability Discussion:**  The Reliable Datagram Sockets (RDS) protocol is a relatively new protocol developed by Oracle for communication between the nodes of a cluster. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes may be able to cause the system to dynamically load a protocol handler by opening a socket using the protocol.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
AIX has RDS protocol installed as part of the ‘bos.net.tcp.client’ fileset. The RDS protocol in primarily used for communication on INFI-Band interfaces. The protocol is manually loaded with the bypassctrl command.  
  
Determine if RDS is currently loaded.  
#genkex | grep rds  
  
If the RDS protocol is loaded, ask the SA if RDS is required by application software running on the system. If so, this is not applicable.  
  
If the RDS protocol is loaded and the protocol is not used by application software, this is a finding.  
  
**Fix Text:**Configure the system to not automatically load the RDS protocol handler.   
  
Check startup scripts for ‘bypasscrtl load rds’ and comment out the bypassctrl commands.  
  
Unload the driver from the kernel.  
# bypassctrl unload rds   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22533  
**Group Title:** GEN007540  
**Rule ID:** SV-38914r1\_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 Transparent Inter-Process Communication (TIPC) protocol is a relatively new cluster communications protocol developed by Ericsson. Binding this protocol to the network stack increases the attack surface of the host. Unprivileged local processes may be able to cause the system to dynamically load a protocol handler by opening a socket using the protocol.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If there is no TIPC protocol handler for the system, this is not applicable.  
  
Transparent Inter-Process Communication (TIPC) protocol is not currently available for the AIX 5 and AIX6 and is therefore not applicable.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22539  
**Group Title:** GEN007660  
**Rule ID:** SV-39507r1\_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:**    
If there is no Bluetooth protocol handler for the system, this is not applicable.  
  
Bluetooth is not currently available for the AIX 5 and AIX 6 platforms and is therefore not applicable.  
  
**Fix Text:**Configure the system to prevent the dynamic loading of the Bluetooth protocol handler.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22541  
**Group Title:** GEN007700  
**Rule ID:** SV-38918r1\_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:**    
AIX comes with IPv6 protocol handler installed and active. The only configured IPv6 address is the loopback localhost adapter.   
  
Check if any other interfaces have IPv6 addresses active.  
  
# ifconfig -a  
  
If any IPv6 addresses are configured on any network interfaces other than loopback and IPv6 is not needed, this is a finding.  
  
**Fix Text:**Unbind the IPv6 protocol handler from the network stack.  
  
Edit /etc/rc.tcpip and comment out autoconf6 to prevent IPv6 from auto starting.  
  
Unconfigure IPv6 addresses from interfaces not used with smit.  
  
#smit chinet6   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22542  
**Group Title:** GEN007720  
**Rule ID:** SV-38922r1\_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:**    
Determine if the IPv6 protocol handler is prevented from dynamic loading.  
  
AIX comes with IPv6 protocol handler installed and active.   
  
The only IPv6 address configured by default is the loopback localhost adapter.   
  
#ifconfig -a  
  
If there is any unneeded IPv6 addresses on network interfaces, this is a finding.  
  
**Fix Text:**There is not an option to not load IPv6.   
  
Remove unnecessary IPv6 addresses from network interfaces via smit.  
  
#smit chinet6   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22543  
**Group Title:** GEN007740  
**Rule ID:** SV-38924r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007740  
**Rule Title:**The IPv6 protocol handler must not be installed 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 kernel to dynamically load a protocol handler by opening a socket using the protocol.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the IPv6 protocol handler is not available as an optional software package for the system, this is not applicable.   
  
AIX has the IPv6 protocol installed with the bos.tcp.net.\* filesets and it is not uninstallable; therefore this is not applicable.   
  
If the system uses IPv6, this is not applicable.  
  
If the IPv6 protocol handler is installed, this is a finding  
  
  
**Fix Text:**No fix can be performed to remove the IPv6 software.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22544  
**Group Title:** GEN007760  
**Rule ID:** SV-38925r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007760  
**Rule Title:**Proxy Neighbor Discovery Protocol (NDP) must not be enabled on the system.  
  
**Vulnerability Discussion:**  Proxy Neighbor Discovery Protocol (NDP) allows a system to respond to NDP 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:**    
If the system does not support proxy NDP, this is not applicable.  
Determine if the system has proxy NDP enabled.  
  
If IPv6 is enabled, determine if any non-local published NDP entries exist on the system.  
# ndp -a  
  
If any NDP entries contain non-local published entries, this is a finding.  
  
  
**Fix Text:**Remove non-local published NDP entries from the system.  
  
# ndp -d <host>  
  
Check system startup scripts for commands publishing NDP entries (such as "ndp -s <int> <host> <hwaddr> pub") and remove them.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22545  
**Group Title:** GEN007780  
**Rule ID:** SV-38926r1\_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:**    
Determine if there are any 6to4 tunnels configured on the system.  
  
#ifconfig –a   
  
If there are any sit or cit adapters in the ifconfig listing, this is a finding.  
  
**Fix Text:**Remove the configuration for any 6to4 tunnels on the system.   
#ifconfig sit0 detach  
#rmdev -dl sit0  
  
#ifconfig cit0 detach  
#rmdev -dl cit0  
  
Set the startup script /etc/rc.net to call autoconf6 with the -6 argument to prevent setting up 6 to 4 tunnels   
  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22546  
**Group Title:** GEN007800  
**Rule ID:** SV-38927r1\_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:**    
Determine if any software providing Teredo is installed on the system. If so, this is a finding.  
  
Software providing the Teredo Tunneling Protocol is not currently available for the AIX platforms and therefore, is not applicable.  
  
If software is available or installed to provide the Teredo Tunneling Protocol on the system, this is a finding.  
  
**Fix Text:**Uninstall the Teredo software from the system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22547  
**Group Title:** GEN007820  
**Rule ID:** SV-38929r1\_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:**    
Determine if any IP tunnels are configured on the system.   
Check for IP tunnels.  
#lstun –a  
#ifconfig –a | grep –e gre –e gif -e cti -e sit  
If any tunnels are listed, this is a finding.  
  
  
**Fix Text:**Remove the configuration for any IP tunnels from the system.   
  
Remove tunnels listed with the lstun command.  
#rmtun –t <Tunnel id> -d  
  
Remove the tunneled IP interfaces.  
#ifconfig <if name> detach  
#rmdev –Rdl <if name>  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22548  
**Group Title:** GEN007840  
**Rule ID:** SV-38931r1\_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:**    
If the DHCP client is needed by the system, this is not applicable.  
  
Determine if the DHCP client is disabled.   
#ps –ef |grep dhcpcd  
If dhcpcd is running, this is a finding.  
  
  
**Fix Text:**Disable the system's DHCP client.   
  
Edit /etc/rc.tcpip, comment out the start of dhcpcd.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22549  
**Group Title:** GEN007850  
**Rule ID:** SV-38963r1\_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:**    
Determine if the system's DHCP client is configured to send dynamic DNS updates.  
  
#grep ^updateDNS /etc/dhcpc.opt /etc/dhcpc.ini  
  
If any lines are returned, this is a finding.  
  
  
**Fix Text:**Configure the system's DHCP client to not send dynamic DNS updates.   
  
Remove / comment updateDNS lines from the /etc/dhcpcd.ini and /etc/dhcpc.opt files.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22550  
**Group Title:** GEN007860  
**Rule ID:** SV-38825r1\_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:**    
Determine if the system is configured to ignore IPv6 ICMP redirect messages. If it is not, this is a finding.  
# /usr/sbin/no –o ipignoreredirects  
If the value returned is not 1, this is a finding.  
  
**Fix Text:**Configure the system to ignore IPv6 ICMP redirect messages.  
# /usr/sbin/no –p –o ipignoreredirects=1  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22551  
**Group Title:** GEN007880  
**Rule ID:** SV-38826r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007880  
**Rule Title:**The system must not send IPv6 ICMP redirects.  
  
**Vulnerability Discussion:**  ICMP redirect messages are used by routers to inform hosts that a more direct route exists for a particular destination. These messages contain information from the system's route table that could reveal portions of the network topology.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# /usr/sbin/no –o ipsendredirects  
If the value returned is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not send IPv6 ICMP redirects.   
# /usr/sbin/no –p –o ipsendredirects=0   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22552  
**Group Title:** GEN007900  
**Rule ID:** SV-38964r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007900  
**Rule Title:**The system must use an appropriate reverse-path filter for IPv6 network traffic, if the system uses IPv6.  
  
**Vulnerability Discussion:**  Reverse-path filtering provides protection against spoofed source addresses by causing the system to discard packets that have source addresses for which the system has no route or if the route does not point towards the interface on which the packet arrived. Depending on the role of the system, reverse-path filtering may cause legitimate traffic to be discarded and, therefore, should be used with a more permissive mode or filter, or not at all. Whenever possible, reverse-path filtering should be used.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system is configured to use reverse-path filtering.   
Examine the IPSec rules on the system.  
# lsfilt -a  
All systems must block inbound traffic destined to the loopback address from other network interfaces.   
  
Additionally, if the system is multihomed and the attached networks are isolated or perform symmetric routing, traffic with source addresses expected on one interface must be blocked when received on another interface.  
  
If filtering is not configured on the system, this is a finding.  
  
**Fix Text:**Configure the system to use reverse-path filtering using IP Sec filters.   
  
Add rules to block traffic with loopback network source addresses from being received on interfaces other than the loopback, such as other ethernet interfaces.  
  
Use smitty or genfilt command to block loopback address from network interfaces.  
#smitty ipsec6  
#genfilt –v6 –a D –s <source address> –m <source netmask> –d <destination address> –M <Destination mask> –c all –o any –O any -p 0 –P 0 –w I –l y –a en0  
  
If the system is multihomed and the attached networks are isolated or perform symmetric routing, add rules to block traffic with source addresses expected on one interface when received on another interface.  
  
#smitty ipsec6   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22553  
**Group Title:** GEN007920  
**Rule ID:** SV-38827r1\_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 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:**    
# /usr/sbin/no –o ip6srcrouteforward  
If the value returned is not 0, this is a finding.  
  
**Fix Text:**Configure the system so it does not forward IPv6 source-routed packets.   
# /usr/sbin/no –p –o ip6srcrouteforward=0   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22554  
**Group Title:** GEN007940  
**Rule ID:** SV-38828r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007940  
**Rule Title:**The system must not accept source-routed IPv6 packets.  
  
**Vulnerability Discussion:**  Source-routed packets allow the source of the packet to suggest routers forward the packet along a different path than configured on the router, which can be used to bypass network security measures. This requirement applies only to the handling of source-routed traffic destined to the system itself, not to traffic forwarded by the system to another, such as when IPv6 forwarding is enabled and the system is functioning as a router.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
# /usr/sbin/no –o ipsrcrouterecv  
If the value returned is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not accept source-routed IPv6 packets.   
# /usr/sbin/no –p –o ipsrcrouterecv=0  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23972  
**Group Title:** GEN007950  
**Rule ID:** SV-38829r1\_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:**    
# /usr/sbin/no –o bcastping  
If the value returned is not 0, this is a finding.  
  
**Fix Text:**Configure the system to not respond to IPv6 multicast ICMP ECHO\_REQUESTs.  
# /usr/sbin/no –p –o bcastping=0  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23953  
**Group Title:** GEN007960  
**Rule ID:** SV-28909r1\_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 preventing 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:**    
Consult vendor documentation concerning the ldd command. If the command provides protection from the execution of untrusted executables, this is not a finding.  
  
Determine the location of the system's ldd command.  
Procedure:  
# find / -name ldd  
If no file exists, this is not a finding.  
  
Check the permissions of the found ldd file.  
# ls -lL <path to ldd>  
  
If the file mode of the file is more permissive than 0000, this is a finding.  
  
**Fix Text:**Disable the ldd command by removing its permissions.  
  
Procedure:  
# chmod 0000 <path to ldd>   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-23828  
**Group Title:** GEN007970  
**Rule ID:** SV-38965r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN007970  
**Rule Title:**If the system is using LDAP for authentication or account information, the system must use a FIPS 140-2 validated cryptographic module (operating in FIPS mode) for protecting the LDAP connection.  
  
**Vulnerability Discussion:**  LDAP can be used to provide user authentication and account information, which are vital to system security. Cryptographic modules used by the system must be validated by the NIST CVMP as compliant with FIPS 140-2. Cryptography performed by unvalidated modules is viewed by NIST as providing no protection for the data.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCNR-1  
  
**Check Content:**    
Determine if the system uses LDAP authentication.   
  
#grep LDAP /etc/security/user  
If no results are returned, this is not applicable.  
  
Determine if the system uses a FIPS 140-2 validated cryptographic module (operating in FIPS mode) for protecting the LDAP connection. If it does not, this is a finding.  
  
**Fix Text:**Configure the system to use a FIPS 140-2 validated cryptographic module (operating in FIPS mode) for protecting the LDAP connection.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22556  
**Group Title:** GEN008000  
**Rule ID:** SV-38830r1\_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:**    
Check if the system is using LDAP authentication.  
  
#grep LDAP /etc/security/user  
If no lines are returned, this vulnerability is not applicable.  
  
Check if the useSSL option is enabled.  
#grep ^useSSL /etc/security/ldap/ldap.cfg  
If ‘yes’ is not the returned value, this is a finding.  
  
Verify a certificate is used for client authentication to the server.  
#grep –I ‘^ldapsslkeyf’ /etc/security/ldap/ldap.cfg  
If no line is found, this is a finding.  
  
List the certificate issuer with IBM GSK.  
#gsk7cmd –cert –list CA –db <certificate keyfile.kdb> -pw <Password>  
  
Make note of the client Key Label  
#gsk7cmd –cert –details –showOID –db <certificate key.kdb> -pw <Password> -label <Key Label>  
  
If the certificate is not issued by DoD PKI or a DoD-approved external PKI, this is a finding.  
  
  
**Fix Text:**Create a key database with DoD PKI or DoD-approved certificate.  
  
#gsk7cmd   
OR  
#ikeyman  
  
Edit /etc/security/ldap/ldap.conf and add or edit the ldapsslkeyf setting to reference a file containing a client certificate issued by DoD PKI or a DoD-approved external PKI.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22557  
**Group Title:** GEN008020  
**Rule ID:** SV-38966r1\_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 and this certificate has 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 LDAP authentication.  
#grep LDAP /etc/security/user  
If no lines are returned, this vulnerability is not applicable.  
  
Verify SSL is enabled.  
#grep ^useSSL /etc/security/ldap/ldap.cfg  
If ‘yes’ is not the returned value, this is a finding.  
  
Verify a server certificate is required and verified by the LDAP configuration.  
#grep –I ‘^ldapsslkeyf’ /etc/security/ldap/ldap.cfg  
Make note of the key database file location.  
  
#gsk7cmd –cert –list CA –db <certificate keyfile.kdb> -pw <Password>  
Make note of the Key Label  
#gsk7cmd –cert –details –showOID –db <certificate key.kdb> -pw <Password> -label <Key Label>  
  
THE IBM GSK Database should only have certificates for the client system and for the LDAP server.  
If more certificates are in the key database than the LDAP server and the client, this is a finding.  
  
**Fix Text:**Install a certificate signed by a DoD PKI or a DoD-approved external PKI .  
  
#gsk7cmd < or > ikeyman  
  
Remove un-needed CA certificates.  
#gsk7cmd < or > ikeyman   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22558  
**Group Title:** GEN008040  
**Rule ID:** SV-38967r1\_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:**    
AIX LDAP SSL uses a key exchange between the LDAP client and the LDAP server.   
  
Verify the LDAP server’s certificate for the client is valid and not revoked. If the clients certificate is expired or revoked, this is a finding.  
  
Check the LDAP client's certificate for the LDAP server certificate is valid. If the server certificate is not valid, this is a finding.  
  
**Fix Text:**Install a valid SSL certificate on the client.  
  
#gsk7cmd < or > ikeyman  
  
Export the client certificate and install the client certificate on the LDAP server.  
  
#gsk7cmd < or > ikeyman  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24384  
**Group Title:** GEN008050  
**Rule ID:** SV-38968r1\_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:**    
Examine the LDAP configuration file(s).   
  
#grep bindpw: /etc/security/ldap/ldap.cfg  
If the returned entry has an unencrypted password (not like “bindpwd:{DES}”) , this is a finding.   
If the LDAP configuration file contains an encrypted password accessible by regular users on the system, this is a finding.  
#ls –l /etc/security/ldap/ldap.cfg  
  
Check for unencrypted SSL keyfile password.  
#grep ‘^ldapsslkeypwd’ /etc/security/ldap/ldap.cfg  
If the returned entry has an unencrypted password (not like “ldapsslkeypwd:{DES}”) , this is a finding.   
  
**Fix Text:**Remove any passwords from LDAP configuration files.   
  
The bindpw (bind password) can be encrypted with the mksecldap command.   
#mksecldap  
  
Stash the SSL key database file with the gsk7cmd or ikeyman commands.  
#gsk7cmd < or > ikeyman  
  
Comment out the ldapsslpwd line to use stashed password. The password stash file must reside in the same directory as the SSL key database, and must have the same name as the key database, but with an extension of .sth instead of .kdb.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22559  
**Group Title:** GEN008060  
**Rule ID:** SV-38969r1\_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 /etc/security/ldap/ldap.cfg file.  
# ls -lL /etc/security/ldap/ldap.cfg  
  
If the mode of the file is more permissive than 0644, this is a finding.  
  
**Fix Text:**Change the permissions of the /etc/security/ldap/ldap.cfg file to 0664 or less permissive.  
  
# chmod 0644 /etc/security/ldap/ldap.cfg   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22560  
**Group Title:** GEN008080  
**Rule ID:** SV-38970r1\_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 /etc/security/ldap/ldap.cfg file.  
# ls -lL /etc/security/ldap/ldap.cfg  
  
If the file is not owned by root, this is a finding.  
  
**Fix Text:**Change the owner of the /etc/security/ldap/ldap.cfg file.  
  
# chown root /etc/security/ldap/ldap.cfg  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22561  
**Group Title:** GEN008100  
**Rule ID:** SV-38971r1\_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 ldap.cfg file.  
  
Procedure:  
# ls -lL /etc/security/ldap/ldap.cfg  
  
If the file is not group-owned by root, bin, security, sys, or system, this is a finding.  
  
**Fix Text:**Change the group owner of the /etc/security/ldap/ldap.cfg file to security, root, bin, sys, or system.  
  
Procedure:  
# chgrp security /etc/security/ldap/ldap.cfg   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22562  
**Group Title:** GEN008120  
**Rule ID:** SV-38972r1\_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 /etc/security/ldap/ldap.cfg file.  
  
Procedure:  
# aceget /etc/security/ldap/ldap.cfg   
Check to see if extended permissions are enabled.   
If extended permissions are enabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the /etc/security/ldap/ldap.cfg file.   
  
# acledit /etc/security/ldap/ldap.cfg   
Disable extended file permissions.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22563  
**Group Title:** GEN008140  
**Rule ID:** SV-38973r1\_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 the SSL Certificate database file and/or directory.  
  
# grep -i '^ldapsslkeyf' /etc/security/ldap/ldap.cfg  
  
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 SSL key database file or directory.  
  
# chown root <certpath>   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22564  
**Group Title:** GEN008160  
**Rule ID:** SV-38974r1\_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:**    
Check the group ownership of the SSL key database file.  
  
Determine the location of the SSL key database.  
# grep -i '^ldapsslkeyf' /etc/security/ldap/ldap.cfg  
  
Check the group ownership of the SSL key database file.  
# ls -lLa <ldap certificate file(s) or directories>  
  
If a certificate file or directory is not group-owned by root, bin, security, sys, or system, this is a finding.  
  
**Fix Text:**Change the group ownership of LDAP client SSL certificate database file to root, security, bin, sys, or system.  
  
Procedure:  
# chgrp system < certificate file >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22565  
**Group Title:** GEN008180  
**Rule ID:** SV-38975r1\_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 SSL certificate key database file and/or directory.  
  
Procedure:  
# grep -i '^ldapsslkeyf' /etc/security/ldap/ldap.cfg   
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 to 0644 or the directory to 0755 or less permissive.  
  
File Procedure:  
# chmod 0644 < SSL key database certpath >   
  
Directory Procedure:  
# chmod 0755 < SSL key database certpath >   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22566  
**Group Title:** GEN008200  
**Rule ID:** SV-38976r1\_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 SSL certificate key database file and/or directory.  
  
# grep -i '^ldapsslkeyf' /etc/security/ldap/ldap.cfg  
  
For each file or directory returned, check the permissions.  
  
# aclget < certpath >  
# aclget < certpath >/< certfile >  
If extended file permissions are enabled, this is a finding.  
  
**Fix Text:**Remove the extended ACL from the SSL certificate key database file.   
  
# acledit < certpath >   
# acledit < certpath >/<certfile >  
Disable the extended file permissions.  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22567  
**Group Title:** GEN008220  
**Rule ID:** SV-38977r1\_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:**    
This check does not apply to AIX. The AIX LDAP SSL implementation uses IBM’s key management routines. The LDAP client configuration loads a key database including CA certificates and host certificates in a \*.key database file. Individual files like the tls\_cert, tls\_cacert, tls\_checkpeer, tls\_crlcheck, and tls\_key are not specified in the AIX LDAP client setup.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22568  
**Group Title:** GEN008240  
**Rule ID:** SV-38978r1\_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:**    
This check does not apply to AIX. The AIX LDAP SSL implementation uses IBM’s key management routines. The LDAP client configuration loads a key database including CA certificates and host certificates in a \*.key database file. Individual files like the tls\_cert, tls\_cacert, tls\_checkpeer, tls\_crlcheck, and tls\_key are not specified in the AIX LDAP client setup.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22569  
**Group Title:** GEN008260  
**Rule ID:** SV-38979r1\_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:**    
This check does not apply to AIX. The AIX LDAP SSL implementation uses IBM’s key management routines. The LDAP client configuration loads a key database including CA certificates and host certificates in a \*.key database file. Individual files like the tls\_cert, tls\_cacert, tls\_checkpeer, tls\_crlcheck, and tls\_key are not specified in the AIX LDAP client setup.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22570  
**Group Title:** GEN008280  
**Rule ID:** SV-38980r1\_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:**    
This check does not apply to AIX. The AIX LDAP SSL implementation uses IBM’s key management routines. The LDAP client configuration loads a key database including CA certificates and host certificates in a \*.key database file. Individual files like the tls\_cert, tls\_cacert, tls\_checkpeer, tls\_crlcheck, and tls\_key are not specified in the AIX LDAP client setup.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22571  
**Group Title:** GEN008300  
**Rule ID:** SV-38981r1\_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:**    
This check does not apply to AIX. The AIX LDAP SSL implementation uses IBM’s key management routines. The LDAP client configuration loads a key database including CA certificates and host certificates in a \*.key database file. Individual files like the tls\_cert, tls\_cacert, tls\_checkpeer, tls\_crlcheck, and tls\_key are not specified in the AIX LDAP client setup.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22572  
**Group Title:** GEN008320  
**Rule ID:** SV-38982r1\_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, 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:**    
This check does not apply to AIX. The AIX LDAP SSL implementation uses IBM’s key management routines. The LDAP client configuration loads a key database including CA certificates and host certificates in a \*.key database file. Individual files like the tls\_cert, tls\_cacert, tls\_checkpeer, tls\_crlcheck, and tls\_key are not specified in the AIX LDAP client setup.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22573  
**Group Title:** GEN008340  
**Rule ID:** SV-38983r1\_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:**    
This check does not apply to AIX. The AIX LDAP SSL implementation uses IBM’s key management routines. The LDAP client configuration loads a key database including CA certificates and host certificates in a \*.key database file. Individual files like the tls\_cert, tls\_cacert, tls\_checkpeer, tls\_crlcheck, and tls\_key are not specified in the AIX LDAP client setup.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22574  
**Group Title:** GEN008360  
**Rule ID:** SV-38984r1\_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:**    
This check does not apply to AIX. The AIX LDAP SSL implementation uses IBM’s key management routines. The LDAP client configuration loads a key database including CA certificates and host certificates in a \*.key database file. Individual files like the tls\_cert, tls\_cacert, tls\_checkpeer, tls\_crlcheck, and tls\_key are not specified in the AIX LDAP client setup.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22575  
**Group Title:** GEN008380  
**Rule ID:** SV-26250r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN008380  
**Rule Title:**A root kit check tool must be run on the system at least weekly.  
  
**Vulnerability Discussion:**  Root kits are software packages designed to conceal the compromise of a system from the SA. Root kit checking tools examine a system for evidence that a root kit is installed. Dedicated root kit detection software or root kit detection capabilities included in anti-virus packages may be used to satisfy this requirement.  
  
**Responsibility:**  System Administrator  
**IAControls:**  DCSL-1  
  
**Check Content:**    
Ask the SA if a root kit check tool is run on the system weekly. If this is not performed, this is a finding.  
  
**Fix Text:**Create an automated job or establish a site-defined procedure to check the system weekly with a root kit check tool.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22576  
**Group Title:** GEN008420  
**Rule ID:** SV-38831r1\_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:**    
Running the sedmgr command without any options will show the settings currently in effect.   
  
#sedmgr  
  
If the value returned for the sedmgr mode is off, this is a finding.  
  
**Fix Text:**Configure the system to use any available memory address randomization techniques. Recommended settings are either to enable stack execution disablement for all suid files or select system executables.   
  
Set sedmgr to enforce on selected files and terminate processes violating stack execution boundaries.  
#sedmgr –m select –o off  
  
OR  
  
Set sedmgr to enforce on setid files and terminate processes violating stack execution boundaries.  
#sedmgr –m setidfiles –o off  
  
After a global system change to the sed, the system should be rebooted.  
#shutdown -Fr   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22577  
**Group Title:** GEN008440  
**Rule ID:** SV-38832r1\_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:**    
Determine if the system uses automated file system mounting tools (such as autofs or automount). AIX can use automount facility.  
  
#ps -ef | grep -v grep | grep automount   
  
If the automount process is running, this is a finding.  
  
  
  
**Fix Text:**Disable the automated file system mounting tools.  
Empty the /etc/auto\_master file   
  
kill automount  
kill < pid of automount >   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22578  
**Group Title:** GEN008460  
**Rule ID:** SV-38833r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008460  
**Rule Title:**The system must have USB disabled unless needed.  
  
**Vulnerability Discussion:**  USB is a common computer peripheral interface. USB devices may include storage devices that could be used to install malicious software on a system or exfiltrate data.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
AIX has server USB drivers installed, such as keyboard, mount, and mass media drivers.  
  
Determine if the system has USB enabled.  
# lsdev -C | grep usb  
#lslpp –l | usb  
  
If usb filesets are installed on the system, USB is enabled and this is a finding.  
  
**Fix Text:**Disable USB devices on the system. Use SMIT to remove the following filesets.  
  
devices.usbif.\*  
  
# smitty remove   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22579  
**Group Title:** GEN008480  
**Rule ID:** SV-38834r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008480  
**Rule Title:**The system must have USB Mass Storage disabled unless needed.  
  
**Vulnerability Discussion:**  USB is a common computer peripheral interface. USB devices may include storage devices that could be used to install malicious software on a system or exfiltrate data.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system uses USB mass storage, this is not applicable.  
#lslpp –l | grep –e devices.usbif.010100 –e devices.usbif.08025 –e devices.usbif.080400  
If these filesets are installed on the system, USB mass storage is enabled and this is a finding.  
  
  
  
**Fix Text:**Disable USB mass storage on the system by using SMIT to remove the following filesets.  
devices.usbif.010100  
devices.usbif.08025002  
devices.usbif.080400   
  
# smitty remove   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22580  
**Group Title:** GEN008500  
**Rule ID:** SV-38930r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008500  
**Rule Title:**The system must have IEEE 1394 (Firewire) disabled unless needed.  
  
**Vulnerability Discussion:**  Firewire is a common computer peripheral interface. Firewire devices may include storage devices that could be used to install malicious software on a system or exfiltrate data.  
  
**Documentable:** YES   
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
If the system needs IEEE 1394, this is not applicable.  
  
AIX does not currently support IEEE 1394 (Firewire).  
  
Determine if IEEE 1394 is enabled on the system. If so, this is a finding.  
  
**Fix Text:**Disable IEEE 1394 on the system.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22582  
**Group Title:** GEN008520  
**Rule ID:** SV-38961r1\_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.  
  
# lsfilt  
# smitty ipsec4  
  
If local firewall is not configured and running, this is a finding.  
  
  
**Fix Text:**Configure the system to use a local firewall.   
Use SMIT to load the IPSEC filesets.  
#smit install  
  
Use SMIT to configure filters.  
#smit ipsec4   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22583  
**Group Title:** GEN008540  
**Rule ID:** SV-38985r1\_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:**    
Determine if the system's local firewall implements a deny-all, allow-by-exception policy.   
  
View the firewall (filter rules) with smit or lsfilt commands.  
  
# smitty ipsec4  
  
# lsfilt  
  
If there is not a deny-all, allow-by-exception policy, this is a finding.  
  
**Fix Text:**Configure the system's local firewall to implement a deny-all,   
allow-by-exception policy.  
  
Firewall rules can be added and activated with SMIT ipsec4 or genfilt command.  
  
#smitty ipsec4  
  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-1013  
**Group Title:** Disable Boot From Removable Media  
**Rule ID:** SV-38835r1\_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 that could 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.   
#bootlist –m normal –o  
The returned values should be hdisk{x}. If the system is setup to boot from a non-hard disk device, this is a finding.   
  
Additionally, ask the SA if the machine is setup for multi-boot in the SMS application. If multi-boot is enabled, the firmware will stop at boot time and request which image to boot from the user. If multi-boot is enabled, this is a finding.  
  
**Fix Text:**Configure the system to only boot from system startup media.  
  
#bootlist –m normal hdisk< x >  
  
Set multi-boot to off in the SMS application   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4246  
**Group Title:** GEN008620  
**Rule ID:** SV-38836r1\_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:**    
Ask the SA if a password has been given to the Service processors ADMIN account. If a password has not been assigned to the service processor, this is a finding.  
  
**Fix Text:**Access the system's service processor. Set a supervisor/administrator password if one has not been set. Disable a user-level password if one has been set.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4247  
**Group Title:** Boot Diskette  
**Rule ID:** SV-38837r1\_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:**    
Check the servers boot lists for the normal, service, both, or prevboot modes.  
  
#bootlist –m <mode> –o  
Ensure hdisk{x} is the only devices listed. If boot devices such as cd{x}, fd{x}. rmt{x}, ent{x} are used, this is a finding.  
  
**Fix Text:**Configure the system to use a bootloader installed on fixed media.   
#bootlist –m normal hdisk0  
#bootlist –m service hdisk0  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-4255  
**Group Title:** /boot partition   
**Rule ID:** SV-4255r4\_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.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24624  
**Group Title:** GEN008710  
**Rule ID:** SV-38986r1\_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:**    
AIX stores the Service processor password in firmware, not on a files ystem and it is not a check.  
  
**Fix Text:**No fix necessary. The boot loaders password is not stored on a filesystem.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22585  
**Group Title:** GEN008740  
**Rule ID:** SV-38987r1\_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:**    
AIX stores the Service processor password in firmware, not on a filesystem and it is not a check.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22586  
**Group Title:** GEN008760  
**Rule ID:** SV-38988r1\_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:**    
AIX stores the Service processor password in firmware, not on a filesystem and it is not a check.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22587  
**Group Title:** GEN008780  
**Rule ID:** SV-38989r1\_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:**    
AIX stores the Service processor password in firmware, not on a filesystem and it is not a check.  
  
**Fix Text:**No fix necessary.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22588  
**Group Title:** GEN008800  
**Rule ID:** SV-26263r1\_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:**    
Determine if the system package management tool cryptographically verifies the authenticity of packages during installation. If it does not, this is a finding.  
  
**Fix Text:**If possible, configure the system package management tool to cryptographically verify the authenticity of packages during installation.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-22589  
**Group Title:** GEN008820  
**Rule ID:** SV-38962r1\_rule  
**Severity: CAT III**  
**Rule Version (STIG-ID):** GEN008820  
**Rule Title:**The system package management tool must not automatically obtain updates.  
  
**Vulnerability Discussion:**  System package management tools can obtain a list of updates and patches from a package repository and make this information available to the SA for review and action. Using a package repository outside of the organization's control presents a risk that malicious packages could be introduced.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Determine if the system package management tool is configured to automatically obtain updated packages. If it is, this is a finding.  
AIX does not automatically obtain updates.  
  
  
**Fix Text:**Configure the system package management tool not to automatically obtain updates.   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-24347  
**Group Title:** GEN009120  
**Rule ID:** SV-39317r1\_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 with 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 IBM documentation to determine the procedures necessary for configuring CAC authentication through PKI. Configure all accounts required by policy to use CAC authentication.   
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29500  
**Group Title:** GEN009140  
**Rule ID:** SV-38704r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009140  
**Rule Title:**The system must not have the chargen service active.  
  
**Vulnerability Discussion:**  When contacted, chargen responds with some random characters. When contacted via UDP, it   
will respond with a single UDP packet. When contacted via TCP, it will continue spewing characters until the client closes the connection. An easy attack is 'ping-pong' in which an attacker spoofs a packet between two machines running chargen. This will cause them to spew characters at   
each other, slowing the machines down and saturating the network. The chargen service is unnecessary and provides an opportunity for DoS attack.   
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active TCP and UDP chargen service entries.  
  
# grep chargen /etc/inetd.conf |grep -v \#  
  
If the chargen service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the chargen service line for both udp and tcp protocols.  
  
Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29501  
**Group Title:** GEN009160  
**Rule ID:** SV-38705r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009160  
**Rule Title:**The system must not have the Calendar Manager Service Daemon (CMSD) service active.  
  
**Vulnerability Discussion:**  The CMSD service for CDE is an unnecessary process that runs a root and increases attack vector of the system. Buffer overflow attacks against the CMSD process can potentially give access to the system.  
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active CMSD service.  
  
# grep cmsd /etc/inetd.conf |grep -v \#  
  
If the CMSD service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the CMSD service.   
  
Restart the inetd service.   
#refresh –s inetd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29502  
**Group Title:** GEN009180  
**Rule ID:** SV-38706r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009180  
**Rule Title:**The system must not have the tool-talk database server (ttdbserver) service active.  
  
**Vulnerability Discussion:**  The ttdbserver service for CDE is an unnecessary service that runs as root and might be compromised.  
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active ttdbserver service.  
  
# grep ttdbserver /etc/inetd.conf |grep -v \#  
  
If the ttdbserver service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out ttdbserver service line.   
  
Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29503  
**Group Title:** GEN009190  
**Rule ID:** SV-38707r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009190  
**Rule Title:**The system must not have the comsat service active.  
  
**Vulnerability Discussion:**  The comsat daemon notifies users on incoming email. This is an unnecessary service and is vulnerable to a flood attack. Running unnecessary services increases the attack vector of the system.  
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active comsat service.  
  
#grep comsat /etc/inetd.conf | grep -v \#  
  
If the comsat service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out comsat service line. Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29504  
**Group Title:** GEN009200  
**Rule ID:** SV-38708r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009200  
**Rule Title:**The system must not have the daytime service active.  
  
**Vulnerability Discussion:**  The daytime service runs as root from the inetd daemon and can provide an opportunity for Denial of Service PING or PING-PONG attacks. The daytime service is unnecessary and it increases the attack vector of the system.  
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for TCP and UDP daytime service.  
  
#grep daytime /etc/inetd.conf | grep -v \#  
  
If the daytime service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out daytime service lines for both TCP and UDP protocols.   
Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29505  
**Group Title:** GEN009210  
**Rule ID:** SV-38709r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009210  
**Rule Title:**The system must not have the discard service active.  
  
**Vulnerability Discussion:**  The discard service runs as root from the inetd server and can be used in Denial of Service attacks. The discard service is unnecessary and it increases the attack vector of the system.  
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for TCP and UDP discard service entries.  
  
#grep discard /etc/inetd.conf | grep -v \#  
  
If the discard service is active, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the discard service line for both TCP and UDP protocols.   
Restart the inetd service.  
#refresh -s inetd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29506  
**Group Title:** GEN009220  
**Rule ID:** SV-38710r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009220  
**Rule Title:**The system must not have dtspc service active.  
  
**Vulnerability Discussion:**  This service is started automatically by the inetd daemon with root permission in response to a CDE client requesting a process to be started on the daemon’s host system. Running the dtscp service is unnecessary and it increases the attack vector of the system.  
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf for the dtspc service.  
  
#grep dtspc /etc/inetd.conf | grep -v \#  
  
If the dtspci service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out dtspc service line.   
  
Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29507  
**Group Title:** GEN009230  
**Rule ID:** SV-38711r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009230  
**Rule Title:**The system must not have the echo service active.  
  
**Vulnerability Discussion:**  The echo service can be used in Denial of Service or SMURF attacks. It can also used at someone else to get through a firewall or start a data storm. The echo service is unnecessary and it increases the attack vector of the system.  
  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf for TCP and UDP echo service entries.  
  
#grep echo /etc/inetd.conf | grep -v \#  
  
If the echo service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the echo service lines for both TCP and UDP.   
  
Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29508  
**Group Title:** GEN009240  
**Rule ID:** SV-38712r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009240  
**Rule Title:**The system must not have Internet Message Access Protocol (IMAP) service active.  
  
**Vulnerability Discussion:**  The IMAP service should not be running unless the system is acting as a mail server for client connections. Running unnecessary services increases the attack vector on the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active IMAP service.  
  
#grep imapd /etc/inetd.conf | grep -v \#  
  
If the IMAP service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the imap2 service line.   
  
Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29509  
**Group Title:** GEN009250  
**Rule ID:** SV-38713r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009250  
**Rule Title:**The system must not have the PostOffice Protocol (POP3) service active.  
  
**Vulnerability Discussion:**  The POP3 service is only needed if the server is acting as a mail server and clients are using applications that only support POP3. Users' ids and passwords are sent in plain text to the POP3 service. If mail client access is needed, consider using IMAP or SSL enabled POP3.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the '/etc/inetd.conf' file for active POP3 service.  
  
#grep pop3 /etc/inetd.conf | grep -v \#  
  
If the POP3 service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out POP3 the service line. Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29510  
**Group Title:** GEN009260  
**Rule ID:** SV-38714r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009260  
**Rule Title:**The system must not have the talk or ntalk services active.  
  
**Vulnerability Discussion:**  The talk and ntalk commands allow users on the same or different systems on converse. The talk daemons are started from the inetd process and run as root. These unnecessary processes increase the attack vector of the system and may cause Denial of Service by scrambling the users display.   
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for talk and ntalk services.  
  
#grep talk /etc/inetd.conf | grep -v \#  
  
If any TCP or UDP talk services are enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out TCP and UDP for the talk service.   
Edit /etc/inetd.conf and comment out TCP and UIDP for the ntalk service.  
  
Restart the inetd service.   
#refresh –s inetd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29511  
**Group Title:** GEN009270  
**Rule ID:** SV-38715r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009270  
**Rule Title:**The system must not have the netstat service active on the inetd process.  
  
**Vulnerability Discussion:**  The netstat service can potentially give out network information on active connections if it is running. The information given out can aid in an attack and weaken the systems defensive posture.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf for active netstat service.  
  
grep netstat /etc/inetd.conf | grep -v \#  
  
If the netstat service is active, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the netstat service line.   
  
Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29512  
**Group Title:** GEN009280  
**Rule ID:** SV-38716r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009280  
**Rule Title:**The system must not have the PCNFS service active.   
  
**Vulnerability Discussion:**  The PCNFS service predates Microsoft’s SMB specifications. If a similar service is needed to share files from a Windows based OS to a UNIX based OS, consider SAMBA.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active PCNFS service.  
  
#grep pcnfsd /etc/inetd.conf | grep -v \#  
  
If the PCNFS service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out the PCNFS service line. Restart the inetd service.   
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29513  
**Group Title:** GEN009290  
**Rule ID:** SV-38717r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009290  
**Rule Title:**The system must not have the systat service active.  
  
**Vulnerability Discussion:**  The systat daemon allows remote users to see the running process and who is running them. This may aid in information collection for an attack and weaken the security posture of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active systat service.  
  
#grep systat /etc/inetd.conf | grep -v \#  
  
If the systat service is enabled, this is a finding.  
  
**Fix Text:**Edit /etc/inetd.conf and comment out systat the service line.   
  
Restart the inetd service.   
  
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29514  
**Group Title:** GEN009300  
**Rule ID:** SV-38718r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009300  
**Rule Title:**The /etc/inetd time service must not be active on the system on the inetd daemon.   
  
**Vulnerability Discussion:**  The time service is an internal inetd function is used by the rdate command. This service is sometimes used to synchronize clocks at boot time. The service is outdated. Use the ntpdate command instead.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for TCP and UDP time service.  
  
grep time /etc/inetd.conf | grep -v daytime | grep -v \#  
  
If the time service is enabled, this is a finding.  
  
**Fix Text:**Edit the /etc/inetd.conf file and comment out the time service line.   
  
Restart the inetd service.   
#refresh –s inetd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29515  
**Group Title:** GEN009310  
**Rule ID:** SV-38719r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009310  
**Rule Title:**The system must not have the rusersd service active.  
  
**Vulnerability Discussion:**  The rusersd daemon gives out a list of current uses on the system. The rusersd daemon is unnecessary and it increases the attack vector of the system by providing information on the current users of the system.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active rusersd service.  
  
#grep rusersd /etc/inetd.conf | grep -v \#  
  
If the rusersd service is enabled, this is a finding.  
  
**Fix Text:**Edit the /etc/inetd.conf file and comment out the rusersd service line.   
  
Restart the inetd service.   
  
#refresh –s inetd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29516  
**Group Title:** GEN009320  
**Rule ID:** SV-38720r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009320  
**Rule Title:**The system must not have the sprayd service active.  
  
**Vulnerability Discussion:**  The sprayd service is sometimes used for network and nfs troubleshooting. The spray service can be used for both buffer overflow and Denial of Service attacks by saturating the network. The sprayd daemon is an unnecessary service.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active sprayd service.  
  
# grep sprayd /etc/inetd.conf | grep -v \#  
  
If the sprayd service is enabled, this is a finding.  
  
**Fix Text:**Edit the /etc/inetd.conf file and comment out the sprayd service line.   
  
Restart the inetd service.   
  
#refresh –s inetd   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29517  
**Group Title:** GEN009330  
**Rule ID:** SV-38721r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009330  
**Rule Title:**The system must not have the rstatd service active.  
  
**Vulnerability Discussion:**  The rstatd can give out information on the running system such as the CPU usage, the system uptime, its network usage and other system information that could potentially aid in an attack. The rstatd service is unnecessary and it weakens the defensive posture of the system. If systems monitoring is needed, use a third party tool or snmp.   
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check the /etc/inetd.conf file for active rstatd service.  
  
#grep rstatd /etc/inetd.conf | grep -v \#  
  
If the rstatd service is enabled, this is a finding.  
  
**Fix Text:**Edit the /etc/inetd.conf file and comment out the rstatd service line.   
  
Restart the inetd service.   
  
#refresh –s inetd  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
**Group ID (Vulid):** V-29518  
**Group Title:** GEN009340  
**Rule ID:** SV-38722r1\_rule  
**Severity: CAT II**  
**Rule Version (STIG-ID):** GEN009340  
**Rule Title:**Xserver login managers must not be running unless needed for X11 session management.  
  
**Vulnerability Discussion:**  Running Xservers and X-login managers when not needed for X11 session management increases the attack vector of the system by running unnecessary services.  
  
**Responsibility:**  System Administrator  
**IAControls:**  ECSC-1  
  
**Check Content:**    
Check to see if X display login managers are running.  
  
#cat /etc/inittab | grep –e /etc/rc.dt –e xdm  
  
If any X server login managers are running, ask the SA if they are necessary for the operation of the system.   
  
If there is unnecessary X server login managers running, this is a finding.  
  
  
  
**Fix Text:**Comment out or remove the X login servers from the /etc/inittab file.  
  
#vi /etc/inittab   
  
Refresh the init process  
  
# init q  
  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**UNCLASSIFIED**