|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1.2 | ALM | /var/pam.d/system-auth | Login failures must be reviewed. | Any repeated login failures must  be investigated as these attempts may result from unauthorized or malicious behavior attempting to  compromise the machine. | Open /etc/pam.d/system-auth file:  # vi /etc/pam.d/system-auth  Append following two pam\_tally.so modules:  auth required pam\_tally.so no\_magic\_root  account required pam\_tally.so deny=5 no\_magic\_rootlock\_time=180 | High |

ln -s /lib64/security/pam\_tally2.so /lib64/security/pam\_tally.so

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1.3 | ALM | 777 files | Systems must be scanned periodically for  world-writable files. | These World Writable files pose  a great risk because they can be  re-written by Hackers to gather information, set off trojan  processes and gain control of the  system. | Use Scripted tools or  manually scan the OS team’s responsible filesystemsfor world-writablefiles with the commands:  find / -type f –perm –o+w-mount -print  find /usr-type f –perm –o+w-mount -print  find /var-type f –perm –o+w-mount -print  find /opt -type f –perm –o+w-mount -print  find /home1 -type f –perm –o+w-mount –print | Medium | Application Configuration and Specification |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3.2 | File System Access  and Management | /tmp | Permissions on the  /tmpand /var/tmp  directories must be set properly to allow multiple user access but prevent users from deleting each other's files. Access permissions must also be configured properly to prevent a vulnerbility. | Permissions on the /tmpand  /var/tmpdirectories must allow  all users to read and write to the  directory without being able to  delete each other's files. There is  also a race condition that exists  in pswhich allows local users to  gain root access if permissions  are set incorrectly on /tmpand  /var/tmp | Chmod the file  permissions to 1777 on  the /tmp and /var/tmp  directories. | Low |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File System Access  and Management | cron  at | Cronand at programs  owned by deactivated  users must be deleted. | Dormant user accounts increase  the risk that unauthorized users  could potentially use these  accounts to gain access to the  system by modifying scheduled  jobs to perform additional  functions. | The system administrator must  remove all jobs associated with the deactivated user that were previously submitted using batch queues, third party scheduling software, the at program or cron.  System admin should remove cronand associate or at files for that user located in:  **/var/spool/cron** | Low |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File System Access  and Management | umask | The default settings for user file creation must be user read,writeand execute, group read. Whenever possible world access must be denied.  Default file creation  for the root user must  be set to a secure  value. | Umasksettings, which are not  secure, increase the risk that  unauthorized users could  potentially gain access to files  created by other users.  In order to protect processes spawned by root, the file security values must be consistently secure. | Set the default global umaskto 022.  This could be achieved by adding an entry of umask022 to the  /etc/profile file or UMASK=022 to  /etc/default/login.  The /etc/profile and the root .profile or .login must contain the statement umask022. This will result in all new files created by root having file permissions of rwxr-x---. | Low |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Services and Network  Configuration | sshd | | The sshdaemon, like  any other remote access mechanism must be configured to not permit direct root access. | | Any system access that does not  enforce accountability is  considered a vulnerability. A  malicious person could access a  system and there might not be  enough information retained to  account for who performed the  malicious actions. | | The following entry must be  in the; /etc/ssh/sshd\_config:  PermitRootLoginno  or  PermitRootLoginwithout password with PKI implementation. | | High | |
| and Network  Configuration | | sftp | | System Configuration | | The .netrcfile contains data for logging in to a remote host over the network for file transfers by sftp. This file resides in the user's home directory on the machine initiating the file transfer. It is required that netrcnot be used. | | Users must not have .netrcfiles in their home directory. If there is need for a .netrcthe permissions must be set to 400 to disallow read access by group and others | | high | | Enable by granted exception basis only. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Services and Network  Configuration | tftpservice | The tftpservice must be disabled. | The tftpservice allows unauthenticated access to a  system and lets users put files on  and get files from the system. A  system with tftpenabled can be  used as a depot for the unauthorized transfer of information. | Make sure the following line is in the /etc/xinetd.d/tftpfile:  disable = yes | High | Kick Start Servers are exempted.  Boot Servers and Network management servers. |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Num** | **Function** | **Specific** | **Control** | **Justification** | **Compliance** | **Priority** | **Comments** |
| 1.3 | ALM | 777 files | Systems must be scanned periodically for  world-writable files. | These World Writable files pose  a great risk because they can be  re-written by Hackers to gather information, set off trojan  processes and gain control of the  system. | Use Scripted tools or  manually scan the OS team’s responsible filesystemsfor world-writablefiles with the commands:  find / -type f –perm –o+w-mount -print  find /usr-type f –perm –o+w-mount -print  find /var-type f –perm –o+w-mount -print  find /opt -type f –perm –o+w-mount -print  find /home1 -type f –perm –o+w-mount –print | Medium | Application Configuration and Specification |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3.2 | File System Access  and Management | /tmp | Permissions on the  /tmpand /var/tmp  directories must be set properly to allow multiple user access but prevent users from deleting each other's files. Access permissions must also be configured properly to prevent a vulnerbility. | Permissions on the /tmpand  /var/tmpdirectories must allow  all users to read and write to the  directory without being able to  delete each other's files. There is  also a race condition that exists  in pswhich allows local users to  gain root access if permissions  are set incorrectly on /tmpand  /var/tmp | Chmod the file  permissions to 1777 on  the /tmp and /var/tmp  directories. | Low |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File System Access  and Management | cron  at | Cronand at programs  owned by deactivated  users must be deleted. | Dormant user accounts increase  the risk that unauthorized users  could potentially use these  accounts to gain access to the  system by modifying scheduled  jobs to perform additional  functions. | The system administrator must  remove all jobs associated with the deactivated user that were previously submitted using batch queues, third party scheduling software, the at program or cron.  System admin should remove cronand associate or at files for that user located in:  **/var/spool/cron** | Low |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| File System Access  and Management | SUID  SGID | All SUID and SGID  programs must be  inventoried and any  unauthorized  programs removed. | The SUID bit, when set to 0,  allows the user executing the  program or script to temporarily  assume the rights of the file  owner (often root). This increases the risk that unauthorized users could  potentially gain privileged access to the system by executing these programs or scripts and terminating them while executing. | The system administrator must  maintain a list of all approved SUID and SGID files available on the system and periodically run the checkuid0 command to compare the output of this program to the baseline file. Any additions to the list must be investigated, and if legitimate, must be added to the baseline file. The initial list must be generated when the machine is ready to be put into production with the following commands:  (SUID) find / -type f -  perm -4000 –print  (SGID) find / -type f -  perm -2000 –print | Medium | Application Configuration / Specification |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| File System Access  and Management | SUID  SGID | SUID and SGID  programs must not  call other programs or  allow shell access. | SUID and SGID programs  which call other programs, such  as editors, may allow an  unauthorized user access to the  shell from within the called  program. | The system  administrator must  review all newly  created and installed  SUID and SGID  programs to verify that  the programs do not  allow access to the  shell. | Medium | Application Configuration / Specification |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| File System Access  and Management | system binaries | Set permissions for  key system files  under /, /bin, /kernel, /boot, /proc, /lib, /platform, /usr,  /etc,/usr/bin, /usr/lib  and /usr/sbinto a  secure setting. | Unauthorized users must not be  given access to key system  directories such as those  contained in /, /bin, /kernel, /boot, /proc, /lib, /platform, /usr, /etc, /usr/bin,  /usr/lib and /usr/sbin(except for  /tmp, /usr/tmp). | The system administrator must maintain the permissions on all directories under /, /bin, /kernel, /boot, /proc, /lib, /platform, /usr, /etc, /usr/bin /usr/lib and /usr/sbin(except for /tmpand /usr/tmp) to be at least as secure as the vendor recommended ownership and permissions. No file under /etc, for instance, needs to be group-writable. System administrators must issue the command chmod–R g-w /etc | Medium | Please refer to “CI baseline files and directory settings” for minimum system requirements. This is a separate document that can change based off of OS revision. |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| File System Access  and Management | umask | The default settings for user file creation must be user read,writeand execute, group read. Whenever possible world access must be denied.  Default file creation  for the root user must  be set to a secure  value. | Umasksettings, which are not  secure, increase the risk that  unauthorized users could  potentially gain access to files  created by other users.  In order to protect processes spawned by root, the file security values must be consistently secure. | Set the default global umaskto 022.  This could be achieved by adding an entry of umask022 to the  /etc/profile file or UMASK=022 to  /etc/default/login.  The /etc/profile and the root .profile or .login must contain the statement umask022. This will result in all new files created by root having file permissions of rwxr-x---. | Low |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Services and Network  Configuration | ftp/sftp | FTP must be disabled on all LINUX machines. | FTP is an insecure file transfer protocol that does not encrypt traffic between systems. SFTP should be used for file transfer as it fully encrypts traffic before sending over the network. | By default FTP is not enabled on LINUX. To ensure that that sftpis enabled login to the server as the root useridand edit the files:  /etc/ssh/ssh\_config  And ensure that the following line is present:  Subsystem sftp/usr/libexec/openssh/sftp-server | Medium | FTP is not NYL  Standard practice.  Enable by granted exception basis only |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Services and Network  Configuration | sshd | The sshdaemon, like  any other remote access mechanism must be configured to not permit direct root access. | Any system access that does not  enforce accountability is  considered a vulnerability. A  malicious person could access a  system and there might not be  enough information retained to  account for who performed the  malicious actions. | The following entry must be  in the; /etc/ssh/sshd\_config:  PermitRootLoginno  or  PermitRootLoginwithout password with PKI implementation. | High |