**Linux Cloud Servers**

**Hardening Guidelines**

# **Notice**

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by Genpact, nor is this document (in whole or in part) to be reproduced or furnished to third parties or made public without the prior express written permission of Genpact.

# **Version Control**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Released on** | **Change** | **Author** | **Approver/Owner** | **Effective Date** |
| 1.0 | 12-08-2016 | Document Creation | Rohit Kohli | Amit Kohli | 11-08-2017 |
| 1.1 | 20-05-2017 | Review, no update | Awinash Goswami | Paramjit Rekhi | 19-05-2018 |
| 1.2 | 07-06-2018 | Review, AWS controls updated | Awinash Goswami | Paramjit Rekhi | 06-06-2019 |

# **Viewership**

SMG-Sun SMEs, Linux and team members, Compliance teams, Poles SPOC

*CONTENTS*

[Notice 1](#_Toc458001192)

[Version Control 1](#_Toc458001193)

[Viewership 2](#_Toc458001194)

[Abbreviations 2](#_Toc458001195)

[Objective 3](#_Toc458001196)

[Scope 3](#_Toc458001197)

[Stake holders 3](#_Toc458001198)

[Definitions 3](#_Toc458001199)

[Process Map 3](#_Toc458001200)

[Detection 5](#_Toc458001201)

[Incidence Logging/escalation 5](#_Toc458001202)

[Procedure: 5](#_Toc458001203)

[Password and account lockout policy 5](#_Toc458001204)

[Auditing Parameters 6](#_Toc458001205)

[Event log Parameters 7](#_Toc458001206)

[User account control & Security options 8](#_Toc458001207)

[Additional Hardening controls 10](#_Toc458001208)

[Windows Server Services Parameters 11](#_Toc458001209)

[Control Mechanisms 15](#_Toc458001210)

[Exception Handling 15](#_Toc458001211)

[Escalation Matrix 15](#_Toc458001212)

[Success Measure 15](#_Toc458001213)

[Potential Risk points 15](#_Toc458001214)

[RACI Matrix 15](#_Toc458001215)

# **Abbreviations**

* SMG – Server Management Group
* OS – Operating System
* InfoSec – Information Security
* ISS – Internet Security Systems

# 

# **Objective**

The objective of this document is to establish procedure for hardening all Windows servers of the Genpact managed domains.

# **Scope**

All Linux, Unix, and Solaris systems in Genpact managed Domains.

# **Stake holders**

1. InfoSec Team
2. SMG-Sun Lead
3. SMG-Sun SPOC
4. All poles Sun, Linux SPOC
5. Datacenter teams

# **Definitions**

NONE

**Guidelines**

* [Genpact Information Security Policy](http://home.intranet.genpact.com/portal/Infosecurity/docs/GENPACT%20Global%20Information%20Security%20Policy.pdf)

# **Process Map**

**Entry Point:**



**Exit Point:** Commissioning of server

# **Detection**

1. Scan all the servers periodically and reports if any vulnerability is found
2. Server Hardening document is periodically reviewed by Genpact InfoSec team. For any changes to the existing document, approval has to be taken from InfoSec team

# **Incidence Logging/escalation**

* Notify members of the InfoSec team
* Notify SPOC for the SMG-Wintel team

**Session Time Out**

Please check parameter “TMOUT=900”in following files.

/etc/bashrc

/etc/profile

Please check following parameters for ssh timeout in /etc/ssh/sshd\_config

ClientAliveInterval 900

ClientAliveCountMax 3

**Setting up Genpact banner**

vi /etc/motd

|-----------------------------------------------------------------|

| GENPACT |

| This system is for the use of authorized users only. |

| Individuals using this computer system without authority, or in |

| excess of their authority, are subject to having all of their |

| activities on this system monitored and recorded by system |

| personnel. |

| |

| In the course of monitoring individuals improperly using this |

| system, or in the course of system maintenance, the activities |

| of authorized users may also be monitored. |

| |

| Anyone using this system expressly consents to such monitoring |

| and is advised that if such monitoring reveals possible |

| evidence of criminal activity, system personnel may provide the |

| evidence of such monitoring to law enforcement officials. |

|-----------------------------------------------------------------|

vi /etc/issue

|-----------------------------------------------------------------|

| GENPACT |

| This system is for the use of authorized users only. |

| Individuals using this computer system without authority, or in |

| excess of their authority, are subject to having all of their |

| activities on this system monitored and recorded by system |

| personnel. |

| |

| In the course of monitoring individuals improperly using this |

| system, or in the course of system maintenance, the activities |

| of authorized users may also be monitored. |

| |

| Anyone using this system expressly consents to such monitoring |

| and is advised that if such monitoring reveals possible |

| evidence of criminal activity, system personnel may provide the |

| evidence of such monitoring to law enforcement officials. |

|-----------------------------------------------------------------|

**Syslog implementation to local folders**

Check following file and parameter.

echo "\*.\* @119.43.85.206" >> /etc/rsyslog.conf

service rsyslog restart

**Note**: IP may vary with respective locations.

**Root Direct Login Blocked**

Please check following parameters in /etc/ssh/sshd\_config for ssh root login.

PermitRootLogin no

**Password policy Implementation**

# vi /etc/login.defs

PASS\_MAX\_DAYS   90

PASS\_MIN\_DAYS   0

PASS\_MIN\_LEN    8

PASS\_WARN\_AGE   80

LOGIN\_RETRIES 3

LOGIN\_TIMEOUT 60

PASS\_MAX\_LEN 8 \*np

PASS\_CHANGE\_TRIES 5 \*np

#vi /etc/pam.d/system-auth

password    requisite     /lib/security/$ISA/pam\_cracklib.so retry=3 minlen=8 lcredit=1 ucredit=1 dcredit=1 ocredit=0

password    sufficient    /lib/security/$ISA/pam\_unix.so nullok use\_authtok md5 shadow remember=24

**Password and Shadow file permissions**

chown root:root /etc/passwd

chown root:root /etc/shadow

chmod 644 /etc/passwd

chmod 400 /etc/shadow

**Procedure to Block System Accounts/Groups**

echo "=== Block System Accounts/Groups ==="

cp -rp /etc/passwd /home/backup/passwd.old

cp -rp /etc/shadow /home/backup/shadow.old

for user in lp news uucp games ; do /usr/sbin/userdel -r $user; done

for group in lp news uucp games ; do /usr/sbin/groupdel $group; done

echo "=== Find unowned files and directories ==="

find / -nouser -o -nogroup

echo "=== Find UIP 0 Account Other than root ==="

awk -F: '($3 == 0) { print $1 }' /etc/passwd

**ntp services:**

echo “server 58.2.47.148” >>/etc/ntp.conf

service ntpd restart

chkconfig ntpd on

ntpq –p

**Note**: NTP server IP may vary with respective locations.

**Access Management**

**### ucmdb ID creation with never expiry ###**

# useradd –m –d /home/ucmdb –s /bin/bash ucmdb // need to append key as well

# passwd –x -1 ucmdb

**### root password reset ###**

# echo “\*\*\*\*\*\*” | passwd --stdin root

**Disable services:**

telnet, finger, rlogin, rsh and rsync, iptables|firewalld, NetworkManager, selinux

[root@GCDLINGGN3TEST01 xinetd.d]# chkconfig --list | egrep -i 'telnet|rsync|finger|rsh|login|iptables|NetworkManager'

NetworkManager 0:off 1:off 2:off 3:off 4:off 5:off 6:off

iptables 0:off 1:off 2:off 3:off 4:off 5:off 6:off

eklogin: off

ekrb5-telnet: off

klogin: off

krb5-telnet: off

rlogin: off

rsh: off

rsync: off

telnet: off

# chkconfig service\_name off

# sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config

# setenforce 0

**Tools/packages need to install**

1. SSM agent
2. DS agent
3. New Relic installation for Prod servers

|  |  |  |
| --- | --- | --- |
| **Control Name** | **Objective** | **Procedures/Commands** |
| Unsupported System Components | Checks to ensure the operating system version in use is a supported version by the vendor. | Determine if the operating system version is a supported release. Refer to the vendors support website to verify that support for it has not expired.   Note: Each organization responsible for the management of the agency's operating systems software shall ensure that unsupported software is removed or upgraded to a supported version prior to a vendor dropping support.  Check the release of the OS:  − Solaris # uname -a   − Linux # uname -R   If the operating system is not a supported release, then this is a finding. |
| Flaw Remediation | Checks to ensure the system is current with vendor released security patches. | Check installed patches:  − Solaris # patchadd -p |grep patch  or  # showrev -p | grep patch    − Linux # RHEL 4. If using standard Redhat Updates; have the administrator use the up2date -l command to check for new updates.  # RHEL 5. If using standard Redhat Updates; have the administrator use the yum check-update command to list available updates. #ALL RHEL cat /etc/redhat-release will provide the maintenance release of the installation. It should be current with the latest maintenance patch release. #SUSE. Have the administrator use the yast2 utility to check for updates. #ALL If regular updates are being performed, INCLUDING the kernel then the uname -r command can be run to check for kernel updates. Kernel version should be compared to the latest vendor patch list to ensure that it is a supports, secure release. Often this check will indicate if regular patching is occurring.  Compare the system output with the most current vendor recommended and security patches. . Program managed specific systems should follow their configuration management cycle which may be longer than a normal vendor cycle. |
| Session Lock | Checks to determine if automatic session termination applies to local and remote sessions. | The SA will configure systems to log out interactive processes (i.e., terminal sessions, ssh sessions, etc.,) after 15 minutes of inactivity or ensure a password protected screen lock mechanism is used and is set to lock the screen after 15 minutes of inactivity. |
| Remote Access | Remote access should be managed through a limited number of managed network access control points | Verify with the System Admin as to whether or not remote connections e.g . ssh s/ftp) are managed through access points(e.g. A jump server for desktop connections, a proxy / firewall for s/ftp) . |
| Session Termination | Checks to see if the information system automatically terminates a remote session after 15 minutes of inactivity. | Ask the administrator if session termination is enabled or admin consoles using X-Windows or Workstations running any UNIX utility remotely. All interactive sessions should employ a method of session termination after a period of inactivity. Have the administrator verify:  env | grep TMOUT  Verify that session ssh / terminal termination is enabled. n the edit ~/.bashrc file or the OS equivalent (i.e. ...cshrc, .profile, etc.) |
| Remote Access | Checks for the existence of remote consoles. | ▪ Solaris  Confirm there is no output from the below mentioned command. # consadm -p   ▪ Linux  Confirm /etc/securetty exists and is empty or contains only the word console or a single tty device. # more /etc/securetty |
| Remote Access | Check to see if the root password is passed over a network in clear text form. | Perform the following to determine if root has logged in over an unencrypted network connection. The first command determines if root has logged in over a network. The second will check to see if ssh is installed.  − Solaris # last | grep "^root " | egrep -v "reboot|console" | more # ps -ef |grep sshd   − Linux # last | grep "^root " | egrep -v "reboot|console" | more # ps -ef |grep sshd  If the output from the 'last' command shows root has logged in over the network and sshd is not running, then this is a finding. |
| Remote Access | Check to see if an encrypted remote access program such as ssh is configured to disable the capability to log on directly as root. | Perform the following to determine if ssh disables root logins:   # find / -name sshd\_config -print  # grep -I <sshd\_config path> permitrootlogin  RHEL 4-5, SLES 9 The permitrootlogins value should be uncommented and set to no.   Note: Speak with the administrator regarding alternative ways of restricting direct root ssh logins with PAM if they suggest that root logins via ssh are disabled and the above check suggests otherwise. |
| Account Management | Checks to ensure all accounts have unique user names. | − Solaris # logins -d   − Linux  # pwck -r  If accounts have the same account name, then this is a finding. |
| Account Management | Checks to ensure groups listed in the passwd file are in /etc/group. | ▪ Solaris # logins -d   Compare with:  # more /etc/group  Confirm each gid referenced in the /etc/passwd file is listed in the /etc/group file.  ▪ Linux  # pwck -r  If a group referenced in the /etc/passwd file is not in the /etc/group file, then this is a finding. |
| Account Management | Check to see if accounts are locked after 90 days of inactivity. | Indications of inactive accounts are those that have no entries in the last log. Check the date in the last log to verify it is within the last 90 days. If an inactive account is not disabled via an entry in the password field in the /etc/passwd or /etc/shadow (or TCB equivalent), check the /etc/passwd file to check if the account has a valid shell. If not, then this is a finding. Non-interactive application accounts may be documented. |
| Least Privilege | Checks to see if the Snmpd.conf file permission is securely configured. | Perform:  # find / -name snmpd.conf # ls -lL <snmpd.conf>  If the snmpd.conf file is more permissive than 700, then this is a finding. |
| Access Enforcement | Checks to see if the root account has world writeable directories in its search path. | As the root user perform the following to check the search path:   # echo $PATH  # ls -ld <each directory in path variable>  If any of the directories in the PATH variable are world writeable, then this is a finding. |
| Access Enforcement | Check to see if the root account can be directly logged into from other than the system console. | ▪ Solaris  Confirm CONSOLE is set to /dev/console. # grep CONSOLE=/dev/console /etc/default/login    ▪ Linux  Confirm /etc/securetty exists and is empty or contains only the word console or a single tty device. # more /etc/securetty |
| Access Enforcement | Check to see if the root account is logged onto directly. | Perform the following to check if root is logging in directly:   # last root |grep -v reboot  If any entries exist for root other than the console, then this is a finding. |
| Access Enforcement | Check to see if there are unowned files. | Perform:  # find / -nouser -print > nousers  and   # find / -nogroup -print > nogroup  If there are any files listed either in the nousers or nogroup files created from the above commands, then this is a finding. |
| Access Enforcement | Check to see if network services daemon file permissions are more permissive than 755. | Perform the following to check the permissions:  − Solaris # ls -la /usr/bin or /usr/sbin    − Linux # ls -la /usr/sbin  If any of the files that are used to start network daemons in the above directories have permissions greater than 755, then 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. |
| Access Enforcement | Check to see if system command permission are more permissive than 755. | Perform:  # ls -lL <system directory> <system files directories are listed below>  to check the permissions for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/usb, /sbin, and /usr/sbin. If the file permissions are greater than 755, and the files are system commands, then this is a finding.  Note: Elevate to Criticality Code of HIGH if world writable. |
| Access Enforcement | Check to see if system files, programs, and directories are not owned by a system account. | Perform:  # ls -lL <system directory> <system files directories are listed below>  to check the owner for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/usb, /sbin, and /usr/sbin. If the files are not owned by a system account or application, then this is a finding. Note: oratab and emtab will be owned by oracle. |
| Access Enforcement | Check to see if the group owner of system files, programs, or directories is not a system group. | Perform:  # ls -lL <system directory> <system files directories are listed below>  to check the group owner for files in /etc, /bin, /usr/bin, /usr/lbin, /usr/usb, /sbin, and /usr/sbin. If the files are not owned by a system group or application group, then this is a finding. |
| Access Enforcement | Check to see if system log file permissions are more permissive than 640. | Most syslog messages are logged to /var/log, /var/log/syslog, or /var/adm directories. Check the permissions by performing the following:   # ls -lL <syslog directory>  If any of the log files permissions are greater than 640, then this is a finding. |
| Access Enforcement | Check to see if manual page file permissions are more permissive than 644. | Check the man pages permissions by performing the following:   # ls -lL /usr/share/man  # ls -lL /usr/share/info  # ls -lL /usr/share/infopage  If any files in the above directories have permissions greater than 644, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/passwd file protection is more permissive than 644. | Check /etc/passwd permissions:  # ls -lL /etc/passwd  If /etc/passwd is more permissive than 644, then this is a finding. |
| Access Enforcement | Checks to ensure library file permissions are securely set. | Check the library permissions by performing the following:   # ls -lL /usr/lib/\* -or  # ls -lL /usr/lib/\* | grep -v lr | grep -v dr  If any of the file permissions are greater than 755, then this is a finding. |
| Access Enforcement | Checks to make sure that the /etc/passwd file is owned by root. | Check /etc/passwd ownership:  # ls -lL /etc/passwd  Check /etc/shadow and equivalent file(s) ownership:     − All Other Platforms # ls -lL /etc/shadow  If the /etc/passwd and /etc/shadow (or equivalent) file is not owned by root, then this is a finding. If HP-UX /tcb directories and files ownerships are not configured as detailed above, then this is a finding. |
| Access Enforcement | Checks to see if the shadow file permissions are more permissive than 400. | Check /etc/shadow and equivalent file(s) permissions:    − All Other Platforms # ls -lL /etc/shadow  If the /etc/shadow (or equivalent) file is more permissive than 400, then this is a finding. If HP-UX /tcb directories and files permissions are not configured as detailed above, then this is a finding. |
| Access Enforcement | Checks to see if home directories have permissions greater than 750. | Issue this command for each user in the /etc/passwd file to display user home directory permissions:  # ls -lLd /<usershomedirectory>  If a user's home directories are more permissive the 750, then this is a finding. Home directories with permissions greater than 750 must be justified and documented with the InfoSec. |
| Access Enforcement | Checks to see if users do own their home directory. | Issue this command for each user in the /etc/passwd file to display user home directory ownership:  # ls -lLd /<usershomedirectory>  If a user's home directory(s) are not owned by the assigned user, then this is a finding. Home directories not owned by the assigned user must be justified and documented with the InfoSec. |
| Access Enforcement | Checks to see if system start-up files are more permissive than 755. | Check run control scripts permissions:  − Solaris # cd /etc # ls -lL rc\* # cd /etc/init.d # ls -l    − Linux  # cd /etc (may vary) # ls -lL rc\* # cd /etc/init.d # ls -l  If run control scripts are more permissive than 755, then this is a finding. |
| Access Enforcement | Checks to see if run control scripts have the sgid or suid bit set. | Check run control scripts for sgid and suid:  − Solaris # cd /etc # ls -lL rc\* # cd /etc/init.d # ls -l    − Linux  # cd /etc (may vary) # ls -lL rc\* # cd /etc/init.d # ls -l  If run control scripts have the sgid or suid bit set, then this is a finding. |
|  |  |  |
| Access Enforcement | Checks to see if run control scripts are not owned by root or bin. | Check run control scripts ownership:  − Solaris # cd /etc # ls -lL rc\* # cd /etc/init.d # ls -l   − Linux  # cd /etc (may vary) # ls -lL rc\* # cd /etc/init.d # ls -l  If run control scripts are not owned by root or bin, then this is a finding. |
| Access Enforcement | Checks to see if run control scripts are not group owned by root, sys, bin, other or the system default. | Check run control scripts group ownership:  − Solaris # cd /etc # ls -lL rc\* # cd /etc/init.d # ls -lL   − Linux  # cd /etc (may vary) # ls -lL rc\* # cd /etc/init.d # ls -lL rc\*  If run control scripts are not group owned by root, sys, bin, other or the system default, then this is a finding. |
| Access Enforcement | Checks to see if global initialization files are group owned by root, sys,bin, other or the system default. | Check global initialization files group ownership:  # ls -l /etc/.login # ls -l /etc/profile # ls -l /etc/bashrc # ls -l /etc/environment # ls -l /etc/security/environ  If global initialization files are not group owned by root, sys, bin, other, or the system default, then this is a finding. |
| Least Privilege | Checks to see if global initialization files are more permissive than 644. | Check global initialization files permissions:  # ls -l /etc/.login # ls -l /etc/profile # ls -l /etc/bashrc # ls -l /etc/environment # ls -l /etc/security/environ  If global initialization files are more permissive than 644, then this is a finding.  Note: check /etc/profile for HP-UX. |
| Least Privilege | Check to see if the root accounts home directory (other than /) is more permissive than 700. | Perform the following as root:   # grep "^root" /etc/passwd | awk -F":" '{print $6}'  # ls -ld <root home directory>  If the permissions of the root home directory are greater than 700, then this is a finding. If the home directory is /, this check should be marked Not Applicable. |
| Access Enforcement | Checks to see if default skeleton dot files are owned by root or bin. | Check skeleton files ownership:  − All Other Platforms  # ls -alL /etc/skel  If skeleton dot files are not owned by root or bin, then this is a finding. |
| Least Privilege | Checks to see if the default skeleton dot file permissions are more permissive than 644. | Check skeleton files permissions:    − All Other Platforms  # ls -alL /etc/skel  If skeleton dot files are more permissive than 644, then this is a finding. |
|  |  |  |
| Access Enforcement | Checks to see if local initialization files are owned by the user or root. | # 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  Note: Can use the following style syntax: # ls -al /home/\*/.login (.cshrc, etc.)  If local initialization files are not owned the home directory user, then this is a finding. Local initialization files not owned by the user must be justified and documented by the InfoSec |
| Least Privilege | Checks to see if the local initialization files permissions are securely configured. | # 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 755) # ls -al /<usershomedirectory>/.dispatch # ls -al /<usershomedirectory>/.emacs # ls -al /<usershomedirectory>/.exrc  Note: Can use the following style syntax: # ls -al /home/\*/.login (.cshrc, etc.)  If local initialization files are more permissive than 740 or the .dtprofile file is more permissive than 755, then this is a finding. |
| Access Enforcement | Checks to see if local initialization files have the sgid or suid bit set. | # ls -la /<usershomedirectory>/.\*   Note: Can use the following style syntax: # ls -al /home/\*/.\* | grep -i rws  If any of the above files have the suid or sgid bit set, then this is a finding. |
| Access Enforcement | Checks to see if the.netrc file exists. | # find / -name .netrc   If the .netrc file exists, then this is a finding. The .netrc must be justified and documented with the InfoSec. |
| Access Enforcement | Checks to see if .rhosts, .shosts, or hosts.equiv files contain other than hosts-user pairs. | # 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 the .rhosts, .shosts, hosts.equiv, or shosts.equiv files contain other than hostname-user pairs and are not justified and documented with the InfoSec, then this is a finding. |
| Access Enforcement | Checks to see if the .rhosts, .shosts, hosts.equiv or shosts.equiv are used. | # find / -name .rhosts # find / -name .shosts # find / -name hosts.equiv # find / -name shosts.equiv  If .rhosts, .shosts, hosts.equiv, or shosts.equiv are found and not justified and documented with the InfoSec, then this is a finding. |
| Access Enforcement | Checks to see if shell files have the sgid bit set. | − All Other Platforms # find / -name "\*sh" For each shell found: # ls -l <shell>  Note: Can use the following style syntax (may vary by OS type): # find / -name "\*sh" -print -exec ls -lL {} \; | grep -i rws   Note: This is required for oracle - it is how oracle log reports run.   If shell files have the sgid bit set, then this is a finding. |
| Access Enforcement | Checks to see if shell files have the suid bit set. | − All Other Platforms # find / -name "\*sh"  For each shell found: # ls -l <shell>  Note: Can use the following style syntax (may vary by OS type): # find / -name "\*sh" -print -exec ls -lL {} \; | grep -i rws   If shell files have the suid bit set, then this is a finding.  Note: The remsh command is sometimes linked to the rsh command and will have the suid bit set; in this case it is not a finding. Determine if that is the case by using ls -li to determine if they share the same inode number. The remsh command is the remote shell command and should not be considered a shell. Solaris uses the /usr/bin/rsh and the /usr/ucb/rsh commands for remote shells, and they should also be ignored here. A restricted shell also exists for bash (rbash). |
| Access Enforcement | Checks to see if shell files exist that are not owned by root or bin. | − All Other Platforms # find / -name "\*sh" For each shell found: # ls -l <shell>  Note: Can use the following style syntax (may vary by OS type): # find / -name "\*sh" -print -exec ls -lL {} \;   Note: This is required for oracle - it is how oracle log reports run.   If shell files are not owned by root or bin, then this is a finding. |
| Access Enforcement | Checks to see if shell files permissions are securely configured. | − All Other Platforms # find / -name "\*sh" For each shell found: # ls -l <shell>  Note: Can use the following style syntax (may vary by OS type): # find / -name "\*sh" -print -exec ls -lL {} \; | grep -i rwxrwx   If shell files are more permissive than 755, then this is a finding. |
| Access Enforcement | Checks to see if an audio device is owned by root. | - Linux # ls -lL /dev/audio\*  If the audio device is not owned by root, then this is a finding. |
| Access Enforcement | Checks to see if an audio device is not group owned by root, sys, or bin. | - Linux # ls -lL /dev/audio\*  If the audio device group ownership is not root, sys, bin, or audio, then this is a finding. |
| Least Privilege | Checks to see if an audio device file permissions are securely configured. | - SOLARIS  # ls -lL /dev/audio - Linux # ls -lL /dev/audio\*  If the permissions are greater than 644, then this is a finding. |
| Access Enforcement | Checks for SUID files; checks to see if this process is performed weekly against the baseline. | find / -perm 4000 |more Ask the SA If the system is checked weekly against the system baseline for unauthorized suid files as well as unauthorized modification to authorized suid files, if not then this is a finding. |
| Least Privilege | Checks for the existence of SGID files; checks to see if they are checked weekly against the baseline. | find / -perm 2000 |more  If the system is not checked weekly against the system baseline for unauthorized sgid files as well as unauthorized modification to authorized sgid files, then this is a finding. |
| Access Enforcement | Checks ensure public directory ownership is properly configured. | find / -type d \( -perm -002 -a -perm -1000 \) |more  If public directories are not owned by root or an application user, then this is a finding. |
| Access Enforcement | Checks to see if public directory group ownership is properly configured. | ls -ld `find / -type d \( -perm -002 -a -perm -1000 \)` |more  If public directories are not group owned by root, sys, bin, other or an application group, then this is a finding. |
|  |  |  |
| Access Enforcement | Checks to see if the system and user default umask is securely configured. | − All other platforms - Global Initialization Files # grep umask /etc/\*  Confirm the global initialization files set the umask to 027.  - Local Initialization Files # grep umask /<usershomedirectory>/.\*  Confirm the local initialization files do not exceed the default umask to 027.  Note: If the default umask is 000 or allows for the creation of world writable files this becomes a Severity Code I finding.  If the system and user default umask is not 027, then this a finding. |
| Access Enforcement | Checks to see if access to the cron utility is controlled via the cron.allow and/or cron.deny files. | Verify the cron.allow and cron.deny files exist:  − Solaris  # ls -lL /etc/cron.d/cron.allow # ls -lL /etc/cron.d/cron.deny    − Linux Red Hat # ls -lL /etc/cron.allow # ls -lL /etc/cron.deny Or  SuSE  # ls -lL /var/spool/cron/allow # ls -lL /var/spool/cron/deny  If the cron.allow or cron.deny files do not exist, then this is a finding. |
| Access Enforcement | Checks to see if the cron.allow file permissions are securely configured. | − Solaris  # ls -lL /etc/cron.d/cron.allow   − Linux Red Hat # ls -lL /etc/cron.allow Or  SuSE  # ls -lL /var/spool/cron/allow  If the cron.allow file is more permissive than 600, then this is a finding. |
| Access Enforcement | Checks to see if default system accounts with the exception of root are listed in the cron.allow file or excluded from the cron.deny file if cron.allow does not exist. | Check for default system accounts in the following:  − Solaris  # more /etc/cron.d/cron.allow   − Linux Red Hat # more /etc/cron.allow Or  SuSE  # more /var/spool/cron/allow  Default accounts (such as bin, sys, adm, and others) will not be listed in the cron.allow file or this will be a finding. |
| Access Enforcement | Checks to see if the cron or crontab directory permissions are securely configured. | − Solaris # ls -ld /var/spool/cron/crontabs    − Linux # ls -ld /var/spool/cron  # ls -ld /etc/cron.d # ls -ld /etc/cron.daily # ls -ld /etc/cron.hourly # ls -ld /etc/cron.monthly # ls -ld /etc/cron.weekly  If the cron or crontab directories are more permissive than 755, then this is a finding. |
|  |  |  |
| Access Enforcement | Checks to see if the cron or crontab directories are owned by root or bin. | − Solaris # ls -ld /var/spool/cron/crontabs   − Linux # ls -ld /var/spool/cron  # ls -ld /etc/cron.d # ls -ld /etc/cron.daily # ls -ld /etc/cron.hourly # ls -ld /etc/cron.monthly # ls -ld /etc/cron.weekly  If the cron or crontab directories are not owned by root or bin, then this is a finding. |
| Access Enforcement | Checks to see if the cron or crontab directories are group owned by root, sys, or bin. | − Solaris # ls -ld /var/spool/cron/crontabs   − Linux # ls -ld /var/spool/cron  # ls -ld /etc/cron.d # ls -ld /etc/cron.daily # ls -ld /etc/cron.hourly # ls -ld /etc/cron.monthly # ls -ld /etc/cron.weekly  If the cron or crontab directories are not group owned by root, sys, or bin, then this is a finding. |
| Access Enforcement | Checks to see if the cron.deny file permission is securely configured. | − Solaris  # ls -lL /etc/cron.d/cron.deny   − Linux Red Hat # ls -lL /etc/cron.deny Or  SuSE  # ls -lL /var/spool/cron/deny   If the cron.deny file is more permissive than 600, then this is a finding. |
| Access Enforcement | Checks to see if the cron.allow file is owned and group owned by root. | − Solaris  # ls -lL /etc/cron.d/cron.allow   − Linux Red Hat # ls -lL /etc/cron.allow Or  SuSE  # ls -lL /var/spool/cron/allow  If the cron.allow file is not owned and group owned by root, sys, or bin, then this is a finding. |
| Access Enforcement | Checks to see if the cron.deny file is owned and group owned by root. | − Solaris  # ls -lL /etc/cron.d/cron.deny   − Linux Red Hat # ls -lL /etc/cron.deny Or  SuSE  # ls -lL /var/spool/cron/deny  If the cron.deny file is not owned and group owned by root, sys, or bin, then this is a finding. |
| Access Enforcement | Checks to see if the at.deny file exists and is empty. | − Solaris  # more /etc/cron.d/at.deny    − Linux # more /etc/at.deny  If the at.deny file exists and is empty, then this is a finding. |
| Access Enforcement | Checks to see if default accounts are listed in the at.allow file. | − Solaris  # more /etc/cron.d/at.allow     − Linux # more /etc/at.allow  Default accounts (such as bin, sys, adm, and others) will not be listed in the at.allow file or this will be a finding. |
| Access Enforcement | Checks to see if the at.allow or at.deny file is more permissive than 600. | − Solaris  # ls -lL /etc/cron.d/at.allow # ls -lL /etc/cron.d/at.deny   − Linux # ls -lL /etc/at.allow # ls -lL /etc/at.deny  If the at.allow or at.deny file(s) is more permissive than 600, then this is a finding. |
| Access Enforcement | Checks to see if the at or equivalent directory is more permissive than 755. | Check the permissions of the at directory by performing the following:   # ls -ld /var/spool/cron/atjobs  Or  # ls -ld /var/spool/atjobs  If the directory permissions are greater than 755, then this is a finding. |
| Access Enforcement | Checks to see if the at directory is owned by root, bin, sys, or daemon. | Check the ownership of the at directory by performing the following:   # ls -ld /var/spool/cron/atjobs  Or  # ls -ld /var/spool/atjobs  If the directory is not owned by root, sys, bin, or daemon, then this is a finding. |
| Access Enforcement | Checks to ensure the AT program is securely configured. | Perform the following to check for at jobs:   # cd /var/spool/cron/atjobs  Or  # cd /var/spool/atjobs  Determine if there are any at jobs by viewing a long listing of the directory. If there are at jobs perform the following to check for any programs that may have a umask more permissive than 027:   # grep umask ./\*  If there are any, this is a finding unless the InfoSec has justifying documentation. If there are no 'at' jobs present, this vulnerability is Not Applicable. |
| Access Enforcement | Checks to see if the at.allow file is owned and group owned by root. | − Solaris  # ls -lL /etc/cron.d/at.allow   − Linux # ls -lL /etc/at.allow  If the at.allow file is not owned and group owned by root, sys, or bin, then this is a finding. |
| Access Enforcement | Checks to see if the at.deny file is owned and group owned by root, sys, or bin. | − Solaris  # ls -lL /etc/cron.d/at.deny   − Linux # ls -lL /etc/at.deny  If the at.deny file is not owned and group owned by root, sys, or bin, then this is a finding. |
| Access Enforcement | Checks to see if the inetd.conf or xinetd.conf file is owned by root or bin. | Check the permissions of inetd.conf file by:  # ls -lL /etc/inetd.conf  Or, for Linux systems  # ls -lL /etc/xinetd.conf   # ls -lL /etc/xinetd.d  This is a finding if any of the above files or directories are not owned by root or bin. |
| Least Privilege | Checks to see if the inetd.conf file permissions are more permissive than 440. The linux xinetd.d is more permissive than 755. | Check the permissions of inetd.conf file by:  # ls -lL /etc/inetd.conf  Or, for Linux systems  # ls -lL /etc/xinetd.conf   # ls -lL /etc/xinetd.d  This is a finding if permissions for the inetd.conf files are greater than 440. In addition, on Linux systems, the /etc/xinetd.d directory permissions should not be greater than 755. |
| Access Enforcement | Checks to see if the services file is owned by root or bin. | ls -lL /etc/services  The services file is not owned by root or bin, then this is a finding |
| Least Privilege | Checks to see if the services file is more permissive than 644. | ls -lL /etc/services  If the services file is more permissive than 644, then this is a finding. |
| Access Enforcement | Checks to see if remote login or remote shell is enabled. | Solaris,  # grep -v "^#" /etc/inetd.conf |grep rlogind  # grep -v "^#" /etc/inetd.conf |grep rshd  Solaris 10  # svcs rlogin  Linux  # grep disable /etc/xinetd.d/rlogin  # grep disable /etc/xinetd.d/rsh  If either rlogin or rsh are found to be enabled, then this is a finding. |
| Access Enforcement | Checks to see if the rexec service is enabled. | Perform the following to determine if the rexec service is enabled:  Solaris,   # grep -v "^#" /etc/inetd.conf |grep rexec  Solaris 10  # svcs rexec |grep disabled  Linux  # grep disable /etc/xinetd.d/rexec  If rexec is found to be enabled, then this is a finding. |
| Access Enforcement | Checks to see if the hosts.lpd is owned by root, bin ,sys or lp. | Look for the presence of a print service configuration file by using the command:   # find /etc -name hosts.lpd -print   If this file does not exist, use the command:   # find /etc -name Systems -print   If this file does not exist, use the command:   # find /etc -name printers.conf  If neither of the files are found, then this check should be marked Not Applicable. Otherwise perform:   # ls -lL <print service file>  If the owner of the file is not root, sys, bin or lp, then this is a finding. |
| Access Enforcement | Checks to see if the permissions on the hosts.lpd file are securely configured. | Look for the presence of a print service configuration file by using the command:   # find /etc -name hosts.lpd -print   If this file does not exist, use the command:   # find /etc -name Systems -print   If this file does not exist, use the command:   # find /etc -name printers.conf  If neither of the files are found, then this check should be marked Not Applicable. Otherwise perform:   # ls -lL <print service file>  and verify the permissions are not greater than 664. If the permissions are greater than 664, then this is a finding. |
| Access Enforcement | Checks to see if the traceroute command owner is root. | − Solaris  # ls -lL /usr/sbin/traceroute  − Linux # ls -lL /usr/sbin/traceroute  If the traceroute command is not owned by root, then this is a finding. |
| Least Privilege | Checks to see if the traceroute command permission is securely configured. | − Solaris  # ls -lL /usr/sbin/traceroute  − Linux # ls -lL /usr/sbin/traceroute  If the traceroute command is more permissive than 700, then this is a finding. |
| Least Privilege | Checks to see if the alias file is owned by root. | Find the aliases file on the system:   # find / -name aliases -depth -print  # ls -lL <alias location> (NOTE: THE -depth OPTION may not be required. Tested on RHEL5) If the file is not owned by root, then this is a finding. |
| Least Privilege | Checks to see if files executed through an alias are securely configured. | Find the aliases file on the system:   # find / -name aliases -depth -print  # more <aliases file location> (NOTE: THE -depth OPTION may not be required. Tested on RHEL5)  Examine the aliases file for any directories or paths that may be utilized. Perform:   # ls -lL <path>  to check the permissions are not greater than 755.  If files executed through an alias have permissions greater than 755, then this is a finding. |
| Access Enforcement | Checks to see if files executed through an alias file are owned by root and reside within a directory owned and writeable only by root. | Find the aliases file on the system:   # find / -name aliases -depth -print  # more <aliases file location> (NOTE: THE -depth OPTION may not be required. Tested on RHEL5)  Examine the aliases file for any directories or paths that may be utilized. Perform:   # ls -lL <path>  Ensure the file and parent directory are owned by root. If it is not, then this a finding. |
| Access Enforcement | Checks to ensure the ftpusers file permissions are securely configured. | Perform the following on the ftpusers file associated with the applicable operating system:   # ls -la <file location>   Locations of the ftpusers file:  Solaris 5.5.1 - 5.8 /etc/ftpusers Solaris 5.9 -5.10 /etc/ftpd/ftpusers  Linux (wu-ftp) /etc/ftpusers Linux (vsftpd) /etc/vsftpd.ftpusers  If the file is not owned by root, then this is a finding. |
| Access Enforcement | Checks the umask for the ftp user account. | To determine the umask of the ftp user, perform the following:   # su - ftp  # umask  If the umask value does not return 077, then this is a finding. |
| Access Enforcement | Checks to see if the tftp daemon has the suid or sgid bit set. | Perform :   # find / -name "\*tftpd" -print   to locate the file. Once the file is located, use the command:   # ls -la <file location>   to check for the suid or sgid bit being set. If either of the bits are set, then this is a finding |
| Access Enforcement | Checks to ensure TFTP is securely configured. | Check the /etc/passwd file to determine if TFTP is configured properly:   # grep tftp /etc/passwd  If a tftp user account does not exist and TFTP is active, then this is a finding. Ensure the user shell is /bin/false or equivalent (/usr/bin/false). If it is not, then this is a finding. Ensure the TFTP user is assigned a home directory (/home/tftpdir). If not, then this is a finding. |
| Access Enforcement | Checks to see if the system is exporting x displays to the world. | Perform the following to determine if access to the X window system is limited to authorized clients:   # xhost  If the above command returns:  "access control disabled, clients can connect from any host", then this is a finding. |
| Access Enforcement | Checks to see if the /etc/syslog.conf is owned by root and file permissions are securely configured. | Check /etc/syslog.conf ownership and permissions:   # ls -lL /etc/syslog.conf  If /etc/syslog.conf is not owned by root or is more permissive than 640, then this is a finding. |
| Access Enforcement | Checks to see if the export configuration file is owned by root. | − Solaris  # ls -lL /etc/dfs/dfstab    − Linux # ls -lL /etc/exports  If the export configuration file is not owned by root, then this is a finding. |
| Least Privilege | Checks to see if the export configuration file permissions are securely configured. | − Solaris  # ls -lL /etc/dfs/dfstab   − Linux # ls -lL /etc/exports  If the export configuration file is more permissive than 644, then this is a finding. |
| Access Enforcement | Checks to see if NFS exported system files and directories are owned by root. | Perform the following to check for NFS exported files systems:   # exportfs -v  This will display all of the exported file systems. For each file system displayed perform and check the ownership:   # ls -lL <filesystem>  If the files and directories are not owned by root, then this is a finding. |
| Access Enforcement | Checks to see if the NFS server is configured to deny client access request that do not include a User ID. | Perform the following to determine if the 'anon' option is set correctly for exported file systems:   # exportfs -v |grep anon  Each of the exported file systems should include an entry to check for the 'anon= 'option being set to -1 or an equivalent (60001, 65534, or 65535). Linux systems use the 'anonuid' option instead of 'anon'. |
| Access Enforcement | Checks to see if the root access option for NFS has been authorized and documented with the InfoSec. | Perform the following to determine if the NFS server is exporting with the root access option:   # exportfs -v | grep "root="  If the option is found on an exported file system, ask the SA if the access is justified and documented with the InfoSec. If it is not, then this is a finding. |
| Least Privilege | Checks to see if NFS file systems exported as writeable have been justified and documented by the InfoSec. | Perform the following to determine if NFS File Systems are writeable:   # exportfs -v |grep rw  If any entries are returned, ask the SA if the file systems have been approved and documented with the InfoSec for export as writable. |
| Least Privilege | Checks to see if the NFS server is configured to restrict file system access to local hosts. | Perform the following to check for access permissions:   # exportfs -v  If the exported filesystems do not contain the 'rw' or 'ro' options, then this is a finding. |
| Access Enforcement | Checks to see if the nosuid and nosgid options are enabled on an nfs client. | Perform the following to determine if nfs clients are mounting file systems with the nosuid and nosgid options:   # mount -v | grep " type nfs " | grep "nosuid"  # mount -v | grep " type nfs " | grep "nosgid"  If the mounted file systems do not have the above two options, then this is a finding and it must be justified and documented with the InfoSec. |
| Access Enforcement | Checks to see if the smb.conf file is owned by root. | Check /etc/samba/smb.conf ownership:   # ls -lL /etc/samba/smb.conf  If /etc/samba/smb.conf is not owned by root, then this is a finding.  Note: Based on the specific system implementation the file path may be /etc/smb.conf |
| Access Enforcement | Checks to see if the smb.conf file is group owned by root. | Check /etc/samba/smb.conf permissions:   # ls -lL /etc/samba/smb.conf  If /etc/samba/smb.conf is not group owned by root, then this is a finding.  Note: Based on the specific system implementation the file path may be /etc/smb.conf |
| Least Privilege | Checks to see if the smb.conf file permissions are securely configured. | Check /etc/samba/smb.conf permissions:   # ls -lL /etc/samba/smb.conf  If /etc/samba/smb.conf is more permissive than 644, then this is a finding.  Note: Based on the specific system implementation the file path may be /etc/smb.conf |
| Access Enforcement | Checks to see if the smb password file is owned by root. | Check /etc/samba/smbpasswd ownership:  # ls -lL /etc/samba/smbpasswd  If /etc/samba/smbpasswd is not owned by root, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/smbpasswd file is group owned by root. | Check /etc/samba/smbpasswd ownership:  # ls -lL /etc/samba/smbpasswd  If /etc/samba/smbpasswd is not group owned by root, then this is a finding. |
| Least Privilege | Checks to see if the /etc/smbpasswd file permission is securely configured. | Check /etc/samba/smbpasswd permissions:  # ls -lL /etc/samba/smbpasswd  If /etc/samba/smbpasswd is more permissive than 600, then this is a finding. |
| Access Enforcement | Checks to see if the grub.conf file is more permissive the 600. | Note: Applies to Solaris 10 and Linux only. Check /etc/grub.conf permissions:  # ls -lL /etc/grub.conf  If /etc/grub.conf is more permissive than 600, then this is a finding |
| Least Privilege | Checks to ensure UID's 0-99 (0-499 Linux) are reserved for system accounts. | # more /etc/passwd  # more /etc/passwd  Confirm all accounts with a uid of 99 and below (499 and below for Linux) are used by a system account. Note: 200 and below for HP-UX.  If a uid reserved for system accounts, 0 - 99 (0 - 499 for Linux), is used by a non-system account without documentation, then this is a finding. A regular account within this range must be justified and documented with the InfoSec. |
| Least Privilege | Checks to ensure GID's 0-99 (0-499 Linux) are reserved for system accounts. | # 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 without documentation, then this is a finding. A regular account within this range must be justified and documented with the InfoSec. |
| Least Privilege | Check to see if an account other than root has a uid of zero. | grep ":0:" /etc/passwd | awk -F":" '{print$1":"$3":"}' |  grep ":0:"  If any accounts are shown in addition to root, then this is a finding. |
| Least Privilege | Checks to see if device file directories are writeable by users other than a system account or as configured by the vendor. | # ls -al /dev # ls -al /devices (Solaris)  Note: Can use the following style syntax (may vary by OS type): # ls -al /dev | grep -i drwx   Check the permissions on the directories and subdirectories that contain device files.  If device file directories are writable by users other than a system account or as configured by the vendor, then this is a finding. |
| Least Privilege | Checks the ownership permissions and location of files with the sgid bit; checks to see if they are documented with the InfoSec. | # find / -perm 2000 |more  If the ownership, permissions, and location of files with the sgid bit set are not baselined with the InfoSec, then this is a finding. |
| Least Privilege | Checks to see if crontab file permissions are securely configured. | − Solaris # ls -lL /var/spool/cron/crontabs/   − Linux # ls -lL /var/spool/cron/ (Permissions of 600) # ls -lL /etc/cron.d/ (Permissions of 600) # ls -lL /etc/crontab (Permissions of 600) # ls -lL /etc/cron.daily/ (Permissions of 700) # ls -lL /etc/cron.hourly/ (Permissions of 700) # ls -lL /etc/cron.monthly/ (Permissions of 700) # ls -lL /etc/cron.weekly/ (Permissions of 700)  If crontab files are more permissive than 600 (700 for some Linux files), then this is a finding. |
| Least Privilege | Checks to see if the cron log file is permissions are securely configured. | − Solaris # ls -lL /var/cron/log   − Linux Red Hat  # ls -lL /var/log/cron   SuSE  # ls -lL /var/log/messages  If the cronlog file is more permissive than 600, then this is a finding. |
| Least Privilege | Checks to see if access to the at utility is controlled via the at.allow and at.deny files. | Verify the at.allow and/or at.deny files exist.  − Solaris  # ls -lL /etc/cron.d/at.allow # ls -lL /etc/cron.d/at.deny    − Linux # ls -lL /etc/at.allow # ls -lL /etc/at.deny  Ensure at least on of the above files exists. |
| Least Privilege | Checks to see if the ftp users file is owned by root. | Perform the following on the ftpusers file associated with the applicable operating system:   # ls -la <file location>   Locations of the ftpusers file:  Solaris 5.5.1 - 5.8 /etc/ftpusers Solaris 5.9 -5.10 /etc/ftpd/ftpusers HPUX 10 /etc/ftpusers HPUX 11 /etc/ftpd/ftpusers AIX /etc/ftpusers Linux (wu-ftp) /etc/ftpusers Linux (vsftpd) /etc/vsftpd.ftpusers  If the file is not owned by root, then this is a finding. |
| Unsuccessful Logon Attempts | Checks to ensure accounts are disabled after 3 unsuccessful login attempts within a 20 minute period. | − Solaris   Confirm LOCK\_AFTER\_RETRIES is set to YES. # grep LOCK\_AFTER\_RETRIES /etc/security/policy.conf  −  − Linux  # more /etc/pam.d/system-auth Confirm the following line is configured; account required /lib/security/pam\_tally.so deny=3 no\_magic\_root reset  If the above settings are not correct, then this is a finding. |
| Audit Generation | Checks to see if auditing is implemented. | Perform the following to determine if auditing is enabled: − Solaris  # ps -ef |grep auditd   − Linux  # ps -ef |grep auditd   If the auditd process is not found, then this is a finding. |
| System Use Notification | Checks to ensure the IRS approved login banner is used. | Login banners will be configured for all services that allow login access to the system. For TCP WRAPPERS, check for hosts.allow and hosts.deny files and then look for banner files associated with them. For ssh, locate the ssh configuration file, sshd\_config or ssh2d\_config. This file is usually located in /etc/sshd, /etc/ssh2, /etc/ssh, or /usr/local/etc. Confirm that the Banner variable contains the full path to the file containing the Logon Warning banner. Other files specific to each vendor are listed below.  − Solaris  Check for logon warning banner display. # more /etc/issue # more /etc/motd # more /etc/dt/config/\*/Xresources (if GUI is implemented) # more /etc/default/telnetd (if telnet is implemented without  TCP\_Wrappers) # more /etc/default/ftpd (if ftp is implemented without  TCP\_Wrappers) # more /etc/ftpd/banner.msg (Solaris 9 and above, if ftp is  implemented without  TCP\_Wrappers)   − Linux  Check for logon warning banner display. # more /etc/issue # more /etc/motd # more /etc/issue.net # more /etc/X11/xdm/Xresources (if GUI is implemented) # more /etc/X11/xdm/kdmrc (if GUI is implemented) # more /etc/X11/gdm/gdm (if GUI is implemented) # more /etc/vsftpd.conf (if ftp is implemented without  TCP\_Wrappers)  If the IRS logon banner is not displayed prior to a logon attempt, then this is a finding. |
| Audit Events | Checks to ensure successful login and logout activity is logged. | − Solaris  Check if successful logons are being logged. # last | more Check if unsuccessful logons are being logged. # ls -l /var/adm/loginlog   − Linux  Check if successful logons are being logged. # last -R | more Check if unsuccessful logons are being logged. # lastb -R | more  If successful and unsuccessful logins and logouts are not logged, then this is a finding. |
| Audit Events | Checks to see if successful and unsuccessful access to the root account is logged. | Check the following log files to determine if access to the root account is being logged. Try to su - and enter an incorrect password.  − Solaris # more /var/adm/sulog    − Linux # more /var/log/messages  or   # more/var/adm/sulog (configurable from /etc/default/su)  If root login accounts are not being logged, then this is a finding. |
| Audit Events | Checks to see if the audit system is configured to audit failed attempts to access files and programs, including FTI files. | − Solaris   # grep flags /etc/security/audit\_control  Confirm flags fd or +fd and -fd is configured.  − Linux For LAUS:  # grep "@rmdir-ops" /etc/audit/filter.conf   # grep "@unlink-ops" /etc/audit/filter.conf  For auditd:  # grep "-a exit,always -S unlink -S rmdir" /etc/audit.rules  (RHEL5 /etc/audit/audit.rules) |
| Audit Events | Checks to see if the audit system is configured to audit login, logout and session initiation. | − Solaris  # egrep "flags|naflags" /etc/security/audit\_control Confirm flags lo or +lo and -lo is configured. Confirm naflags lo or +lo and -lo is configured.  − Linux For LAUS:  # grep process-login /etc/audit/filter.conf |grep always   For auditd:   This is not a finding. Auditd enables this by default in the source code. |
| Audit Events | Checks to see if cron logging is implemented. | − Solaris # ls -lL /var/cron/log # more /etc/default/cron CRONLOG=YES If this line does not exist, this is a finding.   − Linux Cron logging is controlled by the syslog on Linux:   # grep cron\* /etc/syslog.conf  Red Hat  # ls -lL /var/log/cron   SuSE  # ls -lL /var/log/messages  If an entry for cron is not found, then this is a finding. |
| Access Enforcement | Checks to see if the critical sendmail logfile is owned by root. | Perform:   # more /etc/syslog.conf  Ensure the configuration file logs mail.crit, mail.debug, mail.\*, or \*.crit to a file.  Perform:   # ls -lL <file location>  If the files is not owned by root, then this is a finding. |
| Audit Events | Checks to see if the audit system is configured to audit all administrative, privileged and security actions, including all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services and enabling or disabling of audit report generation services. | − Solaris  # grep flags /etc/security/audit\_control Confirm am or +am and -am is configured.  − Linux For LAUS:  # grep "@priv-ops" /etc/audit/filter.conf   # grep "@mount-ops" /etc/audit/filter.conf  # grep "@system-ops" /etc/audit/filter.conf   For auditd the following should be present in /etc/audit.rules: (RHEL5 /etc/audit/audit.rules)    -w /etc/auditd.conf  -w /etc/audit.rules  -a exit,always -S stime -S acct -S reboot -S swapon   -a exit,always -S settimeofday -S setrlimit -S setdomainname  -a exit,always -S sched\_setparam -S sched\_setscheduler |
| Least Privilege | Checks to see if the critical sendmail logfile permissions are securely configured. | Perform:   # more /etc/syslog.conf  Ensure the configuration file logs mail.crit, mail.debug, mail.\*, or \*.crit to a file.  Perform:   # ls -lL <file location>  If the log file permissions are greater than 644, then this is a finding. |
| Audit Events | Checks to ensure critical-level sendmail messages are logged. | Enter the command:   # more /etc/syslog.conf   Ensure the configuration file logs mail.crit, mail.debug, mail.\*, or \*.crit. If the system is not logging critical sendmail messages, then this is a finding. |
| Audit Review, Analysis, and Reporting | Checks to see if the access control program logs each system access attempt. | Normally tcpd logs to the mail or daemon facility in /etc/syslog.conf. Perform the following to determine if syslog is configured to log events by tcpd.   # 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 or maillog  auth.info /var/log/messages  daemon.\* /var/log/messages authpriv /var/log/secure 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. |
| Content of Audit Records | Checks to see if The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. | Ask the administrator if the following items are being recorded with the audit log output. Make note of any exceptions: -- (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. |
| Time Stamps | Checks to ensure system time is synchronized with an authoritative time server (e.g.. NIST, Naval Observatory) | Check if NTP running and verify that the server settings:  ▪ All platforms  # ps -e | egrep "xntpd|ntpd"   Check if ntpdate scheduled to run:  ▪ Solaris  # grep ntpdate /var/spool/cron/crontabs/\*   ▪ Linux  # grep ntpdate /var/spool/cron/\* # grep ntpdate /etc/cron.d/\*  # grep ntpdate /etc/cron.daily/\*I11 # grep ntpdate /etc/cron.hourly/\*  # grep ntpdate /etc/cron.monthly/\*  # grep ntpdate /etc/cron.weekly/\*   If NTP is running or ntpdate is found:  # more /etc/ntp/ntp.conf  Confirm the servers and peers or multicastclient (as applicable) are local or an authoritative U.S. IRS source.  If a non-local/non-authoritative (U.S. IRS approved source) time-server is used, then this is a finding. |
| Protection of Audit Information | Checks to see if system audit logs are restricted to authorized personnel only. | Perform the following to determine the location of audit logs and then check the ownership: − Solaris  # more /etc/security/audit\_control # ls -lLd <audit log dir>   − Linux  # ls -la /var/log/audit.d   # ls -la /var/log/audit/audit.log  If any of the audit log files are readable by unprivileged id's, then this is a finding. |
| Protection of Audit Information | Checks to see if system audit log permissions are securely configured. | Perform the following to determine the location of audit logs and then check the permissions: − Solaris  # more /etc/security/audit\_control # ls -la <audit log dir>    − Linux  # ls -la /var/log/audit.d   # ls -la /var/log/audit/audit.log  If any of the audit log file permissions are greater than 640, then this is a finding. |
| Protection of Audit Information | Checks to see if audit logs are rotated daily. | Perform the following to search the crontab for entries to rotate the audit logs.  # crontab -l # less /etc/logrotate.conf can be checked for daily logrotation as well If a program can be located, this is not a finding. Otherwise, query the SA. If there is one that is demonstrable (and runs automatically), this is not a finding. If the SA runs it manually, it 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. |
| Least Functionality | Checks to see if the system is a print server and the configuration is documented with the InfoSec. | Ask the SA if the system is a print server or a client of another server. If it is either of these, ask the SA if it is documented with the InfoSec. If the printer configuration is not documented with the InfoSec, then this is a finding. |
| Least Functionality | Checks to see if an anonymous ftp server is active and documented by the InfoSec. | Perform the following to determine if a system is capable of anonymous ftp:   # ps -ef |grep ftpd  # grep ftp /etc/passwd  Use the command ftp to activate the 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 successful, ask if the use of anonymous FTP on the system is documented with the InfoSec. If it is not, then this is a finding. |
| Boundary Protection | Checks to see if anonymous ftp is segregated in the network DMZ. | Perform the following to determine if a system is capable of anonymous ftp:   # ps -ef |grep ftpd  # grep ftp /etc/passwd  Ask the SA if the server is on a separate subnet located in a DMZ. If it is not, then this is a finding. |
| Least Functionality | Checks to see if File Service Protocol (FSP) is enabled. | To determine if fsp is enabled, perform the following:   # grep in.fspd /etc/inetd.conf   # netstat -an |grep fspd  If an entry for fsp is found, then this is considered a finding. |
| Least Functionality | Checks to see if TFTP is active. | Perform the following to determine if TFTP is active:  Solaris,   # grep -v "^#" /etc/inetd.conf |grep tftp  Solaris 10   # svcs tftp  Linux   # chkconfig --list | grep tftp  Or  # chkconfig tftp  If TFTP is found to enabled, ask the SA if it is documented with theI InfoSec. This is a finding if it is not documented. |
| Least Functionality | Checks to see if the uucp service is enabled. | Perform the following to determine if uucp is active.  Solaris,    # grep uucp /etc/inetd.conf  Solaris 10  # svcs uucp  Linux  # chkconfig uucp  Or    # chkconfig --list | grep uucp  If UUCP is found to be enabled, then this is a finding. |
| Least Functionality | Checks to see if Snmp does runs on dedicated hardware. | To check if SNMP is used, execute the following command:    # netstat -a | grep LISTEN | grep snmp.   # netstat -a | grep LISTEN | egrep "161|162"  If there is any output, then ask the SA if this is an snmp server. If it is an snmp server, then ask what other applications run on it. If there is anything other than network management software and DBMS software that is used only for the storage and inquiry of snmp data, this is a finding. |
| Least Functionality | Checks to see if the system is a router, if it is not a router, the default gateway must be set. | Perform the following to determine if a default route is defined:   # netstat -r |grep default  If a default route is not defined, then this is a finding. |
| Least Functionality | Checks to see if routing is implemented on dedicated hardware. | Perform the following to determine if the systems is used for routing:   # netstat -a | grep -i listen | grep route  Ask the SA if the system is used for any other services such as web servers, file servers, DNS servers, or applications servers. If it is used for another service, then this is a finding. |
| Least Functionality | Checks to see if Samba is running. | Perform the following to determine if the Samba server is running:   # ps -ef |grep smbd  If a process is returned as running, ask the SA if the Samba server is operationally required. If it is not, then this is a finding. |
| Least Functionality | Checks to see if the server is a internet network news server; if so, it checks to see if it has been authorized. | Perform:  # ps -e | egrep "innd|nntpd"  If an Internet Network News server is running and not justified and documented by the InfoSec, then this is a finding. |
| Identification and Authentication (Organizational Users) | Checks to see if the UNIX host is bootable in single user mode without a password. | − Solaris  # more /etc/default/sulogin (if it exists) Confirm PASSREQ=NO is not configured  By default Solaris 10 requires a password and the /etc/default/sulogin does not exist.  − Linux - # more /etc/inittab  Confirm the following line is configured: ~~:S:wait:/sbin/sulogin |
| Identification and Authentication (Organizational Users) | Checks to see if the unix host is configured to require a password when booted to single user mode and is documented. | Solaris, HP-UX, AIX, and Linux support single-user mode password.   If the UNIX host is not be configured to require a password when booted to single-user mode and is not justified and documented with the InfoSec, then this is a finding. |
| Identification and Authentication (Organizational Users) | Checks to ensure the Unix host is configured to require a password when booted to single user mode and is located in a controlled access area. | Solaris, HP-UX, AIX, IRIX, and Linux support single-user mode password.   − Solaris 9 # cd /etc/rcS.d # grep sulogin \* The sulogin utility should be called from within the svm start up script.  Additionally,   Solaris 10 # more /etc/default/sulogin (if is exists) Confirm PASSREQ=NO is not configured  − Solaris 10 # more /etc/default/sulogin (if is exists) Confirm PASSREQ=NO is not configured   − Linux - # more /etc/inittab  Confirm the following line is configured: ~~:S:wait:/sbin/sulogin  If the UNIX host can not be configured to require a password when booted to single-user mode and is not located in a controlled access area accessible only by SAs, then this is a finding. An access-controlled area is defined as requiring two different checks of an individual's identity and authority before gaining access to the system. |
| Identification and Authentication (Organizational Users) | Check to see if an enabled account on the system is password protected. | Examine the /etc/shadow (or equivalent) looking for accounts with blank passwords using the following commands:   ▪ SOLARIS  # pwck    ▪ HP-UX  # pwck -s or authck -p  ▪ AIX  # pwdck -n ALL  ▪ Linux # grep nullok /etc/pam.d/system-auth  If an entry for nullok is found, then this is a finding on Linux. |
| Authenticator Management | Checks to see if password lengths are compliant with IRS requirements of 8 characters or more. | − Solaris Confirm PASSLENGTH is set to 8 or more. # grep PASSLENGTH /etc/default/passwd    − Linux  Confirm pass\_min\_len is set to 8 or more for each user. # grep minlen /etc/pam.d/passwd  If a password does not contain a minimum of 8 characters, then this is a finding. If the system does not have the capability to enforce greater than 8 characters, then the password length should be set to 8. |
| Authenticator Management | Checks to see if password complexity is enforced when possible depending on the UNIX variant that is deployed. | Verify that a combination of alpha and numeric or special characters is required for a password.  − Solaris 9 and prior This check is not applicable.   − Solaris 10 Confirm MINLOWER is set to at least 1, MINUPPER is set to at least 1, MINSPECIAL is at least 1, and MINDIGIT is at least1. # egrep "MINLOWER|MINUPPER" /etc/default/passwd    − Linux  # egrep lcredit|ucredit /etc/pam.d/system-auth   Lcredit and ucredit should be set to -1. |
| Authenticator Management | Checks to see if passwords are changed every 60 days at a minimum for privileged user accounts and 90 days for normal user accounts. | − Solaris Confirm the max days field (the 5th field) is set to 60 or less for privileged user accounts, 90 or less for normal user accounts, but not 0 for each user. # more /etc/shadow    − Linux  Confirm the max days field (the 5th field) is set to 60 or less for privileged user accounts, 90 or less for normal user accounts, but not 0 for each user. # more /etc/shadow  If passwords are not changed at least every 60 days for privileged user accounts and 90 days for normal user accounts, then this is a finding. |
| Authenticator Management | Checks to ensure authentication responses are not automated/scripted by users. | Interview the InfoSec or SA and ask if passwords can be automated through function keys, scripts, or other methods where passwords may be stored on the system. |
| Authenticator Management | Check to see if passwords cannot be changed more than once every 1 day. | − Solaris Confirm the min days field (the 4th field) is set to 1 or more for each user. # more /etc/shadow   − Linux  Confirm the min days field (the 4th field) is set to 1 for each user. # more /etc/shadow  If passwords can be changed more than once every 24 hours, then this is a finding. |
| Authenticator Management | Check to see if passwords are allowed to be reused within the last 24 changes. | ▪ Solaris Confirm HISTORY is set to 24 or more. # grep HISTORY /etc/default/passwd   ▪ Linux  # ls /etc/security/opasswd # more /etc/pam.d/system-auth |grep password |  grep pam\_unix.so | grep remember  If /etc/security/opasswd does not exist, then this is a finding. If the 'remember' option in /etc/pam.d/system-auth is not set to 24, then this is a finding.  If passwords are reused within the last 24 changes, then this is a finding. |
| Authenticator Management | Check to see if global password configuration files are configured per guidelines. | − Solaris Confirm MINWEEKS is set to 1. # grep MINWEEKS /etc/default/passwd  Confirm MAXWEEKS is set to 8 or less, but not 0. # grep MAXWEEKS /etc/default/passwd  Confirm WARNWEEKS is set to 2 or less. # grep WARNWEEKS  /etc/default/passwd    − Linux  Confirm PASS\_MIN\_DAYS is set to 1. # grep PASS\_MIN\_DAYS /etc/login.defs  Confirm PASS\_MAX\_DAYS is set to 90 or less, but not 0. # grep PASS\_MAX\_DAYS /etc/login.defs  Confirm PASS\_WARN\_DAYS is set to 14 #grep PASS\_WARN\_DAYS /etc/login.defs  If global password configuration files are not configured per guidelines, then this is a finding. |
| Authenticator Feedback | Check to see if the feedback from the information system provides information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information. | Interview InfoSec or SA and ask if any applications or services display the user or service account password during input or after authentication. |
| Cryptographic Module Authentication | Checks to see if the information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module. | Ask the administrator to show how strong crytography is used for authentication. This includes, sshv2, tls, and 128-bit key lengths. Old/weak ciphers or authentication such as sshv1, or ssl <=3, or account password hashes that are not hashed using a current standard hasing algorithm, blf, md5, sha, etc. |
| Cryptographic Protection | Checks to see if the browser is configured for secure socket layer (SSLV2 and SSLv3). | To check if browsers are configured for SSL, select Edit >> Preferences in the browser tool bar, and then select the Privacy and Security menu item. Select the SSL tab and verify that "Enable SSL version 2" and "Enable SSL version 3" is checked under the SSL Protocol versions. If they are not, then this is a finding. (RHEL-FIREFOX Preferences-Advanced-Security) |
| Cryptographic Protection | Checks to see if SSH, or a similar utility is running and SSH v2 is used. | Locate the sshd\_config file:   # find / -name sshd\_config   # more <sshd\_config file location>  Note: Can use the following style syntax (may vary by OS type): # find / -name sshd\_config -print -exec grep -i protocol {} \;   Examine the file. If the variables 'Protocol 2,1' or, 'Protocol 1' are defined on a line without a leading comment, this is a finding.  If the SSH server is F-Secure, the variable name for SSH 1 compatibility is 'Ssh1Compatibility', not 'protocol'. If the variable 'Ssh1Compatiblity' is set to 'yes', then this is a finding. |
| Cryptographic Protection | Checks to see if the Samba web administration tool is used with SSH port forwarding. | SWAT must be utilized with ssh to ensure a secure connection between the client and the server. The ssh daemon on the server must be configured to allow port forwarding. If SWAT is being utilized to administer Samba on the server, perform the following:   # grep AllowTcpForwarding /etc/ssh/sshd\_config  If the line is commented out or set to 'no' and SWAT is in use, then this is a finding. |
| Transmission Confidentiality and Integrity | Checks to see if the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures | Interview the SA or InfoSec to determine if all connections to the server are via \*HTTPS using SSL3.1 or TLS \*SSH or SCP v2 only \*Other communications methods using tunneling via OpenSSL or equivalent FIPS encryption.   Confirm whether all FTI data in transit is encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN). |
| Flaw Remediation | Checks to see if the browser is a supported version. | To view the version number click "Help" then click "About Browser" from the browser tool bar. If the browser version is not supported then this is a finding. |
| Malicious Code Protection | Checks to see if a system vulnerability tool is being run on the system weekly, or at an interval that is compliant with IRS security policy. | Perform the following to check for a security tool executing monthly:   # crontab -l   Check for the existence of a vulnerability assessment tool being scheduled and run monthly. If no entries exist in the crontab, ask the SA if a vulnerability tool is run monthly. In addition, if the tool is run monthly, ask to see any reports that may have been generated from the tool. If a tool is not run monthly, then this a finding. |
| Access Enforcement | Checks to see if the /etc/securetty is owned by root. | # ls -lL /etc/securetty  If /etc/securetty is not owned root, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/securetty file is group owned by root, sys, or bin. | # ls -lL /etc/securetty  If /etc/securetty is not group owned by root, sys, or bin, then this is a finding. |
| Least Privilege | Checks to see if the /etc/securetty is more permissive than 640. | # ls -lL /etc/securetty  If /etc/securetty is more permissive than 640, then this is a finding. |
| Content of Audit Records | Checks to see if the HPUX audomon\_args flag is set to IRS or other more secure settings. | Determine if the following flags are set for auditing:   # tail /etc/rc.config.d/auditing  The AUDOMON\_ARGS flag should be the last line in the file. Look at the arguments and compare them to -p 20, -t 1, -w 90. If any of these differ, this a finding. |
| Least Functionality | Checks to see if the securetcpip command has been used. | The securetcpip command is in /etc. If it is not there, this is a finding.  Perform:   # more /etc/security/config  If the stanza: tcpip: netrc = ftp, rexec is not there, then this is a finding. The stanza indicates the securetcpip command, which disables all the unsafe tcpip commands, (e.g., rsh, rlogin, tftp)has been executed. |
| Account Management | Checks to see if special privileged accounts such as shutdown and halt have been deleted. | Perform the following to check for unnecessary privileged accounts:   # more /etc/passwd  Some examples of unnecessary privileged accounts include halt, shutdown, reboot and who. |
| Account Management | Checks to ensure unnecessary accounts and associated software have are not present on the system. | Perform the following to check for unnecessary user accounts:   # more /etc/passwd  Some examples of unnecessary accounts includes games, news, gopher, ftp. |
| Access Enforcement | Checks the /etc/login.access or /etc/security/access.conf is owned by root. | Check file applicable to the system, login.access or access.conf.  Check /etc/login.access ownership:  # ls -lL /etc/login.access  Check /etc/security/access.conf ownership:  # ls -lL /etc/security/access.conf  If /etc/login.access or /etc/security/access.conf is not owned by root, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/login.access or /etc/security/access.conf is group owned by root. | Check file applicable to the system, login.access or access.conf. .  Check /etc/login.access ownership:  # ls -lL /etc/login.access  Check /etc/login.access ownership:  # ls -lL /etc/security/access.conf  If /etc/login.access or /etc/security/access.conf is not group owned by root, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/login.access or /etc/security/access.conf file is more permissive than 640. | Check file applicable to your system, login.access or access.conf. .  Check /etc/login.access ownership:  # ls -lL /etc/login.access  Check /etc/login.access ownership:  # ls -lL /etc/security/access.conf  If /etc/login.access or /etc/security/access.conf is more permissive than 640, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/sysctl.conf file is not owned by root. | Check /etc/sysctl.conf ownership:  # ls -lL /etc/sysctl.conf  or  # ls -lL /etc/sysconfig/sysctl  If /etc/sysctl.conf is not owned by root, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/sysctl.conf is group owned by root. | Check /etc/sysctl.conf group ownership:  # ls -lL /etc/sysctl.conf  If /etc/sysctl.conf is not group owned by root, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/sysctl.conf is more permissive than 600. | Check /etc/sysctl.conf permissions:  # ls -lL /etc/sysctl.conf  If /etc/sysctl.conf is more permissive than 600, then this is a finding. |
| Access Enforcement | Checks to see if the Linux X86 CTRL-ALT-DEL key sequence has been disabled. | Verify that Linux systems have disabled the <CTRL><ALT><DELETE> key sequence by performing:   # grep ctrlaltdel /etc/inittab  If the line returned is not commented out then this is a finding. |
| Access Enforcement | Checks to see if the /etc/securetty file is group owned by root, sys, or bin. | eck /etc/securetty group ownership:  # ls -lL /etc/securetty  If /etc/securetty is not group owned by root, sys, or bin, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/securetty file owned by root. | Check /etc/securetty ownership:  # ls -lL /etc/securetty  If /etc/securetty is not owned by root, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/securetty file is more permissive than 640. | Check /etc/securetty permissions:  # ls -lL /etc/securetty  If /etc/securetty is more permissive than 640, then this is a finding. |
| Least Functionality | Checks to see if Kickstart or Autoyast are used outside an isolated development lan. | Note: Applies to Solaris 10 and SuSE or Red Hat Linux only. Solaris - Jumpstart Solaris systems utilize bootp to assist Jumpstart. Perform:  # more /etc/bootptab  SuSE - AutoYaST On SuSE systems tftp must be running for AutoYaST to work properly. Check for tftp:  # chkconfig --list tftp  If tftp is found, as the SA if the server is configured for AutoYaST.  Redhat - Kickstart Redhat systems utilize nfs and bootp to assist Kickstart. Perform:  # more /etc/exports  # more /etc/bootptab and ask the SA if any of the exported file systems contain Kickstart images to be installed on a client. |
| Least Functionality | Checks to see if the Linux system is capable of booting multiple operating systems and is not documented with the InfoSec. | Review the applicable boot loader configuration file to ensure it is capable of booting only one operating system. For the grub boot loader, /etc/grub.conf should be reviewed. For the lilo boot loader, /etc/lilo.conf should be reviewed. Locations for these file may differ on older versions of Linux. |
| Least Functionality | Checks to see if the rpc.ugidd daemon is enabled. | To check for the rpc.ugidd daemon perform:   # chkconfig -list rpc.ugidd  Or   # ps -ef | grep -i ugidd  If the daemon is running or installed this is a finding. |
| Least Functionality | Checks to see if the NFS Insecure Option or Insecure Locks options are set. | 1. Determine if an NFS server is running on the system by:    # ps -ef |grep nfsd  If NFS is not running, this test is N/A. If an NFS server is running:   # exportfs -v  2. Confirm that it is not configured with the "insecure" option or "insecure\_locks" option |
| Account Management | Checks to see if the audit\_user file has a different auditing level for specific users. | Perform:   # more /etc/security/audit\_user  If /etc/security/audit\_user has entries other than root, ensure the users defined are audited with the same flags as all users as defined in /etc/security/audit\_control file. |
| Access Enforcement | Checks to see if the audit\_user is owned by root. | Check /etc/security/audit\_user ownership:  # ls -lL /etc/security/audit\_user  If /etc/security/audit\_user is not owned by root, then this is a finding. |
| Access Enforcement | Checks to see if the audit\_user file is group owned by root, sys, or bin. | Check /etc/security/audit\_user group ownership:  # ls -lL /etc/security/audit\_user  If /etc/security/audit\_user is not group owned by root, sys, or bin, then this is a finding. |
| Access Enforcement | Checks to see if the audit \_user file is more permissive than 640. | Check /etc/security/audit\_user permissions:  # ls -lL /etc/security/audit\_user  If /etc/security/audit\_user is more permissive than 640, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/lilo.conf is more permissive than 600. | Applies only to Solaris 10, when Solaris 10 is used to control a Xerox printer.  Check /etc/lilo.conf permissions:  # ls -lL /etc/lilo.conf  If /etc/lilo.conf is more permissive than 600, then this is a finding. |
| Audit Events | Checks to see if the NFS server does have logging implemented. | To enable NFS server logging the 'log' option must be applied to all exported files systems in the /etc/dfs/dfstab. Perform the following to verify NFS is enabled:   # share  The preceding command will display all exported filesystems. Each line should contain a 'log' entry to indicate logging is enabled. If the 'log' entry is not present then this is a finding. If the share command does not return anything, then this is not an NFS server and this is considered Not Applicable. |
| Identification and Authentication (Organizational Users) | Checks to see if the SA ensures that the sec option is not set to none and the default authentication is not set to none. | This check only applies to Solaris. Perform the following on NFS servers:   # grep "^default" /etc/nfssec.conf  Check to ensure the second column does not equal '0'. This would indicate the default is set to none. Perform the following to check currently exported file systems:   # more /etc/exports   Or  # more /etc/dfs/dfstab  If the option 'sec=none' is set on any of the exported file systems, then this is a finding. |
| Access Enforcement | Checks to see if run control scripts execute world writeable programs or scripts. | Perform more command to look in the system startup files to check for files or scripts being executed. Check the permissions on the files or scripts to check if they are world writable. Alternatively, the command    # find / -perm -0002 -type f > wwlist  Will give a list of world writable files that can be checked against the executed files or scripts. If world writeable files are found to be executed from systems startup scripts, then this is a finding. |
| Remote Access | Checks to see if the X server has the correct options enabled. | X servers get started several ways, such as xdm, gdm or xinit. Perform:  # ps -ef |grep X  Output for example:   /usr/X11R6/bin/X -nolisten -ctp -br vt7 -auth /var/lib/xdm/authdir/authfiles/A:0   Check the Xservers file to ensure the following options are enabled:  -audit, -auth.  Xserver files can found in:  /etc/X11/xdm/Xservers /etc/opt/kde3/share/config/kdm/Xservers /etc/X11/gdm/Xservers |
| Remote Access | Checks to see if the Xserver has one of the following options enabled: -ac, -core, -nolock. | X servers get started several ways, such as xdm, gdm or xinit. Perform:  # ps -ef |grep X  Output for example:   /usr/X11R6/bin/X -nolisten -ctp -br vt7 -auth /var/lib/xdm/authdir/authfiles/A:0  The above example show xdm is controlling the Xserver.  Check the Xservers file to ensure the following options are not enabled: -ac, -core, and -nolock .  Xserver files can found in:  /etc/X11/xdm/Xservers /etc/opt/kde3/share/config/kdm/Xservers /etc/X11/gdm/Xservers |

**\*\*\*Exception ( Sun team will take Infosec/server owner approval to provide Xwindow)\*\*\*\***

|  |  |  |
| --- | --- | --- |
| Remote Access | Checks to see if a host using Xwindows host writes .Xauthority files or equivalent. | To check for .Xauthority files being utilized, change directory to a user's home directory and perform:   # ls -la .Xauthority  If the file does not exist, ask the SA if the user is using Xwindows. If the user is utilizing Xwindows and the .Xauthority file does not exist and host based access control is not being used, then this is a finding. |
| Access Enforcement | Checks to see if the xwindows system connections are required If not required, checks to see if they are disabled. | Determine if the X window system is running by:   # ps -ef |grep X  Ask the SA if the X window system is an operational requirement. If it is not, then this is a finding. |
| Access Enforcement | Checks to see if authorized X clients are listed in the X\*.hosts file if the .xauthority utility is not used. | Perform the following to determine if the X server is running:   # ps -ef |grep X  Determine if xauth is being used by:   # 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 none are found and user based access control is not being used, then this is a finding. |

**\*\*\*\* Exception (Sun Team will get approval from application/server owner to continue else kill the xwindow session.) \*\*\***

|  |  |  |
| --- | --- | --- |
| Access Enforcement | Checks to see if access to the xterminal host is limited to authorized clients. | Perform the following to determine if access to the X window system is limited to authorized clients:   # xauth  xauth> list  Ask the SA if the clients listed are authorized. If they are not, then this is a finding. |

**\*\*\*\*\*\*\*\* Exception approval if default user used \*\*\*\*\***

|  |  |  |
| --- | --- | --- |
| Account Management | Check to see if unused default accounts have been disabled. | To determine if unused default system accounts have been disabled perform the following:  − Solaris  # grep "\*LK\*" /etc/shadow  − Linux  # awk -F: '$2 == "\*" {print $0}' /etc/shadow   If there are any unused default system accounts that are not locked or have false for a shell, then this is a finding. The accounts in questions are: guest, demo, games, nuucp, uucp, daemon, bin, man, lpd, sys, nobody, ftp, smtp. Additionally, review the account list for any accounts that would appear to be a site specific test, development or temporary account and ensure these accounts are locked. |

**\*\*\*\*\*\* Sun team will check with application team dependency to follow as provided \*\*\*\*\***

|  |  |  |
| --- | --- | --- |
| Account Management | Checks to see if an access control program is being used. | To determine if tcp wrappers is installed perform the following:  Solaris,   # grep tcpd /etc/inetd.conf  Solaris 10   # svcprop -p defaults inetd | grep tcp\_wrappers    This should return a line with the following:   defaults/tcp\_wrappers boolean true  If the above line contains the word false, then this is a finding on Solaris 10.  Solaris 8 or 9  # grep -i enable\_tcpwrappers /etc/default/inetd  If the value returned is not set to yes and /etc/inetd.conf does not contain tcpd, then this is a finding.  Linux    # rpm -qa |grep tcpd  or Check the services in the /etc/xinetd.d directory that are not disabled for an entry containing noaccess or only\_from.  Ensure an entry returns specifically for tcpd, not tcpdump.  NOTE: Tcpwrappers can also be configured through /etc/host.allow and /etc/hosts.deny. Checks these files for additional access control configuration. |
| Account Management | Checks to see if the access control program is configured to grant and deny system access to specific hosts. | Check for the existence of /etc/hosts.allow and /etc/hosts.deny:   # ls -la /etc/hosts.allow  # ls -la /etc/hosts.deny  # grep "ALL: ALL" /etc/hosts.deny  If the 'ALL: ALL' is in the /etc/hosts.deny file, then any tcp service from a host or network not listed in the /etc/hosts.allow file will not be allowed access. If the entry is not in /etc/hosts.deny or if either of the two files do not exist, then this is a finding. |

**\*\*\*\*\*\*\*\*\*\*\*Genpact infra using HPOV Tools, SNMP trap can we disable.\*\*\*\*\*\*\***

|  |  |  |
| --- | --- | --- |
| Access Enforcement | Checks to see if the snmp community strings have been changed from the default. | Find the snmpd.conf by:   # find / -name snmpd.conf -print  # more snmpd.conf   Search for the community name to check if the password was changed to something other than public, private, snmp-trap or password and which meets the IRS requirements for password construction. The community string will be in plain text. |
| Access Enforcement | Checks to see if the snmpd.conf file is not owned by root and group owned by sys or the application. | Perform:   # find / -name snmpd.conf  # ls -lL <snmpd.conf>  # find / -name \*.mib  If the snmpd.conf file is not owned by root and group owned by sys or the application, then this is a finding. |

**\*\*\*\* No application running using root from Sun Team and same will follow \*\***

|  |  |  |
| --- | --- | --- |
| Access Enforcement | Checks to ensure secure operation of application sessions. | 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.   # ps -ef | more  If the logon session for an application requiring a continuous display does not ensure: - The logon session is not a root session. - The inactivity exemption is justified and documented with the InfoSec. - The display station (e.g., keyboard, CRT) is located in a controlled access area. Then this is a finding. |

**\*\*\*Based on request SA providing sudo access after Genpact SME approval.\*\*\***

|  |  |  |
| --- | --- | --- |
| Access Enforcement | Checks to see if the information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. | Ask the administrator to demonstrate how user and group access is assigned. Find out if roles are assigned for a particular set of users and then that role/group are given only the rights that are required to perform that duty.  The sudo utility could be used for this control objective. |

**\*\*\*\* Privileges account given post genpact SME approval\*\*\*\***

|  |  |  |
| --- | --- | --- |
| Least Privilege | Check to see if privileged accounts on the information system are restricted limited number of individuals with a need to perform administrative duties. | With the help of the SA, review the Administrator group and verify whether or not the person has a valid reason to be in the group. |

**\*\*\*\*\* Sun team will be follow in hardening. If NFS going to implement\*\*\***

|  |  |  |
| --- | --- | --- |
| Access Enforcement | Checks to see if user file systems, removable media, or remote file systems are not mounted with the nosuid option invoked. | mount | grep -v nosuid  Confirm all NFS mounts, floppy & CD drives, and user file systems (e.g., /export/home or /usr/home) are configured with the nosuid option.   If user file systems, removable media, or remote file systems that do not require suid/sgid files are not mounted with the nosuid option invoked, then this is a finding. |

**\*\*\*\*Sun Team will check if any root access provided to public file \*\*\*\***

|  |  |  |
| --- | --- | --- |
| Access Enforcement | Checks to see if there are world writeable files or directories that have not been determined to be public directories. | # find / -type f -perm -002 |more  If there are world writable files, then this is a finding.  # find / -type d -perm -002 |more  If there are world writable directories that are not public directories (e.g., /tmp), then this is a finding. |

**\*\*\*\*\* Sun Team will follow on server if /etc/news file existing.\* \*\*\***

|  |  |  |
| --- | --- | --- |
| Access Enforcement | Checks to see if the /etc/news/nnrp.access file is more permissive than 600. | Check /etc/news/nnrp.access permissions:  # ls -lL /etc/news/nnrp.access  If /etc/news/nnrp.access is more permissive than 600, then this is a finding. |
| Access Enforcement | Checks to see if the files in /etc/news are owned by root or news. | Check /etc/news files ownership:  # ls -al /etc/news  If /etc/news files are not owned by root or news, then this is a finding. |
| Access Enforcement | Checks to see if the /etc/news files group owner is root or news. | Check /etc/news files group ownership:  # ls -al /etc/news  If /etc/news files are not group owned by root or news, then this is a finding. |
| Least Privilege | Checks to see if the /etc/news/hosts.nntp file is more permissive than 600. | Check /etc/news/hosts.nntp permissions:  # ls -lL /etc/news/hosts.nntp  If /etc/news/hosts.nntp is more permissive than 600, then this is a finding. |
| Least Privilege | Checks to see if the /etc/news/nntp.nolimit file permission is securely configured. | Check /etc/news/hosts.nntp.nolimit permissions:  # ls -lL /etc/news/hosts.nntp.nolimit  If /etc/news/hosts.nntp.nolimit is more permissive than 600, then this is a finding. |
| Least Privilege | Checks to see if the /etc/news/passwd/nntp file permission is securely configured. | Check /etc/news/passwd.nntp permissions:  # ls -lL /etc/news/passwd.nntp  If /etc/news/passwd.nntp is more permissive than 600, then this is a finding. |

**\*\*\*\*\*discussion in progress for SA sudo access\*\*\***

|  |  |  |
| --- | --- | --- |
| Separation of Duties | Checks to see if the information system enforces separation of duties through assigned access authorizations. | Ask the administrator if separate roles have been defined for specific tasks. This can be performed using additional groups in UNIX where each role has assigned members that are responsible for a specific task. The SUDO utility, properly configured, could meet this control objective. |

**\*\*\*This has to be done as a process wherein access reconciliation would be done on a periodic basis\*\***

|  |  |  |
| --- | --- | --- |
| Audit Events | Checks to see if the audit system is configured to audit all discretionary access control permission modifications. | − Solaris  # grep flags /etc/security/audit\_control Confirm flags fm or +fm and -fm is configured.  − Linux For LAUS:  # grep "@mode-ops" /etc/audit/filter.conf   # grep "@owner-ops" /etc/audit/filter.conf   (RHEL5 /etc/audit/audit.rules)  For auditd the following system calls should be present in /etc/audit.rules:  -a exit,always -S chmod -S fchmod -S chown -S chown32 -S fchown  -a exit,always -S fchown32 -S lchown -S lchown32 (RHEL5 /etc/audit/audit.rules) |

**\*\*\*Integrated with Qradar \*\***

|  |  |  |
| --- | --- | --- |
| Protection of Audit Information | System and network administrators must not have the ability to modify or delete audit log entries. | 1. Interview the Administrator to identify roles with permissions to modify or delete audit log entries. 2. Interview the Administrator and verify that logs are being |

**\*\*\*\*\*Can you configure management VLAN subnet in allowed host and deny from other?\*\*\*\***

|  |  |  |
| --- | --- | --- |
| Device Identification and Authentication | Checks to see if the information system identifies and authenticates specific devices before establishing a connection. | Ask the administrator if specific hosts or devices have been determined to need to authenticate or identify themselves before a connection can be established? If so, are these hosts required to identify/authenticate by IP address, MAC Address, or via a Radius server? Example: Some UNIX servers use /etc/host.allow and /etc/host.deny files. PAM authentication is also another method. |

**\*\*\*\*\*\*\*Servers which are integrated with Identity manager it will be follow same else sun team will look possibility for manual.\*\*\***

|  |  |  |
| --- | --- | --- |
| Authenticator Management | Checks to see if passwords contain information such as names, telephone numbers, account names, dictionary words, etc. | Interview the SA or InfoSec and ask if passwords are allowed that contain contains information such as names, telephone numbers, account names, dictionary words, etc. |