PRUDENTIAL FINANCIAL, INC

SECURITY ENGINEERING SPECIFICATIONS
FOR RED HAT ENTERPRISE LINUX 8 AND ORACLE LINUX 8
Version 21.1

Contents

A. INTRODUCTION

This document outlines security requirements for Prudential's Red Hat Enterprise Linux 8 and derivative operating systems. It interprets information security controls specified in the Prudential Information Security Control Standards and translates the controls into implementable actions for Red Hat Enterprise Linux 8 and derivative operating. Additionally, it specifies new controls, in addition to those in the Prudential Information Security Control Standard, that are unique to Red Hat Enterprise Linux operating environments but are necessary to properly secure the environments.

This document covers operating system and does not cover the software which are related to infrastructure (e.g. system management software or optional network services). Please see the Appendix and BSC documents, for more detail.

B. APPLICABILITY

Previous UNIX standards are superseded by this document. New systems must be developed/implemented in full compliance to these specifications and existing systems must be brought into compliance. Based on the results of a security risk assessment, business groups that cannot comply with the Prudential Information Security Control Standards should file an exception request, where appropriate, in accordance with the Enterprise Standards exception request process. If running a version lower than specified in the standards, you must file an exception.

This standard is applicable for Red Hat Enterprise Linux 8 and several derivative operating systems:

- Red Hat Enterprise Linux 8 (RHEL 8)
- Oracle Linux 8

C. SECURITY SPECIFICATIONS

This standard is organized into two sections:

- Section 1 provides Baseline Controls that are based on both Prudential standards and NIST and CIS industrial standards that must be implemented on all Prudential Linux systems.
- Section 2 provides High Risk Controls that must be implemented, in addition to the baseline controls, on Prudential Linux systems that are identified as high risk. The process for identifying high-risk systems is defined in the Prudential Information Security Control Standard.

Within each section is a matrix containing the following columns: the controls; a source column identifying whether the source of the control is the Prudential Information Security Control Standards or a new control; a priority rating intended to assist in the prioritization of control implementation based on risk; and implementation columns for Linux. In addition, footnotes describing the risk associated with each control are provided for most controls.

BASELINE CONTROLS

Control	Implementation
1. General User Identification and Authentication Controls	
1.a) System administrators should not login as root. System administrators should login as themselves and switch user (SU) to the root account, when superuser privileges are required. The root account must not be permitted to login over the network.[1] System administrators are permitted to login as root only when booting systems in single user or service mode.	Disable root login from over the network by the following steps: Step 1) /etc/pam.d/login must refer to the PAM securetty module auth. Step 2) Create /etc/securetty file. Allow root to login from /dev/tty1 (Console) and /dev/ttyS0 (Terminal Server.) /etc/securetty file contains a list of tty's that root can log in from.Console tty's are usually /dev/tty1 through /dev/tty6. Serial ports are /dev/ttyS0 and up - Terminal Server ConnectionNetwork tty's are /dev/ttyp1 and up. Related to Qualys Control ID: 3867 Reference: NIST Cyber Security Framework
The setting for SSH server setting	The setting, to disable direct root login, must also be implemented with the 'sshd_config'. The status of the 'PermitRootLogin' must be set to "no" Example: PermitRootLogin no ISO Note: The default setting of OpenSSH for PermitRootLogin setting is 'no' by default it is also acceptable if the setting hasn't been implemented on the host. Related to Qualys Control ID: 2239 Reference: NIST Cyber Security Framework, CIS Benchmark https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-controlling_root_access https://wiki.centos.org/HowTos/Network/SecuringSSH
Administrative Controls may be used if the implementation of technical controls would disable automated remote access activities by the root account that are required to: 1. run business-critical processes 2. run business-critical file transfers 3. safeguard and preserve the consistency and proper function of the Operating System and its supporting subsystems in the event of an emergency.	Administrative Control: System Administrators must log in as their IONs ID and su to the root account. Direct root login to perform non-automated functions is forbidden. All root user access must be logged to authlog, sulog, sudo.log and wtmpx files, according to what is appropriate for the access method used.

[1] Root is a generic user ID.

Control	Implementation
1.b) OpenSSH StrictModes	The StrictModes parameter within the '/etc/ssh/sshd_config' file specifies whether sshd should check file modes and ownership of the user's files and home directory before accepting login. This is normally desirable because novices sometimes accidentally leave their directory or files world-writable. StrictModes parameter must be set to “yes” Example: StrictModes yes Verify the setting $ sudo grep StrictModes /etc/ssh/sshd_config ISO Note: The default setting of OpenSSH for this setting is “yes” and it is also acceptable if the setting hasn’t been implemented on the host. Related to Qualys Control ID: 5290 Reference: CIS Benchmark https://man.openbsd.org/sshd_config
1.c) Print the last user login	The PrintLastLog parameter within the '/etc/ssh/sshd_config' file specifies whether sshd should print the date and time of the last user login when a user logs in interactively. PrintLastLog parameter must be set to “yes” Example: PrintLastLog yes Verify the setting $ sudo grep PrintLastLog /etc/ssh/sshd_config ISO Note: The default setting of OpenSSH for this setting is “yes” and it is also acceptable if the setting hasn’t been implemented on the host. Related to Qualys Control ID: 5287 https://man.openbsd.org/sshd_config
1.d) The time and date of the last user to login to the system must be displayed upon after successfully authenticating to the system.[2]	If /var/log/lastlog exists, the last login time is printed after successfully authenticating to the system.
1.e) When three unsuccessful logins occur, disable the account.[3]	To configure Linux to restrict a user account from logging in after 3 unsuccessful login attempts, the following two files should contain the entries as stated below.

[2] Legitimate users can determine whether an unauthorized user has used their account to access the system.
[3] Unlimited attempts to enter passwords may allow an unauthorized user to guess passwords.

Control	Implementation
	1) The entries in the /etc/pam.d/system-auth file should be stated as follows: auth required pam_faillock.so preauth silent deny=3 unlock_time=0 auth [default=die] pam_faillock.so authfail deny=3 unlock_time=0 auth sufficient pam_faillock.so authsucc deny=3 unlock_time=0 account required pam_faillock.so 2) The entries in the /etc/pam.d/password-auth file should be stated as follows: auth required pam_faillock.so preauth silent deny=3 unlock_time=0 auth [default=die] pam_faillock.so authfail deny=3 unlock_time=0 auth sufficient pam_faillock.so authsucc deny=3 unlock_time=0 account required pam_faillock.so Related to Qualys Control IDs: 9341 (password-auth), 9451 (system-auth)
1.f) Multi Factor Authentication (Optional - This is not applicable if MFA is not enabled)	/etc/pam.d/sshd includes below entry auth required pam_securid.so Related to Qualys Control ID: 12602 (Note: No restriction applied)
A screen saver must be enabled after a maximum of 15 minutes of inactivity. The screen saver must force the user to re-authenticate to the system. NOTE: UEG-managed servers do not have attached monitors; the serial port serves as the console and is connected to a terminal server. In many instances, this control will not be applicable since the lack of a monitor already addresses the risk	The recommended control applies only to Linux desktops. Linux servers do not have attached monitors, therefore screensaver settings are not relevent to secure server configuration. For Linux Desktops: Screen saver locking is dependent upon which window manager is used (xdm, gdm, kde, gnome.) In general, xlock can be invoked to lock any window manager. To enable screensaver locking with Gnome, implement following settings within /etc/dconf/db/local.d/00-screensaver. Note-1: please create the setting file if the file doesn't exist Note-2: The setting can be implemented with other setting file under /etc/dconf/db/*.d . ISO verifies the setting under the directory. [org/gnome/desktop/session] idle-delay=uint32 900 [org/gnome/desktop/screensaver] lock-enabled=true lock-delay=uint32 0 Apply the updated setting # dconf update

Control	Implementation
	Related to Qualys Control ID: 11634 (lock-enabled), 11635 (idle-delay), 11638 (lock-delay) To prevent the user from overriding these settings, create the file /etc/dconf/db/local.d/locks/screensaver with following settings /org/gnome/desktop/session/idle-delay /org/gnome/desktop/screensaver/lock-enabled /org/gnome/desktop/screensaver/lock-delay Users must not override this setting in either their local environment files or by command-line methods. ISO Note: It is highly recommended not to install X Window System if it's not needed. Please do not apply this control if X Window System is not installed on the host. Related to Qualys Control ID: 11636 (idle-delay), 11637 (lock-delay), 13373 (lock-enabled) in /etc/dconf/db/local.d/locks/screensaver References: https://help.gnome.org/admin/system-admin-guide/stable/desktop-lockscreen.html.en https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/using_the_desktop_environment_in_rhel_8/Red_Hat_Enterprise_Linux-8-Using_the_desktop_environment_in_RHEL_8-en-US.pdf
1.g) A user account that is inactive for a period of 60 days must be locked.[4] NOTE: Process accounts are exempt from this requirement.	User account password control parameters are set in Windows Active Directory (communicated through Vintela or SecurPass) and override local Unix server settings. Avoid running the useradd -D -f <value> command with a value of less than 60 to avoid denial of service for legitimate connections Related to Qualys Control ID: 5436
1.h) For the purpose of maintaining separation of duties, requests for Unix account and group provisioning / modification (other than accounts established by OS installation) must be submitted to CSS using the ISAMS system for requisition and approval of Unix server/resource access. Thereafter, CSS will delegate the task of modifying local account and password files to the appropriate local system administration staff. The local administrative staff must not make changes to account and group configurations without direction from CSS (accounts and groups used by the system administration team to	The following widely-deployed infrastructure software accounts and groups are excluded from this provision since they are created automatically at the time of server build or installation of a widely-used infrastructure application:

[4] Accounts that are not used in 60 days may not be needed on the system. Process accounts are exempt from this requirement.

Control	Implementation
manage the operating system are excluded from this rule.)	
1.i) The home directory which is defined in /etc/passwd should be consistent and restricted	The home folders of Non-system local user accounts are defined in /etc/passwd. The home folders must exist and have permission setting 750 or more secure setting. World-Writable permission shouldn't be applied. Note: This control verifies consistency and permission setting of local users' home directory. This control is applicable only for local account. You don't need to create a local account if you don't need it. To fix the issue, review the account to make sure the account is not suspicious. If the account should be being used, create the home directory that is dedicated to the account that owns it. It is preferable to set 750 or more secure setting. World-Writable permission shouldn't be applied. Note: Personal user accounts should be stored and be maintained in Active Directory. Note: Home directories under /prustaff can be provided by NFS share and are excluded from Qualys scan Note: ISO's security scanner is not Active Directory aware so the Qualys controls work only with local accounts Related to Qualys Control ID: 7417 (Existence), 6896 (Permission setting) Reference: NIST Cyber Security Framework
2. Password Controls	
2.a) The minimum length of a password must be eight characters.[5]	/etc/login.defs must have PASS_MIN_LEN set to 8 Note: This control can be applied for local accounts only. But is not applicable for Active Directory based network accounts. The password policy is maintained within AD for the network password. Note: the setting can be obsoleted if PAM is enabled. Please comment it out if you see any errors Related to Qualys Control ID: 1071 Reference: NIST Cyber Security Framework
2.b) Passwords must contain at least one alphabetic and one numeric character. Passwords must not have some form of the user ID embedded in it.[6]	Enforcement of strict passwords is managed by the PAM module. Following line should be implemented.

[5] Reuse of passwords may allow a compromised password to be used over a longer period of time.
[6] Passwords without at least one alpha and one numeric character may be easily guessable.

Control	Implementation
	/etc/pam.d/system-auth password requisite pam_pwquality.so try_first_pass local_users_only retry=3 /etc/pam.d/password-auth password requisite pam_pwquality.so try_first_pass local_users_only retry=3 Following setting must be implemented for both type of the hosts /etc/security/pwquality.conf minlen = 8 dcredit = -1 gecoscheck = 1 Related to Qualys Control IDs: 9494 (minlen in pwquality.conf), 9498 (dcredit in pwquality.conf), 9629 (retry parameter in system-auth), 10731 (retry pameter in password-auth)
2.c) A user's new password cannot be the same as the previous 6 passwords.[5]	This control is defined according to Prudential's Enterprise Password Policy and must be applied. "remember=6" setting must be configured with pam_unix.so in the /etc/pam.d/system-auth file password sufficient pam_unix.so nullok use_authtok sha512 shadow remember=6 Related to Qualys Control IDs: 13242 (system-auth)
2.d) The file or files that store passwords on the host[7]	Access permission for /etc/shadow file must be restricted. chmod 600 /etc/shadow (by default, the /etc/shadow should already not be world readable) Related to Qualys Control ID: 2188 Reference: NIST Cyber Security Framework, CIS Benchmark
2.e) Permission settings for '/etc/passwd' file on the host	The access permission for /etc/passwd must be set as 644 or more secure setting Related to Qualys Control ID: 2152 Reference: NIST Cyber Security Framework, CIS Benchmark
2.f) Passwords must never be sent in clear text across the network[8].	Standard security products can be used to protect passwords while in transit across a network. Refer to the Enterprise Standards Database for a list of approved security products
2.g) User passwords must expire at least every 90 days[9]. System, application installation, and process	If 13 weeks = 91 days then /etc/login.defs must have PASS_MAX_DAYS set to 91. For each account, set the fifth field in the /etc/shadow file to 91.

[7] Files that contain passwords and are world readable will allow any user of the system to use a cracking program to discover passwords for other accounts.
[8] A network sniffer can be used by an unauthorized user to obtain passwords that are sent in cleartext form over a Local Area Network.
[9] Passwords that are used for a long period of time are susceptible to long term password guessing, and a compromised password may be used by an unauthorized user over a longer period of time.

Control	Implementation
accounts plus Prudential Securities trading floor UNIX systems are exempt from this requirement. Password control granularity in Unix is based on weeks, not days. This leaves the choice to either 12 weeks (84 days), or 13 weeks (91 days). Unix cannot be set to 4 weeks since that would override the Windows and AD policy of 90 days and result in locally managed Unix passwords being changed 2 days prematurely, creating a denial of service problem for the end user. Therefore, locally based Unix passwords must be controlled by a local MAXAGE setting of 13 (91 days). The 13 week configuration setting however will only apply to locally based service accounts (which do not have to conform to the 90 day rule), since IONs IDs actually have their password propagated from the Windows environment which IS set to a maximum of 90 days.	Related to Qualys Control ID: 1073
2.h) Weak hash algorithms must not be used	See the latest Encryption Algorithm Engineering Specifications in the ISO's web site. MD5 must not be used. SHA256 or SHA512 are allowed according to Prudential's Data Encryption Algorithm Standards Example: /etc/sysconfig/authconfig PASSWDALGORITHM=sha512 Related to Qualys Control ID: 2801 Reference: NIST Cyber Security Framework
2.i) Password Authentication must be enabled with OpenSSH Server	ChallengeResponseAuthentication setting in the '/etc/ssh/sshd_config' file determines whether or not challenge-response authentication is allowed. ChallengeResponseAuthentication must set to "yes" and PasswordAuthentication must set to "no" ChallengeResponseAuthentication yes PasswordAuthentication no Related to Qualys Control ID 5365, 101415 (ChallengeResponseAuthentication), 3676 (PasswordAuthentication)
2.j) PAM must be enabled with OpenSSH Server	UsePAM setting in the '/etc/ssh/sshd_config' activates the Pluggable Authentication Module using session and account module processing along with ChallengeResponseAuthentication with OpenSSH Server. UsePAM setting must be set to 'yes'

Control	Implementation
	UsePAM yes Related to Qualys Control ID 5381
2.k) Empty password not allowed to login to the host	When password authentication is allowed, the PermitEmptyPasswords parameter within the '/etc/ssh/sshd_config' file specifies whether the server allows direct login to accounts with empty password strings. PermitEmptyPasswords parameter must be set to “no”. Example: PermitEmptyPasswords no Verify the setting $ sudo grep PermitEmptyPasswords /etc/ssh/sshd_config Related to Qualys Control ID: 2240 Reference: CIS Benchmark, NIST Cyber Security Framework https://man.openbsd.org/sshd_config
3. Advisory Warning Messages	
3.a) The warning message should appear prior to login:	Implement the warning message into /etc/issue Text of Advisory Warning Message is found in the *IS Control Standards* section 6.2.5 -- Requirements for Advisory Warning Messages. [10] OpenSSH Server sshd_config file: Banner /etc/issue Related to Qualys Control ID: 2241 (OpenSSH), 3778 (Contents within the /etc/issue file)
3.b) The platform/hardware related information must not be disclosed with the Warning message	If the platform information is disclosed to the user, it may give security related information to a malicious user. Following flags must not be listed. Also, do not include OS name (e.g. Red Hat Enterprise Linux 8) or Kernel version (e.g. Kernel 4.14 or Kernel \r) Please do not leave information about the system in /etc/motd. /etc/issue. Flag | Meaning \m | Hardware type \r | Operating System release

[10] A warning banner is required to deter unauthorized attempts to access a system and to provide due diligence in legal cases.

<table>
<tr><th>Control</th><th>Implementation</th></tr>
<tr><td></td><td>
<table>
<tr><td>\s</td><td>Operating System name</td></tr>
<tr><td>\v</td><td>Operating System version</td></tr>
</table>

/etc/issue.net
<table>
<tr><td>Flag</td><td>Meaning</td></tr>
<tr><td>%m</td><td>Hardware type</td></tr>
<tr><td>%r</td><td>Operating System release</td></tr>
<tr><td>%s</td><td>Operating System name</td></tr>
<tr><td>%v</td><td>Operating System version</td></tr>
</table>

The name or the version of the operating system also should not be hard coded in the setting files.
e.g. “Red Hat Enterprise Linux”, “Oracle Linux” or “Kernel” should also not be in the setting files

Related to Qualys Control ID: 8122 (/etc/issue) 8123 (/etc/motd), 8124 (/etc/issue.net)
Reference: NIST Cyber Security Framework</td></tr>
<tr><td>3.c) File permission settings for login banner setting files</td><td>The permission setting of /etc/issue and /etc/motd file must be set to 644 or MORE SECURE
The Owner and Group should be root:root

Example:
sudo chmod 644 /etc/issue
sudo chmod 644 /etc/motd

Related to Qualys Control ID: 2264 (/etc/issue), 2265 (/etc/motd)
Reference: NIST Cyber Security Framework, CIS Benchmark</td></tr>
<tr><td colspan="2">4. Access Controls</td></tr>
<tr><td>4.a) File permissions on security critical files located in the /etc directories must be set to prevent unauthorized re-configuration of the system[11].</td><td>Set file permissions for security critical files in the /etc directory consistent with the permissions set during installation of the operating system.Qualys PC's module will report any files in /etc that have inadequate permission settings.

Related to Qualys Control ID: 2602</td></tr>
<tr><td>4.b) File permissions on system binaries located in the /usr/bin and /usr/sbin directories must be set to prevent the insertion of unauthorized system binaries[12].</td><td>Set file permissions for security critical files in the /usr/bin and /usr/sbin directories consistent with the permissions set during installation of the operating system.Qualys PC's module will report any files in /usr/bin and /usr/sbin that have inadequate permission settings.</td></tr>
</table>

[11] The /etc directory contains system configuration files that may allow a user to circumvent system security.
[12] The /bin directory contains system binaries that may allow unauthorized users to replace security-related programs with trojan horse copies.

Control	Implementation
	Related to Qualys Control ID: 2624 (/usr/bin), 2617 (/usr/sbin)
4.c) File permissions on library files must be set to prevent the insertion of unauthorized system libraries[13].	Set file permissions for security critical files in the /usr/lib and /usr/share/lib directories consistent with the permissions set during installation of the operating system.Qualys PC's module will report any files in /usr/lib and /usr/share/lib that have inadequate permission settings. Related to Qualys Control ID: 9181 (/usr/lib directory), 9182 (files under /usr/lib)
4.d) File permissions on audit files must be set to prevent unauthorized modification of system audit trails[14].	Set file permissions for security critical files in the /var and /etc subdirectories directories to be consistent with the permissions set during installation of the operating system.
4.e) File permissions on cryptographic-related files must be set to prevent unauthorized access to those files[15].	SSH is the standard encrypted communications software used on Prudential's Unix servers. It installs with appropriately restricted file permissions. Commands to ensure appropriate file permissions: The file must be owned by administrative user and group, such as root:root or root:ssh_keys chmod 640 /etc/ssh*/*key chmod 640 /etc/ssh*/random_seed (if applicable) chmod 644 /etc/ssh*/moduli (where file is present) chmod 700 /.ssh2/hostkeys ensure that the root account's private key is readable by root only (name can vary) Related to Qualys Control ID: 100498 (ssh2), 101399 - 101401 (*key files), 101402 (random_seed), 1001403 (moduli)
4.f) File permissions on cron and at files must be set to restrict access to only the file owner[16].	Set /etc/cron files permissions to 644 or MORE SECURE setting. Note: /etc/cron.allow and /etc/at.deny may not exist example chmod 600 /etc/cron.allow chmod 644 /etc/cron.deny chmod 600 /etc/at.allow chmod 644 /etc/at.deny Related to Qualys Control ID: 5057 (cron.allow), 4772 (at.allow), 5796 (cron.deny), 7356 (at.deny)

[13] The /lib directory contains system libraries that are used by system binaries that may allow unauthorized users to replace security-related libraries with trojan horse copies.
[14] If an unauthorized user can access system audit files, they may be able to modify audit data to prevent detection of the intrusion.
[15] If an unauthorized user can access files that contain encryption keys, they may be able to circumvent security features that rely on the use of cryptography.
[16] If an unauthorized user can access cron or at files, they may be able to execute procedures on behalf of another user. If the other user is root they may be able to circumvent system security features.

<table>
<tr><th>Control</th><th>Implementation</th></tr>
<tr><td>4.g) The following accounts should not be permitted to use the cron and at facilities:[17]

daemon
bin
smtp
nuucp
listen
nobody
noaccess
sync
halt
shutdown
news</td><td>Insert the following list of restricted accounts into the /etc/cron.deny and /etc/at.deny files.
All other OS maintenance accounts have their shells set to /sbin/nologin or /bin/false by default and can not run at or cron jobs

Related to Qualys Control ID:
<table>
<tr><th></th><th>/etc/cron.deny</th><th>/etc/at.deny</th></tr>
<tr><td>daemon</td><td>100457</td><td>100482</td></tr>
<tr><td>bin</td><td>100458</td><td>100483</td></tr>
<tr><td>smtp</td><td>100459</td><td>100484</td></tr>
<tr><td>nuucp</td><td>100460</td><td>100485</td></tr>
<tr><td>listen</td><td>100461</td><td>100486</td></tr>
<tr><td>nobody</td><td>100462</td><td>100487</td></tr>
<tr><td>noaccess</td><td>100463</td><td>100488</td></tr>
<tr><td>sync</td><td>101270</td><td>101274</td></tr>
<tr><td>halt</td><td>101271</td><td>101275</td></tr>
<tr><td>shutdown</td><td>101272</td><td>101276</td></tr>
<tr><td>news</td><td>101273</td><td>101277</td></tr>
</table></td></tr>
<tr><td>4.h) Set file permissions on SUID and SGID files to prevent unauthorized user access. Remove SUID and SGID access to files that are not required for system operation.[18]</td><td>A list of standard allowed Setgid and Setuid files and their appropriate file permissions are maintained in the list in Qualys. Files detected by Qualys that fall outside of this allowed list are flagged during the scan.

The detailed list of criteria for system related SetUID and SetGID files is available in Appendix 3 in this document.

The detailed list of criteria for optional / 3rd party software related SetUID and SetGID files is available in BSC Document

Related to Qualys Control ID: 100558 (SetUID), 100559 (SetGID)
Reference: NIST Cyber Security Framework</td></tr>
<tr><td>4.i) Application user access to command shells must be disabled. Application users must not be able to use escape characters to exit into a command shell[19].</td><td>The last field of each line in the /etc/passwd file should be set to start an application, or should be set to /bin/false. A valid UNIX shell should not be specified for application users.To prevent users from escaping into a command shell, set the trap parameter in the /etc/profile file to null as follows:
trap "" 1 2 3</td></tr>
</table>

[17] These account are not valid user accounts. If they are being used to run cron and at jobs, they are being used by an unauthorized user.
[18] SUID and GUID files may allow an unauthorized user to exit an SUID or GUID process and assume the privileges of the file owner.
[19] Accounts that are allowed shell access maybe used to attack the system and gain privileges of other users.

Control	Implementation
4.j) The default initial file creation mask "umask" must be set to allow read, write, execution by owner only and at most read and execution by group.[20] The umask setting for user home directories should be set to allow read, write, execution by owner only and (at most) read and execute by group. The umask may be more restrictive, but should not be less restrictive.	/etc/login.defs must have UMASK set to 027. Set the default umask parameter in the /etc/profile to 022. This is a user-controlled setting (not controlled by root.) Users are advised to set the umask parameter in their shell's environment file to 027 (.profile, .cshrc, .bashrc.) Related to Qualys Control ID: 3371 (/etc/profile) Reference: NIST Cyber Security Framework
4.k) File permissions on device drivers located in the /dev directory must be set to prevent the insertion of unauthorized device drivers.[21] File permissions on OS device drivers, socket files and named pipes must not be changed from the defaults file permissions that they are created with, or they will not function for the purpose they were intended.	Set file permissions for files in the /dev directory consistent with the permissions set during installation of the operating system. Related to Qualys Control ID: 2628 Reference: NIST Cyber Security Framework
4.l) Directory permissions on security critical /root directory must be set to prevent unauthorized re-configuration of the system	It is not required but is recommended to set permission for /root 700 or more restricted access Example chmod 700 /root Related to Qualys Control ID: 6337 Reference: NIST Cyber Security Framework
4.m) Permission settings for '/etc/rsyslog.conf' file on the host	The access permission must be set as 644 or more secure setting, such as 600. The owner and group of the file must be "root:root". Related to Qualys Control ID: 7369 Reference: NIST Cyber Security Framework
4.n) Permission settings for '/etc/group' file on the host	The access permission for /etc/group must be set to at least 644 or more secure setting. The owner of the file must be "root" account. Related to Qualys Control ID: 2152 Reference: NIST Cyber Security Framework, CIS Benchmark
4.o) Permission setting for /etc/login.defs file	The '/etc/login.defs' file is responsible for defining site-specific configuration requirements within the shadow login suite. The owner of the directory should be 'root' and the permission setting should be set to 644 or MORE SECURE setting

[20] A weak umask setting will result in newly created files that may allow excessive access.
[21] The /bin directory contains system binaries that may allow unauthorized users to replace security-related programs with trojan horse copies.

Control	Implementation
	Verify – You should see 644 or MORE SECURE setting $ ls -l /etc/login.defs Related to Qualys Qualys Control ID: 101392/2261 Reference: NIST Cyber Security Framework
4.p) Permission setting for /etc/profile file	The '/etc/profile' file contains system-wide environment variables such as the file creation mask (UMASK) and terminal types. The owner of the directory should be 'root' and the permission setting should be set to 644 or MORE SECURE setting Verify – You should see 644 or MORE SECURE setting $ ls -l /etc/profile Related to Qualys Qualys Control ID: 101393/2268 Reference: NIST Cyber Security Framework
4.q) Permission setting for /var/spool/cron directory	The '/var/spool/cron' directory contains crontab files used to run commands at pre-defined intervals/times by the 'cron' daemon. The owner of the directory should be 'root' and the permission setting should be set to 644 or MORE SECURE setting Note: You need to update the permission if you have the directory on the host. If you don't have the directory, that should be compliance Verify – You should see 644 or MORE SECURE setting $ ls -l /var/spool/cron Related to Qualys Qualys Control ID: 7554/7555 Reference: NIST Cyber Security Framework
4.r) Permissions set on the file /boot/grub2/grub.cfg	The setting file is used to configure the boot options. The permissions/ownership to the file /boot/grub2/grub.cfg should be restricted in order to prevent non-root/unauthorized users from changing the file. The owner should be root:root and the permission setting should be set to 644 or MORE SECURE setting for /boot/grub2/grub.cfg Verify $ ls -l /boot/grub2/grub.cfg Example of modifying the owner and permission # chown root:root /boot/grub2/grub.cfg # chmod 644 /boot/grub2/grub.cfg Related to Qualys Qualys Control ID: 9340 Reference: NIST Cyber Security Framework

Control	Implementation
4.s) Permission settings for SSH server setting file on the host	Regarding to the controls which are related to SSH server in this document, the setting should not be configured by unauthorized people. The permission setting file should be set to 644 or MORE SECURE setting (if possible, 600 is recommended) Example # chmod 600 /etc/ssh/sshd_conf Related to Qualys Control ID: 2158 (/etc/ssh/sshd_conf) Reference: NIST Cyber Security Framework
4.t) SELinux status	Enable SELinux with enforcing mode, set SELINUX=enforcing within /etc/selinux/config. To verify the current SELinux status execute following command $ sudo sestatus |grep "SELinux status" Verify “SELinux status” is showing “enabled” If the command above is showing “disabled”, please update following line within /etc/selinux/config SELINUX=enforcing or SELINUX=permissive And reboot the system ISO Note: The setting is “permissive” with UEG Managed RHEL 8 / Oracle Linux 8 but “enforcing” is MORE SECURE and is also acceptable. Related to Qualys Control ID: 11435 (Running SELinux enabled/disabled) Reference: CIS Benchmark

4.u) SELinux Mode	To verify the SELinux stting execute following command
	$ sudo grep ^SELINUX= /etc/selinux/config
	SELINUX=permissive
	or
	SELinux Mode must be set to “permissive” or “enforcing”.
	Verify “Mode from config file” with sestatus command
	$ sestatus|grep "Mode from config file"
	Mode from config file: permissive
	
	Verify current mode with getenforce command
	$ sudo getenforce
	Or, verify “current mode” with sestatus command
	$ sudo sestatus |grep "Current mode"
	Execute following commands to apply “permissive (0)” mode or “enforcing (1)” mode
	$ sudo setenforce 0

Control	Implementation
	or $ sudo setenforce 1 Related to Qualys Control IDs: 7431 (Setting within '/etc/selinux/config' file), 10804 (Running SELinux mode), 11436 ('Mode from config file' should be equivalent to the setting within '/etc/selinux/config' file) Reference: CIS Benchmark
4.v) SELinux Policy setting	SELinux policy must be set to targeted (default) or mls (multi-level security). Set SELINUXTYPE targeted or mls within /etc/selinux/config file To verify the setting, execute following command # grep SELINUXTYPE /etc/selinux/config SELINUXTYPE targeted or mls should be returned To verify the current execute following command $ sudo sestatus |grep "Loaded policy name" Verify “SELinux status” is showing “targeted” Related to Qualys Control IDs: 7432 (setting), 12880 (loaded policy) Reference: CIS Benchmark https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/mls

4.w) Do not run service with “unconfined” context is applied	SELinux will not show any errors with unconfined role
	
	There are potentially several reasons why the service is labeled as unconfined
	If the service was not launched by Systemd, please restart the service with Systemd
	$ sudo systemctl restart <name_of_service>
	
	If the service is re-labelled as unconfined with “chcon” command, please re-label the executable with following command
	$ sudo restorecon -Rv </path/to/the/service>
	
	If the service is re-labelled as unconfined with “semanage” command, please re-label the executable with following command
	$ semanage fcontext -d </path/to/the/service>
	OR
	$ semanage fcontext -a -t <context> </path/to/the/service>
	
	Verify if there are any running service with Unconfined context
	$ ps -eZ|grep unconfined

Control	Implementation
	ISO Note: Since Qualys scanner performs SSH access to the host, following processes or commands are used during the scan and are allowed. qualys-cloud-agent, sshd, bash, sh, ps, grep, sed Related to Qualys Control ID: 17165 Reference: CIS Benchmark https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-targeted_policy-unconfined_processes https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-working_with_selinux-selinux_contexts_labeling_files#sect-Security-Enhanced_Linux-SELinux_Contexts_Labeling_Files-Persistent_Changes_semanage_fcontext https://wiki.centos.org/HowTos/SELinux
4.x) Unnecessary SELinux packages should not be installed on the host	Unnecessary package should not be installed from security perspective. Additionally, there are known setroubleshoot exploits such as arbitrary script injection attacks Example $ sudo yum remove setroubleshoot Related to Qualys Control ID: 7427 Reference: CIS Benchmark
4.y) Permission setting for AWS CLI Credentials file	~/.aws/credentials file contains the user's credentials, such as AWS Access Key ID and AWS Secret Access Key, in clear text (with no encryption) for the user's AWS account. The permission setting for ~/.aws/credentials must be set to 700 or more secure setting (Group and Other user must have no access) Note: If AWS CLI is not installed/removed on the host, please do not install the package and remove ~/.aws/credentials file on the host. **Note: UEG is not responsible for your RACF account and your AWS account. If this control is causing violation with Server Compliance, Business is responsible to remediate the issue.** Note: This control is primary for cloud instances. AWS CLI may not be installed on RHEL 8 / Oracle Linux 8 especially if the host is used in on-prem site. That is MORE SECURE and shouldn't cause any violation. Example chmod 600 ~/.aws/credentials Related to Qualys Control ID: 101290

Control	Implementation
4.z) Permission setting for AWS CLI cache directory	~/aws/cli/cache directory contains the cache data between the user and AWS and may contain sensitive data. ~/aws/cli/cache must be set to 700 or more secure setting (Group and Other user must have no access) Note: If AWS CLI is not installed/removed on the host, please do not install the package and remove ~/aws/cli/cache directory on the host. **Note: UEG is not responsible for your RACF account and your AWS account. If this control is causing violation with Server Compliance, Business is responsible to remediate the issue.** Note: This control is primary for cloud instances. AWS CLI may not be installed on RHEL 8 / Oracle Linux 8 especially if the host is used in on-prem site. That is MORE SECURE and shouldn't cause any violation. Example chmod 700 ~/.aws/cli/cache Related to Qualys Control ID: 101380
5. Network Access Controls	
5.a) All network services that are not required to support business applications or system administration must be disabled.	Disable unnecessary network services. The list of services is available in Appendix 1
5.b) NTP service (Chrony) must be installed and must be enabled	From RHEL 8 / Oracle Linux 8, Chrony must be used as default NTP client service, instead of NTPD. NTP Service (Chrony) must be installed and must be enabled. Enable Chrony # systemctl enable chronyd # systemctl start chronyd Verify # systemctl status chronyd ISO Note: Need to clarify which NTP Service should be used as standard in Prudential Related to Qualys Control ID: 11335 (Service status) Reference: CIS Benchmark https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_basic_system_settings/using-chrony-to-configure-ntp https://chrony.tuxfamily.org/doc/3.5/chrony.conf.html

Control	Implementation
	Relevant pool setting must also be configured in your environment for Chrony With GT UEG at Prudential, following setting must be used. pool ntppool-mnncpo.prudential.com iburst ISO Note: If NTP pool is not listed above, please reach out to ISO Vulnerability Management Team. Related to Qualys Control ID: 13138 (pool setting) Reference: CIS Benchmark
5.c) The telnet protocol must not be installed.[22]	The service should not be installed by default. Step 1) To disable telnet-server systemctl disable telnet.socket systemctl stop telnet.socket Step 2) Ensure the service is not started in any of the following places:/etc/rc* files /etc/rc?.d//etc/inittab /var/spool/cron/crontabs Related to Qualys Control ID: 9919 Reference: CIS Benchmark
5.d) The file transfer protocol must not be installed.[23]	The service is not installed with the Red Hat Enterprise Linux by default. Step 1) To disable ftpd systemctl disable vsptfd.service systemctl stop vsptfd.service Step 2) Ensure the service is not started in any of the following places:/etc/rc* files /etc/rc?.d//etc/inittab /var/spool/cron/crontabs Related to Qualys Control ID: 9884 Reference: CIS Benchmark
5.e) The named daemon must only be running on servers that perform the name service function.[24]	Ensure there is no /etc/named.conf file present, and named will not startEnsure the service is not started in any of the following places:/etc/rc* files /etc/rc?.d//etc/inittab /var/spool/cron/crontabs

[22] The telnet protocol sends passwords in cleartext, which is vulnerable to sniffing attacks. In addition, the telnet daemon on certain versions of UNIX are susceptible to denial-of-service attacks.
[23] The ftp protocol sends passwords in cleartext, which is vulnerable to sniffing attacks. In addition, the ftp daemon on certain versions of UNIX can be exploited to obtain remote access.
[24] Certain versions of Bind can be exploited to obtain remote access or cause a denial-of-service.

Control	Implementation
5.f) The remote shell daemon must be disabled.[25]	The service is not installed with the Red Hat Enterprise Linux by default. It is highly recommended not to install the service if you don't need it. Step 1) To disable rsh systemctl disable rsh.socket systemctl stop rsh.socket Step 2) Ensure the service is not started in any of the following places:/etc/rc* files /etc/rc?.d//etc/inittab /var/spool/cron/crontabs Related to Qualys Control ID: 14112 (running service), 9890, 10636 Reference: CIS Benchmark
5.g) The remote login daemon must be disabled.[26]	The service is not installed with the Red Hat Enterprise Linux by default. It is highly recommended not to install the service if you don't need it. Step 1) To disable rlogin systemctl disable rlogin.socket systemctl stop rlogin.socket Step 2) Ensure the service is not started in any of the following places:/etc/rc* files /etc/rc?.d//etc/inittab /var/spool/cron/crontabs Related to Qualys Control ID: 14112 (running service), 9917 Reference: CIS Benchmark
5.h) The remote execution daemon must be disabled.[27]	The service is not installed with the Red Hat Enterprise Linux by default. It is highly recommended not to install the service if you don't need it. Step 1) To disable rexec systemctl disable rexec.socket systemctl stop rexec.socket Step 2) Ensure the service is not started in any of the following places:/etc/rc* files /etc/rc?.d//etc/inittab /var/spool/cron/crontabs

[25] Remote shell is susceptible to IP spoofing attacks that will allow remote access to a system. In addition, it can be exploited to use a compromised system to access other trusted systems.
[26] Remote shell is susceptible to IP spoofing attacks that will allow remote access to a system. In addition, it can be exploited to use a compromised system to access other trusted systems.
[27] Remote execution is susceptible to IP spoofing attacks that will allow remote execution of commands on a system. In addition, it can be exploited to use a compromised system to execute commands on other trusted systems.

Control	Implementation
	Related to Qualys Control ID: 14112 (running service), 9915 Reference: CIS Benchmark
5.i) The talk and ntalk daemons must only be enabled when required to support system administration activities. If talk or ntalk is enabled, the patches required to appropriately secure the service must be applied. [28]	The service is not installed with the Red Hat Enterprise Linux by default. It is highly recommended not to install the service if you don't need it. Step 1) To disable ntalk systemctl disable ntalk.socket systemctl stop ntalk.socket Step 2) Ensure the service is not started in any of the following places:/etc/rc* files /etc/rc?.d//etc/inittab /var/spool/cron/crontabs Related to Qualys Control ID: 14112 (running service), 10729 Reference: CIS Benchmark
5.j) The uucp daemon must be disabled.[29]	The service is not installed with the Red Hat Enterprise Linux by default. It is highly recommended not to install the service if you don't need it. Step 1) To disable uucp systemctl disable uucp systemctl stop uucp Step 2) Ensure the service is not started in any of the following places:/etc/rc* files /etc/rc?.d//etc/inittab /var/spool/cron/crontabs Related to Qualys Control ID: 14112 (running service), 9916
5.k) The tftp daemon must be disabled [30]	tftp is not installed with the Red Hat Enterprise Linux by default. It is highly recommended not to install the service if you don't need it. tftp can be required to run Red Hat Satellite service. systemctl disable tftp.socket systemctl stop tftp.socket Related to Qualys Control ID: 10849 Reference: CIS Benchmark

[28] The talkd damon can be exploited to remotely execute arbitrary commands with root privileges.
[29] If configure incorrectly, UUCP can allow unauthorized remote command execution and copying of remote files.
[30] The tftp daemon does not authenticate remote connections and can allow unauthorized remote access to files and directories.

Control	Implementation
5.l) The finger daemon must be disabled.[31]	The service is not installed by default. Do not install the service. Related to Qualys Control ID: 14112 (running service)
5.m) The netstat daemon must be disabled.[32]	The service is not installed by default. Do not install the service. Related to Qualys Control ID: 14112 (running service)
5.n) The echo daemon must be disabled.[33]	The service is not installed by default. Do not install the service. Related to Qualys Control ID: 14112 (running service), 1329 (tcp), 1267 (udp)
5.o) The discard daemon must be disabled.	The service is not installed by default. Do not install the service. Related to Qualys Control ID: 1576 (tcp) 3902 (udp)
5.p) The time and daytime daemons must be disabled. UEG-managed systems use the ntpd service for time synchronization.	The service is not installed by default. Do not install the service. Related to Qualys Control ID: 1867 (time tcp), 5254 (time udp), 7416 (daytime tcp), 7415 (daytime udp)
5.q) The chargen daemon must be disabled.	The service is not installed by default. Do not install the service. Related to Qualys Control ID: 7438 (tcp), 7437 (udp)
5.r) The rusersd daemon must be disabled.[34]	The service is not installed by default. Do not install the service. Related to Qualys Control ID: 14112 (running service)
5.s) The rwhod daemon must be disabled.[35]	The service is not installed by default. Do not install the service. Related to Qualys Control ID: 14112 (running service), 9918
5.t) The rstatd daemon must be disabled.[36]	The service is not installed by default. Do not install the service. Related to Qualys Control ID: 14112 (running service), 9894
5.u) The imap and pop3 daemons must be disabled.[37]	Dovecot is the default IMAP / POP3 server of the OS. The service is not installed by default. Do not install the service.

[31] The finger daemon provides user information that can be used to attempt access to those accounts. In addition, multiples versions of finger are susceptible to denial-of-service attacks or can be exploited to gain remote access.
[32] The netstat daemon provides system port, connection, and routing information that can be used to attack the system.
[33] The echo utility when fed by characters from the chargen utility can be used to perform a denial-of service attack.
[34] The rusersd daemon provides information about active accounts on a remote system that could be used to attack the system.
[35] The rwhod daemon contains a buffer overflow that can be exploited to cause a server crash.
[36] The rstat daemon provides information about the host, including when the machine was last booted, how much CPU it is using, how many disks it has, and how many packets have reached it that could be used to determine whether the system should be attacked.
[37] A buffer overflow in the IMAP daemon can be exploited to gain privileged remote access to a server with this service enabled.

Control	Implementation
	If you need to remove Dovecot, Example: sudo yum -y remove dovecot Related to Qualys Control ID: 14112 (running service), 9345, 9887
5.v) httpd is only permitted to run on hosts that must run a web server for a legitimate business reason.	Step 1) To disable Apach HTTP Webserver systemctl disable httpd.service systemctl stop httpd.service Step 2) Ensure the service is not started in any of the following places:/etc/rc* files /etc/rc?.d//etc/inittab /var/spool/cron/crontabs
5.w) The SMTP port must be disabled.[38] The Prudential Internet mail gateway is exempt from this requirement.	Remove/Disable Postfix/Sendmail SMTP Service Since running service may contain vulnerability and can be an attack surface, it is highly recommended to disable service or remove the package on the host. Disable SMTP Service sudo systemctl disable postfix sudo systemctl stop postfix Remove Postfix SMTP service sudo yum remove postfix Postfix SMTP with Send-Only Modify inet_interfaces option within /etc/postfix/main.cf inet_interfaces = loopback-only Note: “localhost” or “127.0.0.1” may also work. Qualys Control ID: 7458 (Postfix) Reference: NIST Cyber Security Framework, CIS Benchmark http://www.postfix.org/postconf.5.html#inet_interfaces
5.x) SNMP must be enabled for Enterprise Systems Management functions.	Step 1) To enable snmpd systemctl enable snmpd.service systemctl start snmpd.service Prudential requires the service to collect log files. If the server is in DMZ, this control should not be applicable and be flagged. For more detail, please see ‘DMZ Servers’ section in High Risk Controls.

[38] Past versions of Sendmail contain numerous vulnerabilities that can allow remote root access to a system. In addition, the SMTP commands VRFY and EXPN provide information about users to a potential attacker.

Control	Implementation
	Related to Qualys Control ID: 9882
5.y) The SNMP.CONF must be set to allow SNMP Management only from the following systems: NETINV01 and NETINV02.	"rwcommunity" must not be used. "rocommunity" should be defined according to your Business Unit Configure the /etc/snmp/snmpd.conf files with the entry defined as follows in Prudential. rocommunity prusrv esmsnmp01.prudential.com rocommunity prusrv esmsnmp02.prudential.com rocommunity prusrv esmsnmp03.prudential.com rocommunity prusrv esmsnmp04.prudential.com rocommunity prusrv esmsnmp05.prudential.com rocommunity prusrv esmsnmp06.prudential.com rocommunity prusrv esmsnmp07.prudential.com rocommunity prusrv esmsnmp08.prudential.com rocommunity prusrv esmsnmp09.prudential.com rocommunity prusrv esmsnmp10.prudential.com rocommunity prusrv esmsnmp11.prudential.com rocommunity prusrv esmsnmp12.prudential.com rocommunity prusrv esmsnmp13.prudential.com rocommunity prusrv esmsnmp14.prudential.com rocommunity prusrv esmsnmp15.prudential.com rocommunity prusrv esmsnmp16.prudential.com rocommunity prusrv esmsnmp17.prudential.com rocommunity prusrv esmsnmp18.prudential.com rocommunity prusrv esmsnmp19.prudential.com rocommunity prusrv esmsnmp20.prudential.com rocommunity prusrv esmsnmp21.prudential.com rocommunity prusrv esmsnmp22.prudential.com rocommunity prusrv esmsnmp23.prudential.com rocommunity prusrv esmsnmp24.prudential.com rocommunity prusrv esmsnmp25.prudential.com rocommunity prusrv esmsnmp26.prudential.com rocommunity prusrv esmsnmp27.prudential.com rocommunity prusrv esmsnmp28.prudential.com rocommunity prusrv esmsnmp29.prudential.com rocommunity prusrv esmsnmp30.prudential.com rocommunity prusrv esmsnmp31.prudential.com rocommunity prusrv esmsnmp32.prudential.com rocommunity prusrv esmsnmp33.prudential.com rocommunity prusrv esmsnmp34.prudential.com rocommunity prusrv esmsnmp35.prudential.com

Control	Implementation
	rocommunity prusrv esmsnmp36.prudential.com rocommunity prusrv esmsnmp37.prudential.com rocommunity prusrv esmsnmp38.prudential.com rocommunity prusrv esmsnmp39.prudential.com rocommunity prusrv esmsnmp40.prudential.com rocommunity public 127.0.0.1 Related Qualys Control ID: 5251 (rocommunity), 5252 (rwcommunity)
5.z) NFS exports must conform to Best Practices guidelines posted on the ISO website[39]	* Refrain from creating world-writeable exports * Ensure current patch levels are applied, particularly those which address issues related to NFS * Export only to those hosts which require the resource (avoid world export) * Production data must not be shared to non-Production hosts * disallow non-UEG-managed remote hosts from accessing NFS share data as root NFS Policy Policy can be found on ISO's web site
5.aa) SAMBA must be disabled and should not be used for file sharing	The service is not installed by default and must not be used and the service must not be running on the host. If your business application requires Samba, please file Security Exceptions To disable Samba systemctl disable smb.service systemctl stop smb.service Related to Qualys Control ID: 9878 Reference: NIST Cyber Security Framework
Static routing must be used	Set the default router for the system by entering the IP address for the system's default router in the /etc/sysconfig/network file.
5.bb) X Window System based applications access controls must be enabled. In addition, remote X Window System must only be used over SSH tunnel connections.[40]	It is highly recommended not to use/install X Window System, if X Window System is not needed If X Window System is being used, to prevent remote access to X Window System, implement following setting within /etc/gdm/custom.conf DisallowTCP=true Related to Qualys Control ID: 1745, 101426
5.cc) Random TCP sequence numbers must be used.[41]	Random TCP sequence numbers are used by default.

[39] Certain underlying RPC processes (statd, lockd, mountd) associated with NFS are vulnerable to exploits that allow remote access. In addition, files systems that are exported without appropriate access permissions can allow unauthorized access to system information.
[40] Daemons associated with Xwindows and CDE contain numerous vulnerabilities that can be exploited to allow remote access.
[41] Systems with predictable TCP sequence numbers are susceptible to session hijacking attacks.

Control	Implementation
5.dd) Port assignments and names of all network services used on the system must be identified by the system.	Add port numbers and names for network services used on the system to the /etc/services file.
5.ee) The system must not respond to broadcast ICMP echo requests.[42]	Prevent ping replies by entering the following command: echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts To implement the setting permanently, Implement following value into one of setting file under /usr/lib/sysctl.d/, /run/sysctl.d/ or /etc/sysctl.d/ directory. net.ipv4.icmp_echo_ignore_broadcasts = 1 Note: it is also preferable to enable net.ipv4.icmp_echo_ignore_all but ICMP request/reply can be commonly used for monitoring the host. ISO will not monitor net.ipv4.icmp_echo_ignore_all parameter. Related to Qualys Control ID: 5962 Reference: NIST Cyber Security Framework, CIS Benchmark Note: Although the description of Control ID 5962 look like the control is checking /etc/sysctl.conf, the results look like the control returns the actual setting value on the host
5.ff) The server must be configured to prevent TCP SYN Flooding attacks. [43]	The 'net.ipv4.tcp_syncookies' setting provides for disabling/enabling SYN flood attack protection. Prevent syn flood attacks by entering the following command: echo "1" > /proc/sys/net/ipv4/tcp_syncookies To implement the setting permanently, Implement following value into one of setting file under /usr/lib/sysctl.d/, /run/sysctl.d/ or /etc/sysctl.d/ directory. net.ipv4.tcp_syncookies = 1 Verify $ cat /proc/sys/net/ipv4/tcp_syncookies 1 Related to Qualys Control ID: 7096 Reference: CIS Benchmark Note: Although the description of Control ID 7096 look like if Qualys control is checking /etc/sysctl.conf, the results look like the control returns the actual setting value on the host

[42] System that respond to ICMP echo requests can contribute to network flooding attacks caused by multiple systems responding to broadcast pings.
[43] SYN Flooding attacks result in a denial-of-service to the target server.

Control	Implementation
5.gg) Status of the 'tcp_max_syn_backlog' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.tcp_max_syn_backlog' parameter specifies the maximum number of incomplete TCP connection requests concurrently held in memory. If the number is too small the host can be overwhelmed by a DoS 'SYN flood' attack. **The default setting is set to "128" and you can leave it as is.** Verify the current setting # cat /proc/sys/net/ipv4/tcp_max_syn_backlog If you want to modify the setting, please modify 'net.ipv4.tcp_max_syn_backlog' setting within '/etc/sysctl.conf' file. Please set the value "128" or bigger. Verify the setting # grep ipv4.tcp_max_syn_backlog /etc/sysctl.conf **If you are using the default setting, the command returns no value.** **If you are using a custom setting, you should see "128" or bigger number.** Related to Qualys Qualys Control ID: 1773 Reference: NIST Cyber Security Framework
5.hh) Bogus error broadcast traffic must be ignored	The 'net.ipv4.icmp_ignore_bogus_error_responses' setting allows the system to ignore certain errors caused by bogus broadcast traffic. To implement the setting permanently, Implement following value into one of setting file under /usr/lib/sysctl.d/, /run/sysctl.d/ or /etc/sysctl.d/ directory. net.ipv4.icmp_ignore_bogus_error_responses = 1 Verify $ cat /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses 1 Related to Qualys Control ID: 6836 Reference: NIST Cyber Security Framework, CIS Benchmark
5.ii) Secure Shell (SSH) must be used as a replacement for the telnet, ftp, rsh, rlogin, rexec and rcp network services NOTE: Depending upon the business requirement, Tibco Cyberfusion is an acceptable alternative to SSH	By default, Linux distributions comes installed with OpenSSH. If OpenSSH is used the following directions apply. The directory is located in /etc/ssh. Hostbased authentication can be accomplished by copying the keys onto the file .ssh/authorized_keys. Un-comment the line in /etc/ssh/sshd_config: AuthorizedKeysFile .ssh/authorized_keys

Control	Implementation
for UNIX server access, command execution and file upload/download	For proper banner display, copy from an existing SSH enabled server /etc/issue and un-comment in /etc/sshd_config: #Banner /etc/issue Edit the /etc/ssh/sshd_config file to set the parameter as follows: HostBasedAuthentication no Note: The default setting of HostBasedAuthentication is “no” with no setting value and is acceptable. https://man.openbsd.org/sshd_config#HostbasedAuthentication Related to Qualys Control ID: 2241 (Banner), 5218 (AuthorizedKeyFile) Reference: CIS Benchmark Related to Qualys Control ID: 2278 (HostBasedAuthentication) NIST Cyber Security Framework
5.jj) Ignore user’s .rhosts and .shosts	The IgnoreRhosts parameter within the '/etc/ssh/sshd_config' file specifies whether to ignore per-user .rhosts and .shosts files during HostbasedAuthentication. IgnoreRhosts parameter must be set to “yes” Example: IgnoreRhosts yes Verify the setting $ sudo grep IgnoreRhosts /etc/ssh/sshd_config ISO Note: The default setting of OpenSSH for this setting is “yes” and it is also acceptable if the setting hasn’t been implemented on the host. Related to Qualys Control ID: 2236 Reference: CIS Benchmark, NIST Cyber Security Framework https://man.openbsd.org/sshd_config
5.kk) Ignore user’s known_hosts setting	The IgnoreUserKnownHosts parameter within the '/etc/ssh/sshd_config' file specifies whether ssh server should ignore the user's ~/.ssh/known_hosts during RhostsRSAAuthentication or HostbasedAuthentication and use only the system-wide known hosts file /etc/ssh/known_hosts. IgnoreUserKnownHosts parameter must be set to “yes” Example: IgnoreUserKnownHosts yes Verify the setting $ sudo grep IgnoreUserKnownHosts /etc/ssh/sshd_config

Control	Implementation
	Related to Qualys Control ID: 5275 Reference: NIST Cyber Security Framework https://man.openbsd.org/sshd_config
5.ll) Ignore user's environment options	The PermitUserEnvironment parameter within the '/etc/ssh/sshd_config' file specifies whether ~/.ssh/environment and environment= options in ~/.ssh/authorized_keys are processed by sshd. PermitUserEnvironment parameter must be set to "no" Example: PermitUserEnvironment no Verify the setting $ sudo grep PermitUserEnvironment /etc/ssh/sshd_config ISO Note: The default setting of OpenSSH for this setting is "no" and it is also acceptable if the setting hasn't been implemented on the host. Related to Qualys Control ID: 5279 Reference: CIS Benchmark https://man.openbsd.org/sshd_config
5.mm) The following SSH authentication must be used: 1. Server-to-server processes that perform unattended file transfers using sftp or scp, or scripts that remotely execute commands using SSH must not use host-based authentication. Storing a password in a file, for use in automated sftp/scp/ssh connections, is forbidden. Public keys must be protected.	The following configuration items are specific to Prudential and are set in the /etc/ssh2/ssh-server-config.xml file: Please refer to Prudential's Encryption Algorithm Engineering Specification located in the ISO intranet site to view the list of allowed ciphers. BannerMessageFile -/etc/issue A warning banner located in /etc/issue will be displayed upon initial login using SSH.
6 Tracking, Detection, Monitoring	
6.a) UNIX auditing must be enabled.[44]	The auditd daemon should be running by default. If the service is enabled, execute the following command

[44] Auditing provides a means of detecting unauthorized use of a systems and provides data necessary to perform a forensic analysis in the event of a detected intrusion.

Control	Implementation
	systemctl enable auditd.service If the service is not running, execute the following command: systemctl start auditd.service Related to Qualys Control ID: 9336 Reference: CIS Benchmark
6.b) Native operating system tools should be used to warn or prevent the use of excessive disk space for audit log files.	Linux audit logs are stored in /etc/audit/auditd.log. Tivoli is the standard tool used to monitor filesystem capacity. Filesystem capacity that exceed the defined maximum threshold (can vary from server to server depending upon filesystem size) is detected by Tivoli, and an alert is sent to UEG informing of the condition.
6.c) UNIX auditing must collect all successful session sign-ons and sign-offs and all identification and authentication violations.	This information is collected outside of the auditing subsystem, in the wtmp and authlog files. Wtmp is autoconfigured to collect. For authlog data collection, ensure that the following string is defined in /etc/syslog.conf: auth.info;daemon.info;daemon.debug <tab> /var/log/authlog Note: Please see Appendix-4 to apply settings for UEG Log Management Standards
6.f) UNIX auditing must collect a user ID or process ID for each event.	This is configured "on" by default.
6.g) UNIX auditing must collect the resource accessed for each event.	This is configured "on" by default.
6.h) UNIX auditing must collect the date and time of access for each event.	This is configured "on" by default.
6.i) UNIX auditing must collect the type of event.	This is configured "on" by default.
6.j) UNIX auditing must collect the result of the event (success or failure).	This is configured "on" by default.
6.k) Federal laws and industry standards (identified in section 2.2 of NIST Special Publication 800-92 as: HIPAA, GLBA, SOX, PCI) compel Prudential (as a financial services company, a holder of health records, and a processor of payment card data) to collect, preserve and secure operating system security logs and event logs. As per the UNIX Security Log Management Standard, the following security / event logs must be collected on all UNIX servers, rotated on a daily basis, and archived either to tape or an online repository such as Content Manager so that they are available for security compliance review, and for forensic and evidentiary purposes:	The following files must be configured according to instructions provided in the Log Management Standard: /etc/syslog.conf /etc/logrotate.d/syslog /etc/logrotate.conf /etc/security/audit_watcher See Appendix 4 for the required settings for following setting files /etc/rsyslog.conf,

Control	Implementation
/var/log/authlog /var/log/sudo.log /var/adm/sulog messages log (location varies per OS) cron logs (location varies per OS) wtmp, wtmpx, or btmp log (OS dependent) wtmp, wtmpx, or btmp log (OS dependent) /var/log/secure (Linux) /var/log/maillog (Linux) /var/log/spooler (Linux) /var/log/boot.log (Linux)	/etc/logrotate.d/syslog /etc/logrotate.conf
6.l) Logs should rotate daily.	Set “daily” for log rotate setting within /etc/logrotate.conf. Please also refer to Appendix 4 Example: (verify the setting) $ grep ^daily /etc/logrotate.conf Related to Qualys Control ID: 5636 Reference: NIST Cyber Security Framework
6.m) Log Level setting for sshd_config	LogLevel setting in the /etc/ssh/sshd_config file must be set to INFO or VERBOSE Higher log level provides us more information but DEBUG level may violate the privacy of users. Example: (verify the setting) $ sudo grep LogLevel /etc/ssh/sshd_config Related to Qualys Control ID: 3598 Reference: NIST Cyber Security Framework, CIS Benchmark
6.n) Syslog Facility setting for sshd_config	SyslogFacility in the /etc/ssh/sshd_config file must be set to AUTH or AUTHPRIV. AUTH is the default setting of OpenSSH but AUTHPRIV can be set as default Example: (verify the setting) $ sudo grep SyslogFacility /etc/ssh/sshd_config Related to Qualys Control ID: 5292 Reference: NIST Cyber Security Framework
7. Security Management and Administration	

Control	Implementation
7.a) For each system, system administrators must review available security patches for the operating systems they administer and apply patches as required. Prudential standard operating procedures for patch application should be used.	Please apply latest security patches from the vendor to address vulnerabilities within the required due dates outlined by ISO (In Global Technology, UEG is responsible to updating UNIX/Linux operating systems). Prudential ISO's Server Compliance Process doesn't evaluate if the latest patch is applied on the host. There is a separate Vulnerability Management process defined. Please see Vulnerability Management Process on ISO's site for more detail.
7.b) System administrators must respond to Flexera SVM/Qualys VM advisories within the timeframe that aligns with the color associated with the alert (Red, Orange, Yellow / Severity 1-5). This response may include patching the system or implementing a work-around.[45]	Mitigating controls as well as the risk profile of the system can have a bearing on patching/fix response time.
7.c) System audit files must be archived to backup tape and stored in a secure container.[46]	Audit log files will be archived as part of the normal system backup procedure.
7.d) Security administrators must provide a random password when establishing new user accounts or when resetting locked accounts. This random password must not be shared in email. Users must change the password after successfully logging into the system.[47]	The creation and communication of new passwords is handled by Central Security Services, for both local accounts and accounts stored in AD. UEG is not involved in this process.
7.e) The system must be scanned for .rhosts files. Any .rhosts files that are found must be removed from the system.[48]	Qualys PC is used to scan for the presence of .rhosts files
7.f) The system must be checked for hosts.equiv files. If found, the hosts.equiv file must be removed from the system.[49]	If a hosts.equiv file exists it will be located in the /etc directory. If the file exists, delete it.
7.g) World writeable files must not be used. The system must be scanned for world writeable files. For GLOBAL BUSINESS TECHNOLOGY MANAGEMENT owned files, the system administrator must restrict access to the files, or an exception must be submitted. File permissions on world writeable files belonging to	Restrict access by: • Limiting who is able to log into the system with an unrestricted shell • Controlling who has access to the parent directory via group-membership • Restrict access to NFS exported files by limiting exports only to those hosts that require it

[45] When security alerts are released they typically provide patches or work-arounds to mitigate risk. These fixes need to be applied as soon as possible to prevent widespread exploitation.
[46] Audit files should be archived for forensic purposes and to prevent excessive use of disk space.
[47] If a standard convention is used to select initial passwords, an unauthorized user may be able to guess passwords on newly created accounts.
[48] .rhosts are used to create trust relationships which can extend access to other systems in a trusted network.
[49] These files are used to create trust relationships which can extend access to other systems in a trusted network

Control	Implementation
business unit must be restricted, or an exception must be submitted.[50]	• Restrict write access to NFS exported files by use of (read-only) –o=ro option at the time of export Note: The permission settings which allows Writable permission to 'Other' users, e.g. r—r—rwx, must not be used because the setting causes same risk as World-Writable. The detailed list of criteria for system related World-Writable files and directories is available in Appendix 4 in this document. The detailed list of criteria for optional / 3rd party software related World-Writable files and directories is available in BSC Documents Related to Qualys Control ID: 100695 (/), 100696 (/etc), 100697 (/lib), 100698 (/usr), 100699 (/opt), 100700 (/var), 100701 (/home)
7.h) .netrc files must not be used. The system must be scanned for .netrc files. Any .netrc files that are found must be removed from the system.[51]	The following command can be used to find .netrc files :# find / -mount | grep rhosts ***NOTE: Find cmd must be executed on each local FS Related to Qualys Control ID: 1203 Note: The Qualys control highly likely cause an issue if the users' home directories are mounted through NFS. This control may not be implemented in the policy.
7.i) The integrity of critical system files must be monitored. If critical system files have been altered, Prudential incident response procedures must be used when investigating the changes.[52]	Qualys PC monitors OS files for appropriate permissions, and reports on any files that do not conform to expected settings. Monitoring OS files for change in size, ownership, or content requires a 3rd party software and an operational strategy for determining when changes are appropriate/authorized and when they are not, and how to respond to unauthorized changes.
7.j) Non-operating system development tools must be removed from production servers. The following operating system debugging tools are exempt from this requirement: truss adb | sdb | gdb /usr/proc/bin utilities	Acknowledged
7.j) Generic usernames must not be used, with the exception of the following types of accounts:[53]	Remove generic accounts from the /etc/passwd file and corresponding entries in the /etc/shadow file.
System accounts application service accounts	The list of exempt accounts is available in Appendix 2.

[50] World writeable files permit access to any user on the system.
[51] .netrc files store cleartext passwords that can be used to access accounts on other systems.
[52] Unauthorized users may modify security critical files to gain additional privileges.
[53] User accountability will be lost if user logs into a generic user ID.

Control	Implementation
The system must be checked for generic usernames and they must be removed or replaced. Guest accounts are not permitted.	
7.k) On an as required basis, the ISO must execute network security scans of selected UNIX servers to identify network vulnerabilities in those systems.	The ISO will use network security scanning tools to identify vulnerabilities in UNIX systems. Identified vulnerabilities will be correlated with this standard and prioritized according to the risk index of this standard.
7.l) All UNIX servers must have the appropriate settings configured for the security scan.	The server should be configured to be scannable with Qualys PC Verify that relevant security scanner account is accessible to the server with Vintela Verify that relevant security scanner account can perform su command to collect data to evaluate If the server cannot be scanned with Qualys PC, Qualys Cloud Agent should be installed and should be configured.
7.m) Duplicate user identifiers, user names, group identifiers and group names must not be used. The system must be checked for duplicate user identifiers. If found, one of the duplicate user identifiers must be changed. NOTE: Although these controls were written with the intention of being "locally" applicable (not across an enterprise), our evolution in the areas of account federation, server virtualization and the widespread sharing of storage may call for a reinterpretation, and possible rewrite, of this control so that it applies at an enterprise level. Such a modification requires that a UID/GID reservation system be in place to prevent future collisions.	Check the third field of the /etc/passwd file for duplicate user identifiers. Qualys PC also identifies this type of violation. Additionally, Unix accounts and groups created after 2005 utilize a UID/GID reservation system that prevents a UID/GID from being given out more than once. Owners of existing accounts and groups created prior to 2005 where a collision has been identified must formulate a plan of exit from the condition if a confidentiality, integrity or availability risk is identified as a result of the collision. The security scanner evaluates user names and IDs in /etc/passwd and group names and IDs in /etc/group Related to Qualys Control ID: 2541 (User ID), 2543 (User Name), 2542 (Group ID), 2544 (Group Name)
7.n) User ID 0 and Group ID 0 must not be used for other than root user and root group	UID 0 and GID 0 are assigned to "root" user and "root" group on Linux. UID 0 and GID 0 must not be used for any other local user or group Related to Qualys CID:1159 (UID 0), 3221 (GID 0)
7.o) 'dot (. Or :. Or .:)', 'trailing colon (:$)', 'double-colon (::)' or 'leading colon (^:)' entries should not exist in the $PASS variable for root user	A 'single dot ('.')', a 'trailing colon (:$)', a 'double-colon (::)' or a 'leading colon (^:)' represents 'current directory for some shells on UNIX operating systems. Adding the '.', ':.', '.$' or '::' to the root $PATH can cause execution of malicious code as the root user. Related to Qualys Control ID: 6056 (double-colon), 6057 (trailing colon) 6058 (dot), 6316 (leading colon) Reference: NIST Cyber Security Framework, CIS Benchmark
7.p) Writable access must not be allowed for "root" user's $PATH directory	If malicious user can replace the executable file which can be executed by the "root" user, the system may cause

Control	Implementation
	Related to Qualys Control ID: 6059 (Group accounts), 6060 (Other accounts) Reference: NIST Cyber Security Framework, CIS Benchmark
7.q) Users' dot-files (hidden files) should not be World-Writable	Dot-file is created to store user's environment setting (e.g. .bashrc for bash shell) and contains security related settings, such as $PATH. The access to dot-files should be restricted. Related to Qualys Control ID: 3936 Reference: NIST Cyber Security Framework, CIS Benchmark Note: This control may be / may not be implemented because of the issue with NFS. User's home directory can be accessed with NFS and that means Qualys will potentially establish NFS connection to the network drive per number of controls x per number of users.
7.r) The service account should be available on the host	This control is required for CMDB Discovery The CMDB service account, 'tdiscop' account, is the Active Directory account which is used for CMDB discovery. Vintela or SecurPass should be used to utilize Active Directory account. Example: $ id tdiscop uid=6147(tdiscop) gid=6058(tdiscop) groups=6058(tdiscop) Note: Qualys is not Active Directory aware and this control cannot be verified with Qualys

HIGH RISK CONTROLS

Control	Implementation
1. All High Risk Servers	
N/A	
2. Internet Web Servers	

2.a) NFS must be disabled. [54]	To disable NFS, run the following command:
	
	Example to disable NFS service completely (Recommended)
	$ sudo systemctl mask nfs
	
	Example to disable NFS service during the startup
	$ sudo systemctl disable nfs

2.b) NIS+ or NIS must be disabled.[55] If dynamic routing is required, routing table updates must be authenticated	To disable NIS service, run the one of following commands **Note: NIS Service is required for Vintela. This control is applicable for Non-UEG Managed hosts only.** Example $ sudo systemctl disable ypbind.service
2.c) RPC must be disabled.[56]	To disable RPC, run the one of following commands **Note: RPC Service is required for Vintela. This control is applicable for Non-UEG Managed hosts only.** Example $ sudo systemctl disable rpcbind

[54] Daemons associated with NFS contain numerous vulnerabilities that can be exploited to allow remote access.
[55] NIS and NIS+ services can be exploited to cause a denial-of-service against multiple NIS/NIS+ clients.
[56] Daemons associated with RPC (statd, lockd, mountd) contain numerous vulnerabilities that can be exploited to allow remote access.

Control	Implementation
2.e) Restricted file systems must be used to isolate web server related files and directories from the root file system. [57]	Create a restricted file system by copying a minimum set of files from the UNIX system directories, /usr, /bin, /lib, /etc (which will be necessary to operate the environment) into a new subdirectory of root that will become the restricted file system that will be used to host the web server. Then add the "*" symbol to the shell field of the /etc/passwd file for those users that will operate in the restricted file system. The asterisk will use the chroot system call to restrict access to the restricted file systems. All files and directories associated with the web server should be moved into the restricted file system.
2.f) Only the following types of user groups are permitted access to the web servers restricted file system:[58]	Create the following types of groups in the /etc/group file located within the restricted file system:Sysadmin = rootWebadminWebdevWebauthWebserver = (e.g., netscape, apache)Establish file permissions as follows:Sysadmin — read/write all directoriesWebadmin — read/write all restricted directoriesWebdev — read/write to CGI-BIN directory and document directoryWebauth — read/write to document directoryWebserver — read to CGI-BIN and document directory
System administrator — authorized to administer restricted file system.	Sysadmin = root
Web server administrator — authorized to configure and install web server application.	Webadmin Webdev Webauth
Web developer — authorized to access web server CGI scripts.	Webserver = (e.g., netscape, apache)
Web author — authorized to access web document directories	Establish file permissions as follows:
Web server — an account for the web server. The web server must not run as the root user.	Sysadmin — read/write all directories
The number of users within each group must be minimized to the minimum essential personnel required to operate the web server.	Webadmin — read/write all restricted directories Webdev — read/write to CGI-BIN directory and document directory Webauth — read/write to document directory Webserver — read to CGI-BIN and document directory
2.) Disable the ability to execute code off the stack.[59]	Set the following parameter in the /etc/system file:set noexec_user_stack=1set noexec_user_stack_log =1

[57] A remote attacker that can "walk" the directory structure of a web server can increase their ability to find vulnerable executables that can be used to attack the server or obtain access to operating system configuration or executable files.
[58] Excessive file access privileges can result unauthorized access from the development environment or unauthorized external access to web server configuration files.
[59] Buffer overflow attacks that overflow the stack are frequently used against CGI programs to execute code on a web server. This can lead to remote access to the web server.

Control	Implementation
3. Mail Server	
3.a) The most recent version of Sendmail must be used on UNIX mail servers.[60]	Sendmail security alerts can be obtained from:http://www.sendmail.org/ These alerts are now tracked through the VIM vulnerability monitoring tool.
3.b) Suppress the display of the Sendmail version number when connecting to the mail server's SMTP port.[61]	Change the SMTP login message line in the /etc/mail/sendmail.cf file from: De$j Sendmail $v/$V ready at $b to: $j Server Ready
3.c) Forwarding of SMTP messages must not be enabled by default. Prudential Internet mail servers must only relay to selected domains.[62]	Upgrade to Sendmail version 8.9 or greater to use SMTP relay control features. Insert in the file /etc/mail/relay the list of accepted Prudential relay -domains.
3.d) Disable the Sendmail VRFY command.[63]	Disable the Sendmail VRFY command by adding the novrfy option to the /etc/mail/sendmail.cf file.
3.e) Disable the Sendmail EXPN command.[64]	Disable the Sendmail EXPN command by adding the noexpn option to the /etc/mail/sendmail.cf file.
4. DNS Server	
4.a) The most recent version of Bind must be used on UNIX DNS servers.[65]	Bind security alerts can be obtained from: http://www.isc.org/products/BIND/ These alerts are now tracked through the VIM vulnerability monitoring tool.

[60] Versions of Sendmail as recent as 8.8.8 contain vulnerabilities that can result in unauthorized remote access, relay/spam attacks against other mail servers.
[61] The Sendmail version number may be used to reveal to a potential attacker that a vulnerable version of Sendmail is running on the server.
[62] If the Sendmail server is permitted to relay mail to another domain, the server may be used to spam the mail servers of other organizations.
[63] The Sendmail VRFY command allows a remote user to query a Sendmail server to obtain login names that could potentially be used to attack the system.
[64] The Sendmail EXPN command allows a remote user to query a Sendmail server to obtain mail aliases and mailing lists that could be used to spam users.
[65] A number of bugs in Bind can be exploited to gain remote root access to name servers or to crash the name servers.

Control	Implementation
4.b) Zone transfers from Prudential's primary DNS server must be restricted to Prudential secondary DNS servers.[66]	Enable access control on zone transfer requests by specifying a list of Prudential secondary name servers in the /et/named.boot file as follows: xfrnets address-list where address list is the list of IP addresses for Prudential's secondary name servers.
5. DMZ Servers	
1.a) Allow one-way (from internal network to server) Securepass password synchronization	No specific local settings required.
2) Do not run SNMP[67]	

[66] An attacker posing as a secondary DNS server can perform a zone transfer from the primary DNS sever and obtain network addresses and hostnames for a domain, which can be used to attack the domain.
[67] The risk of running the snmpd client on DMZ based hosts is that an active snmpd port becomes an additional point of entry that can be exploited to gain unauthorized access to a system, and allow an external party to learn and potentially change system configuration settings.

APPENDIX-1. AUTHORIZED AND UNAUTHORIZED SERVICES

DAEMON	CRITERIA	DESCRIPTION	QUALYS CONTROL ID
chargen (tcp)	Forbidden		14112
chargen (udp)	Forbidden		14112
comsat	Forbidden		14112
daytime (stream/tcp)	Forbidden		14112
daytime (dgram/udp)	Forbidden		14112
discard (dgram/udp)	Forbidden		3902
discard (stream/tcp)	Forbidden		1576
dtlogin	Optional		
dtspc	Forbidden		14112
echo (udp/dgram)	Forbidden		14112 / 1267
echo (tcp/stream)	Forbidden		14112 / 1329
exec / rexec	Forbidden		9915
finger	Forbidden		14112
ftp	Forbidden	File Transfer Protocol server. Security Exception should be required	9884
apache2 or httpd	Optional		
imap	Forbidden		14112
instsrv	Forbidden		14112
login	Forbidden		14112
named	Forbidden		9892
netstat	Forbidden		14112
nmbd	Forbidden	Samba NetBIOS Name Server. Security Exception should be required	14112
pcnfsd	Forbidden		14112
pop3	Forbidden		14112
routed	Forbidden		14112
rstatd	Forbidden		14112
rsyslogd	Mandatory		3616 / 9335
rusersd	Forbidden		14112
rwhod	Forbidden		14112
sendmail	Optional		
shell / rsh	Forbidden		9890
smbd	Forbidden	Samba. Security Exception should be required	14112
snmpd	Mandatory		3616
splunkd	Mandatory		3616
sprayd	Forbidden		14112
sshd or sshd2	Mandatory		
talk / ntalk	Forbidden		10729

DAEMON	CRITERIA	DESCRIPTION	QUALYS CONTROL ID
telnet	Forbidden		9919
tftp	Forbidden	Trivial File Transfer Protocol server. Security Exception should be required	10849
ttdbserver	Forbidden		14112
uucp	Forbidden		14112

APPENDIX-2. SETUID AND SETGID FILES

SetUID

Criteria	Description
All files installed as part of base OS SetUID files under following directories in Gold Image are ignored • /bin/.* • /sbin/* • /lib/* • /etc/.* • /tmp/* • /usr/bin/.* • /usr/sbin/* • /usr/lib/* • /usr/local/bin/* • /usr/local/sbin/* • /usr/local/lib/* • /usr/dt/.* • /usr/openwin/.* • /usr/libexec/openssh/ssh-keysign • /usr/libexec/pt-chown • /usr/X11R6/bin/Xorg	Inherited the criteria from section 1.1.1.1.1 in UEG-BSC002 document The detailed evaluation is adjusted to the Gold Image
/lost+found/	Inherited the criteria from section 1.1.1.1.8 in UEG-BSC002 document This directory can be commonly found in UNIX in the root directory of each partition (mount point)

* The detailed list of criteria for optional / 3rd party software related SetUID files is available in Section 3 in Entitlements Specifications

SetGID

Criteria	Description
SetUID files under following directories are ignored • /etc/.* • /opt/.* • /sbin/.* • /usr/bin/.* • /usr/sbin/.* • /usr/dt/.* • /usr/lib/.* • /usr/local/bin/.* • /usr/openwin/.*	Inherited the criteria from section 1.1.1.2.1 in UEG-BSC002 document The detailed evaluation is adjusted to the Gold Image
All files installed as part of base OS	Inherited the criteria from section 1.1.1.2.1 in UEG-BSC002 document The detailed definition is TBD
/lost+found/	Inherited the criteria from section 1.1.1.2.8 in UEG-BSC002 document This directory can be commonly found in UNIX in the root directory of each partition (mount point)

* The detailed list of criteria for optional / 3rd party software related SetGID files is available in Section 3 in Entitlements Specifications

APPENDIX-3. WORLD-WRITABLE FILES AND DIRECTORIES

ACCEPTANCE CRITERIA	DESCRIPTION
All files installed as part of base OS	The criteria should be defined according to the Gold Image
/tmp/*	
/dev/* character device files block device files	usually located in /dev, but can be elsewhere
socket files	used for BSD-style remote procedure calls – can be found anywhere
named pipe (FIFO) files	

* The detailed list of criteria for optional / 3rd party software related World-Writable files and directories is available in Section 4 in Entitlements Specifications

APPENDIX-4. SELINUX RULES

Unconfined Processes

Following processes can be unconfined process and are ignored with Qualys Control ID 17165

Technology	Processes / Commands	Description
Dell Networker Agent Services	nsrpsd nsrexecd vflragentd vflragentd.bin	UEG and the vendor confirmed that the services are part of Dell backup agent services and must be running as unconfined process on the host.
PAMSC (ControlMinder) Agent Services	AgentManager ReportAgent policyfetcher seosd seagent seoswd selogrd	UEG confirmed that the services are part of PAMSC (ControlMinder) Agent Services and should be running as unconfined process on the host.
Microsoft MDATP Agent Services	wdavdaemon crashpad_handle telemetryd_v2	UEG confirmed that the services are part of Microsoft MDATP Agent Services and should be running as unconfined process on the host.
Splunk Forwarder Agent Services	splunkd ueg_network.sh perl	UEG confirmed that the services are part of Splunk Forwarder Agent Services and should be running as unconfined process on the host.
Qualys	qualys-cloud-agent sh, bash, ksh ps grep sed	ISO's security scanner, Qualys, scan the target host with dedicated agent or through SSH access. Since Qualys needs to collect any security related settings, Unconfined permission is required. Qualys performs "ps", "grep" and "sed" command to collect Unconfined process information on the host

APPENDIX-5. QUALYS CONTROLS EXPORT

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
3598	Status of the 'LogLevel' option in the '/etc/ssh/sshd_config' file	The 'LogLevel' parameter in the /etc/ssh/sshd_config file provides the level of verbosity applied when messages are logged from the sshd service. Some of the possible values that can be displayed are: DEBUG, DEBUG1, DEBUG2, DEBUG3, INFO, ERROR, VERBOSE, QUIET and FATAL. In order to ensure the privacy of other users, it should be disallowed that logging be performed using a DEBUG level. Run this check periodically to ensure that level are commensurate with organizational requirements.	The following List String value(s) X indicate the current status of the LogLevel setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^(INFO|VERBOSE|DEBUG[1-3]?)$ OR, any of the selected values below: [x] Setting not found [x] File not found
7297	Status of the 'log_on_success' setting in the /etc/xinetd.conf file	The 'log_on_success' log setting within '/etc/xinetd.conf' file defines what events, hosts, and users are logged upon successful login. As the '/etc/xinetd.conf' file contains critical logging definitions that are used in security and compliance risk management activities, the configuration of the 'log_on_success' setting should be done according to the needs of the business.	The following List String value(s) X indicate the current log_on_success settings within the /etc/xinetd.conf file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
7444	Status of the 'action_mail_acct' setting in file '/etc/audit/auditd.conf'	The 'action_mail_acct' setting in the /etc/audit/auditd.conf file designates an alias or email address to receive alert messages from the audit daemon. A remote or local, operational, email account with '/usr/lib/sendmail' configured can be used as long as an authorized user is available to respond. As alert messages represent critical communication of legal evidence of chronological activity on the host, the 'action_mail_acct' setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current action_mail_acct setting within the /etc/audit/auditd.conf file on the host.	matches regular expression list root OR, any of the selected values below: [ ] Setting not found [ ] File not found
7452	Status of the 'adjtimex' syscall parameter defined in the	The 'adjtimex' syscall parameter tunes the kernel clock on the host. As there are several known exploits involving modifying	The following List String value(s) X indicate the current status of the adjtimex syscall defined in the	matches regular expression list .*adjtimex

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	'/etc/audit/audit.rules' file	the 'kernel clock' settings on the host, this syscall parameter should be configured according to the needs of the business.	/etc/audit/audit.rules file on the host.	OR, any of the selected values below: [x] Setting not found [ ] File not found
7453	Status of the 'clock_settime' syscall defined in the '/etc/audit/audit.rules' file	The 'clock_settime' syscall parameter captures modifications of several timers and internal clocks on the host. As there are several known exploits involving modifying the 'clock_settime' settings on the host, this syscall parameter should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the clock_settime syscall setting within the /etc/audit/audit.rules file on the host.	matches regular expression list .*clock_settime OR, any of the selected values below: [x] Setting not found [ ] File not found
7454	Status of the 'settimeofday' syscall defined in the '/etc/audit/audit.rules' file	The 'settimeofday' syscall parameter captures modifications of the system time on the host. As there are several known exploits involving modifying the 'time of day' settings on the host, this syscall parameter should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the settimeofday syscall defined in the /etc/audit/audit.rules file on the host.	matches regular expression list .*settimeofday OR, any of the selected values below: [x] Setting not found [ ] File not found
7455	Status of the 'stime' syscall parameter defined in the '/etc/audit/audit.rules' file	The 'stime' syscall parameter sets the systems date and time, measured in the number of seconds since 01-01-1970, on the host. As there are several known exploits involving modifying the 'time of day' settings on the host, this syscall parameter should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the stime syscall defined in the /etc/audit/audit.rules file on the host.	matches regular expression list .*stime OR, any of the selected values below: [x] Setting not found [ ] File not found
7456	Status of the '/etc/localtime' setting defined in the	The '/etc/localtime' setting in the '/etc/audit/audit.rules file converts calendar time (timep) into the current timezone of the	The following List String value(s) X indicate the current status of the /etc/localtime setting in the	matches regular expression list .*/etc/localtime

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	'/etc/audit/audit.rules' file	host. As there are several known exploits involving modifying the 'time of day' settings on the host, this syscall parameter should be configured according to the needs of the business.	/etc/audit/audit.rules file on the host.	OR, any of the selected values below: [x] Setting not found [ ] File not found
7465	Status of the 'sethostname' syscall parameter defined in the '/etc/audit/audit.rules' file	The 'sethostname' syscall parameter defines (or renames) the hostname of the current processor. As there several well known concurrent address spoofing, buffer overflow, and code injection exploits involving syscall parameters, 'sethostname' should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the sethostname syscall defined in the /etc/audit/audit.rules file on the host.	matches regular expression list .*sethostname OR, any of the selected values below: [x] Setting not found [ ] File not found
7466	Status of the 'setdomainname' syscall parameter defined in the '/etc/audit/audit.rules' file	The 'setdomainname' syscall parameter defines (or renames) the domain name of the current processor. As there several well known concurrent address spoofing, buffer overflow, and code injection exploits involving syscall parameters, 'setdomainname' should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the setdomainname syscall defined in the /etc/audit/audit.rules file on the host.	matches regular expression list .*setdomainname OR, any of the selected values below: [x] Setting not found [ ] File not found
7467	Status of the 'changes to content or attributes' of the '/etc/issue' as defined in the '/etc/audit/audit.rules' file	The '/etc/issue' parameter monitors and logs any changes to the message displayed prior to login. As there are several well known banner exploits, the '/etc/issue' parameter, defined within the '/etc/audit/audit.rules' file, should be configured according to the needs of the business.	The following List String value(s) X indicate if the /etc/issue file is currently monitored as defined in the /etc/audit/audit.rules file on the host.	matches regular expression list .*/etc/issue OR, any of the selected values below: [x] Setting not found [ ] File not found
7468	Status of the 'changes to content or attributes' of the '/etc/issue.net' as	The '/etc/issue.net' parameter monitors and logs any changes to the '/etc/issue.net' text file displayed prior to login for a telnet	The following List String value(s) X indicate if the /etc/issue.net file is currently monitored as defined	matches regular expression list .*/etc/issue.net

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	defined in the '/etc/audit/audit.rules' file	session. As there are several well known banner exploits, the '/etc/issue.net' parameter, defined within the '/etc/audit/audit.rules' file, should be configured according to the needs of the business.	in the /etc/audit/audit.rules file on the host.	OR, any of the selected values below: [x] Setting not found [ ] File not found
7469	Status of the 'changes to content or attributes' of the '/etc/hosts' as defined in the '/etc/audit/audit.rules' file	The '/etc/hosts' file contains IP addresses associated with hostnames and is monitored for any changes by the '/etc/hosts' setting as defined in the '/etc/audit/audit.rules' file. As there are several known host intrusion and string format exploits, the configuration of the '/etc/hosts' setting within the '/etc/audit/audit.rules' file should be done according to the needs of the business.	The following List String value(s) X indicate if the /etc/hosts file is currently monitored as defined in the /etc/audit/audit.rules file on the host.	matches regular expression list .*/etc/hosts OR, any of the selected values below: [x] Setting not found [ ] File not found
7470	Status of the 'changes to content or attributes' of the '/etc/sysconfig/network' file as defined in the '/etc/audit/audit.rules' file	The /etc/sysconfig/network file is used to specify information about the desired network configuration. Monitoring /etc/sysconfig/network file is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. Logs play an important role in security auditing, incident response, system maintenance and forensic investigation, auditing of '/etc/sysconfig/network' file should be configured as appropriate to the needs of the business.	The following List String value(s) X indicate if the /etc/sysconfig/network file is currently monitored as defined in the /etc/audit/audit.rules file on the host.	matches regular expression list .*/etc/sysconfig/network OR, any of the selected values below: [x] Setting not found [ ] File not found
7472	Status of the 'changes to content or attributes' of the '/var/log/faillog' file	The '/var/log/faillog' file, as defined by the '/etc/audit/audit.rules' file, is designated to log all failed login events on the host. As there are several different types of known access exploits and the 'faillog' file is a legal record of chronological activities on the host, this setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the /var/log/faillog file as defined within the /etc/audit/audit.rules file on the host.	matches regular expression list .*/var/log/faillog OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
				[ ] File not found
7473	Status of the 'changes to content or attributes' of the '/var/log/lastlog' file	The '/var/log/lastlog' file, as defined by the '/etc/audit/audit.rules' file, is designated to log the time the last user successfully logged into the host. As there are several different types of known access exploits and the 'lastlog' file is a legal record of chronological activities on the host, this setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the /var/log/lastlog file as defined within the /etc/audit/audit.rules file on the host.	matches regular expression list .*/var/log/lastlog OR, any of the selected values below: [x] Setting not found [ ] File not found
7475	Status of the 'changes to content or attributes' of the '/var/run/utmp' as defined in the '/etc/audit/audit.rules' file	The '/var/run/utmp' file monitors all users currently logged into the host and is monitored by the '/var/run/utmp' setting within the '/etc/audit/audit.rules' file. As there several well known root exploits targeting /var/run/utmp, this setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the /var/run/utmp file as defined within the /etc/audit/audit.rules file on the host.	matches regular expression list .*/var/run/utmp OR, any of the selected values below: [x] Setting not found [ ] File not found
7476	Status of the 'changes to content or attributes' of the '/var/log/btmp' file as defined in the '/etc/audit/audit.rules' file	The '/var/log/btmp' file, as defined by the '/etc/audit/audit.rules' file, is designated to log all failed login events on the host. As there are several different types of known access exploits and the '/var/log/btmp' file is a legal record of chronological activities on the host, this setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the /var/log/btmp file as defined within the /etc/audit/audit.rules file on the host.	matches regular expression list .*/var/log/btmp OR, any of the selected values below: [x] Setting not found [ ] File not found
7971	Status of the list of 'unprivileged users' attempting to access privileged commands on the host	The 'privileged' commands are restricted to authorized users, but when 'unauthorized users' attempt to execute privileged commands, an audit record is created in a repository and an alert is generated for review and investigation. As attempts by unauthorized users to execute privileged commands is considered 'legal evidence of	The following List String value(s) X indicate the current path, perm, and auid settings within the privileged programs (programs with setuid and/or setgid bits set on execution) on the host. NOTE: According to the CIS Benchmark, the '/etc/audit/audit.rules' file	matches regular expression list path=.* OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		unauthorized activity on the host'; the configuration of these parameters should be carefully done according to the needs of the business.	should be updated to record attempted access by unauthorized users of any privileged commands (privileged commands have setuid and/or setgid on execution).	[ ] File not found
7459	Status of the current content of the '/etc/group' file as defined in the '/etc/audit/audit.rules' file	Including the '/etc/group' file in the '/etc/audit/audit.rules' file ensures any change of content or attributes are immediately audited and reported. As monitoring the '/etc/group' file for changes, tagging these files, and reporting them is a critical security measure; these settings should be configured according to the needs of the business.	The following List String value(s) X indicate the current content of the /etc/group file as defined within the /etc/audit/audit.rules file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
7460	Status of the 'changes to content or attributes' of the /etc/passwd file as defined in the '/etc/audit/audit.rules' file	Including the '/etc/passwd' file in the '/etc/audit/audit.rules' file ensures any change of content or attributes are immediately audited and reported. As monitoring the '/etc/passwd' file for changes, tagging the files, and reporting them enables detection of unauthorized changes. These settings should be configured according to the needs of the business.	The following List String value(s) X indicate the current content or attribute changes of the /etc/passwd file as defined within the /etc/audit/audit.rules file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
7461	Status of the '/etc/gshadow' file as defined in the '/etc/audit/audit.rules' file	Including the '/etc/gshadow' file in the '/etc/audit/audit.rules' file ensures any change of content or attributes are immediately logged and recorded. As monitoring the '/etc/gshadow' file for changes, tagging these files, and reporting them is a critical security measure; these settings should be configured according to the needs of the business.	The following List String value(s) X indicate the current content or attribute changes of the /etc/gshadow file as defined within the /etc/audit/audit.rules file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
7462	Status of the audit rules to watch for filesystem object '/etc/shadow' defined within	Including the '/etc/shadow' file in the '/etc/audit/audit.rules' file ensures any change of content or attributes are immediately audited and reported. As	The following List String value(s) X indicate the current content or attribute changes of the /etc/shadow file as defined within	matches regular expression list .*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	'/etc/audit/audit.rules' file	monitoring the '/etc/shadow' file for changes, tagging these files, and reporting them is a critical security measure; these settings should be configured according to the needs of the business.	the /etc/audit/audit.rules file on the host.	OR, any of the selected values below: [x] Setting not found [x] File not found
7393	Status of the current 'OS release and version' as defined in the '/etc/redhat-release' file.	The current OS release and version defined within the /etc/redhat-release file is used by system administrators to perform their duties in patching and securing the operating system. However, as malicious users will attempt to obtain the current operating system release and version information to mount attacks on the host, the access to this file should be configured according to the needs of the business.	The following List String value(s) X indicate the current supported OS release as defined within the /etc/redhat-release file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
9684	Status of the kernel release currently in use on the host	The operating system vendor releases periodic security updates and software patches to the operating system to support new hardware platforms, deliver new functionality, or fix security vulnerabilities, usability and performance issues among others. Systems should be kept up-to-date with the latest releases as appropriate to the needs of the business in order to prevent attacks and mitigate the risks of vulnerabilities in unpatched or older software.	The List String value of X indicates the status of OS version on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting Not Found
3616	Current list of 'authorized processes' active in memory	The processes running on a host indicate the active programs that are being executed. Processes are made up of several components such as an associated file from where the code is executed, allocated memory address space, etc. It is good practice to periodically review all active processes on a host to ensure only those appropriate and approved are resident. Unknown processes that consume large amounts of system	The following List String value(s) X indicate the current status of the processes running on the system as reported by the ps command output.	contains regular expression list .*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		resources could indicate the presence of malicious code running on the host.		
6316	Status of a 'leading colon (^:)' in the 'root user's $PATH' variable	A leading-colon (^:) is sometimes interpreted as the 'current directory' for some shells on Unix and Unix-like operating systems. This has the same security issue as having a dot (.) in the root user's $PATH. Presence of a leading-colon (^:), double-colon (::) or dot (:.) in the $PATH variable for the 'root' user can cause a binary in the current directory to be preferentially executed over other, originally desired, system binaries of the same name and can cause execution of malicious code as the root user. For example, if the administrator were to log in as 'root' and switch to a directory that had a file called 'cd' within in and that file contained the text 'rm -rf ' this command would act in place of the original system 'cd' command and wipe out the contents to the target directory.	The following List String value(s) X indicate the current status of a leading colon (^:) identified within the root user accounts $PATH variable on the host.	matches regular expression list 161803399999999 OR, any of the selected values below: [x] Setting not found
7404	Status of 'exec|noexec' options set for the removable media within '/etc/fstab' (mounted on '/media')	The 'removable media' setting defined within the /etc/fstab file provides options for the use of removable media. The 'exec or noexec' settings either allow or prevent executing programs from removable media. As there are several known worms and malicious code attacks by using removable media, these mount options should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of all removable media (/dev/cdrom, /dev/usb, /dev/msdos) within the /etc/fstab file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
6056	Status of any 'double-colon (::)' entries within the 'root user's $PATH' variable	A double-colon (::) is sometimes interpreted as the 'current directory' for some shells on Unix and Unix-like operating systems. This has the same security issue as having a dot (.) in the root user's $PATH. Presence of a double-colon or dot in the $PATH variable for the 'root' user can cause a binary in the current directory to be preferentially executed over other, originally desired,	The following List String value(s) X indicate the current status of the $PATH setting for the root user account having a double-colon or empty directory defined within it on the host.	matches regular expression list 161803399999999 OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		system binaries of the same name, so adding the double-colon (::) to the root $PATH can cause execution of malicious code as the root user. For example, if the administrator were to log in as 'root' and switch to a directory that had a file called 'cd' within in and that file contained the text 'rm -rf ' this command would act in place of the original system 'cd' command and wipe out the contents to the target directory.		
6057	Status of a 'trailing colon' in the 'root user's $PATH' variable	A trailing-colon is sometimes interpreted as the 'current directory' for some shells on Unix and Unix-like operating systems. This has the same security issue as having a dot (.) in the root user's $PATH. Presence of a trailing-colon (Path ends with colon), double-colon (::) or dot (:.) in the $PATH variable for the 'root' user can cause a binary in the current directory to be preferentially executed over other, originally desired, system binaries of the same name and can cause execution of malicious code as the root user. For example, if the administrator were to log in as 'root' and switch to a directory that had a file called 'cd' within in and that file contained the text 'rm -rf ' this command would act in place of the original system 'cd' command and wipe out the contents to the target directory.	The following List String value(s) X indicate the current status of the root account $PATH setting having a trailing colon value defined on the host.	matches regular expression list 161803399999999 OR, any of the selected values below: [x] Setting not found
6058	Status of any 'dot (. or :. or .:)' entries within the 'root user's $PATH' variable	A single dot ('.') represents 'current directory' on Unix and Unix-like operating systems. Presence of a dot in the $PATH variable for the 'root' user will cause a binary in the current directory to be preferentially executed over other, originally desired, system binaries of the same name, so adding the ':.' (colon + dot) to the root $PATH can cause execution of malicious code as the root user. For example, if the administrator were to log in as 'root' and	The following List String value(s) X indicate the status of the current working directory (.) defined within the root user account $PATH variable on the host.	matches regular expression list 161803399999999 OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		switch to a directory that had a file called 'cd' within in and that file contained the text 'rm -rf ' this command would act in place of the original system 'cd' command and wipe out the contents to the target directory.		
2541	Current list of 'User accounts having duplicate UID's'	On Unix/Linux type systems, the User Identifier (UID) is an unsigned integer value the kernel employs to identify users. The value that makes up the UID references users found in the /etc/passwd file. There are some rules that apply such as the 'superuser' account should have UID zero (0) or the 'nobody' account being set to the largest value available. UID's ranging from 1 to 100 are, typically, reserved for system use (it is recommended that the UID's from 1 to 1,000 be reserved for use by the system on some platforms). This control can be implemented to periodically obtain a list of user accounts having duplicate UID's to ensure host security has not been compromised. Depending on how the host is managed, multiple user accounts having UID=0 may indicate an intruder has granted themselves root level access to the system.	The following List String value(s) X indicate the current user accounts having duplicate UID's on the host.	does not contain regular expression list [A-Za-z0-9] OR, any of the selected values below: [x] Setting not found
2543	Current list of 'Accounts having duplicate usernames'	The username or user account is an authentication mechanism that provides users access to Information Technology systems. System and network administrators utilize usernames to grant access permissions and provide a mechanism to monitor and audit system user events. In order to ensure user access is appropriate and auditable, unique usernames should be utilized as appropriate to the needs of the business.	The following List String value(s) X indicate the current status of the user accounts having duplicate usernames on the host.	does not contain regular expression list [A-Za-z0-9] OR, any of the selected values below: [x] Setting not found
2641	Current list of 'inactive user accounts' and their 'last login Information' value(s)	Periodic account reviews showing the 'inactive user accounts and their last login information' can be performed to support security and compliance policies. This	This List string value of X returns the information of the Inactive User's last login on the host.	match all regular expression match ^.*:[0-9]+$

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		check can be run against all accounts or only those you specify to quickly determine if unused accounts need to be disabled. This check can also be used in support of incident response activities and act as evidence to show timeliness associated with when specific accounts were last used to support legal investigations. As inactive accounts can provide access for unauthorized activities, this check should be run regularly according to the security and compliance policies of the business.	NOTE : It returns list of all active user name and the inactive days.	OR, any of the selected values below: [x] Last login info not found [x] /var/log/lastlog not found
2784	Current list of 'accounts having no login record'	Login records are useful tools in forensic investigation activities to determine which user accounts accessed systems and/or networks at specific times. On Unix/Linux systems, this recorded login information is maintained within various binary files. In order to capture this critical information, all user account login activity should be logged in the event such information is required to act as evidence in support of any legal action.	The following List string value/s of X returns the list of user account with no login record on the host.	match all regular expression match .* OR, any of the selected values below: [x] User account not found [x] Lastlog not found
7417	Current list of user accounts with 'existing home directories' defined in /etc/passwd and not present on the host (non-system accounts)	Some home directories can be defined in '/etc/passwd' file, but not exist on the file system. Such exceptions leave users without write privileges and local environment variables settings. This check verifies both home directories exist on the file system and in the /etc/password file. This check should be run periodically according to the needs of the business.	The following List String value(s) X indicate the non-system user accounts that do not have their home directories created on the host. ** Note: All exceptions (user accounts without home directories) listed should be reviewed and approved by the organization.	is contained in regular expression list ^(nobody:/)$ ^(cmadmin:/(home|opt)/cmadmin)$ ^([cdhjnwxCDHJNWX][0-9]{6}|([uU][0-9]|uc|UC|vc|VC|[pP][256789dehjlnpDEHJLNP][0-9])[0-9]{5}|((wa|WA)9[0-9TZ][0-9]{4})[a-zA-Z]?):/(prustaff|home)/([cdhjnwxCDHJNWX][0-9]{6}|([uU][0-9]|uc|UC|vc|VC|[pP][256789dehjln

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
				pDEHJLNP][0-9])[0-9]{5}|((wa|WA)9[0-9TZ][0-9]{4})[a-zA-Z]?)$ OR, any of the selected values below: [x] Setting not found
2542	Status of the current list of 'Groups having duplicate GID's'	In the Unix/Linux environment, the Group ID (GID) provides a mechanism to organize and manage system resource permissions. The Group ID uses an integer value to represent each specific group. Users are granted group membership when the associated GID integer value is added to the user's /etc/group file. As the GID value represents a group that provides specific access and permissions to system resources, the use of duplicate Group ID's should be avoided as appropriate to the needs of the business.	The following List String value(s) X indicate the current duplicate GIDs within the /etc/group file on the host.	does not contain regular expression list .* OR, any of the selected values below: [x] No groups found [x] File not found
2544	Current list of 'Accounts having duplicate Group Names'	In the Unix/Linux environment, the Group ID (GID) provides a mechanism to organize and manage system resource permissions. The Group ID uses an integer value to represent each specific group. Users are granted group membership when the associated GID integer value is added to the user's /etc/passwd file. As the GID name represents a group that provides specific access and permissions to system resources, the use of duplicate Group names should be avoided as appropriate to the needs of the business.	The following List String value(s) X indicate the current duplicate group names within the /etc/group file on the host.	does not contain regular expression list .* OR, any of the selected values below: [x] No groups found [x] File not found
4437	Current list of hosts defined within the 'hosts.allow' file	The '/etc/hosts.allow' file indicates the names of the hosts which are permitted to access the local services. All access should be denied by default unless explicitly authorized to prevent a malicious user from performing inappropriate actions against the	The following List String value(s) X indicate the current list of hosts defined within the /etc/hosts.allow file.	matches regular expression list .* OR, any of the selected values below:

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		host. Run this check to ensure only hosts approved by the business are included in the '/etc/hosts.allow' file. NOTE: The '/etc/hosts.allow' file settings depend upon the '/etc/hosts.deny' file default settings set to 'ALL'.		[x] Setting not found [x] File not found
5381	Status of the 'UsePAM' setting in the '/etc/ssh/sshd_config' file	'UsePAM' is a setting within the '/etc/ssh/sshd_config' file. 'UsePAM' activates the Pluggable Authentication Module using session and account module processing along with ChallengeResponseAuthentication and PasswordAuthentication. As there are several known privilege escalation and cache spoofing exploits, the configuration of this setting should be done according to the needs of the business.	The following List String value(s) X indicate the current status of the UsePAM setting defined within the /etc/ssh/sshd_config file.	matches regular expression list [yY][eE][sS] OR, any of the selected values below: [ ] Setting not found [x] File not found
5936	Status of the current setting for 'net.ipv4.conf.all.accept_source_route' network parameter	The 'net.ipv4.conf.all.accept_source_route' setting allows a packet with encapsulated ICMP routing information (that may differ from the routes already specified on the host) to be acted upon. If not disabled, invalid/spoofed source routes can lead to a DoS or redirection of traffic through a 'man-in-the-middle' host, where a malicious user can attempt login replay attacks and/or other exploits, so this value should be set according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv4.conf.all.accept_source_route setting on the host.	equal to 0 OR, any of the selected values below: [x] Setting not found
5956	Status of the current setting for 'net.ipv4.conf.all.accept_redirects' network parameter	The 'net.ipv4.conf.all.accept_redirects' (in /etc/sysctl.conf) function determines whether or not the host will accept redirects to gateways not listed in the host's configuration file. As not setting this appropriately could permit malicious users to spoof a source address and force a packet redirect through an invalid gateway or a 'man-in-the-middle' host with a traffic sniffer, this value should be set according to the needs of the business.	The following Integer value X indicates the current net.ipv4.conf.all.accept_redirects setting on the host.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
5957	Status of the current setting for 'net.ipv4.conf.all.secure_redirects' network parameter	The 'net.ipv4.conf.all.secure_redirects' setting (/etc/sysctl.conf) requires all packets to use only gateways listed in the host's configuration files. Even when only 'secure redirects' are allowed, there exists the possibility of insider threats changing the host's configuration files to add an unauthorized gateway, which would allow the redirecting of traffic through a 'man in the middle' host, so this value should be set according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv4.conf.all.secure_redirects setting on the host. NOTE: The 'net.ipv4.conf.all.secure_redirects' setting should be set to '0', according to the CIS Benchmark.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found
5958	Status of the current setting for 'net.ipv4.conf.default.rp_filter' network parameter	The 'net.ipv4.conf.default.rp_filter' (/etc/sysctl.conf) performs route source validation via a reversed path. As having this setting enabled helps to block 'source address spoofing' attacks, where a malicious user might attempt login replay attacks and/or other exploits, this value should be set according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv4.conf.default.rp_filter setting on the host. NOTE: The 'net.ipv4.conf.default.rp_filter' should be set to '1' (enabled), according to the CIS Benchmark.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found
5959	Status of the current setting for 'net.ipv4.conf.default.accept_source_route' network parameter	The "net.ipv4.conf.default.accept_source_route" parameter indicates whether or not the host accepts packets with the SRR (Send/Receive/Reply message passing) option disabled/enabled. As use of the "net.ipv4.conf.all.accept_source_route" could permit the exploitation of IP trust relationships with spoofed source packets, if the host is not being used for routing, this should disabled and restricted according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv4.conf.default.accept_source_route setting on the host.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found
5961	Status of the current setting for 'net.ipv4.conf.default.secure_redirects' network parameter	The 'net.ipv4.conf.default.secure_redirects' network parameter (in /etc/sysctl.conf) restricts packet traffic to flow through configured gateways. If a false gateway can be inserted in the host's configuration file, redirects can be used to force packets through an invalid gateway or a "man-in-the-middle" host with a traffic sniffer, so this	The following Integer value(s) X indicates the current net.ipv4.conf.default.secure_redirects setting on the host. NOTE: The 'net.ipv4.conf.default.secure_redirects' setting should be configured	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		value should be set according to the needs of the business.	to '0' according to the CIS Benchmark.	
5962	Status of the current setting for 'net.ipv4.icmp_echo_ignore_broadcasts' network parameter	The 'net.ipv4.icmp_echo_ignore_broadcasts' setting (in /etc/sysctl.conf) allows the rejection of broadcast ping packets, which can cause broadcast storms. When networked hosts respond to broadcast pings, each host can add to the traffic exponentially. Enabling this setting will not respond to broadcast pings, such as those used in 'Smurf' attacks, but will allow the hosts to respond to single-source pings, this value should be set according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv4.icmp_echo_ignore_broadcasts setting on the host.	equal to 1 OR, any of the selected values below: [ ] Setting not found
5964	Status of the current setting for 'net.ipv4.conf.default.send_redirects' network parameter	The 'net.ipv4.conf.default.send_redirects' parameter allows or disallows remote ICMP routing redirects on the local host. If the system is not going to be used as a firewall or gateway and this setting is not disabled, malicious users may attempt redirection of traffic through a gateway or host that has a sniffer intercepting the traffic, so this value should be set according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv4.conf.default.send_redirects setting on the host.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found
5965	Status of the current setting for 'net.ipv4.conf.all.send_redirects' parameter	The 'net.ipv4.conf.all.send_redirects' is a network setting within the '/etc/sysctl.conf' file that allows redirection of packets to paths shorter than the originally specified route. As malicious users can attempt to use ICMP redirect packets to change the routing table on the host and redirect traffic to unauthorized destinations, this capability should be set according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv4.conf.all.send_redirects network parameter on the host.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found
5966	Status of the 'net.ipv4.conf.all.log_martians' network parameter	The 'net.ipv4.conf.all.log_martians' parameter initiates the logging of packets from source addresses with no known route. This information can be useful for diagnostic and/or auditing purposes, such	The following Integer value(s) X indicate the current status of the net.ipv4.conf.all.log_martians setting on the host.	greater than or equal to 0 OR, any of the selected values

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		seeking out routing problems or tracking intrusion attempts. However, setting this may also generate a great deal of log content, especially when the host is being used as a firewall.		below: [x] Setting not found
7464	Status of the network parameter 'net.ipv4.conf.default.log_martians'	The 'net.ipv4.conf.default.log_martians' setting logs un-routable source addresses to the kernel log, which may be spoofed packets, to later be examined by the Administrator. As there are several well known spoofing exploits, this setting should be configured according to the needs of the business.	The following Integer value(s) X indicate the current status of the net.ipv4.conf.default.log_martians setting on the host.	in 0:1 OR, any of the selected values below: [x] Setting not found
7500	Status of the 'net.ipv6.conf.default.accept_ra' network parameter on the host	The 'net.ipv6.conf.default.accept_ra' network parameter determines if router advertisements will be accepted (1) or not (0). As there are several well known spoofing and man-in-the-middle attacks, the 'net.ipv6.conf.default.accept_ra' network parameter should be configured according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv6.conf.default.accept_ra network parameter on the host.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found
7505	Status of the 'net.ipv6.conf.all.accept_redirects' network parameter on the host	The 'net.ipv6.conf.all.accept_redirects' network parameter accepts all ICMP redirects of network traffic. As there are several well known spoofing, cache poisoning, and man-in-the-middle exploits, the configuration of the 'net.ipv6.conf.all.accept_redirects' network parameter should be done according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv6.conf.all.accept_redirects network parameter on the host.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found
7506	Status of the 'net.ipv6.conf.default.accept_redirects' network parameter on the host	The 'net.ipv6.conf.default.accept_redirects' network parameter either accepts (1) or rejects (0) ICMP redirects of network traffic. As there are several well known spoofing, cache poisoning, and man-in-the-middle exploits, the configuration of the 'net.ipv6.conf.default.accept_redirects' network parameter should be done according to the needs of the business.	The following Integer value X indicates the current status of the net.ipv6.conf.default.accept_redirects network parameter on the host.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
7096	Status of the current setting for 'net.ipv4.tcp_syncookies' network parameter	The 'net.ipv4.tcp_syncookies' (/etc/sysctl.conf) setting provides for disabling/enabling SYN flood attack protection. When the SYN backlog queue on a given socket overflows, this process sends out 'syncookies,' to tell the transmitting host to reduce throughput, reducing the load ion the circuit, so this value should be set according to the needs of the business.	The following Integer value(s) X indicate the current status of the net.ipv4.tcp_syncookies setting on the host.	greater than or equal to 1 OR, any of the selected values below: [ ] Setting not found
1768	Status of the 'all.accept_redirects' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.conf.all.accept_redirects' (in /etc/sysctl.conf) function determines whether or not the host will accept redirects to gateways not listed in the host's configuration file. As not setting this appropriately could permit malicious users to spoof a source address and force a packet redirect through an invalid gateway or a 'man-in-the-middle' host with a traffic sniffer, this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the net.ipv4.conf.all.accept_redirects setting defined within the /etc/sysctl.conf file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
1778	Status of the 'ipv4.ip_forward' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.ip_forward' network parameter (in /etc/systcl.conf) is responsible for routing behavior/packet forwarding in hosts. If a host is not being used as a firewall or gateway to pass network traffic and the 'ip_forward' parameter is not disabled, this will permit the host to forward unauthorized traffic, so this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the net.ipv4.ip_forward parameters set within /etc/sysctl.conf file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
1091	Status of the number of days before a [Prompt user] password expiration warning prompt is displayed at login	Among the several characteristics that make 'user identification' via password a secure and workable solution is setting the 'expiration warning date' requirement. This establishes the number of days before the host will begin to display 'password expiration warning' messages upon login. Without having a pre-expiration warning message, it is more likely that users will not	The following Integer value X indicates the current PASS_WARN_AGE setting within the /etc/login.defs file on the host.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		prepare for this event, which may contribute to the selection of hard-to-remember or easily broken password sequences, which circumvents the intent of having rules for password complexity enforced. This may cause some users to forget or write down their new password, which can lead either to a system compromise or increased calls to Help Desk resources.		[x] File not found
5226	Status of the 'GatewayPorts' setting in the 'sshd_config' file	The 'GatewayPorts' setting in the 'sshd_config' file allows for the forwarding of connections to the host entry port. As access methods that are not applicable/required should be disallowed to block potential system attack vectors, this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the GatewayPorts setting defined within the /etc/ssh/sshd_config file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
6438	Status of the 'Ownership' settings for the 'NIS, NIS+, and /yp' files	NIS, NIS+ and yp files enable client and server authentication in RPC-based networks. RPC-based services use extremely non-secure authentication and share sensitive network object information with systems and applications using RPC-based services. As with all critical network services, the access settings to these files should be configured according to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions settings for the NIS, NIS+, and/or YP files defined within the /var/yp file on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:.* OR, any of the selected values below: [x] File not found
6439	Status of the 'Permissions' settings for the 'NIS, NIS+, and /yp' files	NIS, NIS+ and yp files enable client and server authentication in RPC-based networks. RPC-based services use extremely non-secure authentication and share sensitive network object information with systems and applications using RPC-based services. As with all critical network services, the access settings to these files should be configured according to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions settings for the NIS, NIS+, and/or YP files defined within the /var/yp file on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r]-[-x][-r]-[-x][.+]*:.* OR, any of the selected values below: [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
7478	Status of the current setting for 'net.ipv6.conf.all.accept_ra' network parameter	The 'net.ipv6.conf.all.accept_ra' network parameter choosing to accept or reject 'router advertisements (ra)'. As this parameter can be targeted by a malicious user for crafting a routing table exploit to set up a man-in-the-middle attack, this parameter should be disabled/restricted as appropriate to the needs of the business.	The following Integer value X indicates the current status of the net.ipv6.conf.all.accept_ra setting on the host.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found
1295	Status of the 'rsync' service	The 'rsync' service is a remote file copy/synchronization program that operates on TCP port 873, fulfilling the same function as the 'Remote Copy Protocol' (RCP), but with many more options and it runs much faster. However, as rsync sends data over the network without encryption and uses plain-text authentication, making it vulnerable to many types of attacks, the use of/access to this service should be restricted appropriately.	The following List string value of X indicates the status of the rsyncd service on the host.	does not contain regular expression list [0-6] OR, any of the selected values below: [x] Service not found
7376	Status of the current 'sendmail' package installed on the host	The 'Sendmail' MTA (mail transfer agent) originated in the Internet's early days, when security was not a primary consideration, so early versions suffered from a variety of security problems. If the host has an unmonitored MTA in operation, this may allow a malicious user to subvert the service to send unauthorized traffic, so use of the 'localhlost' setting for Sendmail daemon, which restricts delivery to local users, should be enabled/disabled as appropriate to the needs of the business.	The following List String value(s) X indicate the current status of the installed sendmail package on the host.	matches regular expression list .* OR, any of the selected values below: [x] Package sendmail is not installed
7377	Status of the currently installed 'postfix' packages on the host	'Postfix' is a free and open-source mail transfer agent (MTA) that routes and delivers electronic mail, intended as an alternative to the widely used Sendmail MTA. If the host has an unmonitored MTA in operation, including identifying installed Postfix packages, this may allow a malicious user to subvert the service to send unauthorized traffic, so the use of and	The following List String value(s) X indicate the currently installed postfix package on the host.	matches regular expression list .* OR, any of the selected values below: [x] Package postfix is not installed

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		access to the Postfix process should be restricted appropriately. If the Postfix application is required for the function of the host, it is recommended that it not be run as UID or GID "0".		
8543	Status of all compilers and assemblers	Compilers and assemblers are development tools enabling code to be assembled and or compiled on the host. As there are several known exploits of installed compilers and assemblers, this check should be regularly run to identify these risks and remove them, according to the needs of the business.	The following List String value(s) X indicate the current compilers and assembler rpms (gcc, java, bin86, dev86, nasm, as) on the host.	matches regular expression list .* OR, any of the selected values below: [x] Compiler and Assembler rpms not found
9706	Status of the freevxfs file system (Modprobe)	The Freevxfs filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	The List string value of X indicates the status of the file systems using modeprobe utility to check if the file system is mountable on the host.	matches regular expression list .*
9707	Status of the jffs2 Filesystems (modprobe)	The jffs2 (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	The List string value of X indicates the status of the file systems using modeprobe utility to check if the file system is mountable on the host.	matches regular expression list .*
9708	Status of the hfs Filesystems (modprobe)	The hfs filesystem type is a hierarchical filesystem that allows to mount Mac OS filesystems. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	The List string value of X indicates the status of the file systems using modeprobe utility to check if the file system is mountable on the host.	matches regular expression list .*
9709	Status of the hfsplus Filesystems (modprobe)	The hfsplus filesystem type is a hierarchical filesystem designed to replace hfs that allows to mount Mac OS filesystems. Disabling mount utility for unnecessary	The List string value of X indicates the status of the file systems using modeprobe utility	matches regular expression list .*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	to check if the file system is mountable on the host.	
9710	Status of the squashfs Filesystems (modprobe)	The squashfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to cramfs). A squashfs image can be used without having to first decompress the image. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	The List string value of X indicates the status of the file systems using modeprobe utility to check if the file system is mountable on the host.	matches regular expression list .*
9711	Status of the udf Filesystems (modprobe)	The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	The List string value of X indicates the status of the file systems using modeprobe utility to check if the file system is mountable on the host.	matches regular expression list .*
9713	Status of the freevxfs file system (lsmod)	The Freevxfs filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	The List string value of X indicates the status of the file systems using lsmod utility to check if the file system is mountable on the host.	matches regular expression list .*
9714	Status of the jffs2 Filesystems (lsmod)	The jffs2 (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the	The List string value of X indicates the status of the file systems using lsmod utility to check if the file system is mountable on the host.	matches regular expression list .*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		server. This should be configured according to the needs of the business.		
9715	Status of the hfs Filesystems (lsmod)	The hfs filesystem type is a hierarchical filesystem that allows to mount Mac OS filesystems. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business	The List string value of X indicates the status of the file systems using lsmod utility to check if the file system is mountable on the host.	matches regular expression list .*
9716	Status of the hfsplus Filesystems (lsmod)	The hfsplus filesystem type is a hierarchical filesystem designed to replace hfs that allows to mount Mac OS filesystems. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	The List string value of X indicates the status of the file systems using lsmod utility to check if the file system is mountable on the host.	matches regular expression list .*
9717	Status of the squashfs Filesystems (lsmod)	The squashfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to cramfs). A squashfs image can be used without having to first decompress the image. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	The List string value of X indicates the status of the file systems using lsmod utility to check if the file system is mountable on the host.	matches regular expression list .*
9718	Status of the udf Filesystems (lsmod)	The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats. Disabling mount utility for unnecessary filesystem types reduces the local attack surface of the server. This should be configured according to the needs of the business.	The List string value of X indicates the status of the file systems using lsmod utility to check if the file system is mountable on the host.	matches regular expression list .*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
1267	Status of the 'echo' service (udp/dgram)	The 'echo-dgram' (UDP) service is a UDP-based Internet protocol, defined in RFC 862. A localhost may connect/transmit data to a remote host that supports this protocol on TCP/UDP port 7: The remote host mirrors the data and retransmits it to the source address(es). This service may be subverted for use in various DoS attacks, by spoofing the source address and overloading the host(s) and/or network with bogus traffic. Also, as the service is owned by root, if corrupted it can lead to the compromise of all information on the host via privilege escalation, so its use and/or access should be restricted appropriately.	The following Integer value of X indicates the status of the 'echo-dgram' service on the host.	Any of the selected values below: [x] Disabled(0) [ ] Enabled(1) [x] Xinetd is disabled [x] Service not found
1329	Status of the 'echo' service (tcp/stream)	The 'echo' service is an Internet protocol, defined in RFC 862. The service usage allows a localhost to connect to a remote host (that supports this protocol) on TCP port 7--The remote host mirrors the data and retransmits it to the source address(es). This service may be subverted for use in various DoS attacks, by spoofing the source address and overloading the host(s) and/or network with data. As the service is owned by root and if corrupted can lead to the compromise of all information on the host via privilege escalation, this use of this service should be disabled or restricted appropriately.	The following Integer value of X indicates the status of the 'echo-stream' service on the host.	Any of the selected values below: [x] Disabled(0) [ ] Enabled(1) [x] Xinetd is disabled [x] Service not found
1576	Status of the 'discard' service (stream/tcp)	The 'discard' service tosses out whatever traffic comes along, becoming a network-based version of '/dev/null,' that works for both TCP and UDP traffic. (It's a very old service, once used for diagnostics.) As 'discard' runs with root-level privileges and could cause a Denial-of-Service outage if compromised, due to all data it touched being discarded, this service should be	The following Integer value of X indicates the status of the discard-stream as a Xinetd service on the host. A value of 1 indicates the service is Enabled; a value of 0 indicates the service is Disabled.	Any of the selected values below: [x] Disabled(0) [ ] Enabled(1) [x] Xinetd service disabled [x] Service not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		disabled/restricted as appropriate to the needs of the business.		
3902	Status of the 'discard' service (dgram/udp)	The 'discard' service tosses out whatever traffic comes along, becoming a network-based version of '/dev/null,' that works for both TCP and UDP traffic. (It's a very old service, once used for diagnostics.) As 'discarded' runs with root-level privileges and could cause a Denial-of-Service outage if compromised, due to all data it touched being discarded, this service should be disabled/restricted as appropriate to the needs of the business.	The following Integer value of X indicates the status of the discard-dgram as a Xinetd service on the host. A value of 1 indicates the service is Enabled; a value of 0 indicates the service is Disabled.	Any of the selected values below: [x] Disabled(0) [ ] Enabled(1) [x] Xinetd is disabled [x] Service not found
6858	Status of the 'disable' setting in the '/etc/xinetd.d/tftp' file	The 'disable' configuration setting in the '/etc/xinetd.d/tftp' file either disables or enables the tftp service. If the setting is 'disable=no'; then the tftp service is enabled. Whereas, if the setting is 'disable=yes'; then the tftp service is disabled. As the 'disable' setting in the '/etc/xinetd.d/tftp' configuration file carries significant risks, this setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the Disable setting defined within the /etc/xinetd.d/tftp file on the host.	does not contain regular expression list ^(Enabled)$ OR, any of the selected values below: [x] Setting not found [x] File not found
6037	Status of 'dev|nodev' options set for the removable media within '/etc/fstab' (mounted on '/media')	The 'dev (device)' or 'nodev (nodevice)' are mount options within the '/etc/fstab' file. The 'dev' mount option enables mounting a removable media device, whereas the 'nodev' mount option prevents the ability to mount any removable media device. Mounting removable media devices enables unauthorized persons to remove sensitive data and accessing file systems from removable media makes it easier for malicious programs and data to be imported onto the organizations network.	The following List String value(s) X indicate the current status of all removable media (/dev/cdrom, /dev/usb, /dev/msdos) within the /etc/fstab file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
6656	Status of the 'O LogLevel' setting in the '/etc/mail/sendmail.cf' file	The '/etc/mail/sendmail.cf' file provides configuration input for the sendmail command; while the 'O LogLevel=' option setting (0 is disabled - 9 is most common)	The following Integer value X indicate the current status of the [sendmail] O LogLevel setting defined within the	greater than or equal to 9

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		provides granular control of sendmail logging. As logging provides critical legal evidence of chronological events on the host, the 'O LogLevel' setting should be configured according to the needs of the business.	/etc/mail/sendmail.cf file on the host.	OR, any of the selected values below: [x] Setting not found [x] File not found
6836	Status of the 'icmp_ignore_bogus_error_responses' setting	The 'icmp_ignore_bogus_error_responses' setting allows the system to ignore certain errors caused by bogus broadcast traffic. As logging all these responses about improper traffic can fill up logfiles and potentially cause a DoS condition, this value should be set according to the needs of the business. NOTE: This value can be readjusted to log warning if necessary for audit/forensic purposes, without a need to reboot the host.	The following Integer value X indicates the current status of the net.ipv4.icmp_ignore_bogus_error_responses setting on the host.	equal to 1 OR, any of the selected values below: [ ] Setting not found
7427	Status of the currently installed 'setroubleshoot' packages on the host	The 'setroubleshoot' service provides information about AVC messages, unauthorized intrusions and configuration errors. As there are known setroubleshoot exploits such as arbitrary script injection attacks, the 'setroubleshoot' package(s) should be configured according to the needs of the business.	The following List String value(s) X indicate the current list of installed setroubleshoot packages on the host. NOTE: The 'setroubleshoot' service should be removed, according to the CIS Benchmark.	does not contain regular expression list setroubleshoot OR, any of the selected values below: [x] Package not found
7477	Status of the '/var/log/wtmp' as defined in the '/etc/audit/audit.rules' file	The '/var/log/wtmp' file is used to record all logins, shutdowns, reboots, and logouts. When the system is in multi-user mode, any system related date stamp changes are written to the '/var/log/wtmp' file. As this file records chronological activities of the host(s) and can serve as legal evidence; the '/var/log/wtmp' setting within the '/etc/audit/audit.rules' file should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the /var/log/wtmp file as defined within the /etc/audit/audit.rules file on the host.	matches regular expression list .*/var/log/wtmp OR, any of the selected values below: [x] Setting not found [ ] File not found
7970	Status of 'perm' audit parameter in the	The 'perm' audit parameter writes an audit record if the file is executed. These 'perm' audit records can monitor the use of	The following List String value(s) X indicate the current path, perm, and auid settings within the	matches regular expression list perm=x\s.*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	'/etc/audit/audit.rules' file on the host	privileged commands by non-privileged users and record them to a event repository for review and investigation. As the 'perm' audit parameter is part of the Audit subsystem and is legal evidence of chronological activity on the host, the configuration of this parameter should be done according to the needs of the business.	privileged programs (programs with setuid and/or setgid bits set on execution) on the host. NOTE: According to the CIS Benchmark, the '/etc/audit/audit.rules' file should be updated to record attempted access by unauthorized users of any privileged commands (privileged commands have setuid and/or setgid on execution).	OR, any of the selected values below: [x] Setting not found [ ] File not found
3916	Status of the 'core dump' (hard) setting	By default, core dump files are world-readable. Yet core dumps, particularly those from set-UID and set-GID processes, may contain sensitive data that should not be viewed by all users on the system. Core files must be named uniquely and written to a protected directory, or the administrator can choose to disable core file creation completely.	The following List String value(s) X indicate the current status of the hard core limit setting within the /etc/security/limits.conf file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
7435	Status of the network parameter 'fs.suid_dumpable' using 'sysctl' utility (runtime)	The network parameter 'fs.suid_dumpable' within the '/etc/sysctl.conf' file limits (or denies) setuid programs from executing core dumps on the host. As there are known exploits involving core dump data, the 'fs.suid_dumpable' parameter should be set according to the needs of the business. NOTE: SCAP and CIS recommend a setting of zero to prevent setuid programs from never make core dumps.	The following Integer value X indicates the current value of the fs.suid_dumpable network parameter on the host. NOTE: The 'fs.suid_dumpable' network parameter should be set to '0', according to the CIS Benchmark.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found
5636	Status of the 'Log Retention and Rotation (daily, weekly, monthly)' settings within '/etc/logrotate.conf' file	Log files generated by the syslog daemon provide information on system security events, such as login authentication and privileged use access. By setting log file 'Retention method' guidelines, system security event information can be maintained to preserve a contiguous audit trail for use in forensic investigation. To ensure log files provide a complete audit	This List string value of X indicates the current status of Rotation of logs. This is normally the same as rotating logs on the first day of the week.	matches regular expression list ^(daily)$ OR, any of the selected values below: [ ] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		trail, retention method options such as file rotation when the log is full, or establishing a timeframe before file overwrite and/or deletion takes place, should be set as appropriate to the needs of the business.		[ ] File not found
5291	Status of the 'Subsystem' setting in the '/etc/ssh/sshd_config' file	'Subsystem' is a setting in the '/etc/ssh/sshd_config' file. This setting applies to Protocol version 2 only and configures an external subsystem; such as a file transfer daemon. As there are known buffer overflow exploits with this setting, the value of this setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the Subsystem setting defined within the /etc/ssh/sshd_config file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
5292	Status of the 'SyslogFacility' setting in the '/etc/ssh/sshd_config' file	'SyslogFacility' is a setting in the '/etc/ssh/sshd_config' file. This setting sends code to the facility when logging sshd(8) messages. As there are known buffer overflow exploits with this setting, the value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the SyslogFacility setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^(AUTH(PRIV)?)$ OR, any of the selected values below: [x] Setting not found [x] File not found
7076	Status of the 'Permissions' settings for the '/etc/shells' file	The '/etc/shells' file contains login shell complete pathnames and several programs consult /etc/shells to determine if a user is a normal user. As there are several known shell injection and privilege escalation exploits, the access configuration to '/etc/shells' should be done according to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions settings for the /etc/shells file.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:/etc/shells OR, any of the selected values below: [x] File not found
8796	Status of the 'GECOS' field within '/etc/passwd' on the host	The GECOS field, within the '/etc/passwd' file, stores additional associated information and can store information in a comma delimited format. As there are several known buffer overflow exploits, the GECOS	The following List String value(s) X indicate the current GECOS field contents from the /etc/passwd file on the host.	matches regular expression list .* OR, any of the selected values below:

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		field should be carefully configured according to the needs of the business.		[x] Setting not found [x] File not found
7458	Status of the 'inet_interfaces' setting in the '/etc/postfix/main.cf' file	The 'inet_interfaces' setting in the '/etc/postfix/mail.cf' file defines the Postfix network interface addresses. As there are known buffer overflow, privilege escalation, and symlink exploits with Postfix, this parameter should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the inet_interfaces setting in the /etc/postfix/main.cf file on the host.	matches regular expression list ^(loopback-only|localhost|127.0.0.1)$ OR, any of the selected values below: [ ] Setting not found [x] File not found
7412	Status of the 'periodically scheduled (crontab)' aide check	AIDE (advanced intrusion detection environment) is an OS package for checking critical file(s) for alteration, while the cron job ensures this check is done on a regular schedule. Any file sizes not matching the approved baseline file size is reported for examination. As there are several known file integrity exploits, the cron job checking the AIDE package should be configured according to the needs of the business.	The following List String value(s) X indicate the periodic file checking (crontab) settings for the AIDE package on the host.	matches regular expression list .* /usr/sbin/aide --check OR, any of the selected values below: [x] Setting not found
8123	Status of the hardware architecture and operating system information (os release, os name, os version) contained in the '/etc/motd' file on the host	The hardware architecture, operating system name, release and version is often displayed in the contents of the '/etc/motd' banner file. As providing hardware, OS, and patch level information in the banner can assist attackers in exploiting the host, this information should be removed from the '/etc/motd' file on the host.	The following List String value(s) X indicate the current contents of the '/etc/motd' file which will be used to display a banner message after successful login. ** Note: The contents of this file require review and approval.	does not contain regular expression list (\\m|\\r|\\s|\\v|\\m|\\S) (Red)[\s\t](Hat)[\s\t](Enterprise)[\s\t](Linux) (Kernel)[\s\t]+([0-9]+|\\r) OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
				[x] File not found
8122	Status of the hardware architecture and operating system information (os release, os name, os version) contained in the warning banner in the '/etc/issue' file on the host	The hardware architecture, operating system name, release and version is often displayed in the contents of the '/etc/issue' banner file. As providing hardware, OS, and patch level information in the banner can assist attackers in exploiting the host, this information should be removed from the '/etc/issue' file on the host.	The following List String value(s) X indicate the current contents of the '/etc/issue' file which will be used to display a banner message at the login prompt. ** Note: The contents of this file require review and approval.	does not contain regular expression list (\\m|\\r|\\s|\\v|\\m|\\S) (Red)[\s\t]*(Hat)[\s\t]*(Enterprise)[\s\t]*(Linux) (Kernel)[\s\t]+([0-9]+|\\r) OR, any of the selected values below: [x] Setting not found [x] File not found
8124	Status of the hardware architecture and operating system information (os release, os name, os version) contained in the '/etc/issue.net' file on the host	The hardware architecture, operating system name, release and version is often displayed in the contents of the '/etc/issue.net' banner file. As providing hardware, OS, and patch level information in the banner can assist attackers in exploiting the host, this information should be removed from the '/etc/issue.net' file on the host.	The following List String value(s) X indicate the current contents of the '/etc/issue.net' file which will be used to display a banner message at the login prompt. ** Note: The contents of this file require review and approval.	does not contain regular expression list (\\m|\\r|\\s|\\v|\\S) (%m|%r|%s|%v) (Red)[\s\t](Hat)[\s\t](Enterprise)[\s\t](Linux) (Kernel)[\s\t]+([0-9]+|\\r) OR, any of the selected values below: [x] Setting not found [x] File not found
1769	Status of the 'default.accept_redirects' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.conf.default.accept_redirects' parameter (/etc/sysctl.conf) allows packets to be redirected through different gateways to reach their final destination. As disabling	The following List String value(s) X indicate the current status of the net.ipv4.conf.default.accept_redir	matches regular expression list .*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		this prevents the host from accepting ICMP Redirect messages, which can forward traffic to non-existent gateways or through a host with a traffic sniffer, this value should be set according to the needs of the business.	ects parameters set within /etc/sysctl.conf file.	OR, any of the selected values below: [x] Setting not found [x] File not found
1770	Status of the 'all_secure_redirects' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.conf.all.secure_redirects' setting (/etc/sysctl.conf) requires all packets to use only gateways listed in the host's configuration files. Even when only 'secure redirects' are allowed, there exists the possibility of insider threats changing the host's configuration files to add an unauthorized gateway, which would allow the redirecting of traffic through a 'man in the middle' host, so this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the net.ipv4.conf.all.secure_redirects parameters set within /etc/sysctl.conf file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
1771	Status of the 'default.secure_redirects' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.conf.default.secure_redirects' network parameter (in /etc/sysctl.conf) restricts packet traffic to flow through configured gateways. If a false gateway can be inserted in the host's configuration file, redirects can be used to force packets through an invalid gateway or a "man-in-the-middle" host with a traffic sniffer, so this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the net.ipv4.conf.default.secure_redirects parameters set within /etc/sysctl.conf file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
1774	Status of the 'net.ipv4.conf.all.accept_source_route' setting within the '/etc/sysctl.conf' file	The 'accept source route (/etc/sysctl.conf)' setting allows a packet with encapsulated ICMP routing information (that may differ from the routes already specified on the host) to be acted upon. If not disabled, invalid/spoofed source routes can lead to a DoS or redirection of traffic through a 'man-in-the-middle' host, where a malicious user can attempt login replay attacks and/or other exploits, so this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the net.ipv4.conf.all.accept_source_route parameters set within /etc/sysctl.conf file.	is contained in regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
1775	Status of the current setting for	The 'net.ipv4.conf.all.rp_filter' parameter is enabled, it prevents source address	The following Integer value X indicate the current status of the	greater than or equal to

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	'net.ipv4.conf.all.rp_filter' network parameter	spoofing attacks on interfaces, by initializing source route verification. If not set, invalid/spoofed source routes can lead to a DoS or redirection of traffic through a 'man-in-the-middle' host, where a malicious user can attempt login replay attacks and/or other exploits, so this value should be set according to the needs of the business.	net.ipv4.conf.all.rp_filter setting on the host. NOTE: The 'net.ipv4.conf.all.rp_filter' should be set to '1' (enabled) according to the CIS Benchmark.	0 OR, any of the selected values below: [x] Setting not found
1776	Status of the 'net.ipv4.conf.default.rp_filter' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.conf.default.rp_filter' (/etc/sysctl.conf) performs route source validation via a reversed path. As having this setting enabled helps to block 'source address spoofing' attacks, where a malicious user might attempt login replay attacks and/or other exploits, this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the net.ipv4.conf.default.rp_filter setting defined within the /etc/sysctl.conf file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
1779	Status of the 'net.ipv4.conf.all.send_redirects' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.conf.all.send_redirects' network parameter (/etc/sysctl.conf) allows ICMP routing redirection. If the system is not going to be used as a firewall or gateway to pass network traffic, and this parameter is not disabled, malicious users may attempt to spoof source addresses or redirect traffic to a host with a network sniffer, so this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the net.ipv4.conf.all.send_redirects setting defined within the /etc/sysctl.conf file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
1780	Status of the 'net.ipv4.conf.default.send_redirects' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.conf.default.send_redirects' parameter allows/disallows remote ICMP routing redirects to be implemented on the local host. If the system is not going to be used as a firewall or gateway and this setting is not disabled, malicious users may attempt redirection of traffic through a gateway or host that has a sniffer intercepting the traffic, so this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the net.ipv4.conf.default.send_redirects setting defined within the /etc/sysctl.conf file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
2263	Permissions set for the '/etc/issue.net' file	The '/etc/issue.net' file provides the text for a logon banner to appear prior to displaying the login prompt. This allows for the administrator of the system to provide a warning to all users regarding acceptable use of the device and provides a legal position for monitoring of activity. As unrestricted access to this file could permit a malicious user to delete or manipulate the information displayed therein, potentially causing embarrassment or even legal issues for the owner, file access should be set as appropriate to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permission settings for the /etc/issue.net file on the host.	matches regular expression list root:root:[-r][-w][-][-r][-][-][-r][-][-][.+]*:/etc/issue.net OR, any of the selected values below: [ ] File not found
2264	Permissions set for the '/etc/issue' file	The '/etc/issue' file provides the text for a logon banner to appear prior to displaying the login prompt. This allows for the administrator of the system to provide a warning to all users regarding acceptable use of the device and provides a legal position for monitoring of activity. As unrestricted access to this file could permit a malicious user to delete or manipulate the information displayed therein, potentially causing embarrassment or even legal issues for the owner, file access should be set as appropriate to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions settings for the /etc/issue file on the host.	matches regular expression list root:root:[-r][-w][-x][-r][-][-][-r][-][-][.+]*:/etc/issue OR, any of the selected values below: [ ] File not found
2272	Permissions set for the '/root/.bash_profile' file	The '/root/.bash_profile' umask variable (in '/root/.bash_profile') does not work as a mask--you must set the permissions to the level that you DO NOT want on a file or directory with a umask. To determine the file/directory permissions for '.bash_profile' that would result from a given umask value, subtract the umask from '666' for files and from '777' for directories. The most common default value for a umask is '022'--this will create default 'file permissions' with a value of '644' ([user]rw- [group]r-- [other]r-	The following List String value(s) X indicate the current Ownership and Permissions set for the /root/.bash_profile file on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:/root/\.bash_profile OR, any of the selected values below: [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		-). Directories will have permissions of '755' ([user]rwx; [group]r-x; [other]r-x) and be searchable by 'group' and 'other.' The most restrictive [file] umask setting is 077 (rwx ------) with owner (rwx), group (no access), and other (no access). The output of this check/test if the result of a 'cat /root/.bash_profile | grep umask' type of command.		
2273	Permissions set for the '/root/.bashrc' file	The '/root/.bashrc' file contains information related to root's login script, such as programming shortcuts and environment variables. As permitting unrestricted access to the '/root/.bashrc' file may allow a malicious user to alter system-wide variables that would allow privilege escalation or rootkit launching, permissions set for this file should be restricted as appropriate to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions set for the /root/.bashrc file on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:/root/\.bashrc OR, any of the selected values below: [x] File not found
2274	Permissions set for the '/root/.tcshrc' file	The 'default UMASK permissions' determine what [default] privilege level will be set upon directories and files created by the user. The usual manufacturer default is '022.' If set at this value, when creating a new file, the resulting default permissions will be '644' (666 minus 022, i.e. -rw-r--r--). When creating a new directory, these default permissions will be 755 (drwxr-xr-x), which sets the access level to (rwx r-x r-x): for owner (rwx), group (read/execute), other (read/execute) access on file access. If users are not properly restricted, sensitive system or business information may be improperly disclosed. The most restrictive setting is 077 and your default file permissions would be 600 (-rw-------) and your default directory permissions would be 700 (drwx------), thus becoming (rwx --- ---): for owner (rwx), group (no access), other (no access). Also, as a malicious user	The following List String value(s) X indicate the current Ownership and Permissions setting within the /root/.tcshrc file on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:/root/\.tcshrc OR, any of the selected values below: [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		could lay the groundwork for a privilege escalation attack by changing the UMASK value in this configuration file, access to this file and its UMASK setting should be restricted appropriately.		
2626	Permissions set for the '/usr' directory	The /usr directory contains sub-directories and files that are shared with other users. Generally, one can find online manual files, language dictionaries and/or other applications here. As with other sensitive data files, these should be protected from inappropriate and/or unapproved access. Implement this check and perform periodic reviews to ensure that only those approved by the owner of the data/system actually have access to this directory and its contents.	The following List String value(s) X indicate the current Ownership and Permissions settings for the /usr directory.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:/usr OR, any of the selected values below: [x] Directory not found
2627	Permissions set for the '/' (root) directory	Hierarchically speaking, '/', or root, is the top most directory in the file system structure. In most cases, only privileged users should have access to this directory. Granting access to the '/' directory makes damaging the system or obtaining confidential information much easier for a malicious user. Maintenance of the permissions granted to the '/' directory requires the highest level of diligence and attention. Consider implementing and performing this check periodically to ensure only appropriate and approved individuals have such access to satisfy audit requirements.	The following List String value(s) X indicate the current Ownership and Permissions settings for the / directory.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:/ OR, any of the selected values below: [x] Directory not found
6499	Permissions set for the '/etc/xinetd.d' directory	The 'xinetd' service provides the traditional network-based services for the host, such as ftp, telnet, and so forth. As remote access to this file can allow unauthorized changes that open up vectors to network-based attacks, remote access to this service can be restricted via the 'only_from' option and should be set according to the needs of the business. NOTE: Applying this setting	The following List String value(s) X indicate the current Ownership and Permissions set for the /etc/xinetd.d directory on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:/etc/xinetd.d OR, any of the selected values below: [x] Directory not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		can have unexpected effects that lock out remote connections, so this alteration should be carefully tested before applying the change to a Production network and access should be limited/monitored in accordance with business needs and requirements.		
7356	Status of the 'Permissions' settings for the '/etc/at.deny' file	The permissions settings for the '/etc/at.deny' file determines which user can set permissions for other users to have read/write/execute access to this file. As the 'at.deny' file uses reverse logic, in that anyone NOT LISTED in the file can use the 'at' command, permissions for this file, or even its existence, should be determined according to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions settings for the /etc/at.deny file.	is contained in regular expression list [a-z]*\:[a-z]*\:[-r][-w][-][-][-][-][-][-][-][.+]*:/etc/at.deny (root):(root):[-r][-w][-][-r][-][-][-r][-][-][.+]*:/etc/at.deny OR, any of the selected values below: [ ] File not found
9704	Status of the access (Permissions,Ownership, Integrity) set for system files	The RPM package manager is a package management system. It is a program used for installing, uninstalling, and managing software packages on the system. Each software package consists of an archive of files along with information about the package like its version, a description etc. Access (Permissions,Ownership, Integrity) should be restricted to system files and directories from unauthorized users and should be configured according to the needs of the business.	The following List String value of X verifies the System File permissions on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting Not Found
100498	Permissions set for the files under '/etc/ssh2/' directory (restricted)	SSH is the standard encrypted communications software used on Prudential's Unix servers. It installs with appropriately restricted file permissions.	The following String value(s) X indicate the files of the /etc/ssh*/*key, /etc/ssh*/moduli, /etc/ssh*/random_seed file(s) with violation for the permission (r---------) on the host.	is contained in regular expression list ^(File not found|No data found)$
2265	Permissions set for the '/etc/motd' file	The message of the day file, '/etc/motd,' is intended to provide the greeting displayed	The following List String value(s) X indicate the current Ownership	matches regular expression list

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		after a user logs in. As unrestricted access to the '/etc/motd' file would allow a malicious user to potentially modify or delete the message warning of the proper use of corporate resources open to unauthorized manipulation, access should be set as appropriate to the needs of the business.	and Permissions settings for the /etc/motd file on the host.	.*:.*:[-r][-w][-][-r][-][-][-r][-][-][.+]*:/etc/motd OR, any of the selected values below: [x] File not found
3866	Permissions set for the '/etc/securetty' file	The '/etc/securetty' file specifies which TTY devices the root user is allowed to login at. 'Root' is, by its nature, is a shared login; there can be only one root user, even though another account can be assigned a '0' userid, which gives the same root-level privileges. Due to the inability to determine just which user has accessed the host as 'root,' direct login as 'root' should not be allowed except via the hosts' console, when this access is physically controlled/monitored, for initial configuration or emergency situations. As access to the file(s) which allow root login via a [local] console/tty connection could allow changes to root login requirements, the file permissions should be restricted appropriately.	This String value X indicates the current Ownership and Permissions set for the /etc/securetty file.	regular expression match .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:.* OR, any of the selected values below: [x] File not found
3868	Status of the contents of the login banner in '/etc/motd'	The message of the day file, '/etc/motd,' is intended to provide the greeting/warning banner displayed AFTER a user successfully authenticates. By displaying an acceptable use policy prior to login provides notification that all user activity is monitored and warns of potential legal consequences from unauthorized use. Also, as unrestricted access to the '/etc/motd' file would permit a malicious user to modify the message content, leaving corporate resources open to unauthorized use and/or manipulation, this 'warning' content should be set as appropriate to the needs of the business. NOTE: If	The following List String value(s) X indicate the current contents of the '/etc/motd' file which will be used to display a banner message after successful login. ** Note: The contents of this file require review and approval.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		separation of the Control governing the 'text content' and a check on the status of 'user permissions' on this file is preferred, to ensure only authorized and appropriate users have the ability to modify the file contents, then consider implementing this control in conjunction with CID-2265, which provides a separate permissions review.		
3778	Status of the contents of the 'login banner' (Windows/Unix/Linux)	The logon banner provides a warning to inappropriate or unapproved users as to the consequences of accessing private systems and data illegally. By producing a legal text message during the login process, all individuals attempting to access the system understand that monitoring of all system activity is performed and all violators may be prosecuted, to the full extent of the law. As implementing a logon banner to deter inappropriate use can provide a foundation for legal action against abuse, this 'warning' content should be set as appropriate to the needs of the business.	The following List String value(s) X indicate the current contents of the '/etc/issue' file which will be used to display a banner message at the login prompt. ** Note: The contents of this file require review and approval.	matches regular expression list (WARNING(!)?[\s\n\r]+)(This[\s]+system,[\s]+owned[\s]+by[\s]+the[\s]+Company,[\s]+may[\s]+be[\s]+used[\s]+only[\s]+by[\s]+authorized[\s]+personnel[\s]+for[\s]+authorized[\s]+purposes\.[\s]+All[\s]+activities[\s]+conducted[\s]+on[\s]+and[\s]+communications[\s]+and[\s]+other[\s]+information,[\s]+including[\s]+personal[\s]+information,[\s]+accessed,[\s]+processed,[\s]+stored,[\s]+or[\s]+transmitted[\s]+using[\s]+the[\s]+system[\s]+may[\s]+be[\s]+examined,[\s]+recorded,[\s]+copied,[\s]+used[\s]+and[\s]+disclosed[\s]+in[\s]+accordance[\s]+with[\s]+applicable[\s]+law\.[\s]+The[\s]+Company[\s]+monitors[\s]+systems[\s]+to[\s]+safeguard[\s]+the[\s]+security[\s]+of[\s]+its[\s]+systems[\s]+and[\s]+data,[\s]+to[\s]+protect[\s]+against[\s]+policy[\s]+violations[\s]+and[\s]+unlawful[\s]+activity,[\s]+to[\s]+administer[\s]+working[\s]+relationships,[\s]+and[\s]+to[\s]+meet[\s]+legal[\s]+obligations[\s]+and[\s]+promises[\s]+to[\s]+business[\s]+partners\.[\s]+By[\s]+proceeding,[\s]+you[\s]+agree[\s]+to[\s]+use[\s]+the[\s]+syste

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
				m[\s]+only[\s]+for[\s]+authorized[\s]+purposes[\s]+and[\s]+in[\s]+accordance[\s]+with[\s]+Company[\s]+policies[\s]+that[\s]+have[\s]+been[\s]+made[\s]+available[\s]+to[\s]+you\.[\s]+For[\s]+additional[\s]+information[\s]+consult[\s]+your[\s]+local[\s]+business(.){1,4}s[\s]+employee[\s]+privacy[\s]+notice[\s]+or[\s]+contact[\s]+your[\s]+local[\s]+Privacy[\s]+Officer\.) OR, any of the selected values below: [ ] Setting not found [ ] File not found
2152	Permissions set for the '/etc/passwd' file	The '/etc/passwd' file stores essential user account information required during login. As unrestricted permissions could potentially allow a malicious user gain access to files containing primary security and user account information, which would allow privilege escalation exploits to be conducted, this file's access should be restricted as appropriate to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions set for the /etc/passwd file on the host.	matches regular expression list .*:.*:[-r][-w]-[-r]--[-r]--[.+]*:/etc/passwd OR, any of the selected values below: [x] File not found
2158	Status of the 'Permissions' settings for the 'sshd_config' file	The '/etc/ssh/sshd_config' file contains configuration parameters for setting up/operating the Secure Shell daemon (sshd). As having this file with unrestricted permissions could facilitate the creation of a number of exploits, such as changing versions to one with security holes, default key generation, or permitting direct root logins based on host address rather than password, access to this configuration file should be restricted as appropriate to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions settings within the /etc/ssh/sshd_config file on the host.	matches regular expression list (root):.*:[-r][-w][-x][-r][-][-x][-r][-][-x][.+]*:/etc/ssh/sshd_config OR, any of the selected values below: [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
2189	Status of the 'Permissions' settings for the '/etc/group' file	The '/etc/group' file contains a list of all groups, the group id numbers, as well as the users defined within them. It is recommended that all users permit 'read (r)' access while permitting 'write (w)' access only to the root user and members of the security group. As unrestricted access on this file's contents could facilitate privilege escalation and/or DoS attacks, user accesses should be limited as appropriate to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions settings within the /etc/group file on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:.etc.group OR, any of the selected values below: [x] File not found
2239	Status of the 'PermitRootLogin' setting in the 'sshd_config' file	The 'PermitRootLogin' value (in '/etc/ssh/sshd_config') allows for 'direct' root login by a remote user/application to resources on the local host. As permitting direct 'root' login under any circumstances, except physically at the console (where facility tracking of user presence can be implemented), is a security risk and necessarily compromises the individual accountability and audit capability that is provided by requiring a 'sudo' connection for root-level activities, this value should be set as appropriate to the needs of the business.	The following List String value(s)X indicate the current PermitRootLogin setting within the /etc/ssh/sshd_config file.	matches regular expression list [nN][oO] OR, any of the selected values below: [x] Setting not found [x] File not found
2702	Permissions set for the '/etc/inittab' file	The '/etc/inittab' file contains the script used by the 'init' command to initialize and control system processes. Autonomous system processes such as getty, daemons, and the shell are initialized through the 'init' command and are required for the systems operation. As unauthorized access to critical system configuration files can allow a malicious user to disrupt system availability, access to the '/etc/inittab' should be restricted as appropriate to the needs of the business.	This String value X indicates the current Ownership and Permissions set for the /etc/inittab file.	regular expression match .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:.* OR, any of the selected values below: [x] File not found
3161	Current list of members defined within the 'root' group (/etc/group)	This control provides a membership listing for the 'root' group within the /etc/group file. Each member of this group has complete control of the system and access must be	The following List String value(s) X indicate the current members of the root group as defined within the /etc/group file.	match any regular expression match .*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		tightly managed. By periodically running this control and comparing the output to a pre-approved list of accounts as determined by the system owner provides assurance that the processes in place supporting logical security administration are effective. The results of such a review can be used as evidentiary support for audit purposes.		
3371	Status of the 'UMASK' set for '/etc/profile'	The 'default UMASK permissions' determine what [default] privilege level will be set upon directories and files created by the user. The usual manufacturer default is '022.' If set at this value, when creating a new file, the resulting default permissions will be '644' (666 minus 022, i.e. -rw-r--r--). When creating a new directory, these default permissions will be 755 (drwxr-xr-x), which sets the access level to (rwx r-x r-x): for owner (rwx), group (read/execute), other (read/execute) access on file access. If users are not properly restricted, sensitive system or business information may be improperly disclosed. The most restrictive setting is 077 and your default file permissions would be 600 (-rw-------) and your default directory permissions would be 700 (drwx------), thus becoming (rwx --- ---): for owner (rwx), group (no access), other (no access). Also, as a malicious user could lay the groundwork for a privilege escalation attack by changing the UMASK value in this configuration file, access to this file and its UMASK setting should be restricted appropriately.	The following List String value(s) X indicate the current status of the Default User UMASK setting defined within the /etc/profile file on the host.	matches regular expression list [0][02][2367] [0][2][2367] OR, any of the selected values below: [ ] Setting not found [ ] File not found
3867	Status of where the 'root account is permitted to login' defined within the '/etc/securetty' file	'Root' is, by its nature, a shared login; there can be only one root user, even though another account can be assigned a '0' userid, which provides the same root-level privileges. Due to the inability to determine just which user has accessed the host as	The following List String value(s) X indicate the current list of authorized consoles defined in the /etc/securetty file on the host. NOTE: The following list of console(s) require review and	is contained in regular expression list ^(([0-9]+/)?tty[S0-9]+)$ ^(hvc[0-9]+)$

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		'root,' direct login as 'root' should not be allowed except via the hosts' console, when this access is physically controlled/monitored, for initial configuration or emergency situations. At all other times, the administrator should access root-level privileges by first accessing his/her individual account, then use a secondary authorization mechanism, such as the 'su' command or the 'sudo' package for root-level work--this provides an audit trail of his/her activities. As access to the file(s) which allow root login via a [local] console/remote connection could allow changes to root login requirements, the file permissions should be restricted appropriately.	approval and any console(s) not in a physically secure location should be removed.	^(hvsi[0-9]+)$ ^(xvc[0-9]+)$ ^(vc/[0-9]+)$ ^(.*sclp.*)$ ^(console)$ OR, any of the selected values below: [x] Setting not found [x] File not found
4438	Status of the hosts defined within the hosts.deny file	The '/etc/hosts.deny' file indicates the names of the hosts which are NOT permitted to access the local services. All access should be denied by default unless explicitly authorized to prevent a malicious user from performing inappropriate actions against the host. Run this check to ensure access control measures are in accordance with the requirements and expectations of the business.	The following List string value of X returns the content of /etc/hosts.deny file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting Not Found [x] File Not Found
5162	Status of the current 'Permissions' settings for the '/var/spool/cron/' directory	The '/var/spool/cron' directories contains crontab files used to run commands at pre-defined intervals/times by the 'cron' daemon. If permissions are not managed and monitored for these directories, access by a malicious user could compromise the system and any sensitive data residing on it as a job could be created to copy the contents of a specific directory/file to a remote location. Run this check periodically to ensure only appropriate and approved individuals have access.	The following List String value(s) X indicate the current Ownership and Permissions defined for the /var/spool/cron directory on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r]-[-x][-r]-[-x][.+]*:/var/spool/cron.* OR, any of the selected values below: [x] Directory not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
5215	Status of the 'AllowGroups' setting in the 'sshd_config' file	The 'AllowGroups' setting defines the user groups permitted login via SSH connections. Access control for critical devices is not only important, for some organizations it is required by law depending on the type of data residing on them. This check can be run periodically to determine if the groups listed within the sshd_config file are appropriate and approved as a malicious user could make changes to accommodate continuous access. As with all critical devices, access to them should be tightly managed and maintained to meet the needs of the business.	The following List String value(s) X indicate the current status of the AllowGroups setting defined within the /etc/ssh/sshd_config file. NOTE: The following List requires review and approval.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
5217	Status of the 'AllowUsers' setting in the 'sshd_config' file	The 'AllowUsers' setting defines the user groups permitted login via SSH connections. Access control for critical devices is not only important, for some organizations it is required by law depending on the type of data residing on them. This check can be run periodically to determine if the users listed within the sshd_config file are appropriate and approved as a malicious user could make changes to accommodate continuous access. To further tighten the access to the target, entries can be made for user and host specification by using the USER@HOST format. As with all critical devices, access to them should be tightly managed and maintained to meet the needs of the business.	The following List String value(s) X indicate the current status of the AllowUsers setting defined within the /etc/ssh/sshd_config file. NOTE: The following List requires review and approval.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
5224	Status of the 'DenyGroups' setting in the 'sshd_config' file	The 'DenyGroups' setting is used to determine the groups that will be denied access to 'ssh' connections on the host. All primary and/or supplementary user accounts associated with those group names listed after this keyword are prevented from logging in. As this is a	The following List String value(s) X indicate the current status of the DenyGroups setting defined within the /etc/ssh/sshd_config file. NOTE: The following List requires review and approval.	matches regular expression list .* OR, any of the selected values below:

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		critical remote access setting and carries significant risks, this setting should be configured according to the needs of the business.		[x] Setting not found [x] File not found
5225	Status of the 'DenyUsers' setting in the 'sshd_config' file	The 'DenyUsers' setting is used to determine the users that will be denied access to 'ssh' connections on the host. All primary and/or supplementary user accounts associated with those user names listed after this keyword are prevented from logging in. As a malicious user could modify this list to open up inappropriate access to unapproved user accounts, this check can be used to ensure only appropriate entries are made in accordance with the strict needs and requirements related to access control for the business.	The following List String value(s) X indicate the current status of the DenyUsers setting defined within the /etc/ssh/sshd_config NOTE: the following List requires review and approval.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
6336	Ownership set for the 'root user account home directory'	Changing the default home directory for the root account provides segregation from the OS distribution and permits the isolated 'root' home directory to have more restricted permissions, preventing viewing of the root system account files by non-root users. Having Group- or World-readable/writable for the root users home directory may enable malicious users to read/modify data or to gain the root system privileges. Disabling/limiting access for users other than root, such as requiring the default home directory UMASK to be at 027, still allows for appropriate discretionary access control to certain files to be read/changed within the root users home directory, while [automatically] blocking access by 'Other' group members, while permitting only 'file execute' privileges by default to approved group members.	The following List String value(s) X indicate the current Ownership and Permissions set for the root user account's HOME Directory on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:.* OR, any of the selected values below: [x] Directory not found
6496	Ownership set for the '/etc/xinetd.conf' file	The 'xinetd' service provides the traditional network-based services for the host, such as ftp, telnet, and so forth. As remote	The following List String value(s) X indicate the current Ownership	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		access to this file can allow unauthorized changes that open up vectors to network-based attacks, remote access to this service can be restricted via the 'only_from' option and should be set according to the needs of the business. NOTE: Applying this setting can have unexpected effects that lock out remote connections, so this alteration should be carefully tested before applying the change to a Production network and access should be limited/monitored in accordance with business needs and requirements.	and Permissions set for the /etc/xinetd.conf file on the host.	x][.+]*:/etc/xinetd.conf OR, any of the selected values below: [x] File not found
6497	Status of the 'Permission' settings for the '/etc/xinetd.conf' file	The 'xinetd' service provides the traditional network-based services for the host, such as ftp, telnet, and so forth. As remote access to this file can allow unauthorized changes that open up vectors to network-based attacks, remote access to this service can be restricted via the 'only_from' option and should be set according to the needs of the business. NOTE: Applying this setting can have unexpected effects that lock out remote connections, so this alteration should be carefully tested before applying the change to a Production network and access should be limited/monitored in accordance with business needs and requirements.	The following List String value(s) X indicate the current Ownership and Permissions set for the /etc/xinetd.conf file on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x][.+]*:/etc/xinetd.conf OR, any of the selected values below: [x] File not found
6636	Status of the '.rhosts' capability within the '/etc/pam.d/*' files	The '.rhosts' capability within the '/etc/pam.d/*' files provides for unauthenticated user login based on the contents of the .rhosts files. As .rhost file content is stored in clear text and could allow unauthorized users to compromise a number of hosts, this capability should be disabled or restricted as per the needs of the business.	The following List String value(s) X indicate the current files with pam_rhosts (support) within the /etc/pam.d/* directory on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
6756	Status of the 'users' listed in the '/etc/vsftpd/ftpusers' file	The '/etc/vsftpd/ftpusers' file lists users who are not allowed to login using the FTP server daemon. The '/etc/vsftpd/ftpusers' file protects the TCP/IP network from several risks by not allowing highly privileged users from logging into the network via FTP. As there are several known privilege escalation exploits, run this check periodically on the status of the '/etc/vsftpd/ftpusers' file according to the needs of the business.	The following List String value(s) X indicate the current list of users defined within the /etc/vsftpd/ftpusers file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
7554	Status of the current 'Ownership' settings for the '/var/spool/cron' directory	The '/var/spool/cron' directory contains crontab files used to run commands at pre-defined intervals/times by the 'cron' daemon. If ownership is not managed and monitored for these directories, access by a malicious user could compromise the system and any sensitive data residing on it as a job could be created to copy the contents of a specific directory/file to a remote location. Run this check periodically to ensure only appropriate and approved individuals have access.	The following List String value(s) X indicate the current Ownership and Permissions defined for the /var/spool/cron directory on the host.	matches regular expression list root:.*:[-r][-w][-x][-r]-[-x][-r]-[-x][.+]*:/var/spool/cron OR, any of the selected values below: [x] Directory not found
7555	Status of the current 'Permissions' settings for the '/var/spool/cron' directory	The '/var/spool/cron' directory contains crontab files used to run commands at pre-defined intervals/times by the 'cron' daemon. If permissions are not managed and monitored for these directories, access by a malicious user could compromise the system and any sensitive data residing on it as a job could be created to copy the contents of a specific directory/file to a remote location. Run this check periodically to ensure only appropriate and approved individuals have access.	The following List String value(s) X indicate the current Ownership and Permissions defined for the /var/spool/cron directory on the host.	matches regular expression list .*:.*:[-r][-w][-x][-r]-[-x][-r]-[-x][.+]*:/var/spool/cron root:root:[-r][-w][-x][-r][-w][-x][-r]-[-x][.+]*:/var/spool/cron OR, any of the selected values below: [x] Directory not found
2188	Permissions set for the '/etc/shadow' file	The '/etc/shadow' file contains a list of all 'usernames,' their 'userid,' 'group id,' and the 'encrypted password.' As unrestricted access on this file's contents could facilitate privilege escalation and/or password	The following List String value(s) X indicate the current Ownership and Permissions set for the /etc/shadow file on the host.	matches regular expression list (root):(root):[-r][-][-][-][-][-][-][-][-][.+]*:/etc/shadow

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		decryption attacks, permissions should be limited as appropriate to the needs of the business.		OR, any of the selected values below: [x] File not found
1260	Status of the 'Common Unix Printing System (cups)' service	The 'cupsrenice' (Common UNIX Printing System) component provides legacy and line printer services for the host. CUPS does not have access control validation, according to settings in 'cupsd.conf,' 'hosts.allow,' or 'hosts.deny' files, such as those used by 'TCP wrappers,' so this service will print any job sent to it. As this has no access control functions it should probably be disabled on any host but a dedicated print server, for there are a number of possible exploits this will support. NOTE: One novel exploit 'printed' system files to an email daemon, then sent the file contents out as SMTP.	The List String value of X indicates the status of the cups service on the host.	matches regular expression list .* OR, any of the selected values below: [x] Service not found
6036	Status of 'suid|nosuid' options set for the removable media within '/etc/fstab' (mounted on '/media')	The 'suid' mount option enables a user id to mount removable media devices, whereas the 'nosuid' mount option prevents any users from mounting removable media devices. Allowing users to mount and access file systems from removable media makes it easier for malicious programs and data to be imported onto the organizations network or enables unauthorized persons to remove sensitive data.	The following List String value(s) X indicate the current status of all removable media (/dev/cdrom, /dev/usb, /dev/msdos) within the /etc/fstab file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
7396	Status of the mount-option 'suid|nosuid' set for '/tmp' partition in file '/etc/fstab'	The 'suid' mount option enables a user id to mount a file system, whereas 'nosuid' mount option prevents any users from mounting file systems. As mounting file systems with 'nosuid' can prevent the introduction of rogue set-UID programs or file tampering (when a file system is mounted 'nosuid', then the set-UID bit on executables is ignored), these mount options should be set according to the needs of business.	The following List String value(s) X indicate the current /tmp setting(s) within the /etc/fstab file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
1071	Status of the 'Minimum Password Length' setting	Among the several characteristics that make 'user identification' via password a secure and workable solution is setting a 'minimum password length' requirement. Each character that is added to the password length squares the difficulty of breaking the password via 'brute force,' which attempts using every combination possible within the password symbol set-space, in order to discover a user's password. While no 'minimum length' can be guaranteed secure, eight (8) is commonly considered to be the minimum for most application access, along with requiring other password security factors, such as increasing the size of the symbol set-space by requiring mixed-cases, along with other forms of password variability creation, increases the difficulty of breaking any password by brute-force attack.	The following Integer value X indicates the current value of the PASS_MIN_LEN setting as defined within the /etc/login.defs file.	greater than or equal to 8 OR, any of the selected values below: [ ] Setting not found [ ] File not found
1072	Status of the 'Minimum Password Age' setting	Among the characteristics that make 'user identification' via password a workable security solution is setting a 'minimum password age.' Without this minimum age requirement, any user(s) who wish to re-use the same password can merely cycle through a number of previously used passwords until returning to the preferred one (this is determined by the 'Password History' setting). While no specific 'minimum password age' can guarantee password security, one (1) day is generally considered to be the shortest length of time permissible, along with requiring other password security factors, such as increasing the variability of the symbol set-space by requiring mixed-cases, special characters, further increases the difficulty of breaking any password using brute-force methods. Consider implementing this	The following Integer value X indicates the current PASS_MIN_DAYS setting within the /etc/login.defs file.	greater than or equal to 0 OR, any of the selected values below: [x] Setting not found [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		control for all account passwords in conjunction with CID 1318 (Password History) and CID 1071 (Minimum Password Length) and CID 1073 (Maximum Password Age).		
1073	Status of the 'Maximum Password Age' setting (expiration) / Accounts having the 'password never expires' flag set	One characteristic that makes 'user identification' via password a secure/workable solution is setting a 'password expiration' requirement. Each time a new password is created, replacing one that has been in place for a given period of time, this resets the difficulty of breaking a password via brute-force to its maximum level; it can also help ensures that a compromised 'hack' account with a password that has expired is then closed. While no 'secure maximum' for limiting the use of a password has been agreed upon, ninety (90) days is considered to be the maximum allowed for most enterprise environments. However, this tactic must be used along with other password security factors, such as increasing the complexity the password set-space by requiring mixed-cases and/or special characters, to further increase the difficulty of breaking any password by brute-force attacks.	The following Integer value X indicates the current status of the PASS_MAX_DAYS setting as defined within the /etc/login.defs file.	in 28:30:35:90:91 OR, any of the selected values below: [ ] Setting not found [ ] File not found
2234	Status of the 'MaxAuthTries' setting in the 'sshd_config' file	The 'MaxAuthTries' parameter in the '/etc/ssh/sshd_config' file specifies the maximum number of authentication attempts permitted per connection. As restricting the number of failed authentication attempts before the server terminates the connection can block malicious users from gaining access to the host by using repetitive brute-force login exploits--trying different passwords until one fits a userid--the authentication login limit setting, to disconnect the remote user, forcing reconnect, to limit the speed of brute	The following List Integer value(s) X indicate the current status of the MaxAuthTries setting defined within the /etc/ssh/sshd_config file.	match all less than or equal to 10 OR, any of the selected values below: [x] Setting not found [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		force attacks, this value should be set as appropriate to the needs of the business.		
3221	Current list of groups within '/etc/group' having 'GID=0' set	The /etc/group file is a text-based file which defines the groups to which users belong under Linux and UNIX operating system. In such environments, permissions are typically organized under three classes or categories: Group, User, and Others. By using groups, a Superuser/Administrator can simultaneously add common access levels across multiple user accounts in an organized manner. This can be very useful when assigning access permissions for additional assets such as drives, printers, etc. In the same manner, a Superuser may also utilize it to delegate additional authority to normal users. With such powerful capabilities associated, it is important to perform periodic reviews of the permissions allotted to ensure only appropriate and approved individuals have this level of control over this function. NOTE: The 'root' account should be the only account to have GID-0 set for '/etc/group,' by default.	The following List String value(s) X indicate the current accounts with GID = 0 set in the /etc/group file on the host.	matches regular expression list ^root$ OR, any of the selected values below: [x] Setting not found [x] File not found
4544	Current list of 'user accounts' having no 'home directory' assigned	This check scans the '/etc/passwd' file to determine if any accounts that do not have a Home Directory assigned exist and returns them as output to be used for evaluation. Running this check periodically can help to ensure the User Account Creation processes are effective and operating as expected. User home directories are sometimes targeted for attack to alter or steal personal data using dot "." files in them or weak permissions set on them. In conjunction with this check, select the optional CID's in the QualysGuard Policy Compliance Control Library to determine the state of these conditions on your systems.	The following List String value(s) X indicate the current User Accounts having no Home Directory set on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
5368	Status of the 'KerberosAuthentication' setting in the '/etc/ssh/sshd_config' file	The 'KerberosAuthentication' setting in the '/etc/ssh/sshd_config' file determines whether or not passwords will be authenticated through the Kerberos KDC. As Kerberos authentication is not required unless a KDC is active, this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the KerberosAuthentication setting defined within the /etc/ssh/sshd_config file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
5436	Status of the 'Maximum number of days of inactivity allowed before a user account is locked out' requirement	The 'Maximum number of days of inactivity allowed before a user account is locked out' requirement shows the amount of time that can pass before an inactive account will be locked out. As inactive accounts pose a threat to system security, with the users who haven't logged in failing to notice bogus login attempts or other anomalies, the value should be set according to the needs of the business.	The following Integer value X indicates the current INACTIVE setting in the /etc/default/useradd file. NOTE: Accounts that are inactive for given number of days or more days be disabled.	less than or equal to 60 OR, any of the selected values below: [x] Setting not found [x] File not found
6356	Status of the 'Reserved Accounts GIDs (0-499)' on the host	Reserved accounts are GIDs within (0-499) and are kept available for system accounts and not reserved for user accounts. As system accounts in the GID range (0-499) carry significant risks to the host, these reserved GID settings should be restricted according to the needs of the business.	The following List String value(s) X indicate the current user accounts having 'Reserved GID's' (0-499) as defined within the /etc/passwd file on the host.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found
8770	Status of the '.shosts' files on the host	The '.shosts' file in the users home directory, specifies whether .rhosts/.shosts files are used in authentication. As permitting the use of these files can be a security risk, as they are not authenticated nor unencrypted and usually world-readable, which presents a serious risk against unauthorized users gaining access to the specified host, this value should be set as appropriate to the needs of the business.	The following List String value(s) X indicate the current .shosts file(s) on the host.	matches regular expression list .* OR, any of the selected values below: [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
2241	Status of the 'Banner' setting in the 'sshd_config' file	The contents of the 'Banner' string in the '/etc/ssh/sshd_config' file are sent to the remote user before authentication is allowed. As implementing a logon banner to deter inappropriate use and can provide a foundation for legal action against abuse, this 'warning' content should be set as appropriate to the needs of the business.	The following List String value(s) X indicate the current status of the Banner setting defined within the /etc/ssh/sshd_config file. NOTE: The following Banner requires review and approval.	matches regular expression list /etc/issue OR, any of the selected values below: [ ] Setting not found [x] File not found
8375	Current list of running processes	The 'Current list of running processes' policy setting provides information about currently running processes on the computer. By default, processes are listed in a hierarchical view called the process tree, which shows parent/child relationships between processes. Malicious processes often imitates the names of legitimate processes, which can make them difficult to identify in Task Manager or in process list. While monitoring the processes always make sure the process is legitimate, it is running by an authorized user, description and cpu/memory usage.	The following List String value(s) X indicate the current status of the processes running on the system as reported by the ps command output.	matches regular expression list .*
9336	Status of Auditd service	The 'Auditd' daemon is used to record system events. Capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring. This should be configured according to the needs of the business.	The List String value of X indicates the status of the auditd service using systemd on the host.	matches regular expression list ^(enabled)$ OR, any of the selected values below: [ ] Setting not found
9880	status of service sendmail using systemd	The 'sendmail' electronic mail service is a mail transfer agent (MTA) included with the system. Although used to transfer electronic mail, it is not required to send or receive mail on most hosts; that is done by the IMAP or POP daemon, which run as separate processes. As the Sendmail service is not required unless the host is	The following List String value(s) X indicate the current status of the sendmail service using systemd.	matches regular expression list .* OR, any of the selected values below: [x] Service Not Found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		being used as a primary MTA and this service has a long history of vulnerabilities, this process should be disabled/restricted as appropriate to the needs of the business.		
9884	Status of service vsftpd using systemd	The '[vs]FTP' (very secure file transfer protocol) daemon/service is used for networked file transfer and replaces the prior FTP program. While more secure than a number of other FTP daemons, it too has had vulnerabilities reported, has a complex configuration requirement, and is owned by 'root' (but can be executed even by anonymous users), so it should be disabled/restricted as appropriate to the business' need.	The following List string value of X indicates the status of the vsftpd service on the host using the systemd utility.	does not contain regular expression list .* OR, any of the selected values below: [x] Service Not Found
9892	Status of service named using systemd	The 'Internet Domain Name Server (named)' service, described in RFCs 1034 and 1035, is the most widely deployed Domain Name Server (DNS) service. As this service has several known vulnerabilities which can cause the redirection of end-user traffic to bogus sites or disclose data about internal host addresses, providing target information for malicious users, this daemon should set disabled/restricted as appropriate to the needs of the business. NOTE: This service is not required for system operation, as all networking name-service requests will be [usually] provided by a dedicated server on the network.	The following List string value(s) X indicate the status of the named service using systemd utility on the host.	matches regular expression list disabled OR, any of the selected values below: [x] Service Not Found
9919	Status of service telnet.socket using systemd	'Telnet' is both a 'user command' and a TCP/IP protocol, most commonly used for accessing remote computers via a command line interface (CLI) on tcp port 23. As telnet streams are transmitted in clear text including any uid/password input, when a telnet session is used for privileged communication(s)/host configuration purposes, the entire session is susceptible	The following List String value X indicates the status of the telnet.socket service using systemd on the host.	does not contain regular expression list .* OR, any of the selected values below: [x] Service Not Found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		to interception by eavesdroppers on the network and this can lead to the session being hijacked or replayed by malicious users, this process should be disabled/restricted according to the needs of the business.		
10849	Status of the service tftp.socket using systemd	The 'tftp.socket' service is being used by the Trivial File Transfer Protocol (TFTP) which is a simple file transfer protocol and is used to automatically transfer configuration or boot machines from a boot server. Data transfer using TFTP protocol is unauthenticated hence, it does not ensure the confidentiality and integrity of the data. The service should be configured according to the needs of the business. NOTE : The service is based on systemctl utility for Red hat Enterprise 7, Centos 7 and Oracle enterprise Linux 7.	The following List string value of X indicates the status of the tftp.socket service on the host using systemctl utility.	is contained in regular expression list ^(?!(disabled)).*$ OR, any of the selected values below: [x] Setting not found
1772	Status of the 'icmp_echo_ignore_broadcasts' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.icmp_echo_ignore_broadcasts' setting (in /etc/sysctl.conf) allows the rejection of broadcast ping packets, which can cause broadcast storms: When these broadcast pings are responded to by networked hosts, each host can add to the traffic exponentially. As enabling this setting will set the system to not respond to broadcast pings, such as those used in 'Smurf' attacks, but will allow the hosts to respond to single-source pings, this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the net.ipv4.icmp_echo_ignore_broadcasts parameters set within /etc/sysctl.conf file.	matches regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
2741	Status of the password history setting (remember)	In order to enforce password history, the 'remember' option must be defined in the 'pam.unix.so' configuration line of the '/etc/pam.d/system-auth' file. In addition, the '/etc/security/opasswd' file must exist for the purpose of storing user's old passwords. If password history standards are not	The following Integer value X indicates the current password history (remember) setting within the pam_unix.so configuration line of the /etc/pam.d/system-auth file.	greater than or equal to 6 OR, any of the selected values below:

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		enforced, a malicious user could potentially obtain a password through Social Engineering or brute-force attacks. This could lead to the compromise of sensitive information or denial of service conditions.		[ ] Setting not found [ ] File not found
7973	Status of the 'open' system call in the '/etc/audit/audit.rules' file on the host	The 'open' system call controls opening of files on the host. If a non-privileged users, non-daemon event, or permission is denied while attempting to open a file on the host, an audit record is written. These 'open' audit records are reported to a repository for review and investigation. As the 'open' system call is part of the Audit subsystem and is legal evidence of chronological activity on the host, the configuration of this system call should be done according to the needs of the business.	The following List String value(s) X indicate the current status of the open system calls within the /etc/audit/audit.rules file on the host.	matches regular expression list open\s OR, any of the selected values below: [x] Setting not found [x] File not found
7974	Status of the 'openat' system call in the '/etc/audit/audit.rules' file on the host	The 'openat' system call controls opening of files on the host. If a non-privileged users, non-daemon event, or permission is denied while attempting to open a file on the host, an audit record is written. These 'openat' audit records are reported to a repository for review and investigation. As the 'openat' system call is part of the Audit subsystem and is legal evidence of chronological activity on the host, the configuration of this system call should be done according to the needs of the business.	The following List String value(s) X indicate the current status of the openat system calls within the /etc/audit/audit.rules file on the host.	matches regular expression list openat.* OR, any of the selected values below: [x] Setting not found [x] File not found
100558	Status of the 'suid' files and programs on the host (CID 8325 Alternative)	The 'suid' setting on files and programs on the host allows these to be run with higher privileges than originally set. As allowing files to be run with elevated privileges can allow abuse by unauthorized users, these settings should be restricted according to the needs of the business. NOTE: This check should be regularly scheduled/reviewed to locate and SUID files that have been installed on the host.	The following List String value(s) X indicate the current suid files and programs on the host.NOTE: The 'suid' files and programs should be reviewed and approved on a regular basis, according to the CIS Benchmark.	contains regular expression list .*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
100559	Status of the 'sgid' files and programs on the host (CID 8326 Alternative)	The SGID setting on files and programs on the host allows these to be run with the higher privileges of the group than that of the logged in user. As allowing files to be run with elevated privileges based on a different group can allow abuse by unauthorized users, these settings should be restricted according to the needs of the business. NOTE: This check should be regularly scheduled/reviewed to locate and SGID files that have been installed on the host.	The following List String value(s) X indicate the current sgid files, ownership, permissions, and programs, to a maxdepth=3, on the host.NOTE: The 'sgid' files and programs should be reviewed and approved on a regular basis, according to the CIS Benchmark.	contains regular expression list .*
5382	Status of the 'UsePrivilegeSeparation' setting in the '/etc/ssh/sshd_config' file	'UsePrivilegeSeparation' is a setting within the '/etc/ssh/sshd_config' file. Until properly authenticated, the 'UsePrivilegeSeparation=yes' setting creates a child process with no privileges for incoming traffic requests. After authentication, a new process is created with privileges of the authenticated user. An additional setting is available 'UsePrivilegeSeparation=sandbox' providing more restrictions for unprivileged processes. As privilege escalation attacks are common strategies deployed by unauthorized users, this setting should be configured according to the needs of the business. NOTE: The default setting is 'yes'	The following List String value(s) X indicate the current status of the UsePrivilegeSeparation setting defined within the /etc/ssh/sshd_config file.	is contained in regular expression list .* OR, any of the selected values below: [x] Setting not found [x] File not found
1773	Status of the 'tcp_max_syn_backlog' setting within the '/etc/sysctl.conf' file	The 'net.ipv4.tcp_max_syn_backlog' network parameter (/etc/sysctl.conf) specifies the maximum number of incomplete TCP connection requests concurrently held in memory. If the number is too small the host can be overwhelmed by a DoS 'SYN flood' attack, so this value should be set as appropriate to the needs of the business.	The following Integer value X indicates the current status of the tcp_max_syn_backlog setting as defined within the /etc/sysctl.conf file.	greater than or equal to 128 OR, any of the selected values below: [ ] Setting not found
2278	Status of the 'HostBasedAuthenticati	The 'HostBasedAuthentication' in '/etc/ssh/sshd_config' specifies whether or not the 'rhosts' or '/etc/hosts.equiv'	The following List String value(s) X indicate the current status of the HostbasedAuthentication	matches regular expression list [nN][oO]

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	on' setting in '/etc/ssh/sshd_config'	authentication, together with successful public key client host authentication, is allowed. As the industry standard is not to use this authentication type, since the '~/.rhosts' and '/etc/hosts.equiv' files bypass the standard password-based user authentication mechanism, specifying remote hosts and users that are allowed access to the local system without supplying a password, this value should be set as appropriate to the needs of the business.	setting defined within the /etc/ssh/sshd_config file.	OR, any of the selected values below: [x] Setting not found [x] File not found
4772	Status of the 'Permissions' settings for the '/etc/at.allow' file	The 'at' command takes the name(s) of commands from standard input and permits the user to specify the time that the commands should be run 'at' and operates with system-level privileges. As the capability to run 'at' commands would be permitted by membership in the 'at.allow' and/or 'crontab.allow' file lists, this could allow the malicious scheduling of a job that would overwrite any system or user file, so the capability to modify either of these files should be restricted appropriately to prevent data and/or system damage or host process subversion.	The following List String value(s) X indicate the current Ownership and Permissions defined for the /etc/at.allow file on the host.	matches regular expression list (root):.*:[-r][-w][-][-][-][-][-][-][.+]*:/etc/at.allow OR, any of the selected values below: [x] File not found
5057	Permissions set for the '/etc/cron.allow' file	The '/etc/cron.allow' contains a list of users who are allowed to run the crontab utility, to submit jobs to be run at scheduled intervals, which are run with root-level privileges. As on most systems, only the root group [root] and user [root] would need the ability to schedule jobs, file access should be restricted according to the needs of the business.	The following List String value(s) X indicate the current Ownership and Permissions for the /etc/cron.allow file on the host.	matches regular expression list (root):.*:[-r][-w][-][-][-][-][-][-][.+]*:/etc/cron\.allow OR, any of the selected values below: [x] File not found
9340	Permissions set on the file /boot/grub2/grub.cfg	The file /boot/grub2/grub.cfg is a main configuration file for making changes on the bootloader(GRUB) menu. The file can not be modified manually, changes to be made	This List String value X indicates the Permissions and ownerships set for the /boot/grub2/grub.cfg file on the host.	matches regular expression list (root):.*:[-r][-w][-x][-r][-][-][-r][-][-][.+]*:/boot/grub2/grub.cfg

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		through the grub2-mkconfig utility. If the file grub.cfg is modified manually using vi or vim, grub will be corrupted. Hence, permissions/ownership to the file /boot/grub2/grub.cfg should be restricted in order to prevent non-root/unauthorized users from changing the file. It should be configured according to the needs of the business.		OR, any of the selected values below: [x] File not Found
9878	Status of service smb using systemd	The 'samba' daemon provides ability to configure linux systems to share file systems and directories with windows desktops. It will advertise the files systems and directories through SMB protocol. Using samba windows users will be able to mount these files and directories on their own systems. This ability may allow malicious users to have access to file system and directories and can compromise the system. This should be configured according to the needs of the business.	The following List string value of X indicates the status of the smb service using systemd utility on the host.	matches regular expression list ^(disabled)$ OR, any of the selected values below: [x] Service Not Found
9882	Status of service snmpd using systemd	The Simple Network Management Protocol (SNMP) daemon can be set to generate and/or receive a great deal of sensitive information (traps) about the internal/networking operations for any number of networked hosts. While it does have basic access controls in place, the information is not encrypted while in transit or at rest and can potentially be read by anyone with a network sniffer or file access. Coupled with the facts that it is only required for monitoring remote hosts via the network, this process should be disabled/restricted according to the needs of the business.	The following List string value of X indicates the status of the snmpd service using systemd utility on the host.	matches regular expression list ^(enabled)$ OR, any of the selected values below: [ ] Service Not Found
12602	Status of the /etc/pam.d/sshd file contents	The /etc/pam.d/sshd file contains PAM Configuration for 'sshd' for authenticating users who connects to the host from remote systems via Secure Shell (SSH). While it	The following List String value(s) of X indicate the status of the 'sshd' service PAM configurations within the /etc/pam.d/sshd file.	matches regular expression list .*

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		can be convenient for remote administration, remote access has associated inherent risks, such as weaker protection, connections from hostile environments and communications over untrusted networks. Limiting privileges and restricting access to change information system components and system-related information is most important for production server security. To prevent any unauthorized access, misuse or tampering, remote access should be restricted/limited as appropriate to the needs of the business.		OR, any of the selected values below: [x] Setting not found [x] File not found
13583	Status of the 'minlen' option within the 'pam_cracklib.so' , 'pam_pwquality' PAM module and /etc/login.defs	Strong passwords protect systems from being hacked through brute force methods. Long password are harder to crack. Password policy configured with PAM modules will take precedence over /etc/login.defs. This setting should be configured according to the business needs and organization's security policies.	The following Integer value X indicates the current value of the PASS_MIN_LEN setting as defined within the /etc/login.defs file.	greater than or equal to 8 OR, any of the selected values below: [ ] Setting not found [ ] File not found OR matches regular expression list ([8-9]|[1-9][0-9]) OR, any of the selected values below: [ ] Setting Not Found [ ] File Not Found
14112	Status of the services installed on the Linux/UNIX host	Non-essential services are a potential point of attack. Disabling such services will reduce the attack surface of the system. Therefore, non-essential services should be	The following List String value(s) of X indicate the status of the systemd services installed on the Linux/UNIX host i.e. whether the	does not contain regular expression list ^(chargen(-stream|-

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	(stopped, running, failed, dead, ...)	disabled or removed from the environment. Review and verify that all the services are in line with the business needs and the organization's security policies.	service is stopped, running, exited, dead, etc.	dgram)?)(\.service|\.socket)?|:|running ^(comsat)(\.service|\.socket)?|:|running ^(daytime(-stream|-dgram)?)(\.service|\.socket)?|:|running ^(discard(-stream|-dgram)?)(\.service|\.socket)?|:|running ^(dovecot)(\.service|\.socket)?|:|running ^(dtspc)(\.service|\.socket)?|:|running ^(echo(-stream|-dgram)?)(\.service|\.socket)?|:|running ^(finger)(\.service|\.socket)?|:|running ^(imap)(\.service|\.socket)?|:|running ^(instsrv)(\.service|\.socket)?|:|running ^(login)(\.service|\.socket)?|:|running ^(netstat)(\.service|\.socket)?|:|running ^(pcnfsd)(\.service|\.socket)?|:|ru

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
				nning ^(pop3)(\.service|\.socket)?|:|running ^(routed)(\.service|\.socket)?|:|running ^(rstatd)(\.service|\.socket)?|:|running ^(rusersd)(\.service|\.socket)?|:|running ^(rwhod)(\.service|\.socket)?|:|running ^(smbd)(\.service)?|:|running (ttdbserver)(\.service|\.socket)?|:|running ^(uucp)(\.service|\.socket)?|:|running OR, any of the selected values below: [x] Services not found
100457	Status of the 'daemon' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the submission of jobs that contain destructive commands. As the crontab jobs run with	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match daemon

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.		
100458	Status of the 'bin' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match bin
100459	Status of the 'smtp' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match smtp

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.		
100460	Status of the 'nuucp' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match nuucp
100461	Status of the 'listen' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match listen

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
100463	Status of the 'noaccess' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match noaccess
100482	Status of the 'daemon' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match daemon
100483	Status of the 'bin' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match bin

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.		
100484	Status of the 'smtp' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match smtp
100485	Status of the 'nuucp' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match nuucp

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.		
100486	Status of the 'listen' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match listen
100487	Status of the 'nobody' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match nobody

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
100488	Status of the 'noaccess' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match any regular expression match noaccess
101270	Status of the 'sync' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match sync
101271	Status of the 'halt' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow'	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match halt

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.		
101272	Status of the 'shutdown' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match shutdown
101273	Status of the 'news' user defined within the '/etc/cron.deny' file (CID 5428 Alternative for Linux)	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be allowed to run the crontab/at jobs, which could allow the	The following List String value(s) X indicate the current inventory of users defined within the /etc/cron.deny file.	match all regular expression match news

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, the 'cron.deny' file creation should be decided in accordance to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.		
101274	Status of the 'sync' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match sync
101275	Status of the 'haltn' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match halt

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.		
101276	Status of the 'shutdown' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match shutdown
101277	Status of the 'news' user defined within the '/etc/at.deny' file (CID 5426 Alternative for Linux)	The 'at.deny' file is used to restrict the use of the 'at' job-scheduling privilege. If an 'at.deny' file exists but does not include a list of all the users who should be denied 'at' privileges (when a comparable 'at.allow' file hasn't been created that permits specific users), any user on the host omitted in 'at.deny' will be allowed to run the at jobs, which could allow the submission of jobs that contain destructive commands. As the 'at' jobs run with root-level privileges, the 'at.deny' file creation should be used in accordance to the needs of the business. WARNING: If the 'at.allow' file does not exist and the 'at.deny' file does exist, all users NOT in the 'at.deny' file can use 'at' by default.	The following List String value(s) X indicate the current contents of the /etc/at.deny file on the host.	match all regular expression match news
101290	Permission setting for AWS CLI Credentials file (~/.aws/credentials)	The AWS Command Line Interface (AWS CLI) is an open source tool that enables you to interact with AWS services using	The following list of path of ~/.aws/credentials have the permission setting which allows	is contained in regular expression list

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		commands with your AWS Account in your command-line shell. ~/.aws/credentials file contains user's AWS Access Key ID and AWS Secret Access Key.	"Group" or "Other" user access to the setting file.	^(File not found|No data found)$
101380	Permission setting for AWS Cache directory (~/.aws/cli/cache)	The AWS Command Line Interface (AWS CLI) is an open source tool that enables you to interact with AWS services using commands with your AWS Account in your command-line shell. ~/.aws/clis/cache directory contains data which may contain user's secret information	The following list of path of ~/.aws/cli/cache have the permission setting which allows "Group" or "Other" user access to the setting file.	contains regular expression list ^(File not found|No data found)$
101392	Permissions set for the '/etc/login.defs' file (CID 2261 Alternative)	The '/etc/login.defs' file is responsible for defining site-specific configuration requirements within the shadow login suite: According to the manufacturer, the existence of this file is mandatory. (System operations will not be prevented without it, but, the host may not operate as expected should the file not exist.) As permitting unrestricted access to the '/etc/login.defs' file could permit a malicious user to potentially alter system files, allowing privilege escalation exploits to be conducted on the shadow login suite, the permissions should be set as appropriate to the needs of the business.	The following String value(s) X indicate the current Ownership and Permissions setting for the /etc/login.defs file on the host.	regular expression match (root):.*:-[-r][-w][-x][-r]-[-x][-r]-[-x][.+]*:/etc/login.defs
101393	Permissions set for the '/etc/profile' file (CID 2268 Alternative)	The '/etc/profile' file contains system-wide environment variables such as the file creation mask (UMASK) and terminal types. Upon login, the system references the parameters defined in the '/etc/profile' file to set the user environment. As the '/etc/profile' contains powerful commands and variables that govern user environment security settings, permissions set for the '/etc/profile' file should be restricted as appropriate to the needs of the business.	This String value X indicates the current Ownership and Permissions set for the /etc/profile file.	regular expression match (root):.*:-[-r][-w][-x][-r][-][-][-][-r][-][-][.]*:/etc/profile
101399	Permissions set for the '/etc/ssh/ssh_host_rsa_key' file	SSH is the standard encrypted communications software used on Prudential's Unix servers. The access	The following String value(s) X indicate the files of the /etc/ssh*/*key file(s) with violation	regular expression match ^(root):(root|ssh_keys):[-][-r][-

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		permission for SSH private key must be restricted.	for the owner (root:root or root:ssh_keys) or for the permission (rw-r-----) on the host.	w][-][- r][-][-][-][-][-][.+]*:/etc/ssh/.*key$ OR, any of the selected values below: [x] Set status Passed for "item not found" error(item not found:2)
101400	Permissions set for the '/etc/ssh/ssh_host_dsa_key' file	SSH is the standard encrypted communications software used on Prudential's Unix servers. The access permission for SSH private key must be restricted.	The following String value(s) X indicate the files of the /etc/ssh*/*key file(s) with violation for the owner (root:root or root:ssh_keys) or for the permission (rw-r-----) on the host.	regular expression match ^(root):(root|ssh_keys):[-][-r][- w][-][- r][-][-][-][-][-][.+]*:/etc/ssh/.*key$ OR, any of the selected values below: [x] Set status Passed for "item not found" error(item not found:2)
101401	Permissions set for the '/etc/ssh/ssh_host_ecdsa_key' file	SSH is the standard encrypted communications software used on Prudential's Unix servers. The access permission for SSH private key must be restricted.	The following String value(s) X indicate the files of the /etc/ssh*/*key file(s) with violation for the owner (root:root or root:ssh_keys) or for the permission (rw-r-----) on the host.	regular expression match ^(root):(root|ssh_keys):[-][-r][- w][-][- r][-][-][-][-][-][.+]*:/etc/ssh/.*key$ OR, any of the selected values below: [x] Set status Passed for "item not found" error(item not found:2)
101402	Permissions set for the '/etc/ssh/ssh_host_ed25519_key' file	SSH is the standard encrypted communications software used on Prudential's Unix servers. The access permission for SSH private key must be restricted.	The following String value(s) X indicate the files of the /etc/ssh*/*key file(s) with violation for the owner (root:root or root:ssh_keys) or for the permission (rw-r-----) on the host.	regular expression match ^(root):(root|ssh_keys):[-][-r][- w][-][- r][-][-][-][-][-][.+]*:/etc/ssh/.*key$ OR, any of the selected values below:

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
				[x] Set status Passed for "item not found" error(item not found:2)
101403	Permissions set for the '/etc/ssh/random_seed' file	SSH is the standard encrypted communications software used on Prudential's Unix servers. The access permission for random_seed must be restricted.	The following String value(s) X indicate the files of the /etc/ssh/random_seed file with violation for the owner (root:root or root:ssh_keys) or for the permission (rw-r-----) on the host.	regular expression match ^(root):(root|ssh_keys):[-][-r][-w][-][-r][-][-][-][-][-][.+]*:/etc/ssh/random_seed$ OR, any of the selected values below: [x] Set status Passed for "item not found" error(item not found:2)
101404	Permissions set for the '/etc/ssh/moduli' file	SSH is the standard encrypted communications software used on Prudential's Unix servers. The access permission for moduli must be restricted.	The following String value(s) X indicate the files of the /etc/ssh/moduli file with violation for the owner (root:root or root:ssh_keys) or for the permission (rw-r-----) on the host.	regular expression match ^(root):(root|ssh_keys):[-][-r][-w][-][-r][-][-][-][.+]*:/etc/ssh/moduli$ OR, any of the selected values below: [x] Set status Passed for "item not found" error(item not found:2)
1867	Status of the 'time-stream' service	The 'time-stream' service is used to provide networked systems machine level time and date information via port 37. This can be run over TCP or UDP connections and this is distinguished via the 'stream' (for TCP) and 'dgram' (for UDP) options. As the manipulation of the host's 'time-tracking' capability is one of the many ways to expose a vulnerability, this service should be disabled/restricted as appropriate to the needs of the business.	The following Integer value of X indicates the status of the time-stream as a Xinetd service on the host. A value of 1 indicates the service is Enabled; a value of 0 indicates the service is Disabled.	Any of the selected values below: [x] Disabled(0) [ ] Enabled(1) [x] Xinetd is disabled [x] Service not found
1159	List of accounts having 'root-level' privileges (UID=0)	Allowing multiple root-level accounts (UID=0) increases the risk of serious harm to the system, as root-level commands can override all normal file system restrictions	The following List String value(s) X indicate the current users with a UID equal to '0' on the host. NOTE: The following list requires	matches regular expression list ^root$

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		and other security measures. As users should not have system-level access privileges that are not required for their job functions, nor should direct root login be allowed if commands such as 'sudo' can be substituted, allowing multiple 'UID=0' accounts, should be restricted/set according to the needs of the business.	review and approval and any unauthorized user accounts with a UID equal to '0' should be immediately documented, removed, and reported.	OR, any of the selected values below: [x] No accounts found
2602	Permissions set for the '/etc' directory	The '/etc' folder contains the host specific configuration files. There are several known vulnerabilities associated with multiple objects contained within the '/etc' folder. An example of these is the iSCSI Enterprise Target exploit that carries the potential for a malicious user to obtain sensitive and/or confidential information. This weakness basically stems from the install script's ability to apply 'world readable' permissions to the '/etc/inetd.conf' file that can be used to access passwords and usernames.	The following List String value(s) X indicate the current Ownership and Permissions set for the /etc directory on the host.	matches regular expression list root:root:[-r][-w][-x][-r][-][-x][-r][-][-x][.+]*:/etc OR, any of the selected values below: [ ] Directory not found
2617	Permissions set for the '/usr/sbin' directory	The '/usr/sbin' folder has several non-vital utilities that Systems Administrators use after the boot process has completed. Some of these utilities include 'chroot,' 'groupadd,' 'kppp,' 'userdel' and 'adduser.' Due to the obvious power of some of these utilities, it is suggested that only appropriate and approved individuals have access to this folder. Another course of 'best practice' is to perform periodic checks against the permissions assigned to this folder to ensure compliance with security policy.	The following List String value(s) X indicate the current Ownership and Permissions of the /usr/sbin directory.	matches regular expression list root:root:[-r][-][-x][-r][-][-x][-r][-][-x][.+]*:/usr/sbin OR, any of the selected values below: [ ] Directory not found
2624	Permissions set for the '/usr/bin' directory	The /usr/bin directory typically exists on Unix and Linus systems containing executables such as used in the boot process. Among the thousands of executable files within /usr/bin, some very powerful and, thus, dangerous, files exist such as telnet and sudo. Consider	The following List String value(s) X indicate the current Ownership and Permissions set for the /usr/bin directory on the host.	matches regular expression list root:root:[-r][-w][-xs][-r][-][-xs][-r][-][-x][.+]*:/usr/bin OR, any of the selected values below:

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		implementing this check to perform periodic reviews of the permissions assigned to ensure only appropriate and approved access is allowed. This can also be used as evidentiary support for audit purposes.		[ ] Directory not found
5251	Status of the SNMP 'rocommunity' community string	The SNMP community strings are commonly used by malicious users to gain access to systems without being approved or assigned such authority by administrators. This is easily done by knowing the default community strings and checking to see if they have been changed from the defaults. This check can be run periodically to ensure that unique strings have replaced the default to protect sensitive systems and data using SNMP for monitoring.	The following List String value(s) X indicate the current status of the SNMP service having public access via rocommunity, rwcommunity, trapcommunity, or com2sec settings defined within the /etc/snmp/snmpd.conf file.	does not contain regular expression list ^(rocommunity)[\s\t]+(public)[\s\t]+((?!(127.0.0.1|localhost)).*)$ OR, any of the selected values below: [x] Setting not found [ ] File not found
5252	Status of the SNMP 'rwcommunity' community string	The SNMP community strings are commonly used by malicious users to gain access to systems without being approved or assigned such authority by administrators. This is easily done by knowing the default community strings and checking to see if they have been changed from the defaults. This check can be run periodically to ensure that unique strings have replaced the default to protect sensitive systems and data using SNMP for monitoring.	The following List String value(s) X indicate the current status of the SNMP service having public access via rocommunity, rwcommunity, trapcommunity, or com2sec settings defined within the /etc/snmp/snmpd.conf file.	is contained in regular expression list 161803399999999 ^(rocommunity[\s\t]+public[\s\t]+(127.0.0.1|localhost))$ OR, any of the selected values below: [x] Setting not found [ ] File not found
5254	Status of the 'time-dgram' service	The 'time-dgram' service is an old protocol that supports synchronized time across a network. This is done using UDP by the client sending an empty datagram to port 37 and the server returning a datagram of length 4 with the time represented in 32-bit binary format. As with TCP based TIME protocol, for UDP there is no connection to build and breakdown. For the most part,	The following Integer value of X indicates the status of the time-dgram as a Xinetd service on the host. A value of 1 indicates the service is Enabled; a value of 0 indicates the service is Disabled.	Any of the selected values below: [x] Disabled(0) [ ] Enabled(1) [x] Xinetd is disabled [x] Service not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		this is an obsolete method that has since been replaced with the Network Time Protocol (NTP). It is recommended to disable this service to reduce all potential attack vectors.		
5365	Status of the 'ChallengeResponseAuthentication' setting in the '/etc/ssh/sshd_config' file	The 'ChallengeResponseAuthentication' setting in the '/etc/ssh/sshd_config' file determines whether or not challenge-response authentication is allowed. As this form of authentication can increase the security of the login process, this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the ChallengeResponseAuthentication setting defined within the /etc/ssh/sshd_config file.	matches regular expression list [yY][eE][sS] OR, any of the selected values below: [ ] Setting not found [x] File not found
5218	Status of the 'AuthorizedKeysFile' setting in the 'sshd_config' file	The 'AuthorizedKeysFile' setting specifies the file where the public keys available for authenticating users for SSH connections to the host will be stored. Key management plays a critical role in access control for critical devices which is not only important, it is required by law for some organizations depending on the type of data residing on them. This check can be run periodically to determine if the key file listed are appropriate and approved as a malicious user could make changes to accommodate continuous access. As with all critical devices, access to them should be tightly managed and maintained to meet the needs of the business.	The following List String value(s) X indicate the current status of the AuthorizedKeysFile setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^[a-zA-Z\./%]*(authorized_keys)$ OR, any of the selected values below: [ ] Setting not found [x] File not found
5796	Permissions set for the '/etc/cron.deny' file	The 'cron.deny' file is used to restrict the use of the crontab privilege. If a 'cron.deny' file exists but does not include a list of all the users who should be denied cron privileges (when a comparable 'cron.allow' file hasn't been created that permits specific users), any user on the host omitted in 'cron.deny' will be ALLOWED to run the crontab/at jobs, which could allow the	The following List String value(s) X indicate the current Ownership and Permissions settings for the /etc/cron.deny file on the host.	is contained in regular expression list (root):.*:[-r][-w][-x][-][-][-][-][-][-][.+]*:/etc/cron\.deny (root):(root):[-r][-w][-x][-r][-w][-x][-r][-][-][.+]*:/etc/cron\.deny

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		submission of jobs that contain destructive commands. As the crontab jobs run with root-level privileges, permissions for the 'cron.deny' file should be configured according to the needs of the business. WARNING: If the 'cron.allow' file does not exist and the 'cron.deny' file does exist, ALL USERS not in the 'cron.deny' file can use 'cron' BY DEFAULT.		OR, any of the selected values below: [ ] File not found
7415	Status of the 'daytime-dgram' service	The 'daytime-dgram' is a network service that retrieves the hosts current date and time. As there are several known DoS exploits for 'daytime-dgram', it should be configured according to the needs of the business. NOTE: CIS recommends disabling the 'daytime-dgram' service.	The following Integer value of X indicates the status of the 'daytime-dgram' service on the host.	Any of the selected values below: [x] Disabled(0) [ ] Enabled(1) [x] Xinetd is disabled [x] Service not found
7416	Status of the 'daytime-stream' service	The 'daytime-stream' network service retrieves the hosts' current date and time. As there are several DoS exploits of the 'daytime-stream' service, it should be configured according to the needs of the business. NOTE: CIS recommends disabling the daytime-stream service.	The following Integer value of X indicates the status of the 'daytime-stream' service on the host.	Any of the selected values below: [x] Disabled(0) [ ] Enabled(1) [x] Xinetd is disabled [x] Service not found
7437	Status of the 'chargen-dgram' service	The 'chargen-dgram' network service is used for testing and debugging systems. The 'chargen-dgram' service receives datagrams and provides an ASCII character from 0 to 512 in response. As there are several known remote attacks associated with this service, it should be configured according to the needs of the business. NOTE: The CIS Benchmark recommends disabling this service.	The following Integer value of X indicates the status of the 'chargen-dgram' service on the host.	Any of the selected values below: [x] Disabled(0) [ ] Enabled(1) [x] Xinetd is disabled [x] Service not found
7438	Status of the 'chargen-stream' service	The 'chargen-stream' network service is used for testing and debugging systems. The 'chargen-stream' service receives	The following Integer value of X indicates the status of the	Any of the selected values below: [x] Disabled(0)

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		connections and provides an ASCII character from 0 to 512 in response. As there are several known remote attacks associated with this service, it should be configured according to the needs of the business. NOTE: The CIS Benchmark recommends disabling this service.	'chargen-stream' service on the host.	[ ] Enabled(1) [x] Xinetd is disabled [x] Service not found
9181	Permissions set for the '/usr/lib' directory	The "/usr/lib/" directory contains dynamic libraries and support static files for the executables at /usr/bin and /usr/sbin. It may also contain helper files, or dynamic libraries that will be accessed only by the required application hosted on the machine, without user intervention. It can be used as a container for plugins and extensions. Permissions of this directory/files to unauthorized owner/users provides the potential to access sensitive information or change the system configuration which could compromise the system's security. It should be configured according to the needs of the business.	The following List string value of X indicates the status of the Permissions and Ownership set for the /usr/lib directory on the host.	matches regular expression list root:root:[-r][-w][-xs][-r]-[-xs][-r]-[-x][.+]*:/usr/lib OR, any of the selected values below: [ ] Directory not found
9182	Permissions set for the /usr/lib files	The "/usr/lib/" directory contains dynamic libraries and support static files for the executables at /usr/bin and /usr/sbin. It may also contain helper files, or dynamic libraries that will be accessed only by the required application hosted on the machine, without user intervention. It can be used as a container for plugins and extensions. Access to this files should be restricted as appropriate to the needs of the business.	The following List string value of X indicates the status of Ownership and Permissions set for the files within /usr/lib directory on the host.	matches regular expression list .*:.*:[-r][-w][-xs][-r]-[-xs][-r]-[-x][.+]*:/usr/lib/.* OR, any of the selected values below: [x] Directory not found
9335	Status of the rsyslog service	The 'rsyslog' service provides important security features such as encryption of log data, connection-oriented log transmission, and database format logging. If the rsyslog service is not activated the system will not have a syslog service running. As there are several remote log exploits, the 'rsyslog'	The List String value of X indicates the status of the rsyslog service using systemd on the host.	matches regular expression list ^(enabled)$ OR, any of the selected values below: [ ] Service not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		service should be activated according to the needs of the business.		
9887	Status of the 'dovecot' service using systemd	The 'dovecot' service is an open-source IMAP and POP3 server for Linux/UNIX-like systems and supports IMAP4rev1, POP3, IPv6, SSL and TLS. As this has been shown to have a vulnerability caused by a password error, which can be exploited via a specially crafted password containing TABs, if the host is not being used as a mail server, this service should be disabled/restricted in accordance with the needs of the business.	The following List String value(s) X indicate the current status of the dovecot service using systemd utility on the host.	does not contain regular expression list ^(enabled)$ OR, any of the selected values below: [x] Service Not Found
9896	Status of service sysstat using systemd	The 'sysstat' service, and its utilities, are used for system logging/monitoring functions. These log entries and monitoring utilities can be used for troubleshooting system performance issues as well as forensic investigations related to security incidents. In addition, 'sysstat' can be used for report generation around performance metrics as they are correlated over a period of time. This check can be used to ensure the 'sysstat' service is set to run by default as a monitoring measure that compliance with the requirements and needs of the business.	The List string value of X indicates the status of the service sysstat using systemd utility on the host.	matches regular expression list .* OR, any of the selected values below: [x] Service Not Found
101426	Status of the '-nolisten tcp' setting (CID 1745 Alternative for RHEL 8 / OL 8)	Ordinary X Windows uses insecure authentication, so a malicious user that gains unauthorized access can easily compromise the host. Using the '-nolisten tcp' requirement in the 'gdm.conf file' forces the X server to ignore port 6000/tcp by default. As this should prevent remote X clients from sending a window to the local host too, while still allowing the forwarding of an X window via Secure Shell, access to the file along with the other setting should be set according to the needs of the business.	This String value X indicates the current status of the DisallowTCP setting defined within the /etc/X11/gdm/gdm.conf file.	match all regular expression match (DisallowTCP=true)|(Setting not found|File not found)|161803399999999|314159265358979 OR, any of the selected values below: [x] Set status Passed for "item not found" error(item not found:2)

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
10663	Status of the 'server' setting within '/etc/chrony.conf' file	The 'chrony' is a daemon which implements the Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. It is designed to perform well in a wide range of conditions, including intermittent network connections, heavily congested networks, changing temperatures and systems that do not run continuously, or run on a virtual machine. This setting should be configured according to the needs of the business.	The following List String value(s) X indicate the status of serversetting within /etc/chrony.conf file on the host.	matches regular expression list .+ OR, any of the selected values below: [x] Setting not found [x] File not found
11335	Status of the chronyd process	The 'chrony' is a daemon which implements the Network Time Protocol (NTP), which is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. It is also designed to perform well in a wide range of conditions, including intermittent network connections, heavily congested networks, changing temperatures and systems that do not run continuously, or run on a virtual machine. This setting should be configured according to the needs of the business.	The following List String value of x indicates current status of chronyd process using ps command on the host.	matches regular expression list ^chrony.+ OR, any of the selected values below: [ ] Setting not found
13138	Status of the 'pool' setting in '/etc/chrony.conf'	The 'pool' setting specifies a pool of NTP servers responsible for the accurate system clock synchronization. The 'chrony' is a daemon which implements the Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. It is designed to perform well in a wide range of conditions, including intermittent network connections, heavily congested networks, changing temperatures and systems that do not run continuously or run on a virtual machine. This setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the 'pool' setting within the /etc/chrony.conf file.	is contained in regular expression list ^(ntppool-(paehow|p1ehow|p2ehow|mnncpo).prudential.com) OR, any of the selected values below: [ ] Setting not found [ ] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
11634	Status of 'lock-enabled' setting in /etc/dconf/db/.*.d/00-screensaver file	The 'lock-enabled' setting is responsible to lock the screen when the screensaver goes active. A session lock or screensaver is a temporary action taken when the user is not physically present on the system, but does not want the system to log out, user re-establishes access using established identification and authentication procedures. To prevent the system from being compromised when the user is not around, this setting should be configured properly.	The following List String value(s) of X indicate the status of 'lock-enabled' setting defined in '/etc/dconf/db/.*.d/00-screensaver' file. Note: The database name is arbitrary, and is defined by the user in 'Profile' within '/etc/dconf/profile', which is the list of databases that dconf consults to find the value for key.	matches regular expression list true OR, any of the selected values below: [ ] Setting Not Found [x] File Not Found
11635	Status of 'idle-delay' time setting in /etc/dconf/db/.*.d/* file	The setting 'idle-delay' specifies the number of seconds before the session is considered idle. A session lock or screensaver is a temporary action taken when the user is not physically present on the system, but does not want the system to log out. In order to prevent the system from being compromised, it is important that the operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. This setting should be configured according to the needs of business.	The following List String value(s) of X indicate the status of 'idle-delay' setting defined in '/etc/dconf/db/.*.d/*' file. Note: The database name is arbitrary, and is defined by the user in 'Profile' within '/etc/dconf/profile', which is the list of databases that dconf consults to find the value for key.	matches regular expression list uint32 [1-9][0-9][0-9]? OR, any of the selected values below: [ ] Setting Not Found [x] Directory Not Found
11636	Status of 'idle-delay' setting in /etc/dconf/db/.*.d/locks/*	The setting 'idle-delay' specifies the number of seconds before the session is considered idle. A session lock or screensaver is a temporary action taken when the user is not physically present on the system, but does not want the system to log out. In order to prevent the system from being compromised, it is important that the operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. This setting should be configured according to the needs of business.	The following List String value(s) of X indicate the status of 'idle-delay' setting defined in '/etc/dconf/db/.*.d/locks/*' directory on the host. Note: The database name is arbitrary, and is defined by the user in 'Profile' within '/etc/dconf/profile', which is the list of databases that dconf consults to find the value for key.	matches regular expression list /org/gnome/desktop/session/idle-delay OR, any of the selected values below: [ ] Setting Not Found [x] Directory Not Found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
11637	Status of 'lock-delay' setting in /etc/dconf/db/.*.d/locks/*	The setting 'lock-delay' specifies the number of seconds after screensaver activation before locking the screen. A session lock or screensaver is a temporary action taken when the user is not physically present on the system, but does not want the system to log out. In order to prevent the system from being compromised, it is important that the operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. This setting should be configured according to the needs of business.	The following List String value(s) of X indicate the status of 'lock-delay' setting defined in '/etc/dconf/db/.*.d/locks/*' directory on the host. Note: The database name is arbitrary, and is defined by the user in 'Profile' within '/etc/dconf/profile', which is the list of databases that dconf consults to find the value for key.	matches regular expression list /org/gnome/desktop/screensaver/lock-delay OR, any of the selected values below: [ ] Setting Not Found [x] Directory Not Found
11638	Status of 'lock-delay' time setting in /etc/dconf/db/.*.d/*	The setting 'lock-delay' specifies the number of seconds after screensaver activation before locking the screen. A session lock or screensaver is a temporary action taken when the user is not physically present on the system, but does not want the system to log out. In order to prevent the system from being compromised, it is important that the operating system must enable a user session lock until that user re-establishes access using established identification and authentication procedures. This setting should be configured according to the needs of business.	The following List string value(s) of X indicate the status of 'lock-delay' setting defined in /etc/dconf/db/.*.d/* file. Note: The database name is arbitrary, and is defined by the user in 'Profile' within '/etc/dconf/profile', which is the list of databases that dconf consults to find the value for key.	matches regular expression list uint32 [1-9][0-9][0-9]? OR, any of the selected values below: [ ] Setting Not Found [x] Directory Not Found
13373	Status of 'lock-enabled' setting in /etc/dconf/db/local.d/locks/*	The 'lock-enabled' setting is responsible to lock the screen when the screensaver goes active. A session lock or screensaver is a temporary action taken when the user is not physically present on the system, but does not want the system to log out, user re-establishes access using established identification and authentication procedures. To prevent the system from being compromised when the user is not around, this setting should be configured properly.	The following List String value(s) of X indicate the status of 'lock-enabled' setting defined in '/etc/dconf/db/(database-name).d/locks/*' files. Note: The database name is arbitrary, and is defined by the user in 'Profile' within '/etc/dconf/profile', which is the list of databases that dconf consults to find the value for key.	matches regular expression list /org/gnome/desktop/screensaver/lock-enabled OR, any of the selected values below: [ ] Setting not found [x] File not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
7431	Status of the 'SELINUX' setting in the '/etc/selinux/config' file	The 'SELinux' setting in the '/etc/selinux/config' file delivers a Mandatory Access Control system in addition to the default Discretionary Access Control feature during the boot process; if enabled. 'SELinux' tags all objects and processes with a security label that is used by the kernel to permit or deny access to the object or process. As there are considerable security and performance risks associated with the 'SELinux' setting, it should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the SELINUX setting in the /etc/selinux/config file.	matches regular expression list (enforcing|permissive) OR, any of the selected values below: [ ] Setting not found [ ] File not found
7432	Status of the 'SELINUXTYPE' setting in the '/etc/selinux/config' file	The 'SELINUXTYPE' setting in the '/etc/selinux/config' file can be configured as 'targeted' or 'mls'. The 'targeted' policy protects processes listed in the targets, while the 'mls' policy offers multi-level security protection. As the SELINUXTYPE setting carries significant security risks to the host, this setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the selinuxtype setting defined within the /etc/selinux/config file.	matches regular expression list targeted|mls OR, any of the selected values below: [ ] Setting not found [ ] File not found
10804	Status of the SELinux current mode (running configuration)	Current mode (running configuration) tells us whether SELinux is currently active or not. SELinux (Security-Enhanced Linux) is a Linux kernel security module that provides mandatory access control security policies. Web applications and services continue to be one of the leading attack vectors to gain access to information and servers. If enforced, SELinux mandatory access controls provide a much stronger security model which can be used to implement a deny-by-default model which only allows what is explicitly permitted. SELinux mode should be configured as appropriate to the needs of the business.	The following List String value(s) of X indicate the status of the Selinux's Current mode on the host. Note: The return value should be 'enforcing' as per DISA benchmarks.	matches regular expression list ^enforcing|permissive$ OR, any of the selected values below: [ ] Setting not found
11435	Status of 'SELinux status' setting in	SELinux can be used to enforce data confidentiality and integrity, as well as	The following List String value(s) of X indicate the status of the	matches regular expression list

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	'sestatus' (running configuration)	protecting processes from untrusted inputs.SELinux policy rules define how processes access files and other processes, if a process is compromised, the attacker only has access to the normal functions of that process, and to files the process has been configured to have access to, which reduces the vulnerability to privilege escalation attacks. This setting should be enabled as appropriate to the needs of the business.	SELinux status on the host. Note: The return value should be 'enabled' as per DISA benchmarks.	^enabled$ OR, any of the selected values below: [ ] Setting Not found
11436	Status of 'Mode from config file' setting in 'sestatus' (running configuration)	SELinux can be used to enforce data confidentiality and integrity, as well as protecting processes from untrusted inputs.SELinux policy rules define how processes access files and other processes, if a process is compromised, the attacker only ha access to the normal functions of that process, and to files the process has been configured to have access to, which reduces the vulnerability to privilege escalation attacks. This setting should be enabled as appropriate to the needs of the business.	The following List String value(s) of X indicate the status of the SELinux's Mode from config file on the host. Note: The return value should be 'enforcing' as per DISA benchmarks.	matches regular expression list enforcing|permissive OR, any of the selected values below: [ ] Setting not found
12880	Status of 'Loaded policy name' setting through 'sestatus' (running configuration)	Security-Enhanced Linux (SELinux) is an implementation of a mandatory access control mechanism in the Linux kernel, checking for allowed operations after standard discretionary access controls are checked. It can enforce rules on files and processes in a Linux system, and on their actions, based on defined policies. SELinux should be configured to meet or exceed the default targeted policy, which constrains daemons and system software only. All other system processes and all remaining userspace programs, as well as any in-house applications, that is everything else on the system, runs in an unconfined domain and is not covered by the SELinux	The following List String value(s) of X indicate the running Loaded policy name for SELinux on the host.	matches regular expression list targeted|mls OR, any of the selected values below: [ ] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		protection model. This setting should be configured according to the needs of the business.		
17165	Status of the unconfined services on the host	This setting specifies the presence of unconfined services running on the system. For unconfined processes, SELinux policy rules are applied, but policy rules exist that allow processes running in unconfined domains almost all access. Processes running in unconfined domains fall back to using DAC rules exclusively. If an unconfined process is compromised, SELinux does not prevent an attacker from gaining access to system resources and data, but of course, DAC rules are still used. configure this setting according to the needs of the business.	The following List String value(s) of X indicate the status of unconfined services present on the host.	is contained in regular expression list (unconfined(_service)?_t):.+(qualys-cloud-ag(ent)?|sshd|(ba|k)?sh|ps|grep|sed)$ (unconfined(_service)?_t):.+(AgentManager|ReportAgent|policyfetcher|seosd|seagent|seoswd|selogrd)$ (unconfined(_service)?_t):.+(nsrpsd|nsrexecd|vflragentd(.bin)?)$ (unconfined(_service)?_t):.+(splunkd|ueg_network.sh|[a-z_]+.sh|perl|sar|tee|awk|sadc)$ (unconfined(_service)?_t):.+(wdavdaemon|crashpad_handle|telemetryd_v2)$ OR, any of the selected values below: [x] Setting Not Found
2236	Status of the 'IgnoreRhosts' setting in the '/etc/ssh/sshd_config' file	The 'IgnoreRhosts' parameter in the '/etc/ssh/sshd_config' file specifies whether .rhosts/.shosts files are used in authentication. As permitting the use of these files can be a security risk, as they are not authenticated or unencrypted and usually world-readable, which presents a serious risk against unauthorized users gaining access to the host, this value should	The following List String value(s) X indicate the current status of the IgnoreRhosts setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^yes$ OR, any of the selected values below: [x] Setting not found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		be set as appropriate to the needs of the business.		[ ] File not found
2240	Status of the 'PermitEmptyPasswords' setting in the 'sshd_config' file	The 'PermitEmptyPasswords' value (in '/etc/ssh/sshd_config') allows for direct login without a password by a remote user/application to resources on the local host, based upon the source IP address, which can be stored in the '/etc/hosts.allow' file. As permitting login without a password under any circumstance, except perhaps when using the PAM configuration challenge/response mechanism or by exchanging certificate keys, is inherently risky, this value should be set as appropriate to the needs of the business.	The following List String value(s) X indicate the current status of the PermitEmptyPasswords setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^no$ OR, any of the selected values below: [x] Setting not found [ ] File not found
3676	Status of the 'PasswordAuthentication' parameter within the '/etc/ssh/sshd_config' file	The 'PasswordAuthentication' parameter within the '/etc/ssh/sshd_config' file is used to deny the use of insecure passwords from the '/etc/passwd' file. Setting this to 'no' places a greater emphasis on the use of more secure public/private encryption keys during the authentication process.	The following List String value(s) X indicate the current status of the PasswordAuthentication setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^no$ OR, any of the selected values below: [ ] Setting not found [ ] File not found
5275	Status of the 'IgnoreUserKnownHosts' setting in the '/etc/ssh/sshd_config' file	The 'IgnoreUserKnownHosts' setting in the '/etc/ssh/sshd_config' file indicates whether or not the sshd service should ignore the user's '.ssh/known_hosts' during an RhostsRSAAuthentication or HostbasedAuthentication. As unnecessary authentication methods can open potential system attack vectors if activated, this value should be set according to the needs of the business.	The following List String value(s) X indicate the current status of the IgnoreUserKnownHosts setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^yes$ OR, any of the selected values below: [ ] Setting not found [ ] File not found
5279	Status of the 'PermitUserEnvironment' setting in the '/etc/ssh/sshd_config' file	The 'permituserenvironment' SSH setting is used to determine whether user environment files are permitted to be sourced. The ability to disable this capability was not available in earlier	The following List String value(s) X indicate the current status of the PermitUserEnvironment setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^no$ OR, any of the selected values

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		versions supporting the use of user specific environment files. This was added to help tighten security by reducing the ability for a user to exploit features such as LD_PRELOAD to circumvent access restrictions.		below: [x] Setting not found [ ] File not found
5287	Status of the 'PrintLastLog' setting in the '/etc/ssh/sshd_config' file	'PrintLastLog' is a setting in the '/etc/ssh/sshd_config' file. This setting configures sshd(8) to print the last users login date and time. As there are known privilege escalation exploits for this setting, the value of the setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the PrintLastLog setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^yes$ OR, any of the selected values below: [x] Setting not found [ ] File not found
5290	Status of the 'StrictModes' setting in the '/etc/ssh/sshd_config' file	'StrictModes' is a setting in the '/etc/ssh/sshd_config' file. This setting configures sshd(8) to check file ownership and modes of users home directory and files before accepting their logon. As there are known vulnerabilities with this setting, such as SQL column truncation exploits, the value of this setting should be configured according to the needs of the business.	The following List String value(s) X indicate the current status of the StrictModes setting defined within the /etc/ssh/sshd_config file.	matches regular expression list ^yes$ OR, any of the selected values below: [x] Setting not found [ ] File not found
9341	Status of the 'Lockout for Failed Password Attempts' setting (pam_faillock in /etc/pam.d/password-auth)	PAM modules (pam_faillock) can be used to temporarily lock user accounts after a number of failed login attempts using configuration files (/etc/pam.d/system-auth and /etc/pam.d/password-auth). This feature is useful in the case of attempted brute force attacks, because even if attacker could guess the password eventually, the target account would be locked and the password would not work. This setting should be monitored to ensure that security baselines for critical systems is maintained according to the needs of the business.	The following list string value of X indicates the status of the pam_faillock.so module within the file /etc/pam.d/password-auth.	contains regular expression list ^(auth[\s\t]+required[\s\t]+pam_faillock.so[\s\t]+preauth[\s\t]+silent[\s\t]+deny=3[\s\t]+unlock_time=0)$ ^(auth[\s\t]+\[default=die\][\s\t]+pam_faillock.so[\s\t]+authfail[\s\t]+deny=3[\s\t]+unlock_time=0)$ ^(auth[\s\t]+sufficient[\s\t]+pam_faillock.so[\s\t]+authsucc[\s\t]+deny=3[\s\t]+unlock_time=0)$

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
				^(account[\s\t]+required[\s\t]+pam_faillock.so)$ OR, any of the selected values below: [ ] Setting Not Found [ ] File Not Found
9451	Status of the 'Lockout for Failed Password Attempts' (pam_faillock in /etc/pam.d/system-auth)	PAM modules (pam_faillock) can be used to temporarily lock user accounts after a number of failed login attempts using configuration files (/etc/pam.d/system-auth and /etc/pam.d/password-auth). This feature is useful in the case of attempted brute force attacks, because even if attacker could guess the password eventually, the target account would be locked and the password would not work. This setting should be monitored to ensure that security baselines for critical systems is maintained according to the needs of the business.	The following list string value of X indicates the status of the pam_faillock.so module within the file /etc/pam.d/system-auth.	contains regular expression list ^(auth[\s\t]+required[\s\t]+pam_faillock.so[\s\t]+preauth[\s\t]+silent[\s\t]+deny=3[\s\t]+unlock_time=0)$ ^(auth[\s\t]+\[default=die\][\s\t]+pam_faillock.so[\s\t]+authfail[\s\t]+deny=3[\s\t]+unlock_time=0)$ ^(auth[\s\t]+sufficient[\s\t]+pam_faillock.so[\s\t]+authsucc[\s\t]+deny=3[\s\t]+unlock_time=0)$ ^(account[\s\t]+required[\s\t]+pam_faillock.so)$ OR, any of the selected values below: [ ] Setting Not Found [ ] File Not Found
9494	Status of the 'minlen' option within the 'pam_pwquality' PAM module	The pam_pwquality module checks configuration of passwords on the host. The 'minlen' setting within the 'pam_pwquality' PAM module controls the minimum length of passwords. As there are several automated password cracking tools for exploiting short passwords to gain unauthorized access to the host, the configuration of this setting	The String value of X indicates the status of the 'minlen' setting within the file /etc/security/pwquality.conf.	matches regular expression list 8 OR, any of the selected values below: [ ] Setting Not Found

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
		should be done according to the needs of the business.		[ ] File Not Found
9498	Status of the 'dcredit' setting within the 'pam_pwquality' PAM module	The pam_pwquality module checks configuration of passwords on the host. The 'dcredit' setting within the 'pam_pwquality' ' PAM module controls the maximum number of digits in passwords. As there are several automated password cracking tools for exploiting weak passwords to gain unauthorized access to the host, the configuration of this setting should be done according to the needs of the business.	The List string value of X indicates the status of the 'dcredit' setting within the /etc/security/pwquality.conf file.	matches regular expression list -1 OR, any of the selected values below: [ ] Setting Not Found [ ] File Not Found
9629	Status of the 'retry' parameter for login attempts defined within '/etc/pam.d/system-auth'	The pam_pwquality module checks configuration of passwords on the host. The 'retry' setting within the 'pam_pwquality' PAM module controls the maximum number of chances user can get to choose strong passwords before password program aborts. As there are several automated password cracking tools for exploiting weak passwords to gain unauthorized access to the host, the configuration of this setting should be done according to the needs of the business.	The Integer value of X indicates the status of the 'retry' setting for pam_pwquality.so module in PAM configuration file '/etc/pam.d/system-auth'.	greater than or equal to 3 OR, any of the selected values below: [ ] Setting Not Found [ ] File Not Found
10731	Status of the 'retry' parameter for login attempts defined within '/etc/pam.d/password-auth'	The pam_pwquality module checks configuration of passwords on the host. The 'retry' setting within the 'pam_pwquality' PAM module controls the maximum number of chances user can get to choose strong passwords before password program aborts. As there are several automated password cracking tools for exploiting weak passwords to gain unauthorized access to the host, the configuration of this setting should be done according to the needs of the business.	The following List String value(s) X indicate the current status of the retry setting defined within the /etc/pam.d/password-auth file.	matches regular expression list 3 OR, any of the selected values below: [ ] Setting not found [ ] File not found
13242	Status of the remember setting for pam_unix.so or pam_pwhistory.so	The 'remember' setting specifies the number of old passwords to be remembered for each user to prohibit	The following List Integer value(s) X indicates the current status of the pam_unix.so or	match all greater than or equal to 6

CID	STATEMENT	DESCRIPTION	EVALUATION	EXPECTED VALUE(S)
	module in /etc/pam.d/system-auth file	password re-use. If password history standards are not enforced, a malicious user could potentially obtain a password through Social Engineering or brute-force attacks. This could lead to the compromise of sensitive information or denial of service conditions. This setting should be configured according to the business needs.	pam_pwhistory.so module's remember setting defined within the /etc/pam.d/system-auth file. The returned value represents the number of old passwords to remember in order to prevent users from re-using them.	OR, any of the selected values below: [ ] Setting Not Found [ ] File Not Found

CHANGE HISTORY

Date	Version	Description
10/23/2020	20.1 DRAFT	• Initial DRAFT version

12/24/2020		• The initial policy for SELinux is added to the Section 4 Access Control.
		  ○ Qualys Control IDs 7431, 7432, 10804, 11435, 11436, 12880, 17165 have also been added
		  ○ Appendix-4 has been added for SELinux
		• OpenSSH setting have been updated regarding the meeting with UEG for 2.i and 2.j in page 10 regarding to Multi-Factor Authentication
		• OpenSSH setting have been improved regarding to the advice from UEG for Qualys Control IDs 2236, 2240, 5275, 5279, 5287 and 5290
		• Controls for Techtia SSH have been removed.
		• Qualys Control ID has been updated for Qualys Control IDs 1267, 1329, 100695-100701
		• Removed the control which requires ‘sysstat’ service disabled. According to the discussion between ISO and UEG, the service can be required with current use cases. No restriction will be applied for Qualys Control ID 9896.
		• PAM setting have been updated for Sections 1.e, 2.b and 2.c in pages 6-7 and 9-10.
		• Added Qualys Policy export to Appendix 5 section
		• Corrected cosmetic issues

01/07/2021		• Updated the list of Unconfined Process in Appendix-4 • Corrected cosmetic issues
01/07/2021	21.1	• Initial Baselined version