**INTEGRA MICRO SYSTEMS (P) LTD.**

**Security Configuration Document**

RHEL 5.X and RHEL6.X

Aug, 2015

DOCUMENT VERSION CONTROL

|  |  |
| --- | --- |
| dOCUMENT TITLE | Secure Configuration Document for RHEL 5.x and 6.X machines |
| DOCUMENT VERSION | 1.0 |
| PREPARED BY | **Mohan Sahu & Amit Tiwari** |
| REVIEWED BY | **Mohan Sahu** |
| APPROVED BY |  |
| EFFECTIVE DATE |  |

DOCUMENT CHANGE CONTROL

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| iSSUE DATE | VERSION | DESCRIPTON | REQUESTED BY | CHANGED BY | APPROVED BY |
|  |  |  |  |  |  |

DOCUMENT DISTRIBUTION LIST

|  |  |  |  |
| --- | --- | --- | --- |
| # | nAME | ORGANIZATION | PURPOSE |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |

DOCUMENT CONTACT DETAILS

|  |  |  |
| --- | --- | --- |
| Role | Name | Email ID |
|  |  |  |
|  |  |  |

**Contents**

[1Purpose 7](#__RefHeading__3834_1468143043)

[2. Security Standard 7](#__RefHeading__3836_1468143043)

[2.1 Control Category 1: User Account Management 7](#__RefHeading__3838_1468143043)

[2.2 Control Category 2: User Right 7](#__RefHeading__3840_1468143043)

[2.3 Control Category 3: Configuration and Supporting Process 8](#__RefHeading__3842_1468143043)

[2.4 Control Category 4: Logging and Auditing 10](#__RefHeading__3844_1468143043)

# Purpose

This document is intended to guide the administrator how to secure the RHEL5.x and 6.x systems. This document represents Integra’s Secure Configuration Document and associated Implementation Procedures.

Each statement in this document shall comprise of:

* **Control standard**: The Control Standard specifies uniform control practices and system parameters to enforce security. Compliance with defined control standards is considered necessary within the Bank, unless their implementation unfavorably impacts business and operational requirements
* **Risk statement**: The Risk Statement provides details on the risk being addressed by the control standard and the possible negative implications of not following the defined control standard.
* **Implementation procedures: Implementation Procedures** are high-level concepts, provided as guidance to the asset owner who would need to perform or configure into the asset to comply with the control standards described in this document. All settings can only be done with administrative privileges. It is strongly recommended that the settings be tested on the staging environment before applying on production environment. It is further recommended that the administrator of the Server make note of the original values while changing the settings.

The Minimum Baseline Standards are designed as a benchmark and where necessary, exceptions may have to be considered for individual assets as a result of operational requirements. These exceptions need to be documented in accordance with the Bank’s procedures for each system.

# 2. Security Standard

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Serial No. | Control Standard | Description | Impact | Remediation |
| **2.1 Control Category 1: User Account Management** | | | | |
| 1. | Password Policy | This determines the properties of the password to be set as per the policy.  PASS\_MAX\_DAYS 99999  PASS\_MIN\_DAYS 0  PASS\_EXPIRY\_WARNING | Inadequate password parameters setting may increase the risk of unauthorized access to the servers by enabling users to configure non-complex or easy to guess passwords which can easily be compromised by the malicious users. | **Remediation**:  **1. Max password days**  Set the PASS\_MAX\_DAYS parameter to 90 in /etc/login.defs: PASS\_MAX\_DAYS 90  Modify active user parameters to match: # chage --maxdays 90 <user>  **2. Min password days**  Set the PASS\_MIN\_DAYS parameter to 7 in /etc/login.defs: PASS\_MIN\_DAYS 7  Modify active user parameters to match: # chage --mindays 7 <user>  **3. Password Expiring Warning**  Set the PASS\_WARN\_AGE parameter to 15 in /etc/login.defs: PASS\_WARN\_AGE 15  Modify active user parameters to match: # chage --warndays 15 <user> |
| 2 | Set Password Creation Requirement Parameters | The pam\_cracklib module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length etc. | Strong passwords protect systems from being hacked through brute force methods. | **Perform the following step:**  Set the pam\_cracklib.so parameters as follows in /etc/pam.d/system-auth: requisite pam\_passwdqc.so min=disabled,disabled,12,8,7 retry=3 |
| 3 | Set Password Expiring Warning Days | The PASS\_WARN\_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days | Providing an advance warning that a password will be expiring gives users time to think of a secure password. | **Remediation:**  Set the PASS\_WARN\_AGE parameter to 15 in /etc/login.defs:  PASS\_WARN\_AGE 15  Modify active user parameters to match: # chage --warndays 15 <user> |
| 4 | Lock Inactive User Accounts | User accounts that have been inactive for over a given period of time can be automatically disabled | Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies. | **Remediation:**  # useradd -D -f 14 |
| 5 | Set Lockout for Failed Password Attempts | Lock out users after 3 unsuccessful consecutive login attempts | Locking out userIDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems. | **Remediation**  Edit the /etc/pam.d/login file and add the auth line below: auth required pam\_tally2.so onerr=fail audit silent deny=3  unlock\_time=24 hrs |
| 6 | Limit Password Reuse | The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords | Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password. | **Remediation**  Set the pam\_unix.so remember parameter to 5 in /etc/pam.d/system-auth: pam\_unix.so sha512 shadow nullok try\_first\_pass use\_authtok remember=5 |
| 7 | Warning Banner for Standard Login Services | The contents of the /etc/issue file are displayed prior to the login prompt on the system's console and serial devices | Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies | **Remediation:**  # touch /etc/motd  # echo "Authorized uses only. All activity may be \  monitored and reported." > /etc/issue  # echo "Authorized uses only. All activity may be \  monitored and reported." > /etc/issue.net  # chown root:root /etc/motd  # chmod 644 /etc/motd  # chown root:root /etc/issue  # chmod 644 /etc/issue  # chown root:root /etc/issue.net  # chmod 644 /etc/issue.net  The content of issue.net:  “This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel." |
| 8 | Remove OS Information from Login Warning Banners | Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system | Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. | **Remediation:**  Edit the /etc/motd, /etc/issue and /etc/issue.net files and remove any lines containing \m, \r, \s or \v. |
| 9 | Boot Loader Password | Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters | Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition | **Remediation:**  Create an encrypted password with grub-md5-crypt:   * # grub-md5-crypt * Enter password: <password> * Reenter password: <password> * Your PBKDF2 is <encrypted-password>   Add the following into /boot/grub/grub.conf or a custom /etc/grub.conf configuration file after timeout:  password --md5 $1$TNUb/1$TwroGJn4eCd4xsYeGiBYq. |
| **2.2 Control Category 2: User Right** | | | | |
| 10 | Permissions on /etc/passwd | The /etc/passwd file contains user account information that is used by many system utilities | It is critical to ensure that the /etc/passwd file is protected from unauthorized write access. | **Remediation:**  Run the following command:  # /bin/chmod 644 /etc/passwd |
| 11 | Permissions on /etc/shadow | The /etc/shadow file is used to store the information about user accounts that is critical to the security of those accounts | If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed password to break it | **Remediation:**  Run the following command:  # /bin/chmod o-rwx,g-rw /etc/shadow |
| 12 | Permissions on /etc/group | The /etc/group file contains a list of all the valid groups defined in the system | The /etc/group file needs to be protected from unauthorized changes by non-privileged users | **Remediation:**  Run the following command:  # /bin/chmod 644 /etc/group |
| 13 | Verify User/Group Ownership on  /etc/passwd  /etc/shadow  /etc/group | The /etc/passwd file contains a list of all the valid userIDs defined in the system, but not the passwords. | These files file need to be protected from unauthorized changes by non-priliveged users | **Remediation:**  Run the following command:  # /bin/chown root:root /etc/passwd  # /bin/chown root:shadow /etc/shadow  # /bin/chown root:root /etc/group |
| 14 | Password Fields are Not Empty | An account with an empty password field means that anybody may log in as that user without providing a password. | All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user. | **Remediation:**  If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account:  # /usr/bin/passwd -l <username> |
| 15 | Permissions on User Home Directories | While the system administrator can establish secure permissions for users' home directories, the users can easily override these. | Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges. | **Remediation:**  Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users |
| 16 | Permissions on bootloader config | Set permission on the your boot loaders config file to read and write for root only | Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. | **Remediation:**  Run the following to set the permissions for /boot/grub/grub.cfg:  # chmod og-rwx /boot/grub/grub.cfg |
| 17 | Account with generic user name | There may be accounts with generic names such as admin etc. | Use of generic user IDs may lead to lack of accountability which may result in failing to trace the intended user in case of a malicious activity performed on the server. | **How to check:**  cat /etc/passwd  Report if there are any user accounts with generic names; admin, administrator, test, user |
| 18 | Disable SSH Root Login | The PermitRootLogin parameter specifies if the root user can log in using ssh | Disallowing root logins over SSH requires server admins to authenticate using their own individual account, then escalating to root via sudo or su. | **Remediation**  Edit the /etc/ssh/sshd\_config file to set the parameter as follows: PermitRootLogin no |
| 19 | Limit Access via SSH | There are several options available to limit which users and group can access the system via SSH | Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system. | **Remediation**:  Edit the /etc/ssh/sshd\_config file to set one or more of the parameter as follows:  AllowUsers <userlist> AllowGroups <grouplist> DenyUsers <userlist> DenyGroups <grouplist> |
| 20 | Restrict root Login to System Console | The file /etc/securetty contains a list of valid terminals that may be logged in directly as root. | Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined. | **Remediation:**  Remove entries for any consoles that are not in a physically secure location. |
| 21 | Non-personal accounts are allowed to directly login onto the system | Non-personal accounts are the ones which are required by the system, but no physical user does login with it. If needed, a user can login with his/her credentials and then switch to another account using -su command. | Unnecessary default accounts may lead an attacker to play with the system settings | **Remediation**  Check for /sbin/nologin or /bin/false on following users (in password file):  root, oracle, samba, apache. |
| 22 | Permissions on /etc/ssh/sshd\_config | The /etc/ssh/sshd\_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root. | The /etc/ssh/sshd\_config file needs to be protected from unauthorized changes by non-priliveged users | **Remediation**:  Run the following command:  # chmod 600 /etc/ssh/sshd\_config |
| **2.3 Control Category 3: Configuration and Supporting Process** | | | | |
| 23 | Install Updates, Patches and Additional Security Software | Periodically patches are released for included software either due to security flaws or to include additional functionality. | Newer patches may contain security enhancements that would not be available through the latest full update | **Remediation**  Run the following command to update all packages on the system:  # yum update all |
| 24 | Disable System Accounts | There are a number of accounts provided with RHEL that are used to manage applications and are not intended to provide an interactive shell. | Important to make sure that accounts that are not being used by regular users are locked to prevent them from being used to provide an interactive shell | **Remediation:**  Accounts that have been locked are prohibited from running commands on the system.  #!/bin/bash  for user in `awk -F: '($3 < 500) {print $1 }' /etc/passwd`; do  if [ $user != "root" ] then  /usr/sbin/usermod -L $user  if [ $user != "sync" ] && [ $user != "shutdown" ] && [ $user != "halt" ]  then  /usr/sbin/usermod -s /usr/sbin/nologin $user  fi  fi  done |
| 25 | Default umask for Users | The default umask determines the permissions of files created by users. | Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. | **Remediation:**  Edit the /etc/login.defs file and set the UMASK parameter as shown: UMASK 077 |
| 26 | World Writable Files | Unix-based systems support variable settings to control access to files. World writable files are the least secure. | Data in world-writable files can be modified and compromised by any user on the system. | **Remediation:**  Removing write access for the "other" category (chmod o-w <filename>) is recommended |
| 27 | Sticky Bit on All World-Writable Directories | Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them. | This feature prevents the ability to delete or rename files in world writable directories that are owned by another user. | **Remediation:**  # df --local -P | awk {'if (NR!=1) print $6'} | xargs -I '{}' find '{}' -xdev -type d -perm -0002 2>/dev/null | chmod a+t |
| 28 | User/Group Owner on bootloader config | Set the owner and group of your boot loaders config file to the root user | Setting the owner and group to root prevents non-root users from changing the file | **Remediation:**  Run the following to change ownership of /boot/grub/grub.conf: # chown root:root /boot/grub/grub.conf |
| 29 | X Window system | The X Window system provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. | Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface. | **Remediation:**  Uninstall X Windows:  # yum groupremove 'X Window System' 'GNOME Desktop Environment' 'Sound and Video' OR  change the default runlevel to 3 in /etc/inittab configuration file. |
| 30 | Network Time Protocol | The Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate | This also ensures log files have consistent time records across the enterprise, which aids in forensic investigations. | **Remediation:**  Install ntp:  # yum install ntp  Ensure the following lines are in /etc/ntp.conf:  restrict -4 default kod nomodify notrap nopeer noquery  restrict -6 default kod nomodify notrap nopeer noquery  Also, make sure /etc/ntp.conf has at least one NTP server specified**:** server <ntp-server> |
| 31 | NFS and RPC services | The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. | If the server does not export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce remote attack surface. | **Remediation:**   * Remove any start links for nfs-kernel-server from /etc/rc\*.d: # rm /etc/rc\*.d/S\*nfs-kernel-server |
| 32 | FTP Server | The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files. | FTP does not protect the confidentiality of data or authentication credentials | **Remediation:**  Remove or comment out start lines in /etc/init/vsftpd.conf:  #start on runlevel [2345] or net-device-up IFACE!=lo |
| 33 | SNMP Server | The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system | The SNMP server communicates using SNMP v1, which transmits data in the clear and does not require authentication to execute commands | **Remediation:**  Remove any start links for snmpd from /etc/rc\*.d:  # rm /etc/rc\*.d/S\*snmpd |
| 34 | Firewall is active | IPtables is an application that allows a system administrator to configure the IPv4 tables, chains and rules provided by the Linux kernel firewall | IPtables provides extra protection for the Linux system by limiting communications in and out of the box to specific IPv4 addresses and ports. | **Remediation:**  Activate iptables:  # service iptables enable |
| 35 | Sudoers Configuration | It determines the system administrators scope | "Inappropriate sudoers configuration increases the risk of unauthorized access to the system.  With 'NOPASSWD' and default ALL = (ALL) ALL set, an attacker may gain unauthorized privileged access to the servers using other users' account and may perform malicious activities." | **How to check:**  Following are UNSAFE in /etc/sudoers file:  e.g. fred ALL = (DB) NOPASSWD: ALL  ALL = (ALL) ALL for users other than root or system admins.  And if required, access to the SUDO command should be limited to 'root' and system administrator's account/group only. Also, it is recommended not to configure the sudoers with 'NOPASSWD' parameter.  Add the following lines to the /etc/audit/audit.rules file. -w /etc/sudoers -p wa -k scope # Execute the following command to restart auditd # pkill -HUP -P 1 auditd |
| 36 | Clear text FTP service | The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files. | Use of clear text service such as FTP enables an attacker to eavesdrop sensitive information including login credentials over network. Further, enabling anonymous login allows users to login with 'anonymous' user and password or without password, which can be used by malicious user to gain unauthorized access to the critical files over FTP. | **Remediation:**  Remove or comment out start lines in /etc/init/vsftpd.conf: #start on runlevel [2345] or net-device-up IFACE!=lo  Remove or comment out any tftp lines in /etc/inetd.conf:  #tftp stream tcp nowait root internal |
| 37 | ‘crontab’ (Cron and At) files setting | The /etc/crontab file is used by cron to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file. | This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges | **Remediation:**  # chown root:root /etc/crontab  # chmod og-rwx /etc/crontab |
| 38 | Restrict at/cron to Authorized Users | Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. | On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. | **Remediation:**  # /bin/rm /etc/cron.deny  # /bin/rm /etc/at.deny  # touch /etc/cron.allow  # touch /etc/at.allow  # chmod og-rwx /etc/cron.allow  # chmod og-rwx /etc/at.allow  # chown root:root /etc/cron.allow # chown root:root /etc/at.allow |
| 39 | User/Group Owner and Permission on /etc/cron.hourly  /etc/cron.daily  /etc/cron.weekly  /etc/cron.monthly  /etc/cron.d | This directory contains system cron jobs that need to run on an a predefined duration | Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges | **Remediation:**  # chown root:root /etc/cron.hourly # chmod og-rwx /etc/cron.hourly  # chown root:root /etc/cron.daily # chmod og-rwx /etc/cron.daily  # chown root:root/etc/cron.weekly  # chmod og-rwx /etc/cron.weekly  # chown root:root /etc/cron.monthly  # chmod og-rwx /etc/cron.monthly  # chown root:root /etc/cron.d  # chmod og-rwx /etc/cron.d |
| 40 | Disable unwanted services | It is advised to disable unwanted services such as NIS, rsh, talk server, telnet etc | These legacy services have inherent vulnerabilities and should be disabled to reduce the attack vector | **Remediation:**  Uninstall the nis package: # yum remove nis  Rsh server:  Remove or comment out any shell, login, or exec lines in /etc/inetd.conf: #shell stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rshd  #login stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rlogind  #exec stream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecd  Uninstall the talk package:  # apt-get purge talk  Remove or comment out any telnet lines in /etc/inetd.conf:  #telnet stream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.telnetd |
| 41 | Security Enhanced Linux (SELinux) | SELinux, one of the Linux kernel security module, is another level of security enhancement to Linux servers that enforces security policies and enables additional controls over access to critical resources, such as files, directories etc. | Disabling SELinux would remove local security mechanism on the system and would completely disable all SELinux functions including file and process labeling, which could lead to problems if you want to re-enable it again later. | **Remediation:**  Remove all instances of selinux=0 and enforcing=0 from /etc/grub.conf.  **Set the SELinux State:**  Edit the /etc/selinux/config file to set the SELINUX parameter:  SELINUX=enforcing  **Set SELinux Policy**:  Edit the /etc/selinux/config file to set the SELINUXTYPE parameter:  SELINUXTYPE=targeted |
| 42 | Disk quota is not defined | Disk quotas are typically implemented on a per-user or per-group basis, a system administrator defines a usage or file quota specific to a certain user or group. | In the absence of quota defined on server, users would not be prevented from consuming an entire file system's resources. A potential attacker may use the same to consume all the resources which in turns may lead to denial of service. | **Remediation**  Recommended that proper disk quota on per user/ per group and/ or file system basis should be configured  Create Empty Quotas File  You need to create empty quotas file in in root of file system using  # touch /export/home/quotas  # chown root:root /export/home/quotas  # chmod 0600 /export/home/quotas  Edit and set user quotas for user vivek using edquota command.  # edquota username  The quotaon command turns on disk quotas for /export/home ufs file systems. Type the command:  # quotaon -v /export/home |
| 43 | Kernel security parameters | Network services should be configured to secure the servers as given below .There are several kernel options in Red Hat Linux that can be configured to increase the overall network security.  net.ipv4.conf.default.send\_redirects = 1  net.ipv4.conf.default.accept\_redirects = 1  net.ipv4.conf.eth0.send\_redirects = 1  net.ipv4.conf.eth0.accept\_redirects = 1  net.ipv4.conf.lo.accept\_source\_route = 1  net.ipv4.conf.lo.send\_redirects = 1  net.ipv4.conf.lo.accept\_redirects = 1  net.ipv4.conf.all.send\_redirects = 1 | In current scenario, an attacker can utilize these settings to launch DOS attacks on the server or use the server as an intermediary in attacks. | **Remediation:**  The kernel security parameters should be configured as follows to enforce kernel level security:  net.ipv4.conf.default.send\_redirects = 0  net.ipv4.conf.default.accept\_redirects = 0  net.ipv4.conf.eth0.send\_redirects = 0  net.ipv4.conf.eth0.accept\_redirects = 0  net.ipv4.conf.lo.accept\_source\_route = 0  net.ipv4.conf.lo.send\_redirects = 0  net.ipv4.conf.lo.accept\_redirects = 0  net.ipv4.conf.all.send\_redirects = 0  Command to check:  sysctl -a |
| 44 | Set SSH Protocol to 2 | SSH is a secure, encrypted replacement for common login services such as telnet, ftp, rlogin, rsh, and rcp. | SSH v1 suffers from insecurities that do not affect SSH v2. | **Remediation:**  Edit the /etc/ssh/sshd\_config file to set the parameter as follows:  Protocol 2  For Kerberos:  # Kerberos options  KerberosAuthentication yes  KerberosOrLocalPasswd no  KerberosTicketCleanup yes |
| **2.4 Control Category 4: Logging and Auditing** | | | | |
| 45 | Separate Partition for /var/log | The /var/log directory is used by system services to store log data. | There are two important reasons to ensure that system logs are stored on a separate partition: protection against resource exhaustion and protection of audit data. | **Remediation:**  For new installations, during installation create a custom partition setup and specify a separate partition for /var/log.  For systems that were previously installed, use the **Logical Volume Manager** (LVM) to create partitions |
| 46 | Configure Audit Log Storage Size | Configure the maximum size of the audit log file | Important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost. | Remediation:  Set the max\_log\_file parameter in /etc/audit/auditd.conf  max\_log\_file = <MB> |
| 47 | Install and Enable auditd Service | Install and turn on the auditd daemon to record system events | The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring. | Remediation:  Install auditd:  #yum install auditd  If needed create proper start links for auditd in /etc/rc\*.d by running the following command from each of the relevant directories:  # ln -s ../init.d/auditd S37auditd |
| 48 | Login and Logout Events | Monitor login and logout events. | Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins | **Remediation:**  Add the following lines to the /etc/audit/audit.rules file.  -w /var/log/faillog -p wa -k logins  -w /var/log/lastlog -p wa -k logins  -w /var/log/tallylog -p wa -k logins # Execute the following command to restart auditd  # pkill -HUP -P 1 auditd |
| 49 | Ensure the rsyslog Service is activated | Once the rsyslog package is installed it needs to be activated. | If the rsyslog service is not activated the system will not have a syslog service running. | **Remediation:**  Set the proper start conditions in /etc/init/rsyslog.conf:  start on filesystem |
| 50 | Configure /etc/rsyslog.conf | The /etc/rsyslog.conf file specifies rules for logging and which files are to be used to log certain classes of messages. | The /etc/rsyslog.conf file specifies rules for logging and which files are to be used to log certain classes of messages. | **Remediation**:  Edit the following lines in the /etc/rsyslog.conf or /etc/rsyslog.d/\* file as appropriate for your environment: \*.emerg :omusrmsg:\*  mail.\* -/var/log/mail mail.info -/var/log/mail.info  mail.warning -/var/log/mail.warn  mail.err /var/log/mail.err  news.crit -/var/log/news/news.crit  news.err -/var/log/news/news.err  news.notice -/var/log/news/news.notice  \*.=warning;\*.=err -/var/log/warn  \*.crit /var/log/warn  \*.\*;mail.none;news.none -/var/log/messages  local0,local1.\* -/var/log/localmessages  local2,local3.\* -/var/log/localmessages  local4,local5.\* -/var/log/localmessages  local6,local7.\* -/var/log/localmessages  Execute the following command to restart  rsyslogd # pkill -HUP rsyslogd |
| 51 | Collect System Administrator Actions - Sudolog | Monitor the sudo log file | Changes in /var/log/sudo.log indicate that an administrator has executed a command or the log file itself has been tampered with | **Remediation:**  Add the following lines to the /etc/audit/audit.rules file.  -w /var/log/sudo.log -p wa -k actions  # Execute the following command to restart auditd  # pkill -HUP -P 1 auditd |
| 52 | Log file permission | A log file must already exist for rsyslog to be able to write to it. | An attackers may misuse the excessive privileges to read/update the contents of a log file and can simply delete the critical log files. | **Remediation**  For sites that have not implemented a secure admin group:  Create the /var/log/ directory and for each <logfile> listed in the /etc/rsyslog.conf or /etc/rsyslog.d/\* files, perform the following commands:  # touch <logfile>  # chown root:root <logfile>  # chmod og-rwx <logfile>  For sites that have implemented a secure admin group:  Create the /var/log/ directory and for each <logfile> listed in the /etc/rsyslog.conf file, perform the following commands (where is the name of the security group):  # touch <logfile>  # chown root:<securegrp> <logfile>  # chmod g-wx,o-rwx<logfile> |
| 53 | Configure rsyslog to Send Logs to a Remote Log Host | The rsyslog utility supports the ability to send logs it gathers to a remote log host running syslogd(8) or to receive messages from remote hosts, reducing administrative overhead. | Storing log data on a remote host protects log integrity from local attacks | **Remediation:**  Edit the /etc/rsyslog.conf file and add the following line (where logfile.example.com is the name of your central log host).  \*.\* @@loghost.example.com  # Execute the following command to restart rsyslogd  # pkill -HUP rsyslogd |

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