**Red Hat Linux Server Hardening Checklist**

The hardening checklists are based on the comprehensive checklists produced by CIS. The [Information Security Office](http://security.utexas.edu) has distilled the CIS lists down to the most critical steps for your systems, with a particular focus on configuration issues that are unique to the computing environment at The University of Texas at Austin.

**How to use the checklist**

Print the checklist and check off each item you complete to ensure that you cover the critical steps for securing your server. The Information Security Office uses this checklist during risk assessments as part of the process to verify that servers are secure.

**How to read the checklist**

**Step** - The step number in the procedure. If there is a [UT Note](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-note) for this step, the note # corresponds to the step #.  
**Check** (√) - This is for administrators to check off when she/he completes this portion.  
**To Do** - Basic instructions on what to do to harden the respective system  
**CIS** - Reference number in the Center for Internet Security [Red Hat Linux Benchmark](https://wikis.utexas.edu/download/attachments/15872036/CIS_RHEL_5.0-5.1_Benchmark_v.1.1.2.pdf?version=1&modificationDate=1292428058000) (PDF, Requires UT EID login.) The CIS document outlines in much greater detail how to complete each step.  
**UT Note** - The [UT Note](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-note) at the bottom of the page provides additional detail about the step for the university computing environment.  
**Cat I** - For systems that include [Category-I data](http://www.utexas.edu/its/policies/opsmanual/dataclassification.php), required steps are denoted with the **!** symbol. All steps are recommended.  
**Cat II/III** - For systems that include [Category-II or -III data](http://www.utexas.edu/its/policies/opsmanual/dataclassification.php), all steps are recommended, and some are required (denoted by the **!**).  
**Min Std** - This column links to the specific requirement for the university in the [Minimum Security Standards for Systems](http://www.utexas.edu/its/policies/opsmanual/secstd.php) document.

**Server Information**

|  |  |
| --- | --- |
| **MAC Address** |  |
| **IP Address** |  |
| **Machine Name** |  |
| **Asset Tag** |  |
| **Administrator Name** |  |
| **Date** |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Step** | √ | **To Do** | **CIS** | **UT Note** | **Cat I** | **Cat II/III** | **Min Std** |
|  |  | **Preparation and Installation** |  |  |  |  |  |
| 1 |  | If machine is a new install, protect it from hostile network traffic, until the operating system is installed and hardened. |  | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r1) | **!** |  | [5.1](http://www.utexas.edu/its/policies/opsmanual/secstd.php#51) |
| 2 |  | Set a BIOS/firmware password and/or - configure the device boot order to prevent unauthorized booting from alternate media. | 8.8 |  | **!** |  | [4.1](http://www.utexas.edu/its/policies/opsmanual/secstd.php#41) |
|  |  | **Patches, Packages and Initial Lockdown** |  |  |  |  |  |
| 3 |  | Operating system and application services security patches should be installed expediently and in a manner consistent with change management procedures. | 2.1 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r2) | **!** |  | [5.2](http://www.utexas.edu/its/policies/opsmanual/secstd.php#52) |
| 4 |  | Configure SSHNote: Services used to transfer [Category-I data](http://www.utexas.edu/its/policies/opsmanual/dataclassification.php) shall be encrypted. | 2.3 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r4) | **!** |  | [5.6](http://www.utexas.edu/its/policies/opsmanual/secstd.php#56) |
| 5 |  | Enable system accounting (install package sysstat). | 2.4 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r5) | **!** |  | [6.1](http://www.utexas.edu/its/policies/opsmanual/secstd.php#61) |
| 6 |  | Enable and test OS and Applications logging. | n/a | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r6) | **!** |  | [6.1](http://www.utexas.edu/its/policies/opsmanual/secstd.php#61) |
|  |  | **Minimize xinetd network services** |  |  |  |  |  |
| 7 |  | Disable any services and/or applications started by xinetd or inetd that are not being utilized. | 3.1t | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r7) | **!** |  | [5.4](http://www.utexas.edu/its/policies/opsmanual/secstd.php#54) |
| 8 |  | Limit connections to services running on the host to authorized users of the service (utilize firewall and other access control technology) | 3.2 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r8) | **!** |  | [5.5](http://www.utexas.edu/its/policies/opsmanual/secstd.php#55) |
|  |  | **Minimize boot services** |  |  |  |  |  |
| 9 |  | Disable GUI login if possible. | 4.4 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r9) | **!** |  |  |
| 10 |  | Disable unused standard boot services. | 4.6 |  | **!** |  |  |
| 11 |  | Disable X Font Server, If Possible | 4.5 |  |  |  |  |
|  |  | **Logging** |  |  |  |  |  |
| 12 |  | Configure an NTP server. | n/a | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r11) | **!** |  |  |
| 13 |  | All administrator or root access must be logged. | 6 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r12) | **!** |  | [6.4](http://www.utexas.edu/its/policies/opsmanual/secstd.php#64) |
|  |  | **Files/Directory Permissions/Access** |  |  |  |  |  |
| 14 |  | Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested. | 7.4 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r13) | **!** |  | [5.9](http://www.utexas.edu/its/policies/opsmanual/secstd.php#59) |
|  |  | **System Access, Authentication, and Authorization** |  |  |  |  |  |
| 15 |  | Ensure that the configuration files for PAM, /etc/pam.d/\* are secure. | 8.1 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r14) | **!** | **!** | [5.12](http://www.utexas.edu/its/policies/opsmanual/secstd.php#512) |
| 16 |  | Enable the terminal security file/restrict root logins to system console. | 8.6 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r15) | **!** | **!** | [4.1](http://www.utexas.edu/its/policies/opsmanual/secstd.php#41) |
|  |  | **Warning Banners** |  |  |  |  |  |
| 17 |  | If network or physical access services are running - ensure the university warning banner is displayed. | 10.1 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r16) | **!** | **!** | [5.10](http://www.utexas.edu/its/policies/opsmanual/secstd.php#510) |
| 18 |  | If the system allows logins via a graphical user interface, create a warning banner for it. | 10.2 |  |  |  |  |
|  |  | **Anti-Virus Considerations** |  |  |  |  |  |
| 19 |  | Install and enable anti-virus software. | 12 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r18) | **!** | **!** | [3.1](http://www.utexas.edu/its/policies/opsmanual/secstd.php#31) |
| 20 |  | Configure to update signature daily on AV. | 12 | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r19) | **!** | **!** | [3.3](http://www.utexas.edu/its/policies/opsmanual/secstd.php#33) |
|  |  | **Additional Security Notes** |  |  |  |  |  |
| 21 |  | Systems will provide secure storage for Category-I data as required by confidentiality, integrity, and availability needs. Security can be provided by means such as, but not limited to, encryption, access controls, filesystem audits, physically securing the storage media, or any combination thereof as deemed appropriate. | n/a | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r20) | **!** | **!** | [5.7](http://www.utexas.edu/its/policies/opsmanual/secstd.php#57) |
| 22 |  | Integrity checking of critical operating system files should be enabled and tested. Third-party tools may also be used to implement this. | n/a | [§](https://wikis.utexas.edu/display/ISO/Redhat+Linux+Hardening+Checklist#RedhatLinuxHardeningChecklist-r21) | **!** | **!** | [5.8](http://www.utexas.edu/its/policies/opsmanual/secstd.php#58) |

**UT Note: Addendum**

This list provides specific tasks related to the computing environment at The University of Texas at Austin.

|  |  |
| --- | --- |
| 1 | If other alternatives are unavailable, this can be accomplished by installing a SOHO router/firewall in between the network and the host to be protected. |
| 2 | Install and use the yum-security plugin.  To install the plugin run:  yum install yum-security  To list all updates that are security relevant, and get a reutrn code on whether there are security updates use:  yum --security check-update  To apply updates that are security relevant use:  yum --security update |
| 3 | If you decide to utilize [SSH](http://www.openssh.com), the ISO highly recommends the following:   * Change the port from port 22 to something/anything else. There are scripts online that malicious hackers can use against an SSH server. These scripts always attack port 22 since most people do not change the default port. * Restrict access to the SSH port using a hardware or software firewall. * Do not allow root logins via SSH. * If possible, use keys with passphrase instead of just passwords. To create rsa keys, follow these commands: * ssh-keygen \--t rsa * ssh server "mkdir .ssh; chmod 0700 .ssh"   scp ./ssh/ida\_rsa.pub server:.ssh/authorized\_keys2   * + The CIS Solaris Benchmark covers some suggested basic settings to place in the configuration file.  You may also want to visit the [SSL Web site](http://www.openssl.org/). |
| 4 | System accounting gathers baseline system data (CPU utilization, disk I/O, etc.) every 10 minutes. The data may be accessed with the sar command (part of the sysstat package), or by reviewing the nightly report files named /var/log/sa/sar\*. Once a normal baseline for the system has been established, unauthorized activity (password crackers and other CPU-intensive jobs, and activity outside of normal usage hours) may be detected due to departures from the normal system performance curve. |
| 5 | The psacct package contains several utilities for monitoring process activities, including ac, lastcomm, accton, and sa.   * **ac** displays statistics about how long users have been logged on. * **lastcomm** displays information about previously executed commands. * **accton** turns process accounting on or off. * **sa** summarizes information about previously executed commands. |
| 6 | Disable any xinetd services you do not absolutely require by setting "disable=yes" in /etc/xinetd.d/\*.  If no xinetd services are required, disable xinetd altogether  sudo service xinetd stop; sudo chkconfig xinetd off  Configure TCP wrappers for access control.  Edit /etc/hosts.deny to include this entry as the first uncommented line in the file: ALL:ALL  Ensure /etc/hosts.allow is edited appropriately to allow the administrator(s) to connect.  Unless "r" commands (i.e., rsh, rlogin) are required, remove or empty the file /etc/hosts.equiv.  If "r" commands are required, consider replacing them with a secure alternative such as SSH.  Verify that you have disabled any unnecessary startup scripts under /etc, /etc/rc\*.d, or /etc/init.d (or startup script directory for your system) and disabled any unneeded services from starting in these scripts.  Unnecessary services can be disabled with:  $ sudo chkconfig off  To check what services are listening use:  $ lsof \| grep '\*:'&nbsp;  OR  $ sudo netstat \--tulp  Much more detailed information regarding services is available in the CIS benchmark documents.  Red Hat also provides a text-based interface for changing startup services:  ntsysv  For example, the command  ntsysv \--level 345  configures runlevels 3, 4, and 5. |
| 7 | Red Hat comes with iptables. Below is a list of some iptables resources:  <http://firehol.sourceforge.net>  <http://sourceforge.net/projects/fwbuilder>  <http://www.simonzone.com/software/guarddog> |
| 8 | A simple way to disable the GUI is to change the default run level. Edit the file /etc/inittab. Look for the line that contains the following:  id:5:initdefault:  Replace the "5" with "3". The line will then read:  id:3:initdefault: |
| 9 | ITS Networking operates two stratum 2 NTPv4 (NTP version 4) servers for [network time synchronization services for university network administrators](http://www.utexas.edu/its/ntp/). |
| 10 | Examples: syslogRed Hat:<http://www.redhat.com/docs/manuals/enterprise/RHEL-AS-2.1-Manual/cluster-manager/s1-software-syslog.html> |
| 11 | * Check in /etc/sudoers to see who has sudo rights * Check in /etc/groups to see what groups your users belong to * Check in /etc/passwd and/or /etc/shadow for blank passwords * Check the strength of users' passwords with tools such as [John the Ripper](http://www.openwall.com/john/) * Seek approval from [IT Owner](http://www.utexas.edu/its/glossary/iso#GL_Owner). Consider using a simple dictionary for easily guessed passwords. * Develop a procedure to report and remediate easily guessed passwords. |
| 12 | Ensure the following are set in /etc/pam.d/other:   * auth  required pam\_deny.so * auth   required pam\_warn.so * account  required pam\_deny.so * account  required pam\_warn.so * password  required pam\_deny.so * password  required pam\_warn.so * session  required pam\_deny.so * session  required pam\_warn.so * session  required pam\_deny.so  Warn will report alerts to syslog. |
| 13 | Ensure that the terminal security file (for example, /etc/securetty or /etc/ttys) is configured to deny privileged (root) access. On a Red Hat box, this means that no virtual devices (such as /dev/pty\*) appear in this file. |
| 14 | The text of the [university's official warning banner](http://www.utexas.edu/its/policies/banner.php) can be found on the ITS Web site. You may add localized information to the banner as long as the university banner is included. |
| 15 | There are few viruses that infect Linux computers; therefore, it is understandable for most Linux servers to have an exception to this rule. See the Operations Manual for information on the [exception process](http://www.utexas.edu/vp/it/policies/uts165/index.php).  You may choose any proven anti-virus product. One option is [ClamAV](http://www.clamav.net). |
| 16 | There are few viruses that infect Linux computers; therefore, it is understandable for most Linux servers to have an exception to this rule. See the Operations Manual for information on the [exception process](http://www.utexas.edu/vp/it/policies/uts165/index.php). |
| 17 | There are a variety of methods available to accomplish this goal. Two good candidates are TrueCrypt (free) and [GNUPG](http://www.gnupg.org) (free). |
| 18 | There is a license fee for Tripwire. The Tripwire management console can be very helpful for managing more complex installations.  AIDE is a free tool [available from SourceForge](http://sourceforge.net/projects/aide).  [SamHain](http://la-samhna.de/samhain/) is another free tool, as is [OSSEC HIDS](http://www.ossec.net/). |