

[HOME \(/\)](#) [QUICK LINKS ∨ \(/\)](#) [POLICIES ∨ \(/POLICIES\)](#)[RESEARCH \(/CONSENSUS\)](#) [SUPPORT TOPICS ∨ \(/EDUCATION-OUTREACH\)](#)[REPORT VIOLATION \(/VIOLATION\)](#) [CONTACT \(/CONTACT\)](#)

RED HAT ENTERPRISE LINUX 7

[Q SEARCH](#)

HARDENING CHECKLIST

The hardening checklists are based on the comprehensive checklists produced by CIS. The [Information Security Office](http://security.utexas.edu/) (<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** for this step, the note number corresponds to the step number.

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 Enterprise Linux 7 Benchmark v1.1.0](#)

(https://benchmarks.cisecurity.org/downloads/multiform/index.cfm?do=download&download=linux/CIS_Red_Hat_Enterprise_Linux_7_Benchmark_v1.1.0.pdf&first=&last=&org=&er)

The CIS document outlines in much greater detail how to complete each step.

UT Note - The **UT 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** (http://security.utexas.edu/policies/data_classification.html) data (http://security.utexas.edu/policies/data_classification.html), required steps are denoted with the ! symbol. All steps are recommended.

Cat II/III - For systems that include **Category-II or -III** (http://security.utexas.edu/policies/data_classification.html) data (http://security.utexas.edu/policies/data_classification.html), 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 \(/policies/standards_systems\)](#) document.

SERVER INFORMATION

Server Information

MAC Address	
IP Address	
Machine Name	
Asset Tag	
Administrator Name	
Date	

CHECKLIST

Checklist

Step	✓	To Do	CIS	UT Note	Cat I	Cat II/III	N
		Preparation and Installation					
1		If machine is a new install, protect it from hostile network traffic, until the operating system is installed and hardened.		<u>S</u>	!	!	<u>4</u> (/

Step	To Do	CIS	UT Note	Cat I	Cat II/III	N
2	Set a BIOS/firmware password. HOME (7) QUICK LINKS (7) POLICIES (7) POLICIES (7)			!		<u>4</u> (/
3	Configure the device boot order to prevent unauthorized booting from alternate media. RESEARCH (7) CONSENSUS (7) SUPPORT TOPICS (7) EDUCATION-OUTREACH (7)					
4	Use the latest version of RHEL if possible. RESTORE (7) RHEL (7) RHEL (7) CONTACT (7) CONTACT (7)			!	!	<u>4</u> (/
	Filesystem Configuration					
5	Create a separate partition with the nodev, nosuid, and noexec options set for /tmp	1.1.1-.4	<u>S</u>			
6	Create separate partitions for /var, /var/log, /var/log/audit, and /home	1.1. {5,7,8,9}	<u>S</u>			
7	Bind mount /var/tmp to /tmp	1.1.6				
8	Set nodev option to /home	1.1.10				
9	Set nodev, nosuid, and noexec options on /dev/shm	1.1.14-16				
10	Set sticky bit on all world-writable directories.	1.1.17				
	System Updates					
11	Register with Red Hat Satellite Server so that the system can receive patch updates.	1.2.1	<u>S</u>	!	!	<u>4</u> (/
12	Install the Red Hat GPG key and enable gpgcheck.	1.2.2-.3				
	Secure Boot Settings					
13	Set user/group owner to root, and permissions to read and write for root only, on /boot/grub2/grub.cfg	1.5.1-.2	<u>S</u>			
14	Set boot loader password.	1.5.3				
15	Remove the X window system.	3.2	<u>S</u>			
16	Disable X font server.					
	Process Hardening					
17	Restrict core dumps.	1.6.1	<u>S</u>			
18	Enable randomized virtual memory region placement.	1.6.2	<u>S</u>	!		

Step	To Do	CIS	UT Note	Cat I	Cat II/III	N
	OS Hardening HOME (/) QUICK LINKS (/) POLICIES (/POLICIES) RESEARCH (/RESEARCH) CONSENSUS (/CONSENSUS) SUPPORT TOPICS (/SUPPORT TOPICS) EDUCATION-OUTREACH (/EDUCATION-OUTREACH)					
19	Remove legacy services (e.g., telnet-server; rsh, rlogin, rcp; yperv, ybind, yftpd, yftpd-server, talk, talk-server).	2.1.{1,3-10}		!	!	
20	Disable any services and applications started by xinetd or inetd that are not being utilized.		<u>S</u>	!	!	<u>4</u> (/)
21	Remove xinetd, if possible.	2.1.11	<u>S</u>	!		
22	Disable legacy services (e.g., chargen-dgram, chargen-stream, daytime-dgram, daytime-stream, echo-dgram, echo-stream, tcpmux-server).	2.1.{12-18}		!	!	
23	Disable or remove server services that are not going to be utilized (e.g., FTP, DNS, LDAP, SMB, DHCP, NFS, SNMP, etc.).			!		<u>4</u> (/)
24	Set daemon umask.	3.1				
	Network Security and Firewall Configuration					
25	Limit connections to services running on the host to authorized users of the service via firewalls and other access control technologies.	4.7	<u>S</u>	!	!	<u>4</u> (/)
26	Disable IP forwarding.	4.1.1				
27	Disable send packet redirects.	4.1.2				
28	Disable source routed packet acceptance.	4.2.1				
29	Disable ICMP redirect acceptance.	4.2.2				
30	Enable ignore broadcast requests.	4.2.5				
31	Enable bad error message protection.	4.2.6				
32	Enable TCP/SYN cookies.	4.2.8				
	Remote Administration Via SSH					
33	Set SSH protocol to 2.	6.2.1	<u>S</u>	!	!	<u>4</u> (/)
34	Set SSH loglevel to INFO.	6.2.2	<u>S</u>	!	!	
35	Disable SSH root login.	6.2.8	<u>S</u>			

Step	To Do	CIS	UT Note	Cat I	Cat II/III	N
36	Set SSH permissions to prevent empty passwords to be used. HOME (/) > QUICK LINKS > (/) > POLICIES > (/) > POLICIES	6.2.9		!	!	
	System Integrity and Intrusion Detection					
37	Install and configure AIDE. RESEARCH (/CONSENSUS) > SUPPORT TOPICS > (/EDUCATION-OUTREACH)	1.3.1-.2	<u>S</u>			<u>4</u> (/)
38	Configure selinux. REPORT VIOLATION (/VIOLATION) > CONTACT (/CONTACT)	1.4.1-.6	<u>S</u>			
39	Install and configure OSsec HIDS. OSsec		<u>S</u>			
40	Configure network time protocol (NTP).	3.6	<u>S</u>	!		
41	Enable system accounting (auditd).	5.2	<u>S</u>	!		<u>4</u> (/)
42	Install and configure rsyslog.	5.1.1-.4	<u>S</u>	!		
43	All administrator or root access must be logged.			!		<u>4</u> (/)
44	Configure log shipping to separate device/service (e.g. Splunk (https://ut.service-now.com/utss/catalogoverview.do?sysparam_citems_id=2bc53c004f8f924031eb7bcd0210c772))).	5.1.5	<u>S</u>			
	Files/Directory Permissions/Access					
45	Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.		<u>S</u>	!		<u>4</u> (/)
	PAM Configuration					
46	Ensure that the configuration files for PAM, /etc/pam.d/* are secure.	6.3	<u>S</u>	!	!	<u>4</u> (/)
47	Upgrade password hashing algorithm to SHA-512.	6.3.1		!		
48	Set password creation requirements.	6.3.2	<u>S</u>	!	!	
49	Restrict root login to system console.	6.4	<u>S</u>			
	Warning Banners					
50	If network or physical access services are running, ensure the university warning banner is displayed.	6.2.14, 8.1	<u>S</u>	!	!	<u>4</u> (/)

Step	To Do	CIS	UT Note	Cat I	Cat II/III	N
51	If the system allows logins via a graphical user interface, ensure the university warning banner is displayed prior to login.	8.3 (/POLICIES)	<u>S</u>	!		
	Anti-Virus Considerations					
52	Install and enable anti-virus software.	CONTACT (/CONTACT)	<u>S</u>			<u>4</u> (/)
53	Configure to update the signature daily on AV.		<u>S</u>			<u>4</u> (/)
	Additional Security Notes					
54	Systems will provide secure storage for Confidential (Category-I) University Data as required. 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.					

UT NOTE: ADDENDUM

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

UT Note: Addendum

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.
5	Since /tmp is intended to be world writable, creating a separate partition for it can prevent resource exhaustion. Setting nodev prevents users from creating or using block or special character devices. Setting noexec prevents users from running binary executables from /tmp. Setting nosuid prevents users from creating set userid files in /tmp.
6	Multiple partitions are recommended to protect against resource exhaustion conditions if a partition fills up, as well as to allow for the setting of various options on individual partitions to support increased security (e.g. nodev, nosuid, noexec).

11	<p>Install and use the yum-security plugin. To install the plugin run:</p> <p>yum install yum-security</p> <p>To list all updates that are security relevant, and get a return code on whether there are security updates use:</p> <p>yum --security check-update</p> <p>To apply updates that are security relevant use:</p> <p>yum --security update</p>
13	<p>Setting user/group ownership to root and file permissions to read and write only for root is recommended to prevent non-root users from viewing or changing the boot parameters.</p>
15	<p>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:</p> <p>id:5:initdefault:</p> <p>Replace the "5" with "3". The line will then read:</p> <p>id:3:initdefault:</p>
17	<p>Core dumps are intended to help determine why a program aborted. They may contain sensitive or confidential data from memory. It is recommended that core dumps be disabled or restricted. The system should be configured to prevent setuid programs from creating core dumps.</p>
18	<p>Add the following line to the /etc/sysctl.conf file:</p> <p>kernel.randomize_va_space = 2</p>

20	<p>Disable any xinetd services you do not absolutely require by setting "disable=yes" in /etc/xinetd.d/*.</p> <p>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. 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.</p> <p>REPORT VIOLATION (/VIOLATION) CONTACT (/CONTACT)</p> <p>Unnecessary services can be disabled with:</p> <p>Q SEARCH</p> <p>\$ sudo chkconfig off</p> <p>To check what services are listening use:</p> <p>\$ lsof \ grep '*:'&nbsp;</p> <p>or</p> <p>\$ sudo netstat \--tulp</p> <p>Much more detailed information regarding services is available in the CIS benchmark documents.</p> <p>Red Hat also provides a text-based interface for changing startup services: ntsysv</p> <p>For example, the command</p> <p>ntsysv \--level 345</p> <p>configures runlevels 3, 4, and 5.</p>
21	<p>If no xinetd services are required, disable xinetd altogether:</p> <p>sudo service xinetd stop; sudo chkconfig xinetd off</p>

25	<p>RHEL7 comes with firewalld, however iptables may be installed and used instead. This is documented at: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Using_Firewalls.html (https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Using_Firewalls.html)</p> <p>POLICIES ~ (/POLICIES)</p> <p>RESEARCH (/CONSENSUS) SUPPORT TOPICS ~ (/EDUCATION-OUTREACH)</p> <p>Below is a list of some iptables resources:</p> <p>http://firehol.sourceforge.net (http://firehol.sourceforge.net/)</p> <p>http://sourceforge.net/projects/fwbuilder (http://sourceforge.net/projects/fwbuilder)</p> <p>http://www.simonzone.com/software/guarddog (http://www.simonzone.com/software/guarddog)</p> <p>REPORT VIOLATION (/VIOLATION) CONTACT (/CONTACT)</p> <p>Q SEARCH</p>
33	<p>If you decide to utilize <u>SSH</u> (http://www.openssh.com/), the ISO highly recommends the following:</p> <ul style="list-style-type: none"> • 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 almost always only attack port 22 since most people do not change the default port. • Use SSH2 (by setting Protocol 2 in the sshd_config file) as it remediates many vulnerabilities from SSH1. • Restrict access to the SSH port using a hardware or software firewall. • If possible, use keys with passphrase instead of just passwords. To create rsa keys, follow these commands: <ul style="list-style-type: none"> ◦ 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. <p>You may also want to visit the <u>SSL Web site</u> (http://www.openssl.org/).</p>
34	<p>INFO is a basic logging level that will capture user login and logout activity. Other logging levels may be used, but may generate more noise. The DEBUG logging level is not recommended for production servers.</p>
35	<p>Do not permit root logins via SSH. If root access over SSH is absolutely necessary, require administrators to authenticate with an individual account first and then use su or sudo. This is to prevent remote brute force attacks against the root user account as well as to create an audit trail of administrative activity in the event of a compromise.</p>
37	<p>There is a license fee for Tripwire. The Tripwire management console can be very helpful for managing more complex installations.</p> <p>AIDE is a free tool available from SourceForge (http://sourceforge.net/projects/aide).</p> <p>SamHain (http://la-samhna.de/samhain/) is another free tool, as is OSSEC HIDS (http://www.ossec.net/).</p>

38	<p>Many resources exist for understanding and configuring SELinux:</p> <ul style="list-style-type: none"> • http://www.selinuxproject.org/page/Main_Page (http://www.selinuxproject.org/page/Main_Page) • https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/SELinux_Users_and_Administrators_Guide/ (https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/SELinux_Users_and_Administrators_Guide/) <p>SELinux is enabled by default with RHEL systems and should not be disabled unless absolutely necessary.</p>
39	<p>OSSEC is a free, open-source host-based intrusion detection system, which performs log analysis, file integrity checking, and rootkit detection, with real time alerting, in an effort to identify malicious activity. It is available at http://www.ossec.net/ (http://www.ossec.net/).</p>
40	<p>ITS Networking operates two stratum 2 NTPv4 (NTP version 4) servers for <u>network time synchronization services for university network administrators</u> (http://www.utexas.edu/its/ntp/).</p>
41	<p>Auditd monitors various system activity, such as system logins, authentications, account modifications, and SELinux denials. These records may help administrators identify malicious activity or unauthorized access.</p>
42	<p>Rsyslog is a third-party package which is intended to replace the standard syslog daemon. The CIS benchmark has several recommendations for configuring rsyslog. Some benefits of rsyslog include transmission of logs over TCP and support for encryption of log data when transmitting over a network.</p>
44	<p>It is highly recommended that logs are shipped from any Category I devices to a service like Splunk, which provides log aggregation, processing, and real-time monitoring of events among many other things. This helps to ensure that logs are preserved and unaltered in the event of a compromise, in addition to allowing proactive log analysis of multiple devices.</p> <p>Splunk licenses are available through ITS at no charge. ITS also maintains a centrally-managed Splunk service that may be leveraged.</p>
45	<ul style="list-style-type: none"> • 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 <u>John the Ripper</u> (http://www.openwall.com/john/) • Seek approval from <u>IT Owner</u> (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.

46 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
- Q SEARCH

Warn will report alerts to syslog.

- 48** To require strong passwords, in compliance with section 5.18 of the Information Resources Use and Security Policy:
- For RHEL 6: **HOME (/)** **QUICK LINKS ^ (/)** **POLICIES ^ (/POLICIES)**
- In /etc/pam.d/system-auth, add or change the file as required to read:
- password required pam_cracklib.so
 retry=3 difok=5 minlen=8 lcredit=-1 dcredit=-1 ocredit=-1
 password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok
 remember=10
 password required pam_deny.so
 password required pam_warn.so**
- For RHEL 7:
- In /etc/security/pwquality.conf, add:
- difok = 5
 minlen = 8
 minclass = 1
 maxrepeat = 0
 maxclassrepeat = 0
 lcredit = -1
 ucredit = 0
 dcredit = -1
 ocredit = -1
 gecoscheck = 1**
- In /etc/pam.d/system-auth, add or change the file as required to read:
- password required pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
 password sufficient pam_unix.so sha512 shadow try_first_pass use_authtok remember=10
 password required pam_deny.so**
- 49** 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.

50	<p>The text of the <u>university's official warning banner</u> (http://security.utexas.edu/policies/login_banner.html) can be found on the ITS Web site. You may add localized information to the banner as long as the university banner is included.</p> <p>HOME (/) QUICK LINKS ~ (/) POLICIES ~ (/POLICIES)</p>
51	<p>The text of the <u>university's official warning banner</u> (http://security.utexas.edu/policies/login_banner.html) can be found on the ITS Web Site. You may add localized information to the banner as long as the university banner is included.</p> <p>RESEARCH (/CONSENSUS) SUPPORT TOPICS ~ (/EDUCATION-OUTREACH)</p> <p>REPORT VIOLATION (/VIOLATION) CONTACT (/CONTACT)</p>
52	<p>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 <u>exception process</u> (https://security.utexas.edu/exception/).</p> <p>Q&A</p> <p>You may choose any proven anti-virus product. One option is ClamAV (http://www.clamav.net/).</p>
53	<p>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 <u>exception process</u> (https://security.utexas.edu/exception/).</p>
54	<p>There are a variety of methods available to provide encrypted storage. Two good candidates are <u>LUKS</u> (https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-LUKS_Disk_Encryption.html) and GNUPG (http://www.gnupg.org/) (free).</p>



(<https://www.youtube.com/channel/UC45Gmiso>) (https://www.facebook.com/ut_iso/)

[HOME \(/\)](#)[QUICK LINKS ^ \(/\)](#)[POLICIES ^ \(/POLICIES\)](#)

INFORMATION SECURITY OFFICE

[RESEARCH \(/CONSENSUS\)](#)[SUPPORT TOPICS ^ \(/EDUCATION-OUTREACH\)](#)

Copyright © 2008-20, Information Security Office. All rights reserved.

[Privacy Policy](#) (<https://www.utexas.edu/web-privacy-policy>) | [Accessibility Policy](#) (<https://www.utexas.edu/web-accessibility-policy>)

[REPORT VIOLATION \(/VIOLATION\)](#) — [CONTACT \(/CONTACT\)](#)

Q SEARCH

 **TEXAS** (<https://www.utexas.edu/>)

