Red Hat Enterprise Linux 7 Hardening Checklist

The hardening checklists are based on the comprehensive checklists produced by CIS. The Information Security Office 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 # 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 Enterprise Linux 7 Benchmark v1.1.0. 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 data, required steps are denoted with the **!** symbol. All steps are recommended.
Cat II/III - For systems that include Category-II or -III data, 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 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 Physical Security					
1		If machine is a new install, protect it from hostile network traffic until the operating system is installed and hardened.		§	**!**	**!**	5.1
2		Set a BIOS/firmware password.			**!**		4.1
3		Configure the device boot order to prevent unauthorized booting from alternate media.					
4		Use the latest version of RHEL possible.	1.7		**!**	**!**	5.2
		Filesystem Configuration					
5		Create a separate partition with the nodev, nosuid, and noexec options set for /tmp.	1.1.1-.4	§			
6		Create separate partitions for /var, /var/log, /var/log/audit, and /home.	1.1.{5,7,8,9}	§			
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	§	**!**	**!**	5.2
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	§			
14		Set boot loader password.	1.5.3				
15		Remove the X Window system.	3.2	§			

16		Disable X Font Server.					
		Process Hardening					
17		Restrict core dumps.	1.6.1	§			
18		Enable Randomized Virtual Memory Region Placement.	1.6.2	§	!		
		OS Hardening					
19		Remove legacy services (e.g., telnet-server; rsh, rlogin, rcp; ypserv, ypbind; tftp, tftp-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.		§	!	!	5.4
21		Remove xinetd, if possible.	2.1.11	§	!		
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.)			!		5.4
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	§	!	!	5.5
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	§	!	!	5.6
34		Set SSH LogLevel to INFO.	6.2.2	§	!	!	
35		Disable SSH Root login.	6.2.8	§			
36		Set SSH PermitEmptyPasswords to No.	6.2.9		!	!	
		System Integrity and Intrusion Detection					
37		Install and configure AIDE.	1.3.1-.2	§			5.8
38		Configure SELinux.	1.4.1-.6	§			
39		Install and configure OSSec HIDS.		§			
		Logging					
40		Configure Network Time Protocol (NTP).	3.6	§	!		
41		Enable system accounting (auditd).	5.2	§	!		6.1
42		Install and configure rsyslog.	5.1.1-.4	§	!		
43		All administrator or root access must be logged.			!		6.4
44		Configure log shipping to separate device/service (e.g. Splunk).	5.1.5	§			
		Files/Directory Permissions/Access					
45		Integrity checking of system accounts, group memberships, and their associated privileges should be enabled and tested.		§	!		5.9
		PAM Configuration					
46		Ensure that the configuration files for PAM, /etc/pam.d/* are secure.	6.3	§	!	!	5.12
47		Upgrade password hashing algorithm to SHA-512.	6.3.1		!		
48		Set password creation requirements.	6.3.2	§	!	!	
49		Restrict root login to system console.	6.4	§			
		Warning Banners					
50		If network or physical access services are running, ensure the university warning banner is displayed.	6.2.14, 8.1	§	!	!	5.10
51		If the system allows logins via a graphical user interface, ensure the university warning banner is displayed prior to login.	8.3	§	!		
		Anti-Virus Considerations					

52		Install and enable anti-virus software.		§			3.1
53		Configure to update signature daily on AV.		§			3.3
		Additional Security Notes					
54		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.		§	!	!	5.7

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.
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	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`

13	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.

15	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:`

17	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.
18	Add the following line to the /etc/sysctl.conf file: `kernel.randomize_va_space = 2`

20	Disable any xinetd services you do not absolutely require by setting "disable=yes" in /etc/xinetd.d/*.
	
	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.
	
	Unnecessary services can be disabled with:
	
	`$ sudo chkconfig off`
	
	To check what services are listening use:
	
	`$ lsof  | grep '*:' `
	
	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.

21	If no xinetd services are required, disable xinetd altogether: `sudo service xinetd stop; sudo chkconfig xinetd off`
25	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 Below is a list of some iptables resources: http://firehol.sourceforge.net http://sourceforge.net/projects/fwbuilder http://www.simonzone.com/software/guarddog

33	If you decide to utilize SSH, 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 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:
	
	`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.

34	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.

35	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.
37	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. SamHain is another free tool, as is OSSEC HIDS.
38	Many resources exist for understanding and configuring SELinux: • 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/ SELinux is enabled by default with RHEL systems and should not be disabled unless absolutely necessary.
39	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/.
40	ITS Networking operates two stratum 2 NTPv4 (NTP version 4) servers for network time synchronization services for university network administrators.
41	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.
42	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.
44	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. Splunk licenses are available through ITS at no charge. ITS also maintains a centrally-managed Splunk service that may be leveraged.
45	• 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 • Seek approval from IT 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 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:
	
	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	The text of the university's official warning banner can be found on the ITS Web site. You may add localized information to the banner as long as the university banner is included.
51	The text of the university's official warning banner can be found on the ITS Web site. You may add localized information to the banner as long as the university banner is included.
52	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. You may choose any proven anti-virus product. One option is ClamAV.
53	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.
54	There are a variety of methods available to provide encrypted storage. Two good candidates are LUKS and GNUPG (free).