Red Hat Enterprise Linux 5 (RHEL5) Hardening Document

Prepared By

Information Security Group (ISG)

Document Details:

Document Name	Red Hat Enterprise Linux (RHEL 5) Hardening Document
Business	Reliance Retail
Department	
Document Creation Date	02.08.2008
Complied by	Manas Ranjan Biswal and Kishan Kendre
Reviewed by	Rama Mohan V.V.S and Puneet Dahiya
Approved by	Sh. D.P.Dube

Red Hat Enterprise Linux 5 Document

Contact Information:

All clarifications and further information regarding the contents of this document can be requested from the following person(s):

	Primary contact	Secondary contact
Name	Puneet Dahiya	Rama Mohan V.V.S
E-mail	Puneet.dahiya@ril.com	Ramamohan.vatyam@ril.com
Mobile	+91-9987004475	+91-9987001939
Office Phone	+91-22-44772511	+91-22-44772333
Office Address		

RHEL 5 OS HARDENING

1.0	**PATCHES, PACKAGES AND INITIAL LOCKDOWN**
1.1	Apply the latest OS patches.
1.2	Configure (IP/Host based) SSH.
2.0	**MINIMIZATION OF XINETD NETWORK SERVICES**
2.1	Disable the standard xinetd services. *Refer: Annexure A*
2.2	Configure TCP Wrappers and Firewall to limit access to the Server.
2.3	Disable Telnet.
2.4	Disable FTP.
2.5	Disable rlogin/rsh/rcp.
2.6	Disable TFTP Server.
2.7	Disable dovcot.
3.0	**MINIMIZATION OF BOOT SERVICES**
Change the inetd/boot services according to the recommendation. *Refer: Annexure B*	
3.1	Set the System daemon umask to at least 027.
3.2	Disable xinetd Services. (If inetd services are disabled, then xineted services should be disabled)
3.3	Disable GUI login (X Windows).

PCI Compliance Red Hat Enterprise Linux 5 Document

3.4	Disable X Font Server.
3.5	Disable all the Standard Boot services. *Refer: Annexure B*
3.6	Disable SMB (Windows File Sharing) processes.
3.7	Disable NFS Server processes.
3.8	Disable NFS Client processes.
3.9	Disable NIS Server processes.
3.10	Disable NIS Client processes.
3.11	Disable the RPC Portmap process.
3.12	Disable netfs script.
3.13	Disable the Printer Daemon processes.
3.14	Disable Web Server processes. *Refer: Annexure B*
3.15	Disable SNMP processes.
3.16	Disable DNS Server process.
3.17	Disable SQL Server processes.
3.18	Disable Squid Cache Server.
3.19	Disable Kudzu hardware detection.
4.0	**SYSTEM NETWORK PARAMETER TUNING**
4.1	Set net.ipv4.tcp_max_syn_backlog=4096

PCI Compliance Red Hat Enterprise Linux 5 Document

4.2	Set net.ipv4.tcp_syncookies=1
5.0	**LOGGING**
5.1	Save the messages sent to Syslog AUTHPRIV facility in \etc\log\secure file.
5.2	Restrict permissions on System Log files to users.
5.3	Configure syslogd to send logs to a remote LogHost.
6.0	**FILE AND DIRECTORY PERMISSIONS/ACCESS**
6.1	Add 'nodev' option to appropriate partitions in /etc/fstab.
6.2	Add 'nosuid' and 'nodev' option for removable media in /etc/fstab.
6.3	Disable user-mounted removable file systems.
6.4	Set passwd, shadow and group file permissions to 644.
6.5	Check for all unauthorized SUID/SGID System executables. If present, then remove.
6.6	Check for all unowned directories and files. If present, then remove.
6.7	Disable the USB devices.
7.0	**SYSTEM ACCESS, AUTHENTICATION AND AUTHORIZATION**
7.1	Remove .rhosts support in PAM Configuration Files.
7.2	Prevent X Server from listening on Port 6000/tcp.
7.3	Restrict at/cron to other users.

PCI Compliance Red Hat Enterprise Linux 5 Document

7.4	Restrict permissions on the crontab files.
7.5	Restrict root logins to system console.
7.6	Set GRUB password.
7.7	Authentication for Single-User mode should be created
7.8	Restrict NFS client requests to the privileged ports.
7.9	Disable Syslog to accept messages.
8.0	**USER ACCOUNTS AND ENVIRONMENT**
8.1	Block login to system accounts.
8.2	No accounts should be with empty password fields.
8.3	Set account expiration parameters on the active accounts.
8.4	Do not include '.' or Group/World-writable directory in Root's $PATH.
8.5	User Home Directories should be Mode 0750.
8.6	User Dot-Files should not be World-Writable.
8.7	Set default umask for users.
8.8	Limit access to the Root account from su.
9.0	**WARNING BANNERS**
9.1	Create warning messages while attempting to log on.

PCI Compliance Red Hat Enterprise Linux 5 Document

10.0 MISC ODDS AND ENDS	
10.1	Enable and configure the auditd and sysstat services.
10.2	Check for the existence of any duplicate userIDs. If present, then remove.
10.3	Force permissions on root's home directory to be 0700.
10.4	Utilize PAM to enforce UserID password complexity.
10.5	Restrict permissions to 0644 on /usr/share/man and /usr/share/doc content.
10.6	Set permissions on cron scripts known to be executed by cron to be 0600.
11.0 ADDITIONAL SECURITY MEASURES	
13.1	Enable TCP SYN cookie protection.
13.2	Remove unnecessary packages associated with the startup scripts.
13.3	Do not install any unnecessary package & evaluate every installed package.
13.4	Install and configure sudo.
13.5	Remove all compilers and assemblers.
13.6	Ensure that no unauthorized/duplicate UID 0 accounts exist.

PCI Compliance Red Hat Enterprise Linux 5 Document

ANNEXURE – A:

Xinetd Services	Red Hat default state	Recommendation
amanda: amandaidx:	off off	off off
amidxtape: auth:	off off	off off
chargen-dgram: chargen-stream:	off off	off off
cvs: daytime-dgram:	off off	off off
daytime-stream: discard-dgram:	off off	off off
discard-stream: echo-dgram:	off off	off off
echo-stream eklogin:	off off	off off
ekrb5-telnet: gssftp:	off off	off off
klogin: krb5-telnet:	off off	off off
kshell: ktalk:	off off	off off
ntalk: rexec:	off off	off off
rlogin: rsh:	off off	off off
rsync: talk:	off off	off off
tcpmux-server: telnet:	off off	off off
tftp: time-dgram:	off off	off off
time-stream: uucp:	off off	off off

PCI Compliance Red Hat Enterprise Linux 5 Document

ANNEXURE – B:

3.5	Standard Boot Services			
	apcid	hidd	netplugd	rusersd
	amd	hplip	network	rwhod
	anacron	httpd	NetworkManager	saslauthd
	apmd	ibmasm	nfs	sendmail
	arptables_jf	ip6tables	nfslock	setroubleshoot
	aprwatch	ipmi	nscd	smartd
	atd	irda	ntpd	smb
	autofs	iscsi	openibd	snmpd
	avahi-daemon	iscsid	ospf6d	snmptrapd
	avahi-dnsconfd	isdn	ospfd	spamassassin
	bpgd	kadmin	pand	squid
	bluetooth	kdump	pcscd	tog-pegasus
	bootparamd	kprop	portmap	tomcat5
	capi	krb524	postgresql	tux
	conman	krb5kdc	privoxy	winbind
	cups	kudzu	psacct	wine
	cyrus-imapd	ldap	radvd	wpa_supplicant
	dc_client	lisa	rarpd	xend
	dc_server	lm_sensors	rdisc	xendomains
	dhcdbd	mailman	readahead_early	xfs
	dhcp6s	mcstrans	readahead_later	xinetd
	dhcpd	mdmonitor	rhnsd	ypbind
	dhcrelay	mdmpd	ripd	yppasswdd
	dovecot	microcode_ctl	ripngd	ypserv
	dund	multipathd	rpcgssd	ypxfrd
	firstboot	mysqld	rpcidmapd	yum-updatesd
	gpm	named	rpcsvcgssd	zebra
	haldaemon	netfs	rstatd	

PCI Compliance Red Hat Enterprise Linux 5 Document

3.14	Mention the Web Server used. If Apache is required, Hardening of Apache Web server is required.			
3.0	**INETD/BOOT SERVICES**	**DEFAULT BOOT STATE APPLICABLE TO EACH LEVEL**	**RECOMMENDATION LEVEL 3**	**LEVEL 5**
	Acpid amd	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Anacron apmd	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off
	arptables_jf arpwatch	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Atd **auditd**	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off on	off on
	Autofs avahi-daemon	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:on 4:on 5:on 6:off	off off	off off
	avahi-dnsconfd bgpd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Bluetooth bootparamd	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Capi conman	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	cpuspeed **crond**	0:off 1:on 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	on on	on on
	Cups cyrus-imapd	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	dc_ client dc_server	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Dhcdbd dhcp6s	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Dhcpd dhcrelay	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	dovecot dund	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	firstboot gpm	0:off 1:off 2:off 3:on 4:off 5:on 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off
	haldaemon hidd	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off
	hplip httpd	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Ibmasm innd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	ip6tables ipmi	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	iptables irda	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	on off	on off
	Irqbalance iscsi	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:on 4:on 5:on 6:off	on off	on off
	Iscsid isdn	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off
	Kadmin kdump	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Kprop krb524	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	krb5kdc	0:off 1:off 2:off 3:off 4:off 5:off 6:off	off	off

PCI Compliance Red Hat Enterprise Linux 5 Document

	kudzu	0:off 1:off 2:off 3:on 4:on 5:on 6:off	off	off
	ldap lisa	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	lm_sensors mailman	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	mcstrans mdmonitor	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off of	off off
	mdmpd **messagebus**	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	of on	off on
	microcode_ctl multipathd	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	mysqld named	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	netfs netplugd	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	network NetworkManager	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	NetworkManagerDispatcher nfs	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	on off	on off
	nfslock nscd	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	ntpd openibd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off
	ospf6d ospfd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	pand pcscd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off
	portmap postgresql	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	privoxy psacct	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	radiusd radvd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Rarpd rdisc	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	readahead_early readahead_later	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:off 4:off 5:on 6:off	off off	off off
	Restorecond rhnsd	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:on 4:on 5:on 6:off	on off	on off
	Ripd ripngd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Rpcgssd rpcidmapd	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:off 3:on 4:on 5:on 6:off	off off	off off
	Rpcsvcgssd rstatd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Rusersd rwhod	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	saslauthd sendmail	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off
	setroubleshoot smartd	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off

PCI Compliance Red Hat Enterprise Linux 5 Document

	smb snmpd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	snmptrapd spamassassin	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Squid **sshd**	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off on	off on
	syslog **sysstat**	0:off 1:off 2:on 3:on 4:on 5:on 6:off 0:off 1:off 2:on 3:on 4:off 5:on 6:off	on on	on on
	tog-pegasus tomcat5	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	tux vncserver	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	vsftpd winbind	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	wpa_supplicant xend	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off
	xendomains xfs	0:off 1:off 2:off 3:on 4:on 5:on 6:off 0:off 1:off 2:on 3:on 4:on 5:on 6:off	off off	off off
	Xinetd ypbind	0:off 1:off 2:off 3:on 4:on 5:on 6:off\ 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Yppasswdd ypserv	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:off 4:off 5:off 6:off	off off	off off
	Ypxfrd yum-updatesd	0:off 1:off 2:off 3:off 4:off 5:off 6:off 0:off 1:off 2:off 3:on 4:on 5:on 6:off	off off	off off
	zebra	0:off 1:off 2:off 3:off 4:off 5:off 6:off	off	off

PCI Compliance Red Hat Enterprise Linux 5 Document