FINCSIRT

Red Hat Linux| CentOS Server Hardening Guide

v. 1.0

Contents

Introduction

This manual is based on the CIS Benchmark and it is a derived version which address the must have security controls which the servers need to be implemented with and hardened. This guide covers the Red Hat Enterprise Linux 7 which is the latest version in Red Hat. FINCSIRT recommends that you always use the latest OS and the security patches to stay current on security.

Server Hardening Policy

FINCSIRT highly recommend that the organization have a minimum security standard hardening policy and to that, this guide can be attached as an annexure. Purpose of the policy will be to make sure any server that is deployed and going to be deployed to be properly hardened and maintain a baseline security standard while uplifting the internal information security resiliency against rapidly advancing threats.

1. Filesystem Configuration

1.1. Create Separate Partition for /tmp with nodev, nosuid and noexec options

The /tmp directory is a world-writable directory used for temporary storage by all users and some applications.

Red Hat Enterprise Linux 7

*Edit the file /etc/fstab. Add the text **nodev, nosuid, noexec** to the list of mount options in column 4.*

- *The **nodev** mount option specifies that the filesystem cannot contain special devices*
- *The **nosuid** mount option specifies that the filesystem cannot contain set userid files.*
- *The **noexec** mount option specifies that the filesystem cannot contain executable binaries.*

1.2. Create separate partitions for /var, /var/log, /var/log/audit, and /home

The /var directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.

The /var/log directory is used by system services to store log data.

The auditing daemon, auditd, stores log data in the /var/log/audit directory.

Red Hat Enterprise Linux 7

For new installations, check the box to "Review and modify partitioning" and create a separate partition for /var, /var/log, /var/log/audit, and /home.

For systems that were previously installed, use the Logical Volume Manager (LVM) to create partitions.

1.3. Bind Mount the /var/tmp directory to /tmp

Binding /var/tmp to /tmp establishes an unbreakable link to /tmp that cannot be removed (even by the root user). It also allows /var/tmp to inherit the same mount options that /tmp owns, allowing /var/tmp to be protected in the same /tmp is protected.

Red Hat Enterprise Linux 7

 # mount --bind /tmp /var/tmp

and edit the /etc/fstab file to contain the following line:

/tmp /var/tmp none bind 0 0

1.4. Add nodev Option to /home

When set on a file system, this option prevents character and block special devices from being defined, or if they exist, from being used as character and block special devices.

Red Hat Enterprise Linux 7

Edit the /etc/fstab file and add nodev to the fourth field (mounting options) for /home mount entry

1.5. Set nodev, nosuid, and noexec options on /dev/shm

The nodev mount option specifies that the /dev/shm (temporary filesystem stored in memory) cannot contain block or character special devices.

The nosuid mount option specifies that the /dev/shm (temporary filesystem stored in memory) will not execute setuid and setgid on executable programs as such, but rather execute them with the uid and gid of the user executing the program.

Set noexec on the shared memory partition to prevent programs from executing from there.

Red Hat Enterprise Linux 7

Edit the /etc/fstab file and add nodev, nosuid, noexec to the fourth field (mounting options). Look for entries that have mount points that contain /dev/shm.

2. System Updates

2.1. Verify Red Hat GPG Key is installed and check enabled

Red Hat cryptographically signs updates with a GPG key to verify that they are valid.

Red Hat Enterprise Linux 7

Compare the GPG fingerprint with the one from Red Hat's web site at http://www.redhat.com/security/team/key. The following command can be used to print the installed release key's fingerprint, which is actually contained in the file referenced below:

 # gpg --quiet --with-fingerprint /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

The gpgcheck option, found in the main section of the /etc/yum.conf file determines if an RPM package's signature is always checked prior to its installation.

Red Hat Enterprise Linux 7

Edit the /etc/yum.conf file and set the gpgcheck to 1 as follows:

gpgcheck=1

3. Boot Loader Security

3.1. Secure the Boot Loader

Set user/group owner to root, and permissions to read and write for root only, on /boot/grub2/grub.cfg.

Red Hat Enterprise Linux 7

 # chown root:root /boot/grub2/grub.cfg

This changes the owner of the file to root

#chmod og-rwx /boot/grub2/grub.cfg

This removes Read , Write , Execute permissions from Group and Others.

3.2. Set 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

Red Hat Enterprise Linux 7

 # grub2-mkpasswd-pbkdf2

Enter password: <password>

Reenter password: <password>

Your PBKDF2 is <encrypted-password>

Add the following into /etc/grub.d/00_header or a custom /etc/grub.d configuration file:

cat <<EOF

set superusers="<user-list>"

password_pbkdf2 <user> <encrypted-password>

EOF

Run the following to update the grub configuration:

 # grub2-mkconfig -o /boot/grub2/grub.cfg

4. Process Hardening

4.1. Restrict Core dumps

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user. Setting a hard limit on core dumps prevents users from overriding the soft variable.

Red Hat Enterprise Linux 7

Add the following line to the /etc/security/limits.conf file.

** hard core 0*

Add the following line to the /etc/sysctl.conf file.

fs.suid_dumpable = 0

4.2. Enable Randomized Virtual Memory Region Placement

Set the system flag to force randomized virtual memory region placement. Randomly placing virtual memory regions will make it difficult for to write memory page exploits as the memory placement will be consistently shifting.

Red Hat Enterprise Linux 7

Add the following line to the /etc/sysctl.conf file.

kernel.randomize_va_space = 2

5. Operating System Hardening

5.1. Remove Legacy Services

Existence of legacy applications with existing security vulnerabilities is a major security risk for any kind of system.

Red Hat Enterprise Linux 7

#yum erase telnet-server telnet

This will remove telnet server and clients

 # yum erase rsh-server rsh

This will remove the Berkeley rsh-server and related binaries

 # yum erase ypserv ypbind

This will remove the NIS server and related binaries

 # yum erase tftp-server tftp

This will remove the Tftp server and related binaries

 # yum erase talk talk-server

This will remove the Talk server and related binaries

5.2. Remove xinetd

The eXtended InterNET Daemon (xinetd) is an open source super daemon that replaced the original inetd daemon. The xinetd daemon listens for well-known services and dispatches the appropriate daemon to properly respond to service requests.

Red Hat Enterprise Linux 7

 # yum erase xinetd

5.3. Disable Legacy Services

Existence of legacy services with existing security vulnerabilities is a major security risk for any kind of system.

Red Hat Enterprise Linux 7

 # chkconfig chargen-dgram off

 # chkconfig chargen-stream off

 # chkconfig daytime-dgram off

 # chkconfig daytime-stream off

 # chkconfig echo-dgram off

 # chkconfig echo-stream off

 # chkconfig tcpmux-server off

*** At the same time remove any services which are not being utilized (e.g., FTP, DNS, LDAP, SMB, DHCP, NFS, SNMP, etc.)*

5.4. Set Daemon umask

Set the default umask for all processes started at boot time. Setting the umask to 027 will make sure that files created by daemons will not be readable, writable or executable by any other than the group and owner of the daemon process and will not be writable by the group of the daemon process.

Red Hat Enterprise Linux 7

Add the following line to the /etc/sysconfig/init file.

umask 027

6. Network Service Hardening

6.1. Enable a Firewall

Restrict the access to the services for relevant end users using a firewall. RHEL consist of iptables which is a firewall.

Red Hat Enterprise Linux 7

 # systemctl enable firewalld

6.2. Disable IP forwarding.

The net.ipv4.ip_forward flag is used to tell the server whether it can forward packets or not. If the server is not to be used as a router, this ensures that a server with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Red Hat Enterprise Linux 7

Set the net.ipv4.ip_forward parameter to 0 in /etc/sysctl.conf:

net.ipv4.ip_forward=0

Modify active kernel parameters to match:

 # /sbin/sysctl -w net.ipv4.ip_forward=0

 # /sbin/sysctl -w net.ipv4.route.flush=1

6.3. Disable send packet redirects.

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

Red Hat Enterprise Linux 7

Set the net.ipv4.conf.all.send_redirects&net.ipv4.conf.default.send_redirects parameters in /etc/sysctl.conf:

net.ipv4.conf.all.send_redirects=0

net.ipv4.conf.default.send_redirects=0

Modify active kernel parameters to match:

 # /sbin/sysctl -w net.ipv4.conf.all.send_redirects=0

 # /sbin/sysctl -w net.ipv4.conf.default.send_redirects=0

 # /sbin/sysctl -w net.ipv4.route.flush=1

6.4. Disable ICMP Redirect Acceptance

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Red Hat Enterprise Linux 7

Set the net.ipv4.conf.all.accept_redirects and

net.ipv4.conf.default.accept_redirects parameters to 0 in /etc/sysctl.conf:

net.ipv4.conf.all.accept_redirects=0

net.ipv4.conf.default.accept_redirects=0

Modify active kernel parameters to match:

 # /sbin/sysctl -w net.ipv4.conf.all.accept_redirects=0

 # /sbin/sysctl -w net.ipv4.conf.default.accept_redirects=0

 # /sbin/sysctl -w net.ipv4.route.flush=1

6.5. Enable Ignore Broadcast Requests

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Red Hat Enterprise Linux 7

Set the net.ipv4.icmp_echo_ignore_broadcasts parameter to 1 in /etc/sysctl.conf:

net.ipv4.icmp_echo_ignore_broadcasts=1

Modify active kernel parameters to match:

 # /sbin/sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1

 # /sbin/sysctl -w net.ipv4.route.flush=1

6.6. Enable Bad Error Message Protection

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages

Red Hat Enterprise Linux 7

Set the net.ipv4.icmp_ignore_bogus_error_responses parameter to 1 in /etc/sysctl.conf:

net.ipv4.icmp_ignore_bogus_error_responses=1

Modify active kernel parameters to match:

 # /sbin/sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1

 # /sbin/sysctl -w net.ipv4.route.flush=1

6.7. Enable Bad Error Message Protection

Attackers use SYN flood attacks to perform a denial of service attacked on a server by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the server to keep accepting valid connections, even if under a denial of service attack.

Red Hat Enterprise Linux 7

Set the net.ipv4.tcp_syncookies parameter to 1 in /etc/sysctl.conf:

net.ipv4.tcp_syncookies=1

Modify active kernel parameters to match:

 # /sbin/sysctl -w net.ipv4.tcp_syncookies=1

 # /sbin/sysctl -w net.ipv4.route.flush=1

7. Remote Administration Hardening

7.1. Set SSH protocol to 2

SSH v1 suffers from insecurities that do not affect SSH v2

Red Hat Enterprise Linux 7

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

Protocol 2

7.2. Reduce Unnecessary Logs

SSH provides several logging levels with varying amounts of verbosity. DEBUG is specifically not recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information. INFO level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

Red Hat Enterprise Linux 7

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

LogLevel INFO

7.3. Disable SSH Root login.

Disallowing root logins over SSH requires server admins to authenticate using their own individual account, then escalating to root via sudo or su. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Red Hat Enterprise Linux 7

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

PermitRootLogin no

7.4. Block login to accounts with empty passwords

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

Red Hat Enterprise Linux 7

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

PermitEmptyPasswords no

7.5. Set SSH Banner

Banners are used to warn connecting users of the particular site's policy regarding connection. Consult with your legal department for the appropriate warning banner for your site.

Red Hat Enterprise Linux 7

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

Banner /etc/issue.net

8. System Logging

8.1. Configure Network Time Protocol (NTP)

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured as NTP clients to synchronize their clocks (especially to support time sensitive ecurity mechanisms like Kerberos). This also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Red Hat Enterprise Linux 7

Set the following restrict parameters in /etc/ntp.conf:

restrict default kod nomodify notrap nopeer noquery

restrict -6 default kod nomodify notrap nopeer noquery

Also, make sure /etc/ntp.conf has an NTP server specified:

server <ntp-server>

Note: <ntp-server> is the IP address or hostname of a trusted time server. Configuring an NTP server is outside the scope of this document.

Ensure -u ntp:ntp in options in /etc/sysconfig/ntpd:

OPTIONS="-u ntp:ntp"

8.2. Enable system accounting

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Red Hat Enterprise Linux 7

 # systemctl enable auditd

** It is recommended to configure auditd daemon per organizational policies to ensure proper audit trails*

8.3. Install and configure rsyslog.

The security enhancements of rsyslog such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

Red Hat Enterprise Linux 7

 # yum install rsyslog

 # systemctl enable rsyslog

This will install and activate rsyslog client on the system

Edit the following lines in the /etc/rsyslog.conf file as appropriate for your environment:

auth,user. /var/log/messages*

kern. /var/log/kern.log*

daemon. /var/log/daemon.log*

syslog. /var/log/syslog*

lpr,news,uucp,local0,local1,local2,local3,local4,local5,local6. /var/log/unused.log*

Execute the following command to restart rsyslogd

 # pkill -HUP rsyslogd

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 file, 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>

8.4. Configure rsyslog to Send Logs to a Remote Log Host

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

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

Note: The double "at" sign (@@) directs rsyslog to use TCP to send log messages to the server, which is a more reliable transport mechanism than the default UDP protocol.

9. Authentication Module (PAM) configuration

9.1. Upgrade password hashing algorithm to SHA-512

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

Red Hat Enterprise Linux 7

#authconfig --passalgo=sha512 –update

If existing users were created without the sha512, it is recommended to force reset al user account passwords

9.2. Set password creation requirements.

Strong passwords protect systems from being hacked through brute force methods.

Red Hat Enterprise Linux 7

Set the pam_pwquality.so parameters as follows in /etc/pam.d/system-auth

password requisite pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=

Set the following settings in /etc/security/pwquality.conf:

minlen=14 -- password must be 14 characters or more

dcredit=-1 -- provide at least 1 digit

ucredit=-1 -- provide at least one uppercase character

ocredit=-1 -- provide at least one special character

lcredit=-1 -- provide at least one lowercase character

----------End----------