**SECURE DELIVERY LIFECYCLE FOR**

**Linux RedHat**

**ICT Security Compliances and certification**

**25/01/2017**

Index

[1 SCOPE AND APPLICATION 3](#_Toc445308807)

[2 HARDENING CHECHKLIST LINUX 3](#_Toc445308808)

[2.1 grub password and Boot option 3](#_Toc445308809)

[2.2 Filesystem Configuration 4](#_Toc445308810)

[2.3 Disable System Accounts 7](#_Toc445308811)

[2.4 Additional Process Hardening 7](#_Toc445308812)

[2.5 Configure SSH 8](#_Toc445308813)

[2.6 IPtables 10](#_Toc445308814)

[2.7 Advanced Intrusion Detection Enviroment (Aide) 10](#_Toc445308815)

[2.8 Os Services 10](#_Toc445308816)

[2.9 Special Purpose Services 12](#_Toc445308817)

[2.10 Network Configuration and Firewalls 16](#_Toc445308818)

[2.11 Configure IPV6 20](#_Toc445308819)

[2.12 Configure PAM 20](#_Toc445308820)

[2.13 Warning Banners 21](#_Toc445308821)

[2.14 System maintenance 21](#_Toc445308822)

1. SCOPE AND APPLICATION

The following document may be applied to hardening processes of operating systems.

This guideline’s aim is to integrate and increase all the current security policies of the organization.

It’s focused on Red Hat 7 distribution and designed according to the highest standards of security in IT field like CIS (Center of internet security) Redhat Guidelines.

1. HARDENING CHECHKLIST LINUX

***Disable Interactive Boot***

The PROMPT option provides console users the ability to interactively boot the system and select which services to start on boot .

Set the PROMPT parameter in /etc/sysconfig/init to no.

PROMPT=no

## Filesystem Configuration

***Create Separate Partition for /tmp***

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

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

***Set nodev option for /tmp Partition***

Edit the /etc/fstab file and add nodev to the fourth field (mounting options). See the

fstab manual page for more information.

***Set nosuid option for /tmp Partition***

Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create set userid files in /tmp.

# mount -o remount,nosuid /tmp

Run the following commands to determine if the system is configured as recommended.

# grep /tmp /etc/fstab | grep nosuid

# mount | grep /tmp | grep nosuid

If either command emits no output then the system is not configured as recommended.

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options). See the

manual page for more information.

***Set noexec option for /tmp Partition***

The noexec mount option specifies that the filesystem cannot contain executable binaries.

Run the following commands to determine if the system is configured as recommended.

# grep /tmp /etc/fstab | grep noexec

# mount | grep /tmp | grep noexec

If either command emits no output then the system is not configured as recommended, so:

Edit the /etc/fstab file and add noexec to the fourth field (mounting options). See the

manual page for more information.

# mount -o remount,noexec /tmp

***Add nodev Option to /dev/shm Partition***

Edit the /etc/fstab file and add nodev to the fourth field (mounting options of entries that have mount points that contain /dev/shm. See the fstab(5) manual page for more information.

# mount -o remount,nodev /dev/shm

***Add nosuid Option to /dev/shm Partition***

Edit the /etc/fstab file and add nosuid to the fourth field (mounting options). Look for entries that have mount points that contain /dev/shm. See the fstab(5) manual page for more information.

# mount -o remount,nosuid /dev/shm

***Add noexec Option to /dev/shm Partition***

Edit the /etc/fstab file and add noexec to the fourth field (mounting options). Look for entries that have mount points that contain /dev/shm. See the fstab(5) manual page for more information.

# mount -o remount,noexec /dev/shm

## Disable System Accounts

Accounts not used must be disabled.

## Configure SSH

***Set SSH Protocol to 2***

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

Protocol 2

***Set LogLevel to INFO***

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

LogLevel INFO

***Set Permissions on /etc/ssh/sshd\_config***

If the user and group ownership of the /etc/ssh/sshd\_config file are incorrect, run the following command to correct them:

# chown root:root /etc/ssh/sshd\_config

If the permissions are incorrect, run the following command to correct them:

# chmod 600 /etc/ssh/sshd\_config

***Set SSH MaxAuthTries to 3 or Less***

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

MaxAuthTries 3

***Set SSH PermitEmptyPasswords to No***

PermitEmptyPasswords no

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

***Set Idle Timeout Interval for User Login***

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

ClientAliveInterval 300

ClientAliveCountMax 0

***Limit Access via SSH***

Access via SSH is managed via dedicated software (Centrify direct control, Power Broker). Operation configures the /etc/ssh/sshd\_config file to grant ssh access only nominal users:

AllowGroups <grouplist>

***Disable SSH Root Login***

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

PermitRootLogin no

## Advanced Intrusion Detection Enviroment (Aide)

The AIDE package must be installed on systems .

## Os Services

***Remove rsh-server***

# yum erase rsh-server

***Remove rsh***

# yum erase rsh

***Disable NIS Client***

# yum erase ypbind

***Disable NIS Server***

# yum erase ypserv

***Remove tftp***

# yum erase tftp

***Remove tftp-server***

# yum erase tftp-server

***Remove talk***

# yum erase talk

***Remove talk-server***

# yum erase talk-server

***Disable chargen-dgram***

Disable the chargen-dgram service by running the following command:

# chkconfig chargen-dgram off

***Disable chargen-stream***

Disable the charge n-stream service by running the following command:

# chkconfig chargen-stream off

***Disable daytime-dgram***

Disable the daytime-dgram service by running the following command:

# chkconfig daytime-dgram off

***Disable daytime-stream***

Disable the daytime-stream service by running the following command:

# chkconfig daytime-stream off

***Disable echo-dgram***

Disable the echo-dgram service by running the following command:

# chkconfig echo-dgram off

***Disable echo-stream***

Disable the echo-stream service by running the following command:

# chkconfig echo-stream off

***Disable tcpmux-server***

Disable the tcpmux-server service by running the following command:

# chkconfig tcpmux-server off

## Special Purpose Services

***Remove the X Window System***

Unless specifically required, graphical login access via the X Window System must be disabled in order to reduce the potential attack surface.

Edit the /etc/inittab file to set the default runlevel as follows:

id:3:initdefault

***Remove Avahi Server***

# chkconfig avahi-daemon off

***Remove DHCP Server***

# yum erase dhcp

***Remove LDAP***

If the server will not need to act as an LDAP client or server, it is recommended that the software be disabled to reduce the potential attack surface.

If LDAP is running on the system and is not needed, remove it as follows:

# yum erase openldap-servers

# yum erase openldap-clients

***Remove DNS Server***

Unless a server is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.

# yum erase bind

***Remove HTTP Server***

Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.

# yum erase httpd

***Remove Samba***

If there is no need to mount directories and file systems to Windows systems, then this service can be deleted to reduce the potential attack surface.

# yum erase samba

***Remove HTTP Proxy Server***

If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.

# yum erase squid

***Remove SNMP Server***

# yum erase net-snmp

***Disable Postfix***

If there is no need for Postfix it is recommended to disable the service.

## Network Configuration and Firewalls

Modify Network Parameters (Host Only)

The following network parameters determine if the system is to act as a host only. A system is considered host only if the system has a single interface, or has multiple interfaces but will not be configured as a router.

***Disable IP Forwarding***

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

***Disable Send Packet Redirects***

Set the net.ipv4.conf.all.send\_redirects and

net.ipv4.conf.default.send\_redirects parameters to 0 in /etc/sysctl.conf:

net.ipv4.conf.all.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

***Enable RFC-recommended Source Route Validation***

Setting these flags is a good way to deter attackers from sending your server bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your server, you will not be able to enable this feature without breaking the routing.

Set the net.ipv4.conf.all.rp\_filter and net.ipv4.conf.default.rp\_filter

parameters to 1 in /etc/sysctl.conf:

net.ipv4.conf.all.rp\_filter=1

net.ipv4.conf.default.rp\_filter=1

Modify active kernel parameters to match:

# /sbin/sysctl -w net.ipv4.conf.all.rp\_filter=1

# /sbin/sysctl -w net.ipv4.conf.default.rp\_filter=1

***Enable TCP SYN Cookies***

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.

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

## Configure IPV6

***Disable IPv6***

If IPv6 is not to be used, it is recommended to disable it to reduce the attack surface of the system.

Edit /etc/sysconfig/network, and add the following line:

NETWORKING\_IPV6=no

Create the file /etc/modprobe.d/ipv6.conf and add the following lines:

options ipv6 disable=1

Perform the following command to turn ip6tables off:

# /sbin/chkconfig ip6tables off

## System maintenance

***Set Permissions on /etc/passwd***

# /bin/chmod 644 /etc/passwd

***Set Permissions on /etc/shadow***

# /bin/chmod 000 /etc/shadow

***Verify Permissions on /etc/gshadow***

# /bin/chmod 000 /etc/gshadow

***Verify Permissions on /etc/group***

# /bin/chmod 644 /etc/group

***Verify User/Group Ownership on /etc/passwd***

# /bin/chown root:root /etc/passwd

***Verify User/Group Ownership on /etc/shadow***

# /bin/chown root:root /etc/shadow

***Verify User/Group Ownership on /etc/gshadow***

# /bin/chown root:root /etc/gshadow

***Verify User/Group Ownership on /etc/group***

# /bin/chown root:root /etc/group