

This is a walk-through guide for installing RHEL on a server / VM.

It contains the steps it takes to create a server which is fairly hardened down, up to NSA standards.

1) Disk Partitioning

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

(Some system directories should be placed on their own

partitions (or logical volumes). This allows for better

separation and protection of data.)

sudo nano /etc/fstab

-------------------------------------------------------------------------

mount size settings

-------------------------------------------------------------------------

/ 500 gb (\*) defaults 1 1 / 0 0

/boot 5 gb (\*\*\*\*) defaults,nosuid,noexec,nodev 1 2

/tmp 80 gb (\*\*\*\*) defaults,nosuid,noexec,nodev 1 2

/var 80 gb (\*\*) defaults,nosuid 1 2

/var/log 80 gb (\*\*\*\*) defaults,nosuid,noexec,nodev 1 2

/var/ftp 500 gb (\*\*\*) defaults,nosuid,nodev 1 2

/var/www 500 gb (\*\*\*) defaults,nosuid,nodev 1 2

/home 1 tb (\*\*\*) defaults,nosuid,nodev 1 2

swap 32 gb (\*)

/media 2 tb (\*\*\*) defaults,nosuid,nodev 1 2

/dev/shm (\*\*\*\*) defaults,nosuid,noexec,nodev 1 2

-------------------------------------------------------------------------

(leger)

(\*) = defaults 1 1 / 0 0 (the default given by the system)

(\*\*) = defaults,nosuid 1 2

(\*\*\*) = defaults,nosuid,nodev 1 2

(\*\*\*\*) = defaults,nosuid,noexec,nodev 1 2

-------------------------------------------------------------------------

# Bind /var/tmp to /tmp

# add to bottom of fstab

sudo nano /etc/fstab

...........................................

/tmp /var/tmp none rw,noexec,nosuid,nodev,bind 1 2

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

2) Boot Loader Password

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

During install make sure you selected "encrypt LVM disk"

For the Gold Image VM use this default password:

P@$sW0rDP@$sW0rD

this can be used for both the grub loader and

also the LUKS LVM encryption prompt.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

3) Default root and user account password for gold image

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

change this before deploying the VM or install:

P@$sW0rD

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

4) First Boot Config

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Firewall

Leave set to “Enabled.” Only check the “Trusted Services” that this system

needs to serve. Uncheck the default selection of SSH if the system does not

need to serve SSH.

SELinux

Leave SELinux set to “Enforcing” mode.

Kdump Leave Kdump off unless the feature is required, such as for kernel development

and testing.

Set Up Software Updates

If the system is connected to the Internet now, click “Yes, I’d like to register

now.” This will require a connection to either the Red Hat Network servers

or their proxies or satellites. This can also be configured later as described

in Section 2.1.2.1.

Create User

If the system will require a local user account, it can be created here.

Even if the system will be using a network-wide authentication system

as described in Section 2.3.6, do not click on the “Use Network Login...”

button. Manually applying configuration later is preferable.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Edit .bashrc files

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

copy and paste the following into the .bashrc files:

nano .bashrc

su - root

sudo nano /etc/skel/.bashrc

##################################################################

# COPY AND PASTE - START HERE

#

#################################################################

#============================================================

#

# ALIASES AND FUNCTIONS

#

# Arguably, some functions defined here are quite big.

# If you want to make this file smaller, these functions can

#+ be converted into scripts and removed from here.

#

#============================================================

#-------------------

# Personnal Aliases

#-------------------

alias top='htop'

alias rm='rm -i'

alias cp='cp -i'

alias mv='mv -i'

# -> Prevents accidentally clobbering files.

alias mkdir='mkdir -p'

alias h='history'

alias j='jobs -l'

alias which='type -a'

alias ..='cd ..'

# Pretty-print of some PATH variables:

alias path='echo -e ${PATH//:/\\n}'

alias libpath='echo -e ${LD\_LIBRARY\_PATH//:/\\n}'

alias du='du -kh' # Makes a more readable output.

alias df='df -kTh'

#-------------------------------------------------------------

# The 'ls' family (this assumes you use a recent GNU ls).

#-------------------------------------------------------------

# Add colors for filetype and human-readable sizes by default on 'ls':

alias ls='ls -h --color'

alias lx='ls -lXB' # Sort by extension.

alias lk='ls -lSr' # Sort by size, biggest last.

alias lt='ls -ltr' # Sort by date, most recent last.

alias lc='ls -ltcr' # Sort by/show change time,most recent last.

alias lu='ls -ltur' # Sort by/show access time,most recent last.

# The ubiquitous 'll': directories first, with alphanumeric sorting:

alias ll="ls -lv --group-directories-first"

alias lm='ll |more' # Pipe through 'more'

alias lr='ll -R' # Recursive ls.

alias la='ll -A' # Show hidden files.

alias tree='tree -Csuh' # Nice alternative to 'recursive ls' ...

#-------------------------------------------------------------

# Tailoring 'less'

#-------------------------------------------------------------

alias more='less'

export PAGER=less

export LESSCHARSET='latin1'

export LESSOPEN='|/usr/bin/lesspipe.sh %s 2>&-'

# Use this if lesspipe.sh exists.

export LESS='-i -N -w -z-4 -g -e -M -X -F -R -P%t?f%f \

:stdin .?pb%pb\%:?lbLine %lb:?bbByte %bb:-...'

# LESS man page colors (makes Man pages more readable).

export LESS\_TERMCAP\_mb=$'\E[01;31m'

export LESS\_TERMCAP\_md=$'\E[01;31m'

export LESS\_TERMCAP\_me=$'\E[0m'

export LESS\_TERMCAP\_se=$'\E[0m'

export LESS\_TERMCAP\_so=$'\E[01;44;33m'

export LESS\_TERMCAP\_ue=$'\E[0m'

export LESS\_TERMCAP\_us=$'\E[01;32m'

#-------------------------------------------------------------

# Spelling typos - highly personnal and keyboard-dependent :-)

#-------------------------------------------------------------

alias xs='cd'

alias vf='cd'

alias moer='more'

alias moew='more'

alias kk='ll'

# funny log in

# fortune | cowsay | lolcat

umask 077

##################################################################

# COPY AND PASTE - END HERE

#

#################################################################

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

5) add MOTD / Issue message for login

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

copy and paste MOTD-file contents into

nano /etc/motd

nano /etc/issue

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

6) Disable Desktop for boot up.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

systemctl set-default multi-user.target # sets it to boot to CLI mode.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

7) get list of services to disable:

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

systemctl list-units --type service

EXAMPLE: Disable extra un-needed services

--------------------------------------------

cd

mkdir scripts

cd scripts/

touch ShutDownExtraServices.sh

nano ShutDownExtraServices.sh

# Copy and paste this into the text file:

#!/bin/sh

systemctl status alsa-state.service; # loaded active running Manage Sound Card State (restore and store)

systemctl disable alsa-state.service;

systemctl status avahi-daemon.service; # loaded active running Avahi mDNS/DNS-SD Stack

systemctl disable avahi-daemon.service;

systemctl status bluetooth.service; # loaded active running Bluetooth service

systemctl disable bluetooth.service;

systemctl status cups.service; # loaded active running CUPS Printing Service

systemctl disable cups.service;

systemctl status fprintd.service; #loaded failed failed Fingerprint Authentication Daemon

systemctl disable fprintd.service;

systemctl status gdm.service; #loaded active running GNOME Display Manager

systemctl disable gdm.service;

systemctl status ModemManager.service; #loaded active running Modem Manager

systemctl disable ModemManager.service;

systemctl status rhnsd.service; # loaded failed failed LSB: Starts the Spacewalk Daemon

systemctl disable rhnsd.service;

systemctl status smartd.service; #loaded active running Self Monitoring and Reporting Technology

systemctl disable smartd.service;

systemctl status wpa\_supplicant.service; # wifi daemon.

systemctl disable wpa\_supplicant.service;

systemctl disable yum-cron.service

chmod 711 ShutDownExtraServices.sh

sudo ./ShutDownExtraServices.sh

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

8) Disable ICMP redirect support

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# Disable ICMP redirect support

# These settings can be added to /etc/sysctl.conf to make them permanent

# Issue the following commands as root:

nano /etc/sysctl.conf

nano /usr/lib/tuned/virtual-guest/tuned.conf

nano /usr/lib/sysctl.d/00-system.conf

###############################################

# COPY N PASTE - START HERE

#

##############################################

# Disable netfilter on bridges.

net.bridge.bridge-nf-call-ip6tables = 0

net.bridge.bridge-nf-call-iptables = 0

net.bridge.bridge-nf-call-arptables = 0

# 2016/09/21 Disabling ICMP:

net.ipv4.conf.all.accept\_redirects=0

net.ipv4.conf.default.accept\_redirects=0

net.ipv4.conf.all.secure\_redirects=0

net.ipv4.conf.default.secure\_redirects=0

# 2016/09/21 Disable Source Routing

net.ipv4.conf.all.accept\_source\_route=0

net.ipv4.conf.all.forwarding=0

net.ipv6.conf.all.forwarding=0

# 2016/08/25 Disable TCP timestamp response

net.ipv4.tcp\_timestamps=0

# Set fs.suid\_dumpable to 0 per security requirements

fs.suid\_dumpable = 0

# Per CCE: Set kernelrandomizevaspace = 2 in /etc/sysctl.conf

kernelrandomizevaspace = 2

# Set net.ipv4.conf.default.send\_redirects to 0 per security requirements

net.ipv4.conf.default.send\_redirects = 0

# Set net.ipv4.conf.all.send\_redirects to 0 per security requirements

net.ipv4.conf.all.send\_redirects = 0

# Set net.ipv4.ip\_forward to 0 per security requirements

net.ipv4.ip\_forward = 0

# Set net.ipv4.conf.all.accept\_redirects to 0 per security requirements

net.ipv4.conf.all.accept\_redirects = 0

# Set net.ipv4.conf.all.secure\_redirects to 0 per security requirements

net.ipv4.conf.all.secure\_redirects = 0

# Set net.ipv4.conf.all.log\_martians to 1 per security requirements

net.ipv4.conf.all.log\_martians = 1

# Set net.ipv4.conf.default.log\_martians to 1 per security requirements

net.ipv4.conf.default.log\_martians = 1

# Set net.ipv4.conf.default.accept\_redirects to 0 per security requirements

net.ipv4.conf.default.accept\_redirects = 0

# Set net.ipv4.conf.default.secure\_redirects to 0 per security requirements

net.ipv4.conf.default.secure\_redirects = 0

# Set net.ipv4.icmp\_echo\_ignore\_broadcasts to 1 per security requirements

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

# Set net.ipv4.icmp\_ignore\_bogus\_error\_responses to 1 per security requirements

net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1

# Set net.ipv4.tcp\_syncookies to 1 per security requirements

net.ipv4.tcp\_syncookies = 1

# Set net.ipv6.conf.all.accept\_ra to 0 per security requirements

net.ipv6.conf.all.accept\_ra = 0

# Set net.ipv6.conf.default.accept\_ra to 0 per security requirements

net.ipv6.conf.default.accept\_ra = 0

# Set net.ipv6.conf.all.accept\_redirects to 0 per security requirements

net.ipv6.conf.all.accept\_redirects = 0

# Set net.ipv6.conf.default.accept\_redirects to 0 per security requirements

net.ipv6.conf.default.accept\_redirects = 0

###############################################

# COPY N PASTE - END HERE

#

##############################################

# save and exit

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

9) Package Signature Checking Globaly Active

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

force yum to check package signatures:

nano /etc/yum.conf

(in the [main] section look for and edit to this:)

.....................

gpgcheck=1

..........................

( [Ctrl + x], y - to exit and save)

...........................................................

do the same for the other repos

..........................

nano /etc/yum.repos.d

(in the [main] section look for and edit to this:)

.....................

gpgcheck=1

..........................

( [Ctrl + x], y - to exit and save)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

10) AIDE install and config

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

AIDE is a tripwire like IDS. do the following:

(install)

.......................................

yum install aide

(build, store, test DB)

.......................................

/usr/sbin/aide --init

cp /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

/usr/sbin/aide --check

nano /etc/crontab

(add this line)

# AIDE Scan

05 4 \* \* \* root /usr/sbin/aide --check

( [Ctrl + x], y to exit )

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

11) Verify Package Integrity with RPM

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

use the rpm command to verify if the files differ from what is expected by the RPM db:

rpm -qVa

rpm -qVa | awk '$2="c" {print $}' > /var/log/InstallLogs/RPMVerify.txt

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

12) Restrict Consoldev access

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

restrict to root only.

...........................................

nano /etc/security/console.perms.d/50-default.perms

# permission definitions

#<console> 0660 <floppy> 0660 root.floppy

#<console> 0660 <sound> 0600 root

...

#<xconsole> 0600 /dev/console 0600 root.root

#<console> 0600 <dri> 00600 root

----------------------------

nano /etc/security/console.perms

<console=tty[0-9] [0-9]\* vc/[0-9] [0-9]\* :0\.[0-9] :0

<xconsole>=:0\.[0-9] :0

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

13) Disable mounting uncommon Filesystems

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

append to file:

nano /etc/modprobe.conf

install cramfs /bin/true

install freevxfs /bin/true

install jffs2 /bin/true

#install hfs /bin/true

#install hfspluse /bin/true

install squashfs /bin/true

install udf /bin/true

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

14) world writable dirs with sticky bits set

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

(do for each partition)

find PARTITION -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print > /var/log/InstallLog/DirsStickyBit.txt

cat /var/log/InstallLog/DirsStickyBit.txt | less

..........

(run this command for each dir)

chmod +t /dir

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

15) unauthorized world writable files

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

same things as above.

find PARTITION -xdev -type f -perm -0002 -print > /var/log/InstallLog/UnauthWorldWrite.txt

chmod o-w fileName

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

16) Find and Repair Unowned Files

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

same as above:

find PARTITION -xdev \( -nouser -o -nogroup \) -print > /var/log/InstallLog/UnownedFiles.txt

.............................................

(verify world-writable dirs have ownership)

find PARTITION -xdev -type d -perm -0002 -uid +500 -print > /var/log/InstallLog/WWUnownedFiles.txt

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

17) setting umask defaults for filesystem

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

( add to the following)

..............................................................................

sudo nano /etc/sysconfig/init

umask 027

..............................................................................

sudo nano /etc/profile

sudo nano /etc/bashrc

sudo nano /etc/kshrc

sudo nano /etc/csh.cshrc

umask 077

..............................................................................

sudo nano /etc/login.def

UMASK 077

..............................................................................

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

18) linux single user mode

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# Enable authorization for linux single user mode

#

nano /etc/sysconfig/init

# add this line

SINGLE=/sbin/sulogin

# save and exit

nano /etc/inittab

# add this line

~:S:wait:/sbin/sulogin

# save and exit

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Edit '/etc/securetty'

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# Edit '/etc/securetty' entries

# Remove all the entries in /etc/securetty except

# console, tty[0-9]\* and vc\[0-9]\*

# NOTE: instead of deleting them, us "#" to comment them out.

# the document says to also disable root logon over ssh. however,

# this is a needed function for daily remote administration.

# technicly each admin should have a admin group account that we can

# ssh to, and then use sudo to make a change.

nano /etc/securetty

# add a "#" to the ones listed below...

console

vc/1

vc/2

vc/3

vc/4

vc/5

vc/6

vc/7

vc/8

vc/9

#vc/10

#vc/11

tty1

tty2

tty3

tty4

tty5

tty6

tty7

tty8

tty9

#tty10

#tty11

#ttyS0

#ttysclp0

#sclp\_line0

#3270/tty1

#hvc0

#hvc1

#hvc2

#hvc3

#hvc4

#hvc5

#hvc6

#hvc7

#hvsi0

#hvsi1

#hvsi2

#xvc0

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

19) Disable interactive boot

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

(use with caution)

nano /etc/sysconfig/init

PROMPT=no

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

20) disable core dumps of kernel and memory

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

sudo nano /etc/security/limits.conf

\* hard core 0

................................

sudo nano /etc/sysctl.conf

fs.suid\_dumpable = 0

..................................

sudo nano /etc/profile

ulimit -S -c 0.> /dev/null 2>&1

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

21) edit console.perms

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# ....................................................

# NOTE\* the file name for RHEL 7 might be called

# /etc/security/console.perms.d/50-default.perms

# and

# /etc/security/console.perms

mkdir /etc/security/console.perms.d/

cp /etc/security/console.perms /etc/security/console.perms.d/50-default.perms

nano /etc/security/console.perms.d/50-default.perms

# /etc/security/console.perms

#

# This file determines the permissions that will be given to priviledged

# users of the console at login time, and the permissions to which to

# revert when the users log out.

# format is:

# <class>=list of regexps specifying consoles or globs specifying files

# file-glob|<class> perm dev-regex|<dev-class> \

# revert-mode revert-owner[.revert-group]

# the revert-mode, revert-owner, and revert-group are optional, and default

# to 0600, root, and root, respectively.

#

# For more information:

# man 5 console.perms

#

# This file should not be modified.

# Rather a new file in the console.perms.d directory should be created.

# file classes -- these are regular expressions

<console>=tty[0-9][0-9]\* vc/[0-9][0-9]\* :[0-9]+\.[0-9]+ :[0-9]+

# COMMENT OUT THIS LINE....

#<xconsole>=:[0-9]+\.[0-9]+ :[0-9]+

# device classes -- see console.perms.d/50-default.perms

# permission definitions -- see console.perms.d/50-default.perms

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

22) Reset umask value

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# Reset umask value

# set the umask value to 077 for root and other user accounts

# this can be put at the top of the text files. should be done

# for all the users. and also the /etc/skel directory.

# For the Oracle application account the umask needs to be set to

umask 027

# For the Oracle database account the umask needs to be set to

umask 022

nano /etc/login.def

# copy and paste the text to the top of the file.

UMASK 077

# copy and paste this to the bottom of the files:

umask 077

ls -al

nano .login

nano /etc/profile # these are for system wide defaults

nano /etc/bashrc

nano /etc/kshrc

nano /etc/csh.cshrc

nano /etc/skel/.profile # these are for default setup when accounts are created

nano /etc/skel/.bashrc

nano /etc/skel/.kshrc

nano /etc/skel/.csh.cshrc

nano .profile # these are in the exsiting account home directories.

nano .bashrc

nano .kshrc

nano .csh.cshrc

su - oracle

nano .profile # these are in the exsiting account home directories.

nano .bashrc # umask 027 or 022

nano .kshrc

nano .csh.cshrc

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

23) VSFTPD setup

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

[ftp://ftpuser@caprica.hsc.net.ou.edu](mailto:ftp://ftpuser@caprica.hsc.net.ou.edu)

sudo yum install vsftpd;

sudo mkdir /etc/ssl/private

sudo openssl req -x509 -nodes -newkey rsa:4096 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

sudo nano /etc/vsftpd/vsftpd.conf

###############################################

#add to end of /etc/vsftpd/vsftpd.conf

###############################################

# add follows to the end

# specify root directory ( if don't specify, users' home directory become FTP home directory)

local\_root=public\_html

# use localtime

use\_localtime=YES

# turn off for seccomp filter ( if you cannot login, add this line )

seccomp\_sandbox=NO

pasv\_address=10.64.82.16

pasv\_min\_port=40000

pasv\_max\_port=40010

pasv\_promiscuous=YES

pasv\_enable=YES

# where x.x.x.x will be the IP address of the server.

pam\_service\_name=vsftpd

userlist\_enable=YES

tcp\_wrappers=YES

ssl\_enable=YES

allow\_anon\_ssl=YES

force\_local\_data\_ssl=YES

force\_local\_logins\_ssl=YES

ssl\_tlsv1=YES

ssl\_sslv2=YES

ssl\_sslv3=YES

rsa\_cert\_file=/etc/ssl/private/vsftpd.pem

rsa\_private\_key\_file=/etc/ssl/private/vsftpd.pem

##############################################################

sudo systemctl start vsftpd;

sudo firewall-cmd --add-service=ftp --permanent

sudo systemctl restart firewalld

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

24) Setup ClamAv on RHEL

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# Setup this is a setup guid to configure ClamAV after installing it.

# The daily cron job scans the entire server every day.

# The hourly cron job scans files which were created or

# modified within the last hour. This should provide rapid

# notification of any infection without sacrificing performance.

# Each time the scan runs it checks the scan logs to see if

# there were any infected files found, and if so immediately

# sends notification via email.

Inital config of FreshClam

...........................................................................

# first edit the /etc/freshclam.conf file and select the settings you want.

sudo nano /etc/freshclam.conf

# after editing the file, run a freshclam update.

sudo freshclam

...........................................................................

CRONTAB:

............................................................................

# setup crontab to get freshclam updates:

sudo nano /etc/crontab

# Add the following lines to crontab:

# Update ClamAV database

0 01 \* \* \* /usr/bin/freshclam

CRON.DAILY:

............................................................................

# next we are going to setup clam scan automation

# for the cron.daily:

sudo nano /etc/cron.daily/clamscan\_daily

#################################################

# CLAMSCAN\_DAILY = START COPY N PASTE HERE #

#################################################

#!/bin/bash

# Log rotation

logrotate -f /etc/logrotate\_clamscan.conf

# email subject

SUBJECT=”VIRUS DETECTED ON `hostname`!!!”

# Email To ?

[EMAIL=”recipient@ngc.com”](mailto:EMAIL%3D”recipient@ngc.com”)

# Log location

LOG=/var/log/clamav/clamscan.log

check\_scan () {

# Check the last set of results. If there are any “Infected” counts that aren’t zero, we have a problem.

if [ `tail -n 12 ${LOG} | grep Infected | grep -v 0 | wc -l` != 0 ]

then

EMAILMESSAGE=`mktemp /tmp/virus-alert.XXXXX`

echo “To: ${EMAIL}” >> ${EMAILMESSAGE}

echo “From: [clamav@ngc.com”](mailto:clamav@ngc.com”) >> ${EMAILMESSAGE}

echo “Subject: ${SUBJECT}” >> ${EMAILMESSAGE}

echo “Importance: High” >> ${EMAILMESSAGE}

echo “X-Priority: 1″ >> ${EMAILMESSAGE}

echo “`tail -n 50 ${LOG}`” >> ${EMAILMESSAGE}

sendmail -t < ${EMAILMESSAGE}

fi

}

clamscan -r / –exclude-dir=/sys/ –quiet –infected –log=${LOG}

check\_scan

#################################################

# CLAMSCAN\_DAILY = END COPY N PASTE HERE #

#################################################

# Now we need to chmod the file

sudo chmod +x /etc/cron.daily/clamscan\_daily

CRON.HOURLY:

............................................................................

# now we need to set up clamscan for hourly scans in

# the cron.hourly settings:

sudo nano /etc/cron.hourly/clamscan\_hourly

#################################################

# CLAMSCAN\_HOURLY = START COPY N PASTE HERE #

#################################################

#!/bin/bash

# email subject

SUBJECT=”VIRUS DETECTED ON `hostname`!!!”

# Email To ?

[EMAIL=”recipient@ngc.com”](mailto:EMAIL%3D”recipient@ngc.com”)

# Log location

LOG=/var/log/clamav/clamscan.log

check\_scan () {

# Check the last set of results. If there are any “Infected” counts that aren’t zero, we have a problem.

if [ `tail -n 12 ${LOG} | grep Infected | grep -v 0 | wc -l` != 0 ]

then

EMAILMESSAGE=`mktemp /tmp/virus-alert.XXXXX`

echo “To: ${EMAIL}” >> ${EMAILMESSAGE}

echo “From: [clamav@ngc.com”](mailto:clamav@ngc.com”) >> ${EMAILMESSAGE}

echo “Subject: ${SUBJECT}” >> ${EMAILMESSAGE}

echo “Importance: High” >> ${EMAILMESSAGE}

echo “X-Priority: 1″ >> ${EMAILMESSAGE}

echo “`tail -n 50 ${LOG}`” >> ${EMAILMESSAGE}

sendmail -t < ${EMAILMESSAGE}

fi

}

find / -not -wholename ‘/sys/\*’ -and -not -wholename ‘/proc/\*’ -mmin -61 -type f -print0 | xargs -0 -r clamscan –exclude-dir=/proc/ –exclude-dir=/sys/ –quiet –infected –log=${LOG}

check\_scan

find / -not -wholename ‘/sys/\*’ -and -not -wholename ‘/proc/\*’ -cmin -61 -type f -print0 | xargs -0 -r clamscan –exclude-dir=/proc/ –exclude-dir=/sys/ –quiet –infected –log=${LOG}

check\_scan

#################################################

# CLAMSCAN\_HOURLY = END COPY N PASTE HERE #

#################################################

# Run chmod on the file so it can execute:

sudo chmod +x /etc/cron.hourly/clamscan\_hourly

............................................................................

# Make the logrotate configuration file for clamscan

sudo nano /etc/logrotate\_clamscan.conf

#####################################################

# LOGROTATE\_CLAMSCAN>CONF = START COPY N PASTE HERE #

#####################################################

/var/log/clamav/clamscan.log {

rotate 30

daily

ifempty

missingok

nocompress

}

# Remove the ClamAV test virus files

#rm -rf /usr/share/doc/clamav-0.97.7/test/

# Manual scanning with ClamAV

# Scan a specific file

#clamscan /opt/file.txt

# Scan a directory

#clamscan /opt

# Scan the contents of a directory and all sub-directories

#clamscan -r /opt

#####################################################

# LOGROTATE\_CLAMSCAN.CONF = END COPY N PASTE HERE #

#####################################################

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

25) fixing libvirt virtual network bug. (If needed)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

# this fix is for a bug in the libvirt lib, which resets sysctl.conf and

# tuned.conf and resets ip forwarding to 1.

# this fix is taken from the follwoing article and was found by Pamula Cherry

# <http://www.cyberciti.biz/faq/linux-kvm-disable-virbr0-nat-interface/>

# perform this in teh vSphere console so

# if network cuts out, you can still have access

ifconfig # to see if is there

virsh net-list

# then removed with

virsh net-destroy default;

virsh net-undefine default;

systemctl restart libvirtd;

ifconfig;

reboot

# ssh back in

# Show current state of settings in Proc file system.

cat /proc/sys/net/ipv4/conf/all/forwarding;

cat /proc/sys/net/ipv4/conf/all/accept\_redirects;

cat /proc/sys/net/ipv4/conf/all/secure\_redirects;

cat /proc/sys/net/ipv4/conf/default/accept\_redirects;

cat /proc/sys/net/ipv4/conf/default/secure\_redirects;

# manualy set settings in proc file system.

echo 0 > /proc/sys/net/ipv4/conf/all/forwarding;

echo 0 > /proc/sys/net/ipv4/conf/all/accept\_redirects;

echo 0 > /proc/sys/net/ipv4/conf/all/secure\_redirects;

echo 0 > /proc/sys/net/ipv4/conf/default/accept\_redirects;

echo 0 > /proc/sys/net/ipv4/conf/default/secure\_redirects;

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

26) Disable rhnsd Daemon

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disable the update Daemon for centos and rhel

sudo systemctl disable rhnsd.service

sudo systemctl disable yum-updatesd.service

...........................................................

create a cronjob to run yum update

...........................................................

(install nano for easier editing of txt files)

yum install nano

nano /etc/cron.weekly/cron.weekly

(add the following, and then press [Ctrl + x] to exit, press y to save)

#!/bin/sh

# Run yum update once a week

/usr/bin/yum -R 120 -e 0 -d 0 -y update yum

/usr/bin/yum -R 10 -e 0 -d 0 y update

sudo chmod +x /etc/cron.weekly/cron.weekly

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

#############################################################################

SPECIALIZED REMEDIATIONS

#############################################################################

NOTE: these are only used in rare instances when called for on the

rapid 7 scan.

======================================================================

Enable TCP MD5 Signatures

#####################################################################

Estimated time: 4 hours

Enable the TCP MD5 signature option as documented in RFC 2385.

It was designed to reduce the danger from certain security attacks

on BGP, such as TCP resets. This will address the following issue:

TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation).

<http://www.ietf.org/rfc/rfc2385.txt>

Locate and fix vulnerable traffic inspection devices along the

route to the target

..........

# run this command at prompt:

grep TCP\_MD5 /boot/config-\*

# this should be enabled, and white listed on all the servers.

Use a Stronger Diffie-Hellman Group

######################################################

# Estimated time: 15 minutes

# Please refer to this guide to deploying Diffie-Hellman

# for TLS for instructions on how to configure the server to use 2048-bit or stronger

# Diffie-Hellman groups with safe primes.

# This will address the following 2 issues:

# Diffie-Hellman group smaller than 1024 bits (tls-dh-prime-under-1024-bits)

# Diffie-Hellman group smaller than 2048 bits (tls-dh-prime-under-2048-bits)

Disable TLS/SSL support for RC4 ciphers

#######################################################

# Configure the server to disable support for RC4 ciphers.

# For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for

# instructions on disabling rc4 ciphers. The following recommended configuration

# provides a higher level of security. This configuration is compatible with

# Firefox 27, Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1

# protocols are not recommended in this configuration. Instead, use

# TLSv1.1 and TLSv1.2 protocols.

#Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSAAES256-

GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-

SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-

SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-

SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSAAES256-

SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

# This will address the following issue: TLS/SSL Server Supports RC4

# Cipher Algorithms (CVE-2013-2566) (rc4-cve-2013-2566).

Generate random Diffie-Hellman parameters

#####################################################

# Configure the server to use a randomly generated Diffie-Hellman group.

# It's recommend that you generate a 2048-bit group. The

# simplest way of generating a new group is to use OpenSSL:

openssl dhparam -out dhparams.pem 2048

# To use the DH parameters in newer versions of Apache (2.4.8 and newer) and

# OpenSSL 1.0.2 or later, you can directly specify your

# DH params file as follows:

SSLOpenSSLConfCmd DHParameters "{path to dhparams.pem}"

# If you are using Apache with LibreSSL, or Apache 2.4.7 and OpenSSL 0.9.8a

# or later, you can append the DHparams you generated

# earlier to the end of your certificate file and reload the configuration.

# For other products see the remediation steps suggested by the original researchers.

# This will address the following issue: TLS/SSL Server Is Using Commonly Used Prime

# Numbers (tls-dh-primes).

Disable TLS/SSL support for 3DES cipher suite

###################################################################

# Configure the server to disable support for 3DES suite.

# For Microsoft IIS web servers, see Microsoft Knowledgebase article 245030 for

# instructions on disabling 3DES cipher suite. The following recommended configuration

# provides a higher level of security. This configuration is compatible with Firefox 27,

# Chrome 22, IE 11, Opera 14 and Safari 7. SSLv2, SSLv3, and TLSv1 protocols are not

# recommended in this configuration. Instead, use TLSv1.1 and TLSv1.2 protocols.

# Refer to your server vendor documentation to apply the recommended cipher configuration:

ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSAAES256-

GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-

SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-

SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-

SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSAAES256-

SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

# This will address the following issue: TLS/SSL Server Supports 3DES Cipher

# Suite (ssl-3des-ciphers).

Fix the subject's Common Name (CN) field in the certificate

################################################################

# The subject's common name (CN) field in the X.509 certificate should be

# fixed to reflect the name of the entity presenting the certificate

# (e.g., the hostname). This is done by generating a new certificate usually

# signed by a Certification Authority (CA) trusted by both the client and server.

# This will address the following issue: X.509 Certificate Subject CN Does Not

# Match the Entity Name (certificate-common-namemismatch).

Obtain a new certificate from your CA and ensure the server configuration is correct

######################################################################################

# Ensure the common name (CN) reflects the name of the entity presenting the

# certificate (e.g., the hostname). If the certificate(s) or any

# of the chain certificate(s) have expired or been revoked, obtain a new

# certificate from your Certificate Authority (CA) by following their

# documentation. If a self-signed certificate is being used, consider

# obtaining a signed certificate from a CA.

# References: Mozilla: Connection Untrusted ErrorSSLShopper:

# SSL Certificate Not Trusted ErrorWindows/IIS certificate chain config

# Apache SSL configNginx SSL configCertificateChain.io

# This will address the following issue: Untrusted TLS/SSL server X.509 certificate

# (tls-untrusted-ca).

# <https://certificatechain.io/>

Disable HTTP TRACE Method for Apache

######################################

# Disable HTTP TRACE Method for Apache

# Estimated time: 2 hours

# Apache HTTPD

# Newer versions of Apache (1.3.34 and 2.0.55 and later) provide a

# configuration directive called TraceEnable. To deny TRACE

# requests, add the following line to the server configuration:

TraceEnable off

# For older versions of the Apache webserver, use the mod\_rewrite

# module to deny the TRACE requests:

RewriteEngine On

RewriteCond %{REQUEST\_METHOD} ^TRACE

RewriteRule .\* - [F]

# This will address the following issue: HTTP TRACE Method Enabled (http-trace-method-enabled).

# FIX: this is the fix for this issue:

# added the following line to the bottom of the

# httpd.conf file in /etc/httpd/conf:

TraceEnable off

Restrict database access

####################################

# Restrict database access

# Estimated time: 30 minutes

# Configure the database server to only allow access to trusted systems.

# For example, the PCI DSS standard requires you to place the

# database in an internal network zone, segregated from the DMZ

# This will address the following issue: Database Open Access (database-open-access).

Upgrade MySQL

###################################

# Estimated time: 1 hour

# As of January 25th, 2005, there does not exist an official fix from the

# MySQL development team. However, several vendors have

# provided their own patches:

# Debian has released fixes to their stable (woody) and unstable (sid)

# branches: <http://www.debian.org/security/2005/dsa-647>

# This will address the following issue: MySQL mysqlaccess Temporary File

# Symlink Attack (unix-mysql-mysqlaccess-temp-file).

# NOTE: the system is not a debian system, and trying to install a debian based package on

# a RHEL / Oracle based system may break the application.

# we have ran yum updates for mysql, and will need to keep

# the packaged from Oracle.

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

EMAIL LOG

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

=============================================================================

BASH LOG

=============================================================================

=======================================================================================

#########################################################################################