1]Make Sure you have separate mount point for below mention mount points.

/usr /var /opt /temp /home and data directory for application should be separate.

LVM would be best option in-case we are falling short for disk space.

2]Check for unwanted services and disabled it if not required.

Systemctl list-units -t service

Netstat -tulpn

Systemctl disable service

3]SSH Configuration

Vi /etc/ssh/sshd\_config

PermitRootLogin no #keep Root login no

Allowusers username

Port 64521 #custom port

Protocol 2

Banner /etc/issue.net

Systemctl restart sshd.service

4]Banner

vi /etc/issue.net

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

# Welcome to Katerra #

# All connections are monitored and recorded #

# Disconnect IMMEDIATELY if you are not an authorized user! #

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

5]Lockdown Cron if not using

Echo ALL >> /etc/cron.deny

6]Turn on SELINUX

Setenforce 1

Vi /etc/Selinux/config

SELINUX=enforcing /Permissive

:wq!

Sestatus

7]TURN OFF IPV6

Vi /etc/sysconfig/network

NETWORKING\_IPV6=NO

IPV6INIT=No

8] Enable Secure (high quality) Password Policy

vi /etc/security/pwquality.conf

Number of characters in the new password that must not be present in the

old password.

difok = 1

Minimum acceptable size for the new password

minlen = 8

The maximum credit for having digits in the new password.

dcredit = 1

minimum number of uppercase characters

ucredit = 1

minimum number of lowercase characters

lcredit = 1

other characters in the new password

ocredit = 1

9]Change password Expiration for all users

Vi /etc/login.defs

PASS\_MAX\_DAYS 60

PASS\_MIN\_DAYS 0

PASS\_WARN\_AGE 7 ##Save and exit

Chage -M 60 -m 0 -W 7 Username

Passwd -l username ##Lock down user

Passwd -u username ##Unlock particular user

10]Set Last logon Access Date

vi /etc/pam.d/system-auth

session required pam\_lastlog.so showfailed #below session required pam\_limits.so

retry=5 # in line pam\_pwquality.so try\_first\_pass local\_users\_only retry=3

remember=3 #in Password sufficient pam\_unix.so line

11] deny all tcp wrappers

echo "ALL:ALL" >> /etc/hosts.deny

echo "sshd:ALL" >> /etc/hosts.allow

12]Check for empty passwd in shadow file and remove that user.

cat /etc/shadow | awk -F: '($2==""){print $1}'

userdel -r username

13] Enable auditing in the server.

systemctl enable auditd.service

systemctl start auditd.service

cd /etc/audit/

vi auditd.conf

max\_log\_file = 30MB

num\_logs = 5

space\_left\_action = SYSLOG

admin\_space\_left\_action = SUSPEND

action\_mail\_acct = root

service auditd restart

14]CHECK FOR UPDATES FOR SYSTEM

Yum check -update

Yum updates

Yum list installed #check for install remove unwanted pckg

yum remove postfix #By default postfix is installed remove it.

Yum group remove “X window System”

Yum remove package

15] Remove unwanted services

yum remove xinetd

yum remove telnet-server

yum remove rsh-server

yum remove rsh

yum remove ypbind

yum remove ypserv

yum remove tftp-server

yum remove bind

yum remove dovecot

yum remove squid

yum remove net-snmpd

16] Disable Unwanted services

systemctl disable xinetd

systemctl disable rexec

systemctl disable rsh

systemctl disable rlogin

systemctl disable ypbind

systemctl disable tftp

systemctl disable certmonger

systemctl disable cgconfig

systemctl disable cgred

systemctl disable cpuspeed

systemctl disable kdump

systemctl disable mdmonitor

systemctl disable messagebus

systemctl disable netconsole

systemctl disable ntpdate

systemctl disable oddjobd

systemctl disable portreserve

systemctl disable qpidd

systemctl disable quota\_nld

systemctl disable rdisc

systemctl disable saslauthd

systemctl disable atd

systemctl disable nfslock

systemctl disable named

systemctl disable dovecot

systemctl disable squid

systemctl disable snmpd

systemctl disable rpcgssd

systemctl disable rpcsvcgssd

systemctl disable rpcidmapd

systemctl disable cups

17] Enable below mention services

systemctl enable irqbalance

systemctl enable crond

18] Disable uncommon filesystem.

echo "install cramfs /bin/false" > /etc/modprobe.d/cramfs.conf

echo "install freevxfs /bin/false" > /etc/modprobe.d/freevxfs.conf

echo "install jffs2 /bin/false" > /etc/modprobe.d/jffs2.conf

echo "install hfs /bin/false" > /etc/modprobe.d/hfs.conf

echo "install hfsplus /bin/false" > /etc/modprobe.d/hfsplus.conf

echo "install squashfs /bin/false" > /etc/modprobe.d/squashfs.conf

echo "install udf /bin/false" > /etc/modprobe.d/udf.conf

19]IGNORE ICMP REQUEST IF REQUIRED Like in DB Server

Vi /etc/sysctl.conf

net.ipv4.icmp\_echo\_ignore\_all = 0 #allow icmp packets

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1 #Ignore Broadcast

net.ipv4.conf.all.accept\_source\_route=0 #Disable source routing

ipv4.conf.all.forwarding=0 #Disable ICMP forwading

net.ipv6.conf.all.disable\_ipv6 = 1 #Disable IPV6

net.ipv6.conf.default.disable\_ipv6 = 1

net.ipv6.conf.lo.disable\_ipv6 = 1

net.ipv4.conf.all.rp\_filter=2 #Disable Reverse path forwading

:wq!

sysctl -p #Reload changes

20] Enable firewalld

Systemctl enable firewalld.service

Systemctl start firewalld.service

Systemctl mask iptables

Firewall-cmd –list-all

Firewall-cmd—reload

firewall-cmd --lockdown-on

semanage port -a -t ssh\_port\_t -p tcp 64521 #if Selinux is enforcing

semanage port -a -t http\_port\_t -p tcp 8080

21]Disable useless SUID and GUID on commands

##if SUID and GUID are set on binary command the any user can run that command

With root privileges.

find / -path /proc -prune -o -type f \( -perm -4000 -o -perm -2000 \) -exec ls -l {} \;

chmod u-s /path/to/binary\_file ##remove SUID

chmod g-s /path/to/binary\_file ##remove GUID

22]Check for Unowned files and directories and removed it.

find / -nouser -o -nogroup -exec ls -l {} \;

23]Modify Environment variables to make history cmd available with timestamp.\

Cd /root/

Ls -alrt

Vi .bashrc

echo 'HISTTIMEFORMAT="%d/%m/%y %T "' >> .bashrc'

echo ‘PROMPT\_COMMAND="history -a"’ >> .bashrc

echo ‘TMOUT=120’ >> .bashrc ##Disconnect idle ssh

source .bashrc ## reload

24]Enable sudo logs in /etc/sudoers and make users in /etc/sudoers file to provide access.

Defaults log\_host, log\_year, logfile="/var/log/sudo.log"