RH342 EXAM

Q1. There is a disk file located at /root/disk.img. The disk files key file is located at /root/key.txt.
Configure the disk in such a way that you can open the disk file with the password flectrag and the password should be located at the key slot 6 and other key slots should remain unchanged.

Answers
cryptsetup luksOpen /root/disk.img <mapper name> --key-file /root/key.txt

cryptsetup luksAddKey /root /disk.img --key-file /root/key.txt --key-slot 6
(enter password flectrag)

Q2. The permission of the directory /var/spool/tmp should be 1777 (rwxrwxrwt) but some malicious program keeps changing the permissions at random time intervals. Another administrator found a workaround to fix this issue and has applied a temporary fix to solve the issue. Fix the initial issue which keeps changing the permission and remove the workaround which was implemented.

Answers
There is a file in the /etc/cron.d folder which runs the command chmod 777 /var/spool/tmp at regular intervals. it was named fixperms, This is the temporary fix, remove it!

rm –rf /etc/cron.d/fixperms

ll /var/spool/tmp
By looking at 'top' utility or journalctl you can find out python service which is running time with high mem (top - > Ctrl+m sort by memory). Get the PID of it and check in running processes (ps aux | grep <pid>), you will find gnome-messagebus service . So stop it.and change permission into

chmod 1777 /var/spool/tmp and check if it change again automatically.
systemctl stop gnome-messagebus.service

\# systemctl disable gnome-messagebus.service

Q3. servera and serverb configured as LDAP clients and user Bodhi couldn't able to login.And check using kinit.

Answers
\# getent passwd Bodhi (shows user)
\# ssh bodhi@localhost (not working)
\# journalctl
Check in journalctl log and it says that there isn't a pam module installed in a particular location a yum whatprovides to that location and it gave a pam module to install.
\# yum install <pam_krb.so
\# getent passwd bodhi
\# ssh bodhi@localhost (working)
Kinit bodhi@EXAMPLE.COM(when you type password you should not get any errors)

Q4. Iscsi problem which says chap authentication to be used, once fixed #fdisk –l should shows output of Iscsi disk.

Answers
The initiator name is incorrect fix it (take correct initiator name from targetcli from Icsci server)
\# vim /etc/iscsi/initiatorname.iscsi à Initiatorname=xxxxxxxxxxx:servera
The CHAP authentication is disabled so enable it in the configs and configure iscsi with the
update command or delete the nodes folder
rm –rf /variscsi/nodes/*
\# vim /etc/iscsi/iscsi.conf à uncomment CHAP (enable)
Discover
Login
\# lsblk
\# fdisk –l

Q5. There is an lvm which is to be mounted (/mnt/ext3lv) and it should persist after
reboots.

Answers
Use the vgcfrgrestore to restore the lvm since its not there.
#vgcfgrestore –l vg00
Then use the
lvchange –an /dev/vg00/lv00
lvchange –ay /dev/vg00/lv00
mkdir /mnt/ext3lv
echo "/dev/vg00/lv00 /mnt/ext3lv ext3 defaults 0 0" >> /etc/fstab
mount –a

6. There is an application called godsworth which does not work which has to be
fixed.

Answers
godsworth
yum install ltrace
ltrace godsworth (says /etc/hell.conf is missing)
touch /etc/hell.conf
godsworth (is working now)

Q7. Set up ipv6 on two servers (server and serverb)

Answers
Get the two addresses from the additional information and add it to ETH1 not
ETH0
Serverb ipv6 address already setup and static.
But not in servera.
nmcli connection modify 'eth1' ipv6.address x:x:x:x:x:x:x:x/64 ipv6.method
manual
connection.id 'System eth1'

nmcli connection down eth1 ; nmcli connection up 'System eth1'
(If need make connection id to System eth1, I did like above way)
Check each server by ping6 command

Q8. Configure ssh with ipv6 between the two servers which you configured above

Answers
Serverb can ssh6 to servera, but servera can not ssh6 serverb
#ssh -6 servera (success)
#ssh -6 serverb (failed).
Change sshd config in serverb. Go to /etc/ssh/sshd_config and comment
#ListenAddress
0.0.0.0
Line and restart sshd service. Now try ssh -6 serverb from servera.

Q9. There is a boot issue on a server fix it. The user jack needs to be able to create 50 files of size 1mb each at the location /var/tmp. Assign ip addresses which persist across boots so that ssh can be initiated from the outside using user malik.

Answers
The grub file of the server has a string (load) in the initramfs line which needs to be remove and In linux16 line at the end console=blankconsole will be there remove that as well
CTRL+X
Use grub2-mkconfig –o /boot/grub2/grub.cfg to fix the grub. Then reboot again.
The configure an ipv4 address by looking at the additional information.
#nmcli connection modify 'eth1' ipv4.address 'x.x.x.x/24' ipv4.gateway 'y.y.y.y' ipv4.method
manual connection.autoconnect yes connection.id 'System eth1'
nmcli connection down eth1 ; nmcli connection up 'System eth1'
(try to ssh serverd using given different given user user)
ssh malik @serverd (should work from outside)
df –h (has enough disk space)
df –ih (inode filled in /var/tmp)

It is logical volume and check whether volume group has enough space to increase LV.
umount /var/tmp
lvextend –L +40M /dev/vg01/lv01
vim /etc/fstab à **/dev/vg01/lv01 /var/tmp ext3 defaults 0 0**
resize2fs /dev/vg01/lv01
df –ih (have enough space for inodes now)

Q10. Get the following performance metrics. (pmlogger archive should download)
When in minutes post the hour,does the one minute cpu load first start to increase
When in minutes post the hour does the one minute cpu load drop to lower than one
What is the maximum one minute cpu load (discard the decimal point and don't round up)

Answers
yum install pcp
systemctl start pmcd
pminfo | grep load
pmval –a <file> kernel.all.load | less
pmval –a <file> kernel.all.load | awk '/^[[:digit:][:punct:][:space:]]*$/{print}' | less
pmval –a <file> kernel.all.load | awk '/^[[:digit:][:punct:][:space:]]*$/{print}' | awks '$2 < 1
{pint}'
pmval –a <file> kernel.all.load | awk '/^[[:digit:][:punct:][:space:]]*$/{print}' | sort –nk2

Q11. Start the httpd server and make it boot persistently

Answers
There is a drop in file which set memory to only a 100MB (/etc/systems/system/httpd.service.d/httpd.conf)
COmment that memory configuration and daemon-reload

Then you get another error saying, Apache server could not bind to port 80 make_sock
Make sure you are not declaring Listen 80 twice in .conf files. And then restart httpd.
fuser -k -n tcp 80

Q12. Add the user jack and set his password to trootent
Both the useradd and passwd commands are not working.

Answers
strace useradd
which useradd
yum whatprovides <useradd command path>
yum install <pkg>
Use strace & ltrace to isolate the issue and fix it. Then add the user and set the password.

Q13. Update the vsftpd application

Answers
Cannot update the vsftpd application n because it has a versionlock locking it.
yum versionlock delete vsftpd
yum update vsftpd (not working)
rpm –V vsftpd (go to that conf file and remove attribute set there)
Chattr –I /etc/vsftpd/vsftpd.conf
yum update vsftpd
yum versionlock add vsftpd

Q14. Execute the " wget <some kind of URL>" command on a particular server, if it does notwork fix the issue

Answers
The wget does not resolve the FQDN of a particular server (but IP does, that means kind of

domain name resolving issue is there). /etc/resolve.conf has corrects config, but /etc/nsswitch.conf has an entry which is wrong and overwites default DNS configs. Add the
entry given to below for dns to start working (DO NOT change /etc/hosts)
hosts: files dns

Q15. Compile the stp file in particular location and configure the server in such a way so that the user stapuser can run it Packages:

Answers
 systemstap, stap-prep already installed.Compile the stp file in the normal way (till step 4)
Make the folder path /lib/modules/VERSION/systemtap and add the compiled program to that location.

Then add stapuser to the group stapusr,
P.S : note the difference in the two names .

Q16. Create an sos report which contains The string emergency Information about the nfsserver subsystem Should contain no information about the grub2 susbsytem.

Answers
Sos package already installed, get needfull commands from sosreport -l ---help
sosreport -e nfsserver -n grub2 --name emergency

Q17. Download the sos report at location http://myserver/soslog.tgz.Find the number of :
i) successful logins with the uid 91910
ii) total number of successful authentications
iii) total number of failed logins

Answers
Extract archive file and move to var/log/secure log file.

cat /var/log/secure | grep 91910 à get the username
grep 'session opened for user dummy' /var/log/secure
grep –i 'accepted password' /var/log/secure
grep –i 'failed password' /var/log/secure

Q18. Application running on serverb is communicating with another
server(my.org.example.com) and it is sending out a password periodically.
Capture the password and submit on the test box

Answers
Login to serverb with -X (ssh -X root@serverb)
yum install wireshark-gnome
Launch it (capture any ports) and Capture data for 2 minutes
Get the ip address of my.org.example.com by pinging.
Add a filter **ip.dst == <IP Address of my.org.example.com>**
Check **Follow TCP Stream** for password