Ensure all the tasks are implemented with firewalld and SELinux enabled. Your server should be able to survive a reboot. Good luck!

1. Interrupt the boot process and reset the root password. Change it to “wander” to gain access to the system.

Press e at first GRUB menu
At linux line, add ***systemd.unit=\rescue.target***
ctrl-x [reboot]
Enter password for maintenance
$ sudo  passwd root
systemctl reboot

**2. Repos are available from the repo server at http://repo.eight.example.com/BaseOS and http://repo.eight.example.com/AppStream for you to use during the exam.**

```
$ sudo  vi /etc/yum.repos.d/http.repo
[BaseOS]
name=BaseOS
baseurl=http://repo/BaseOS
enable=1
gpgcheck=0

[AppStream]
name=AppStream
baseurl=http://repo/AppStream
enable=1
gpgcheck=0

$ yum -v repolist
<- - output omitted - ->

Repo-id      : AppStream
Repo-name    : AppStream
<- - output omitted - ->
Repo-filename: /etc/yum.repos.d/http.repo

Repo-id      : BaseOS
Repo-name    : BaseOS
<- - output omitted - ->
Repo-filename: /etc/yum.repos.d/http.repo
Total packages: 6,330
```

3. The system time should be set to your (or nearest to you) timezone and ensure NTP sync is configured.

Set timezone
$ sudo  timedatectl list-timezones
$ sudo  timedatectl set-timezone America/Los_Angeles

NTP sync
$ sudo  timedatectl set-ntp true
$ sudo  systemctl restart chronyd
$ sudo  chronyc sources

firewall
$ sudo  firewall-cmd --add-service=ntp --permanent
$ sudo  firewall-cmd --reload

4. Add the following secondary IP addresses statically to your current running interface. Do this in a way that doesn't compromise your existing settings:
    a. IPV4 - 10.0.0.5/24
    b. IPV6 - fd01::100/64

$ ifconfig
$ sudo  nmcli connection down enp0s3
$ sudo  nmcli connection modify enp0s3 +ipv4.addresses "10.0.0.5/24"
$ sudo  nmcli connection modify enp0s3 +ipv6.addresses "fd01::100/64"
$ sudo  nmcli connection up enp0s3

5. Enable packet forwarding on system1. This should persist after reboot.

$ sudo  ssh vagrant@system1

[user@vagrant]$ sudo vi /etc/sysctl.conf
#IPv4
net.ipv4.ip_forward=1

#IPv6
net.ipv6.conf.all.forwarding = 1
net.ipv6.conf.all.disable_ipv6 = 0

6. System1 should boot into the multi-user target by default and boot messages should be present (not silenced).

$ sudo  ssh vagrant@system1

[user@vagrant]$ sudo  systemctl get-default
multi-user.target

$ sudo vi /etc/default/grub  -->  remove rhgb and quiet
$ sudo grub2-mkconfig --output=/boot/grub2/grub.cfg

7. Create a new 2GB volume group named “vgprac”.

```
$ sudo fdisk --list
[sudo] password for admin:
Disk /dev/sda: 15 GiB, 16106127360 bytes, 31457280 sectors
<- - output omitted - ->

Device     Boot   Start      End  Sectors  Size Id Type
/dev/sda1  *       2048  1953791  1951744  953M 83 Linux
/dev/sda2       1953792 23465983 21512192 10.3G 8e Linux LVM

$ sudo fdisk /dev/sdals
Command : n # new partition
Command : p # primary
Partition Number: 3
First Sector: default 2048
Last Sector: +2G
Command : w # write to disk and quit

Create physical volume
$ sudo pvcreate /dev/sda3
  Physical volume "/dev/sda3" successfully created.

Create volume group from physical volume
$ sudo vgcreate vgprac /dev/sda3
  Volume group "vgprac" successfully created
```

8. Create a 500MB logical volume named “lvprac” inside the “vgprac” volume group.

```
Create logical volume
$ sudo lvcreate -L 500M -n lvprac vgprac
  Logical volume "lvprac" created.
```

9. The “lvprac” logical volume should be formatted with the xfs filesystem and mount persistently on the /mnt/lvprac directory.

Format to xfs
$ sudo mkfs.xfs /dev/vgprac/lvprac

$ sudo blkid /dev/vgprac/lvprac
/dev/vgprac/lvprac: UUID="378eb12d-1037-485f-b381-c99b9c2ccbf6" TYPE="xfs"

Add drive to fstab
$ sudo vi /etc/fstab
UUID=52da3055-4ea3-4a98-8299-50cf5761129f /mnt/lvprac xfs defaults 0 0

$ sudo systemctl daemon-reload

$ sudo reboot

10. Extend the xfs filesystem on “lvprac” by 500MB.

$ sudo lvextend -L +500M /dev/vgprac/lvprac

$ sudo xfs_growfs /mnt/lvprac/
<- - output omitted - ->
data blocks changed from 128000 to 256000

11. Use the appropriate utility to create a 10TiB thin provisioned volume.

$ sudo lvcreate -L 100M -T vgprac/thin
Thin pool volume with chunk size 64.00 KiB can address at most 15.81 TiB of data.
Logical volume "thin" created.

$ sudo lvcreate -V 10T -T vgprac/thin -n thin_vol
WARNING: Sum of all thin volume sizes (10.00 TiB) exceeds the size of thin pool vgprac/thin and the size of whole volume group (<2.00 GiB).
WARNING: You have not turned on protection against thin pools running out of space.

WARNING: Set activation/thin_pool_autoextend_threshold below 100 to trigger automatic extension of thin pools before they get full.
Logical volume "thin_vol" created.

12. Configure a basic web server that displays “Welcome to the web server” once connected to it. Ensure the firewall allows the http/https services.

```
$ sudo  yum install httpd

$ sudo systemctl start httpd
$ sudo systemctl enable httpd

# firewall-cmd --add-service=http --permanent
# firewall-cmd --add-service=http
# echo "Welcome to the web servers" > /var/www/html/index.html

vi /etc/www/html/index.html
<html>
<body>Welcome to the web server</body>
</html>

$ sudo systemctl restart httpd
```

13. Find all files that are larger than 5MB in the /etc directory and copy them to /find/largefiles

```
$ sudo mkdir -p /find/largefiles

$ sudo find /etc -size +5M -exec cp {} /find/largefiles \;
```

14. Write a script named awesome.sh in the root directory on client1.
    a. If “me” is given as an argument, then the script should output “Yes, I’m awesome.”
    b. If “them” is given as an argument, then the script should output “Okay, they are awesome.”
    c. If the argument is empty or anything else is given, the script should output “Usage ./awesome.sh me|them”

```
$ sudo vi /home/user/awesome.sh

#!/bin/bash

# rhcsa script

case $1 in
  me)
    echo "Yes, I'm cool"
    ;;
  them)
    echo "OK, they are fine too"
     ;;
  *)
    echo "Usage ./awesome.sh me|them"
  exit 1
  ;;
esac

$ sudo chmod a+x awesome.sh
$ sudo./awesome.sh me|them
```

15. Create users phil, laura, stewart, and kevin.
    a. All new users should have a file named “Welcome” in their home folder after account creation.
    **b. All user passwords should expire after 60 days and be atleast 8 characters in length.**
    c. phil and laura should be part of the “accounting” group. If the group doesn’t already exist, create it.
    d. stewart and kevin should be part of the “marketing” group. If the group doesn’t already exist, create it.

```
$ sudo  groupadd marketing
$ sudo  groupadd accounting
$ sudo cat /etc/group
<- - output omitted - ->
apache:x:48:
accounting:x:1001:
marketing:x:1002:
$

$ sudo useradd phil -p phil -G accounting
$ sudo useradd laura -p laura -G accounting
$ sudo useradd stewart -p stewart  -G marketing
$ sudo useradd kevin -p kevin -G marketing

$ sudo cat /etc/group
<- - output omitted - ->
accounting:x:1001:phil,laura
marketing:x:1002:stewart,kevin

$ sudo cat /etc/passwd
<- - output omitted - ->
phil:x:1001:1003::/home/phil:/bin/bash
laura:x:1002:1004::/home/laura:/bin/bash
stewart:x:1003:1005::/home/stewart:/bin/bash
kevin:x:1004:1006::/home/kevin:/bin/bash

$ sudo chage -M 60 phil
$ sudo chage -M 60 laura
```

$ sudo chage -M 60 stewart
$ sudo chage -M 60 kevin

$ sudo vi /etc/security/pwquality.conf
Uncomment this line
> minlen = 8
$ sudo passwd laura
Changing password for user laura.
New password:
BAD PASSWORD: The password is shorter than 8 characters

$ sudo touch /home/kevin/welcome.txt
$ sudo touch /home/laura/welcome.txt
$ sudo touch /home/phil/welcome.txt
$ sudo touch /home/stewart/welcome.txt

16. Only members of the accounting group should have access to the “/accounting” directory. Make laura the owner of this directory. Make the accounting group the group owner of the “/accounting” directory.

$ sudo  mkdir /home/accounting
$ sudo  chown laura:accounting /home/accounting
$ sudo chmod 1770 /home/accounting

drwxrws---.  2 laura  accounting  6 Feb 11 21:30 accounting

17. Only members of the marketing group should have access to the “/marketing” directory. Make stewart the owner of this directory. Make the marketing group the group owner of the “/marketing” directory.

$ sudo  mkdir /home/marketing
$ sudo  chown stewart:marketing /home/marketing
$ sudo chmod 1770 /home/marketing

drwxrws---.  2 stewart marketing  6 Feb 11 21:30 marketing

18. New files should be owned by the group owner and only the file creator should have the permissions to delete their own files.

```
$ sudo chmod 1770 /home/accounting

$ sudo chmod 1770 /home/marketing
```

19. Create a cron job that writes “This practice exam was easy and I’m ready to ace my RHCSA” to /var/log/messages at 12pm only on weekdays.

```
$ sudo  vi /etc/crontab

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed
  *  0  *  *  * root       echo 'This practice exam was easy and I’m ready to ace my RHCSA' >> /var/log/messages
```

References


1. https://redhat-certs.slack.com/archives/CHDDTG4V6/p1578556372012800?thread_ts=1578556372.012800
2. https://www.thegeekdiary.com/what-is-suid-sgid-and-sticky-bit/