**Part 1:**

pvcreate /dev/sda2 /dev/sda3 #create physical memories

vgcreate -s 16M vg1 /dev/sda2 /dev/sda3 #create volume group vg1 and set 16M extends

lvcreate -l 50 -n lvm02 /dev/vg1 #create a logical volume with 50 extends

mkfs -t ext4 /dev/vg1/lvm02 #create a new file system and make it ext4

mkdir -p /mnt/data #create mounting directory

vim /etc/fstab #open fstab file

/dev/vg1/lvm02 /mnt/data ext4 defaults 0 0 #assign lvm02 to be mounted automatically in

#mnt/data

mount -a #mount the mentioned volumes in the file

**Part 2:**

**1+2)**

useradd user1 #create user1

passwd user1 #change password to redhat

vim /etc/ssh/sshd\_config #open sshd\_config to remove user1 ssh access

#add DenyUsers user1 line to the file

groupadd TrainingGroup #create the group TrainingGroup

usermod -a -G TrainingGroup user1 #assign user1 to TrainingGroup group

usermod -u 601 user1 #change user1 id to 601

cat /etc/passwd | less #check changes

systemctl restart sshd #restart ssh service to apply changes

ssh user1@172.20.30.30 #attempt ssh connection for user1

#Permission denied, please try again.

**3)**

useradd user2 #create user2

useradd user3 #create user3

groupadd admin #create admin group

usermod -a -G admin user2 #assign user2 to admin group

usermod -a -G admin user3 #assign user3 to admin group

passwd user2 #change password to redhat

passwd user3 #change password to redhat

visudo #open visudo file to change user3 permissions

#add the line (user3 ALL=(ALL) ALL) to give

#full root permissions

**Part 3:**

On machine 1:

ssh-keygen -t rsa #generate ssh key

cat /root/.ssh/id\_rsa.pub #open id\_rsa.pub to copy public key

On machine 2:

vim /root/.ssh/authorized\_keys #open authorized\_keys file and paste the public

#key in it

ssh root@192.168.204.217 #attempt ssh connection

**Part 4:**

cp /etc/fstab /var/tmp/ #copy file

mv /var/tmp/fstab /var/tmp/admin #change file name to “admin”

setfacl -m u:user1:rwx /var/tmp/admin #allow user1 to fully access the file

setfacl -m u:user2:--- /var/tmp/admin #deny user2 from all access to the file

**Part 5:**

setenforce 1 #make SElinux run in Enforcing mode

**Part 6:**

vim script.sh #create a script file and fill it with a script that runs

#for 10 minutes

sh script.sh & #execute script in the background

ps #check for the process id

kill 27525 #kill the process using its id

ps

**Part 7:**

cd /var/www/html/pub/zabbixzone/6Server/x86\_64/

wget -q -r -t1 --no-parent -nd --mirror <https://repo.zabbix.com/zabbix/4.4/rhel/7/x86_64/>

#download all packages to local machine

mkdir -p /home/mypackage\_dir/repository #make directory for repository

cp \* /home/mypackage\_dir/repository #copy all package files to the new directory

createrepo /home/mypackage\_dir/repository/

#create the repository

vi /etc/yum.repos.d/customrepo.repo #create the repo file for the repository and fill it with

#the following:

[local]

name=My RPM System Package Repo

baseurl=file:///home/mypackage\_dir/repository

enabled=1

gpgcheck=0

yum-config-manager --disable \* #disable all the repositories

yum-config-manager --enable local #enable the new repository

yum install zabbix-web #install the packages

yum install zabbix-server

yum install zabbix-agent

**Part 8:**

firewall-cmd --zone=public --add-port=80/tcp --permanent

#add port 80 and make changes permanent

firewall-cmd --zone=public --add-port=443/tcp --permanent

#add port 443 and make changes permanent

**Part 9:**

vim /home/cronscript.sh #create a script file and write a script that will output

# logged in users to a file

chmod +x /home/cronscript.sh #make the file executable

crontab -e #open the crontab scheduler and assign the file to

#execute at 1:30 AM

**Part 10:**

yum install mariadb-server #install the package

iptables -A INPUT -i eth0 -p tcp --dport 3306 -j ACCEPT

#add the port

iptables -A OUTPUT -p tcp -m tcp --dport 3306 -j ACCEPT

systemctl start mariadb.service #starting the service

systemctl enable mariadb.service #enabling the service

mysql -u root -p #connect to mariadb using ‘root’

MariaDB [(none)]> CREATE USER user@localhost IDENTIFIED BY 'mariadb';

MariaDB [(none)]> CREATE DATABASE studentdb;

MariaDB [(none)]> USE studentdb;

MariaDB [studentdb]> CREATE TABLE students (firstname VARCHAR(20), lastname

VARCHAR(20), program VARCHAR(40), expgrad SMALLINT UNSIGNED, number

VARCHAR(7) NOT NULL,PRIMARY KEY(number));

MariaDB [studentdb]> INSERT INTO students (firstname,lastname,program,expgrad,number)

VALUE ('Allen','Brown','mechanical',2017,'110-001'),('David','Brown','mechanical',2017,'110-002'),('Mary','Green','mechanical',2018,'110-003'),('Dennis','Green','electrical',2018,'110-004'),('Joseph','Black','electrical',2018,'110-005'),('Dennis','Black','electrical',2020,'110-006'),('Ritchie','Salt','computer science',2020,'110-007'),('Robert','Salt','computer science',2020,'110-008'),('David','Suzuki','computer science',2020,'110-009'),('Mary','Chen','computer science',2020,'110-010');

mysql -u user -p #connect to mariadb using ‘user’