1 adduser -u 1005 exam

[root@host58 ~]# id exam

uid=1007(exam) gid=1007(exam) groups=1007(exam)

2 vi /etc/sudoers

3 [root@host58 ~]# touch c.txt

root@host58 ~]# touch d.txt

4 [root@host57 ~]# adduser exam

passwd exam

Changing password for user exam.

New password:

BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word

Retype new password:

passwd: all authentication tokens updated successfully. [root@host58 .ssh]# ssh-keygen

Generating public/private rsa key pair.

Enter file in which to save the key (/root/.ssh/id\_rsa):

/root/.ssh/id\_rsa already exists.

Overwrite (y/n)? y

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in /root/.ssh/id\_rsa.

Your public key has been saved in /root/.ssh/id\_rsa.pub.

The key fingerprint is:

d2:3e:ac:50:a8:4e:da:83:6e:da:7e:c5:4f:bf:ea:27 root@host58.hpe

The key's randomart image is:

+--[ RSA 2048]----+

| |

| |

| |

| . . |

| ..o S |

| . .o+. |

| .o .. o+. |

|.B. .. .E.o |

|\*o=o ..o+.. |

|  |
| --- |
|  |

[root@host58 .ssh]# ssh-copy-id -i id\_rsa.pub exam@192.168.70.57

/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed

/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys

exam@192.168.70.57's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'exam@192.168.70.57'"

and check to make sure that only the key(s) you wanted were added.

[root@host58 .ssh]# ssh exam@192.168.70.57

[exam@host57 ~]$

5 tail -n 20 /var/log/secure | cat > tmp/file.txt

rsync –avrh /tmp/

7. [root@host58 .ssh]# groupadd testing

[root@host58 .ssh]# usermod –G testing exam

8 [root@host58 ~]# rpm -qa | grep telnet

[root@host58 ~]# rpm -ivh telnet-1.2-166.4.1.i586.rpm

9 ln file.text /tmp/

10 [root@host58 var]# tar -czf var.tar.g log

tar: log/audit/audit.log: file changed as we read it

[root@host58 var]# ls

abc.tar.bz2 comp empty kerberos lock nis run var.tar.g

adm crash games lib log opt spool yp

cache db gopher local mail preserve tmp

[root@host58 var]#

Question Set A

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

1. Create user with id 1005

2. make that user sudo user

3. create two empty file

4. create another user with same name in other server and share SSH keys with that user

5. redirect last 20 lines of /var/log/secure to a file in /tmp/file.txt directory

6. using rsync to copy a directory to /tmp in another server in /tmp and both directories should synchronised.

7. create a group named "testing" and add the user with id 1005 to that group

8. check whether "Telnet" package is installed , if yes remove using "rpm" command . Download package from internet and install it again using "rpm" command . (do not use yum).

9. Create a hardlink of testing.txt in /tmp directory and append the metadata of the file to /tmp/file.txt

10. create a tar file of /var/log using gz method

Question set B

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

1.Use find command to find full path of ntp.log

2.Create a file linux.txt and make it executable

3.install httpd service using yum

4.findout the process which is using most memory and kill that process

5.create a soft link and a hardlink of a file to any other directory

6.create a user " google" with no shell access and delete that user

7. using rsync copy a directory to another server /tmp and remove the source files

8.create another user with same name in other server and share SSH keys with that user

9.check whether "locate" command is installed , if yes remove using "rpm" command and Download package(package name :mlocate) from internet and install it again using "rpm" command . (do not use yum).

10.upload a putty.exe file to /tmp directory and download testing.txt file you created to desktop using Winscp.

Qusetion set C

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

1. Create a grouuop named "Anonymous"

2. Create an user and add that user to group "Anonymous"

3. Change the primary and secondary group of that user to "Anonymous"

4. create a directory and copy that directoty to another server using ssh

5. Create a file "permissions" and change the permission as it can only be read by others but it should have every permission for user and group

6. using rsync copy a directory to another server to /tmp/

7.create another user with same name in other server and share SSH keys with that user

8.check whether "ftp" package is installed , if yes remove using "rpm" command . Download package from internet and install it again using "rpm" command . (do not use yum).

9.create tar file using bz2 for /var directory and extract that in /tmp directory

10.remove ntp server using yum and install it again and start the service (no need of configuration)

Question set D

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

1. create a user "Ankara" with uid 1012 and make that user sudo user

2. Create a group "training" and add user Ankara to that group

3. Create a file "Testing.txt" as ankara user and change the group of file to "training " and this file should have every permission for owner and group but only execution permission for others.

4. using rsync and SSH copy a directory to any other server .

5. upload a putty.exe file to /tmp directory and download testing.txt file you created to desktop using Winscp.

6. check whether "vsftpd" command is installed , if yes remove using "rpm" command and Download package(package name :vsftpd) from internet and install it again using "rpm" command . (do not use yum).

7.create another user with same name in other server and share SSH keys with that user

8.from /var/log/secure find lines with "failure" and forward them to /tmp/failure.txt

9.create another user with same name in other server and share SSH keys with that user

10. using yum install httpd server and start the server