**Question 1: Archive, List, and Restore Files As user1 on server1, execute the tar command to create a gzip-compressed archive of the /etc directory. Run the tar command again to create a bzip2-compressed archive of the /etc directory. Compare the file sizes of the two archives. Run the tar command and uncompress and restore both archives without specifying the compression tool used. (Hint: Compression and Archiving).**

**Ans.**

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated with medium confidence

**Question 2: Practice the vim Editor As user1 on server1, create a file called vipractice in the home directory using vim. Type (do not copy and paste) each sentence from Lab 3-1 on a separate line (do not worry about line wrapping). Save the file and quit the editor. Open vipractice in vim again and reveal line numbering. Copy lines 2 and 3 to the end of the file to make the total number of lines in the file to 6. Move line 3 to make it line 1. Go to the last line and append the contents of the .bash\_profile. Substitute all occurrences of the string “Profile” with “Pro File”, and all occurrences of the string “profile” with “pro file”. Remove lines 5 to 8. Save the file and quit vim. Provide a count of lines, words, and characters in the vipractice file using the wc command. (Hint: File Editing).**

**Ans.**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Graphical user interface, text

Description automatically generated**

**Question 3: Manipulate File Permissions As user1 on server1, create file file11 and directory dir11 in the home directory. Make a note of the permissions on them. Run the umask command to determine the current umask. Change the umask value to 0035 using symbolic notation. Create file22 and directory dir22 in the home directory. Observe the permissions on file22 and dir22, and compare them with the permissions on file11 and dir11. Use the chmod command and modify the permissions on file11 to match those on file22. Use the chmod command and modify the permissions on dir22 to match those on dir11. Do not remove file11, file22, dir11, and dir22 yet. (Hint: File and Directory Access Permissions).**

**Ans.**

**A picture containing text

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

**Text

Description automatically generated**

**Graphical user interface, text

Description automatically generated**

**A picture containing application

Description automatically generated**

**Graphical user interface

Description automatically generated with medium confidence**

**Question 4: Apply ACL Settings As root on server1, create file testfile under /tmp. Apply ACL settings on the file so that user2000 gets 7, user3000 gets 6, and user4000 gets 4 permissions. Create users. Remove the ACLs for user2000, and verify. Remove all remaining ACLs at once, and confirm. (Hint: Access Control Lists).**

**Ans.**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Question 5: As root on server1, execute the last, lastb, and lastlog commands, and observe the outputs. Check which users have recently logged in and out of the system successfully (last) and unsuccessfully (lastb). List the timestamps when the system was last rebooted (last). Check the last login status for each user (lastlog). Use the vim editor to record your results. (Hint: User Login Activity and Information).**

**Ans.**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Graphical user interface, text

Description automatically generated**

**Question 6: As root on server1, add a rule for user5000 to the /etc/sudoers file to allow this user full root access on the system. Make sure that this user is not prompted for a password when they use sudo to execute a command. Now switch into this user account and try running sudo vgs, and see if that works. (Hint: Substituting Users and Doing as Superuser).**

**Ans.**

**Text

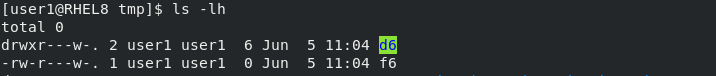
Description automatically generated**

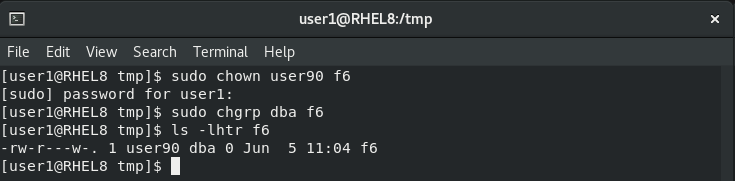
**Text

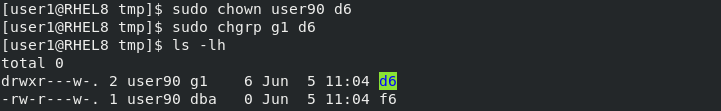
Description automatically generated**

**Question 7: As user1 on server1, create file f6 and directory d6 under /tmp. Change owning user for f6 to user90 (create user) using sudo chown, and owning group to dba with sudo chgrp. Change owning user and group on d6 to user90:g1 (create group) recursively using sudo chown. (Hint: Owing User and Owning Group).**

**Ans.**

****

****

****

**Question 8: As user1 with sudo on server1, open two terminal sessions. Run the top command in terminal 1. Run the pgrep or ps command in terminal 2 to determine the PID and the nice value of top. Stop top on terminal 1 and relaunch at a lower priority (+8). Confirm the new nice value of the process in terminal 2. Issue the renice command in terminal 2 and increase the priority of top to -10, and validate. (Hint: Processes and Priorities).**

**Ans.**

**Text

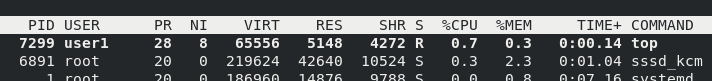
Description automatically generated with low confidence**

**Shape

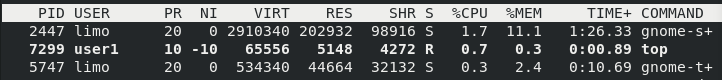
Description automatically generated with low confidence**

**A picture containing rectangle

Description automatically generated**

****

****

****

**Question 9: Install and Manage Individual Packages As user1 with sudo on server1 and using the dnf command, list all installed and available packages separately. Show which package contains the /etc/group file. Install the package policycoreutils. Review /var/log/yum.log for confirmation. Perform the following on the policycoreutils package: (1) show information, (2) list dependencies, and (3) remove it. (Hint: Individual Package Management).**

**Ans.**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Question 10: Install and Manage Modules As user1 with sudo on server1 and using the dnf command, list all modules. Identify which modules, streams and profiles are installed, default, disabled, and enabled from the output. Install the default stream of the development profile for module php, and verify. Remove the module. (Hint: Module Management).**

**Ans.**

**Text

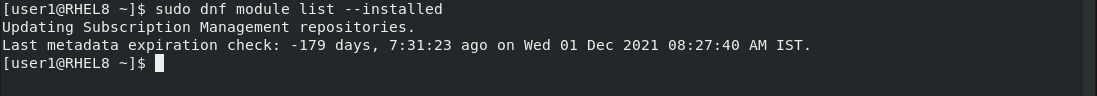
Description automatically generated**

**Text

Description automatically generated**

**Graphical user interface, text

Description automatically generated**

****

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**