Faculty of Technology and Engineering

U & P U. Patel Department of Computer Engineering

Date: 20/06/2024

Practical 2

Aim: User Administration

1. Manage local users, groups and creation of multiple users from excel sheet
2. Control access to files

Commands for reference:
System Administrator: su, adduser, addgroup, rmuser, shutdown
Control Access: chmod, umask

Exercise – 2

PART A

Manage local users, groups and creation of multiple users from excel sheet

1. Run id command to view the current user and group information.
2. display the current working directory.
3. print the value of HOME and PATH variable to determine the home directory and user's executable's path respectively.
4. Run su and su - command. Observe the output for the same.what is the main difference between them?
5. Run sudo su at the shell prompt to become the root user.
6. Run id command to view the current user and group information.
7. display the current working directory.
8. print the value of HOME and PATH variable to determine the home directory and user's executable's path respectively.
9. Exit the current user's shell to return to the student user's shell
10. Attempt to view the last five lines of /var/log/auth.log without using sudo
11. Attempt to view the last five lines of /var/log/auth.log using sudo
12. Attempt to make a copy of /etc/rpc as /etc/rpcOLD without using sudo
13. Attempt to make a copy of /etc/rpc as /etc/rpcOLD with sudo.
14. Attempt to delete /etc/rpcOLD without using sudo
15. Attempt to delete /etc/rpcdOLD with sudo
16. check the UID for root user, administrator and local users.
17. Adduser user01.
18. Create the group group01 with the GID of 10000.

19. Create the group group02
20. Examine /etc/group to verify the supplemental group memberships.
21. Use the usermod -aG command to add a user to a supplementary group. Add user01 to the group created.
22. Observe /etc/group and /etc/passwd

PART B

Control access to files

1. Check the permission of files created.
2. Check the permission of directories created.
3. Set read and write permissions for others with numeric mode to file1.txt
4. Remove write permission for user, group and others to folder CE.
5. Create a directory 5CE under CE. Observe the response.
6. Set read, write and execute permissions for user, group and others to 5CE.
7. Set read and execute permission for group and no permission for other to file2.txt.
8. Change the ownership of file to user01
9. Change the group ownership of file to group01
10. Change the ownership of both group and user at the same time.
11. Set the special permissions on directory.
    a. The *setuid* permission on an executable file means that commands run as the user owning the file, not as the user that ran the command. One example is the passwd command:run `ls -l /usr/bin/passwd`
    b. The special permission *setgid* on a directory means that files created in the directory inherit their group ownership from the directory, rather than inheriting it from the creating user. run `ls -ld /run/log/journal`
    c. the *sticky bit* for a directory sets a special restriction on deletion of files. Only the owner of the file (and root) can delete files within the directory. run `ls -ld /tmp`
12. Set the setusid, setgid and sticky bit for different files and perform the operations accordingly.
13. Display the current value of shell's mask.
14. Check the permission of directories.
15. Check the permission of files.
16. Set the umask to 542.
17. Check the permission of files and directories.
18. Try to open the file and directory created.
19. Try to open the file as other user.
20. Take a snapshot and prepare file for submission.