Linux Exam (Practical based)

1. Copy the file /etc/passwd to /tmp/passwd.bak.
2. Move the file /tmp/passwd.bak to the directory /root/backups/.
3. Use chage to set the password of user john to expire in 5 days.
4. Change the ownership of the file /root/report.txt to user alice and group devops.
5. Set read, write, and execute permissions for the owner, and no permissions for group and others on /root/secret.txt.
6. Grant full permissions to a file /root/superfile.sh only for the root user.
7. Apply an ACL to file /root/project.txt so that user david has read and write access.
8. Modify the default umask value to 027 and create a new file to reflect the change.
9. Create a new user named devadmin.
10. Create a new group named ops_team.
11. Create a user deploy with primary group ops_team.

12. Create a user analyst with secondary group ops_team but a different primary group.
13. Create a hard link to /root/data.txt named /root/data_hardlink.txt.
14. Create a symbolic (soft) link to /root/data.txt named /root/data_softlink.txt.
15. Display the first 15 lines of the file /etc/passwd.
16. Display the last 7 lines of the file /etc/group.
17. Create a file named devops_notes.txt inside /home/student/ and copy it to /var/tmp/.
18. Move the file /var/tmp/devops_notes.txt to /opt/reports/.
19. Set the file /opt/reports/devops_notes.txt so that only the group owner can read and write it.
20. Set ownership of the directory /opt/reports to user manager and group qa_team.
21. Add execute permission only for others on the file /usr/local/bin/startup.sh.
22. Assign ACL permission to user sam to have execute-only access on /usr/local/bin/startup.sh.

23. Change the umask value temporarily to 0022 and create a new directory secure_folder in /tmp.
24. Create a group auditlog and a user loguser with that group as the primary group.
25. Create a user support and add them to both auditlog and qa_team as secondary groups.
26. Create a soft link to /var/log/syslog named /tmp/syslog_link and a hard link named /tmp/syslog_hard.
27. Create a user named trainer with no home directory.
28. Create a user named intern with /home/intern_data as the custom home directory.
29. Modify the shell of user intern to /bin/bash.
30. Lock the user account testuser.
31. Unlock the user account testuser.
32. Delete the user oldstaff and remove their home directory along with the account.
33. Create a group named docker_users and assign user deploy to this group.
34. Change the primary group of user developer to engineering.

35. Add the user auditor to the groups compliance and security as secondary groups.
36. List all the groups that user alice belongs to.
37. A group named sysadmin. A user ryan who belongs to sysadmin as a secondary group. Auser sarah who also belongs to sysadmin as a secondary group. A user harry who does
not have access to an interactive shell on the system, and who is not a member of
sysadmin. ryan, sarah and harry should all have their password as atenorth.

38. Group ownership of /common/admin is to be set to sysadmin. The directory should bereadable, writable, and accessible to members of sysadmin, but not to any other user. (Itis understood that root has access to all files and directories on the system.)
Files created in /common/admin should automatically have group ownership set to the
sysadmin group.