User Administration:

1. Create user account xyz with comment testing
2. Change the min number of days to change password to be 3 days
3. Change the maximum number of days to change the password after 90 day
4. Change the warning before the account disabled
5. Create a directory called /depts with a sales, hr, and web directory within the /depts directory.
6. Using the chgrp and chown command, set the group ownership of each directory to the group with the matching name.
7. Create 6 users 2 in each group sales, hr and web and give them password
8. Let the newly created files for each user with the group name and protect it from delete using special permissions.
9. Create a directory with permissions rwxrwx---, grant a second group (sales) r-x permissions
10. create a file on that directory and grant read and write to a second group (sales)
11. set the the owning group as the owning group of **any newly created** file in that directory.
12. Grant your colleagues a collective directory called /opt/research, where they can store generated research results. Only members of group profs and grads should be able to create new files in the directory, and new file should have the following properties:
    a. the directory should be owned by root
    b. new files should be group owned by group grads
    c. group profs should automatically have read/write access to new files
    d. group interns should automatically have read only access to new files
    e. other users should not be able to access the directory and its contents at all.
13. Configure sudoers file to allow user3 and user4 to use /usr/sbin/useradd and /usr/sbin/usermod commands, while allowing user5 only to use fdisk command.
14. Create user account hhh using user3
15. Try to view the partitions of the system using the account of user5
16. use at to execute command tar cvf /home.tar tar five minutes from now
17. use cron command to create backup from /etc directory and compress it with gzip tool every day at mid night and store it in user root’s home dir.