1. Install Ubuntu in either VMware or VirtualBox
2. Find the path where the following files and directory are located

* shadow
* directory
* grub
* sudo
* python
* log
* interfaces
* fonts.config
* dnscache
* dmesg
* kernel of ubuntu

1. Use the grep command and list out all the following then save it in a file

* find all words ending with "ing"
* count the number of words that ends with "ing"
* find all the words starting with "be"
* Find the exact word "test"
* Find all words that start with "m" and ends with "t"
* find the MAC addresses
* find the telephone addresses
* find the email addresses
* find the social security number
* find out the IP addresses

1. Make 30 folders with the name folder\_1 through folder\_30 in your home directory
2. Make folders folder\_21 to folder\_30 hidden
3. Create 15 .txt files (hint: use the touch command in the terminal)
4. Install vim
5. Copy files 1 to 7 to folder 1
6. Move the rest of the files to folder 2
7. List out all the hidden folders in your home directory
8. Configure so that the user uid start from 2000 and allow only 100 users to be created
9. Create 30 users
10. Assign passwords for each user
11. Login as user 1,2,4, 20 and 28 then designate the home directories to which they can log on
12. Configure the Password policy such that:

* Passwords must have lower case, upper case, symbols and numbers.
* Password must be hashed with 512
* Minimum length must be 8
* Password should not be the same as the username
* Set password history to 10
* Add expiration date for the account to 6 months from the date you created the account
* Set the max days after which the user must change passwords
* Set minimum number of days allowed between password changes to 15
* Give a 10 day warning before the password expires
* Make it inactive if the account is expired(for new and for existing users)
* Set the minimum number of attempts for login to 5
* Change the login lockout time to 5 minutes
* Set the login time out equal to 120 seconds.
* Make root’s password the same as your password.
* Configure so that the users have to create a new password when they login the first time

1. Make sure you record failed logins
2. Make sure successful logins are also recorded
3. Write down the ENV\_PATH and ENV\_SUPATH
4. Set encryption to SHA 512 and encrypt for 10000 rounds.
5. Configure so that users 1 to 5 can login anytime.
6. Configure so that users 6 to 10 can only login on Monday, Wednesday and Friday from 8am to 6pm.
7. Configure so that users 11 to 20 can only login on weekdays from 9am to 5pm.
8. Configure so that users 21 to 30 can only login on weekdays from 8am to 8pm.
9. Find out when user 1 last logged on to the system.
10. Create 5 more users with admin rights.
11. Give user 25 to 30 admin rights.
12. Configure so that user 30 has auto-login set.
13. Create 4 groups named CEO, marketing, developer, and worker with 2 users in each of the group, and transfer the 30 users created earlier in the group.
14. Write down the permission of shadow file.
15. Write down the owner of the shadow file.
16. Give yourself ownership of folder\_1 through folder\_10.
17. Make group CEO the owner of folder\_11 to folder 15.
18. List all the groups that you made.
19. Create a file named test, test\_1 and test\_2 and write down the default permissions of the file.
20. Change the permission of test so that only the owner has read write permissions of that file
21. Change the permission of test\_1 so that owner has read write and execute permissions, the group have read and execute permissions and other users have no permission.
22. Change the permission of test\_2 so that the owner, group and user have read, write, and execute rights.
23. Create folders CEO, developer, and marketing in the home directory. Configure so that only the CEO group can access the CEO folder, the developer group can access the developer folder, and the marketing group can access the marketing folder.
24. Lock accounts for user 20, 21, 23, 25, 11, and 19.
25. Update and upgrade your ubuntu.
26. Write down your encrypted password.