1. What is the size of MBR and what does it contain?

    - The master boot record is a category of boot sector and the very first sector found in computer mass storage media such as fixed disks and removable computer drives.
    - Provides the information on loading the operating system and also on the partition of the hard disk
    - Programs in MBR determine which partition needs to be used while booting.
    - A master boot record is generally 512 bytes.

2. In which file you can write commands which you want to run whenever Linux system starts/restarts?

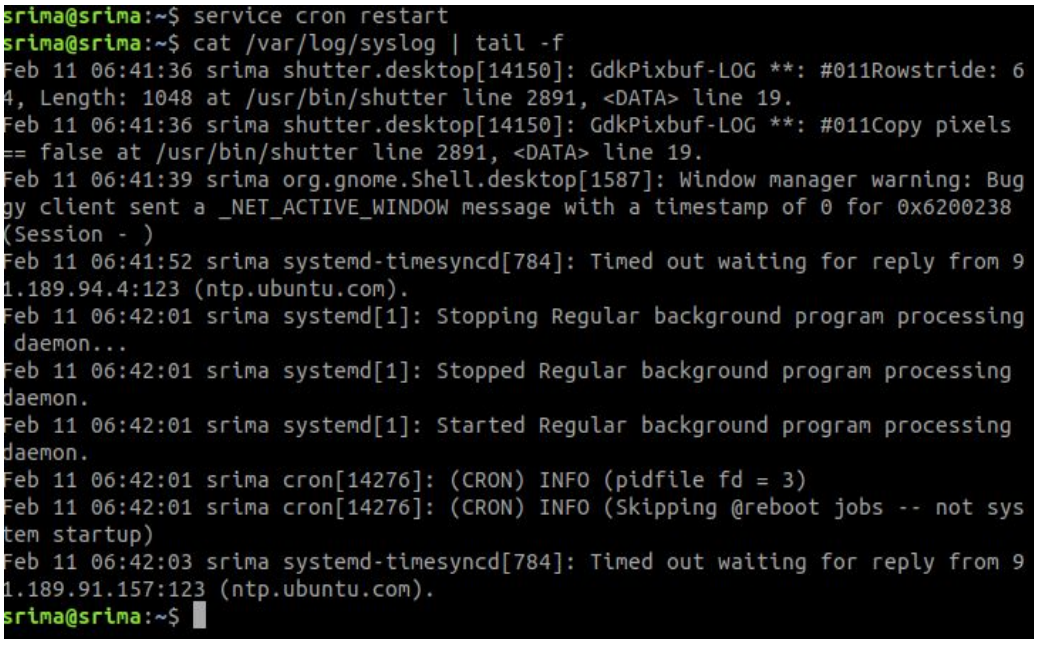
    Ans) rc.local

3. Reboot the system using runlevel.

    Ans) init 6

4. Restart cron service.

    Ans) service cron restart



5. Create an ext4 filesystem.

   It is done after creating a partition using mkfs.ext4 command.

6. Mount the created filesystem on /partition directory.

   Temporary mount:

   mkdir /mnt
   mount -t /dev/sda1 /mnt

   To permanently mount, make an entry in the file /etc/fstab

7. Difference between LVM and RAID.

LVM	RAID
To create a redundant or striped block device with redundancy using other physical block devices.	Multiple volumes can be created crossing multiple physical devices, remove physical devices without loosing data, resize the volumes, create snapshots, etc
A RAID device is a physical grouping of disk devices in order to create a logical presentation of one device to an Operating System for redundancy or performance or a combination of the two.	LVM is a logical layer that that can be manipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.
RAID is either a software or a hardware technique to create data storage redundancy across multiple block devices based on required RAID levels.	LVM is a software tool to manage large pool of storage devices making them appear as a single manageable pool of storage resource.

8. Create a LVM(Slide 13)

Create PV
pvcreate /dev/sda1

Create VG
vgcreate myvg /dev/sda1 /dev/sda2

Create LVM

lvcreate -n vo -L 10G myvg

9. Create a RAID1 device

10. Create a swapfile of 500Mb

sudo swapon --show
free -h
df -h
sudo fallocate -l 1G /swapfile
sudo chmod 600 /swapfile
ls -lh /swapfile
sudo mkswap /swapfile
echo '/swapfile none swap sw 0 0' | sudo tee -a /etc/fstab
mount -a

11. Set setuid and setgid on two different files.

```
ubuntu@ip-172-31-2-130:~$ mkdir demo
ubuntu@ip-172-31-2-130:~$ cd demo/
ubuntu@ip-172-31-2-130:~/demo$ touch demo
ubuntu@ip-172-31-2-130:~/demo$ ls -l demo
-rw-rw-r-- 1 ubuntu ubuntu 0 Feb 11 12:30 demo
ubuntu@ip-172-31-2-130:~/demo$ chmod 4664 demo
ubuntu@ip-172-31-2-130:~/demo$ ls -l demo
-rwSrw-r-- 1 ubuntu ubuntu 0 Feb 11 12:30 demo
ubuntu@ip-172-31-2-130:~/demo$
```

```
ubuntu@ip-172-31-2-130:~/demo$ ll
total 8
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 11 12:32 ./
drwxr-xr-x 6 ubuntu ubuntu 4096 Feb 11 14:46 ../
-rwSrw-r-- 1 ubuntu ubuntu    0 Feb 11 12:30 demo
-rw-rw-r-- 1 ubuntu ubuntu    0 Feb 11 12:32 demo2.txt
ubuntu@ip-172-31-2-130:~/demo$ chmod 2664 demo2.txt
ubuntu@ip-172-31-2-130:~/demo$ ll
total 8
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 11 12:32 ./
drwxr-xr-x 6 ubuntu ubuntu 4096 Feb 11 14:46 ../
-rwSrw-r-- 1 ubuntu ubuntu    0 Feb 11 12:30 demo
-rw-rwSr-- 1 ubuntu ubuntu    0 Feb 11 12:32 demo2.txt
ubuntu@ip-172-31-2-130:~/demo$
```

12. What is the use of Sticky bit.

Ans) Normally, for deleting files , one doesn't need permission , hence one user can easily delete other's files. To prevent this, sticky bit is used. On applying sticky bit, A user can read others file, execute it but cannot delete it. When a directory's **sticky bit** is set, the filesystem treats the files in such directories in a special way so only the file's owner, the directory's owner, or root can rename or delete the file.

13. Create a user and add it to one secondary group.

```
ubuntu@ip-172-31-2-130:~$ sudo adduser srima
Adding user `srima' ...
Adding new group `srima' (1001) ...
Adding new user `srima' (1001) with group `srima' ...
Creating home directory `/home/srima' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for srima
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
ubuntu@ip-172-31-2-130:~$ sudo groupadd mygroup
ubuntu@ip-172-31-2-130:~$ sudo usermod -G srima mygroup
usermod: user 'mygroup' does not exist
ubuntu@ip-172-31-2-130:~$ sudo usermod -G mygroup srima
ubuntu@ip-172-31-2-130:~$ id srima
uid=1001(srima) gid=1001(srima) groups=1001(srima),1002(mygroup)
ubuntu@ip-172-31-2-130:~$
```

14. Lock this user.

```
ubuntu@ip-172-31-2-130:~$ sudo usermod -L srima
```

```
ubuntu@ip-172-31-2-130:~$ sudo grep srima /etc/shadow
srima:!$6$S.KdWq/M$Fk8L1LVQunoJRzXthM8xdJ7iOA8/X7uV3DqJrTFcMiLXINVMNvfPzjAse7RVx
C32h6jDiwm3hIzgNrL1gyt7N.:18303:0:99999:7:::
```

15. Give this user full access (without password).

```
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/
sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
srima  ALL=(ALL) NOPASSWD: ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

```
ubuntu@ip-172-31-2-130:~$ sudo vi /etc/sudoers
ubuntu@ip-172-31-2-130:~$ sudo su srima
srima@ip-172-31-2-130:/home/ubuntu$
```

16. Delete the create user after taking backup of it home directory.

```
ubuntu@ip-172-31-2-130:~$ tar -czpvf backup.tar.gz /home/srima
tar: Removing leading `/' from member names
/home/srima/
/home/srima/.profile
/home/srima/.bashrc
/home/srima/.bash_logout
```

```
ubuntu@ip-172-31-2-130:~$ sudo userdel srima
ubuntu@ip-172-31-2-130:~$ id srima
id: ‘srima’: no such user
ubuntu@ip-172-31-2-130:~$
```

17. Create a file with some content. Change all lower case letter to upper case letter and save output to another file using redirections.

```
ubuntu@ip-172-31-2-130:~$ cat somefile.txt | tr a-z A-Z > uppercase.txt
ubuntu@ip-172-31-2-130:~$ cat uppercase.txt
 THIS IS DEMO FILE FOR ASSIGNMENT
ubuntu@ip-172-31-2-130:~$
```

18. Set nice value of a process to -1.

```
ubuntu@ip-172-31-2-130:~$ ps aux | grep cron
root         790  0.0  0.3  31748  3272 ?        Ss   11:50   0:00 /usr/
sbin/cron -f
ubuntu     14965  0.0  0.1  14856  1032 pts/1    S+   19:21   0:00 grep
--color=auto cron
ubuntu@ip-172-31-2-130:~$ sudo renice -n -1 -p 790
790 (process ID) old priority 0, new priority -1
ubuntu@ip-172-31-2-130:~$
```

19. Get list of all files used by “telnet”.

```
ubuntu@ip-172-31-2-130:~$ sudo dpkg -L telnet
/.
/usr
/usr/bin
/usr/bin/telnet.netkit
/usr/share
/usr/share/doc
/usr/share/doc/telnet
/usr/share/doc/telnet/BUGS
/usr/share/doc/telnet/README.gz
/usr/share/doc/telnet/README.telnet
/usr/share/doc/telnet/README.telnet.old.gz
/usr/share/doc/telnet/changelog.Debian.gz
/usr/share/doc/telnet/copyright
/usr/share/lintian
/usr/share/lintian/overrides
/usr/share/lintian/overrides/telnet
/usr/share/man
/usr/share/man/man1
/usr/share/man/man1/telnet.netkit.1.gz
/usr/share/menu
/usr/share/menu/telnet
ubuntu@ip-172-31-2-130:~$
```

20. Check if port 22 is listening using netstat and telnet command.

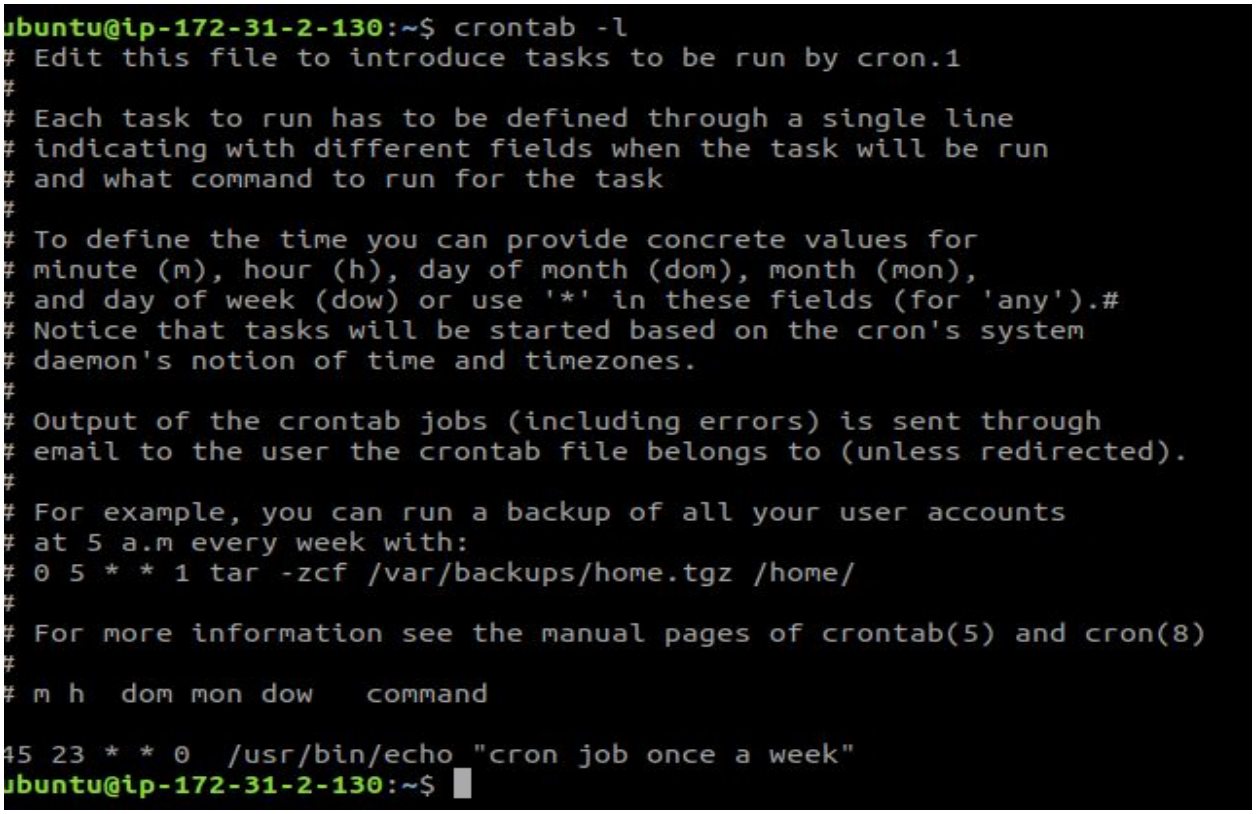
Using netstat

```
ubuntu@ip-172-31-2-130:~$ netstat -tnlp | grep 22
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LI
STEN       -
tcp6       0      0 :::22                   :::*                    LI
STEN       -
```

Using telnet

```
ubuntu@ip-172-31-2-130:~$ telnet 172.31.2.130 22
Trying 172.31.2.130...
Connected to 172.31.2.130.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3
```

21. Create a cron job which runs once in a week at 23:45.



22. Difference between dig and traceroute

Traceroute command : It shows the path of a packet going from your host/computer through each of the individual routes that handle the packet and time required for it to go from one router to another up to the final host/destination.

Dig Command: dig(Domain Information Groper) query DNS related information like a record, cname, mxrecord etc. This command is used to solve DNS related queries.