Assignment 3: Advanced LINUX

Trainee Name : Arun Parmar

Mentor Name : Mr. Ravi Kumar

College Name : UPES

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

   The Master Boot Record (MBR) is the information in the first sector of any hard disk or diskette that identifies how and where an operating system is located so that it can be boot (loaded) into the computer's main storage or random access memory. The Master Boot Record is also sometimes called the "partition sector" or the "master partition table" because it includes a table that locates each partition that the hard disk has been formatted into.

   Total size of MBR is 512 bytes, which is divided as follows:

   -446 bytes Bootloader

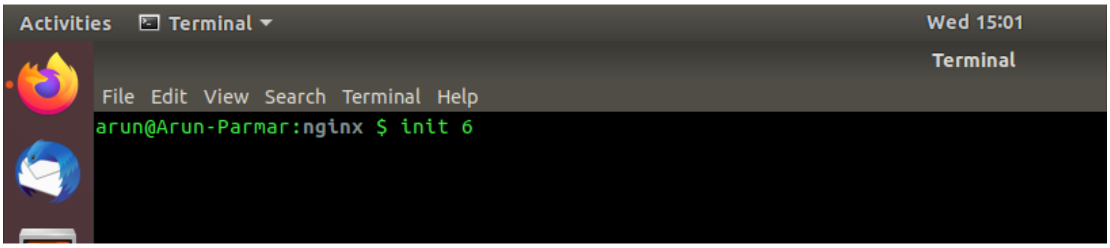
   -64 bytes (4 * 16 bytes) Partition Tables

   -2 bytes Magic Number which is AA55H

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

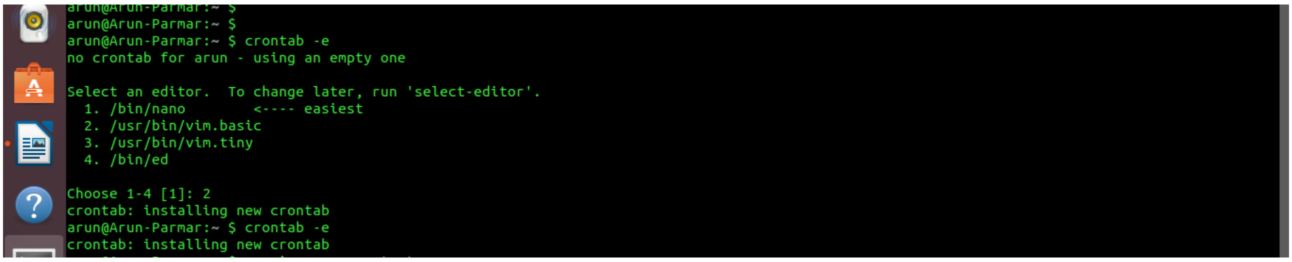
   We can use the ‘rc.local’ file located in ‘/etc/’ to execute our scripts and commands at startup. We will make an entry to execute the script in the file & every time when our system starts, the script will be executed. But we need to make this file /etc/c.local, executable. rc. local is not present already. But if we want to execute some command at run time, rc. Local can be created in /etc and commands can be executed.

3. Reboot the system using runlevel.

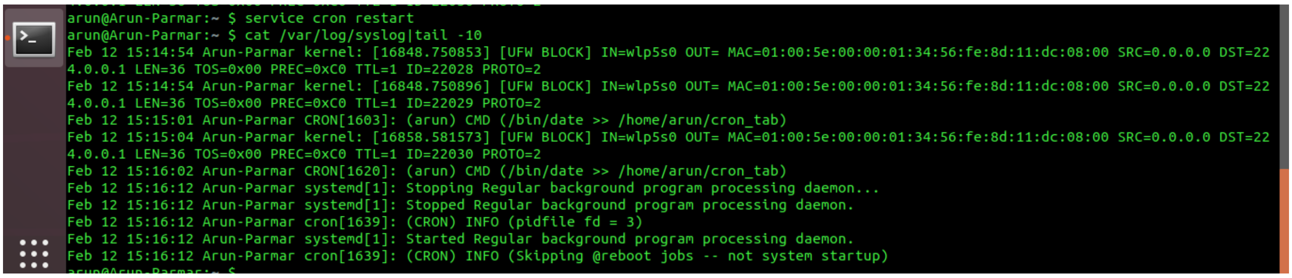


```
arun@Arun-Parmar:nginx $ init 6
```

4. Restart cron service.



```
arun@Arun-Parmar:~ $
arun@Arun-Parmar:~ $
arun@Arun-Parmar:~ $ crontab -e
no crontab for arun - using an empty one

Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.basic
  3. /usr/bin/vim.tiny
  4. /bin/ed

Choose 1-4 [1]: 2
crontab: installing new crontab
arun@Arun-Parmar:~ $ crontab -e
crontab: installing new crontab
```

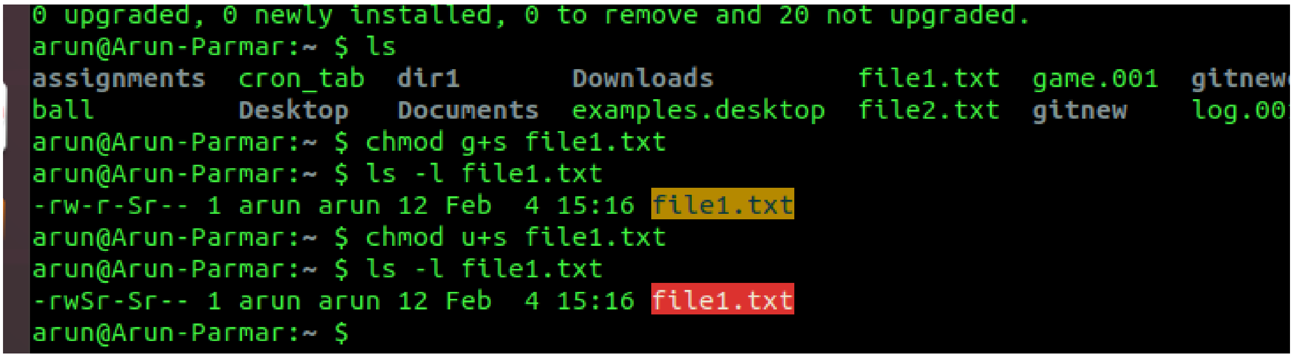


```
arun@Arun-Parmar:~ $ service cron restart
arun@Arun-Parmar:~ $ cat /var/log/syslog|tail -10
Feb 12 15:14:54 Arun-Parmar kernel: [16848.750853] [UFW BLOCK] IN=wlp5s0 OUT= MAC=01:00:5e:00:00:01:34:56:fe:8d:11:dc:08:00 SRC=0.0.0.0 DST=22
4.0.0.1 LEN=36 TOS=0x00 PREC=0xC0 TTL=1 ID=22028 PROTO=2
Feb 12 15:14:54 Arun-Parmar kernel: [16848.750896] [UFW BLOCK] IN=wlp5s0 OUT= MAC=01:00:5e:00:00:01:34:56:fe:8d:11:dc:08:00 SRC=0.0.0.0 DST=22
4.0.0.1 LEN=36 TOS=0x00 PREC=0xC0 TTL=1 ID=22029 PROTO=2
Feb 12 15:15:01 Arun-Parmar CRON[1603]: (arun) CMD (/bin/date >> /home/arun/cron_tab)
Feb 12 15:15:04 Arun-Parmar kernel: [16858.581573] [UFW BLOCK] IN=wlp5s0 OUT= MAC=01:00:5e:00:00:01:34:56:fe:8d:11:dc:08:00 SRC=0.0.0.0 DST=22
4.0.0.1 LEN=36 TOS=0x00 PREC=0xC0 TTL=1 ID=22030 PROTO=2
Feb 12 15:16:02 Arun-Parmar CRON[1620]: (arun) CMD (/bin/date >> /home/arun/cron_tab)
Feb 12 15:16:12 Arun-Parmar systemd[1]: Stopping Regular background program processing daemon...
Feb 12 15:16:12 Arun-Parmar systemd[1]: Stopped Regular background program processing daemon.
Feb 12 15:16:12 Arun-Parmar cron[1639]: (CRON) INFO (pidfile fd = 3)
Feb 12 15:16:12 Arun-Parmar systemd[1]: Started Regular background program processing daemon.
Feb 12 15:16:12 Arun-Parmar cron[1639]: (CRON) INFO (Skipping @reboot jobs -- not system startup)
arun@Arun-Parmar:~ $
```

5. Difference between LVM and RAID.

S.No.	RAID	LVM
1.	RAID is used for redundancy.	LVM is a way in which you partition the hard disk logically and it contains its own advantages.
2.	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 anipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.
3.	RAID is a way to create a redundant or striped block device with redundancy using other physical block devices.	LVM usually sits on top of RAID blocks or even standard block devices to accomplish the same result as a partitioning, however it is much more flexible than partitions. You can create multiple volumes crossing multiple physical devices, remove physical devices without loosing data, resize the volumes, create snapshots, etc
4.	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. LVM can be used to manage a large pool of what we call Just-a-bunch-of-Disk (JBOD) presenting them as a single logical volume and thereby create various partitions for software RAID.
5.	RAID is NOT any kind of Data backup solution. Its a solution to prevent one of the SPOFs (Single Point of Failure) i.e. DISK failure. By configuring RAID you are just providing an emergency substitute for the Primary disk. It NEVER means that you have configured DATA backup.	LVM is a disk management approach that allows us to create, extend, reduce, delete or resize the volume groups or logical volumes.

6. Set setuid and setgid on two different file.



```
0 upgraded, 0 newly installed, 0 to remove and 20 not upgraded.
arun@Arun-Parmar:~ $ ls
assignments  cron_tab  dir1       Downloads         file1.txt  game.001  gitnew
ball         Desktop   Documents  examples.desktop  file2.txt  gitnew    log.00
arun@Arun-Parmar:~ $ chmod g+s file1.txt
arun@Arun-Parmar:~ $ ls -l file1.txt
-rw-r-Sr-- 1 arun arun 12 Feb  4 15:16 file1.txt
arun@Arun-Parmar:~ $ chmod u+s file1.txt
arun@Arun-Parmar:~ $ ls -l file1.txt
-rwSr-Sr-- 1 arun arun 12 Feb  4 15:16 file1.txt
arun@Arun-Parmar:~ $
```

7. What is the use of Sticky bit.

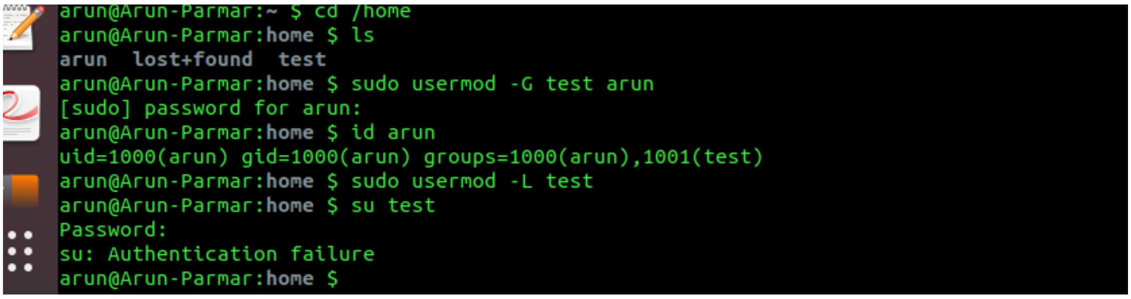
– The sticky bit is primarily used on shared directories.

– It is useful for shared directories such as /var/tmp and /tmp because users can create files, read and execute files owned by other users, but are not allowed to remove files owned by other users.

– For example if user bob creates a file named /tmp/bob, other user tom can not delete this file even when the /tmp directory has permission of 777. If sticky bit is not set then tom can delete /tmp/bob, as the /tmp/bob file inherits the parent directory permissions.

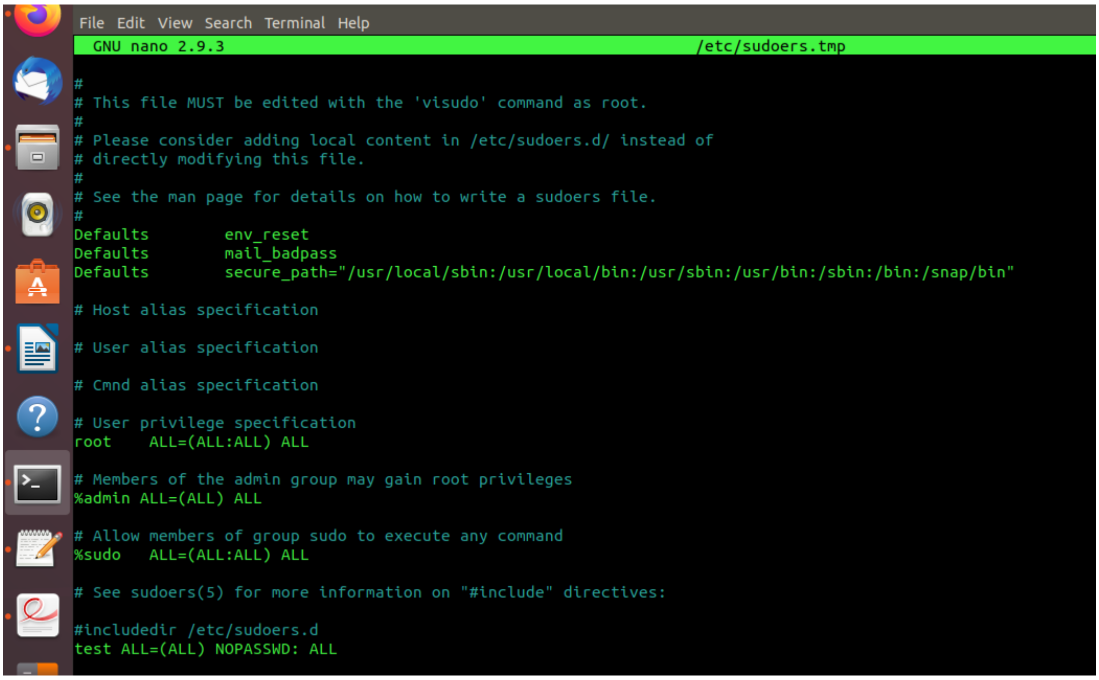
8. Create a user and add it to one secondary group.

9. Lock this user.



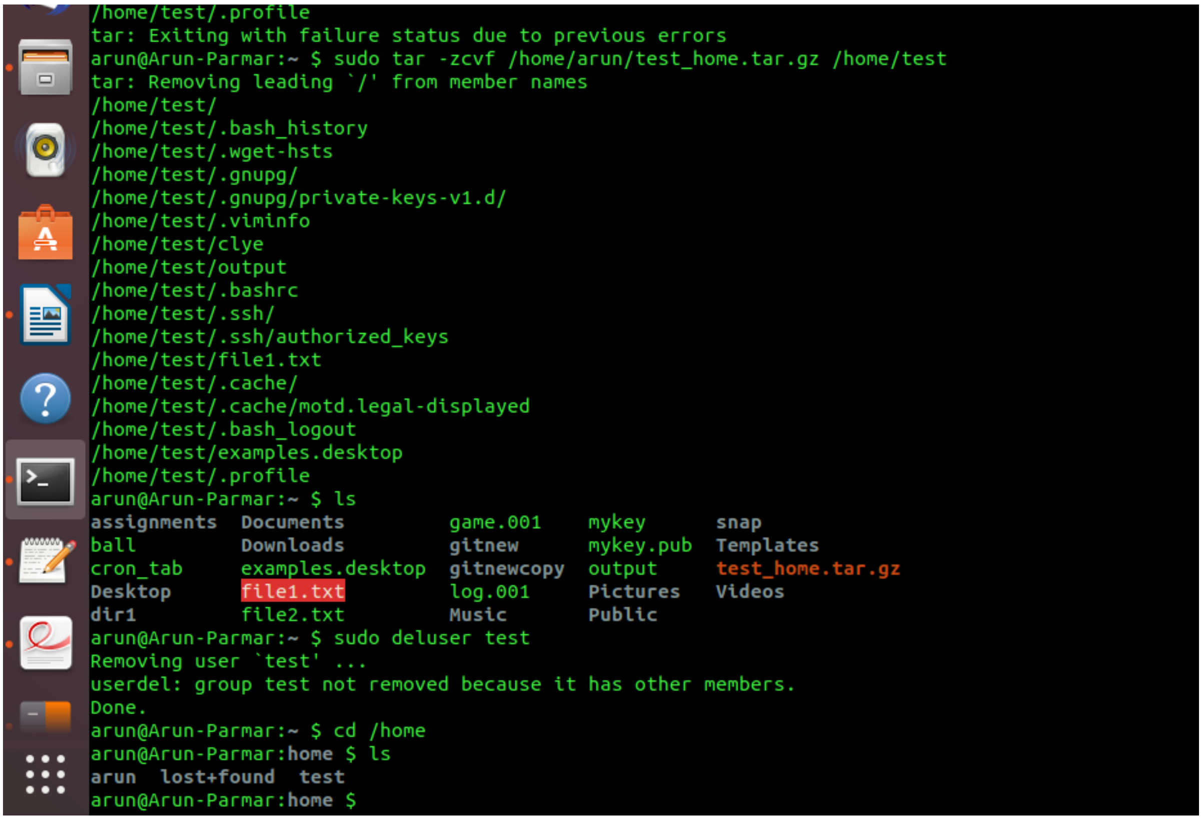
```
arun@Arun-Parmar:~ $ cd /home
arun@Arun-Parmar:home $ ls
arun  lost+found  test
arun@Arun-Parmar:home $ sudo usermod -G test arun
[sudo] password for arun:
arun@Arun-Parmar:home $ id arun
uid=1000(arun) gid=1000(arun) groups=1000(arun),1001(test)
arun@Arun-Parmar:home $ sudo usermod -L test
arun@Arun-Parmar:home $ su test
Password:
su: Authentication failure
arun@Arun-Parmar:home $
```

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



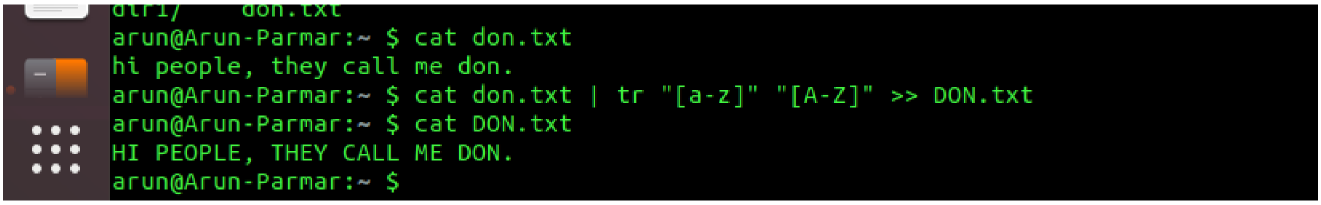
```
 GNU nano 2.9.3                                          /etc/sudoers.tmp

#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
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

# 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

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
test ALL=(ALL) NOPASSWD: ALL
```

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



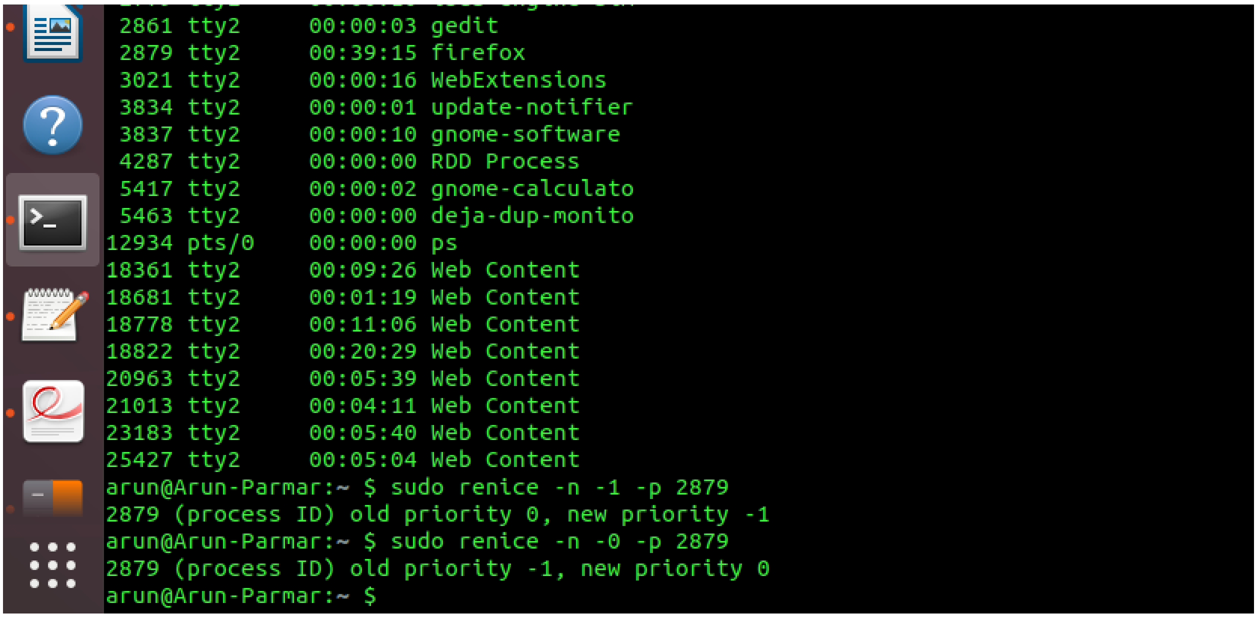
```
/home/test/.profile
tar: Exiting with failure status due to previous errors
arun@Arun-Parmar:~ $ sudo tar -zcvf /home/arun/test_home.tar.gz /home/test
tar: Removing leading `/' from member names
/home/test/
/home/test/.bash_history
/home/test/.wget-hsts
/home/test/.gnupg/
/home/test/.gnupg/private-keys-v1.d/
/home/test/.viminfo
/home/test/clye
/home/test/output
/home/test/.bashrc
/home/test/.ssh/
/home/test/.ssh/authorized_keys
/home/test/file1.txt
/home/test/.cache/
/home/test/.cache/motd.legal-displayed
/home/test/.bash_logout
/home/test/examples.desktop
/home/test/.profile
arun@Arun-Parmar:~ $ ls
assignments  Documents         game.001    mykey      snap
ball         Downloads         gitnew      mykey.pub  Templates
cron_tab     examples.desktop  gitnewcopy  output     test_home.tar.gz
Desktop      file1.txt         log.001     Pictures   Videos
dir1         file2.txt         Music       Public
arun@Arun-Parmar:~ $ sudo deluser test
Removing user `test' ...
userdel: group test not removed because it has other members.
Done.
arun@Arun-Parmar:~ $ cd /home
arun@Arun-Parmar:home $ ls
arun  lost+found  test
arun@Arun-Parmar:home $
```

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



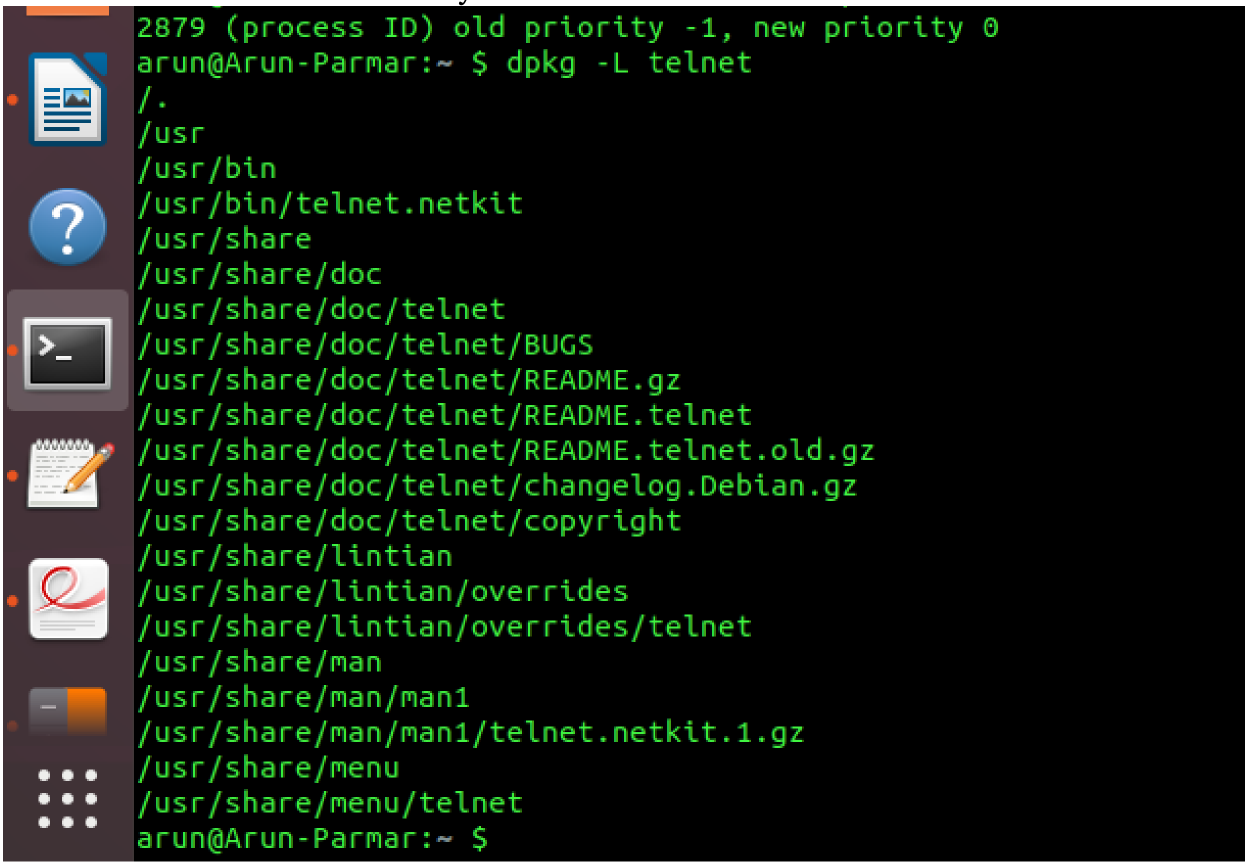
```
dir1/     don.txt
arun@Arun-Parmar:~ $ cat don.txt
hi people, they call me don.
arun@Arun-Parmar:~ $ cat don.txt | tr "[a-z]" "[A-Z]" >> DON.txt
arun@Arun-Parmar:~ $ cat DON.txt
HI PEOPLE, THEY CALL ME DON.
arun@Arun-Parmar:~ $
```

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



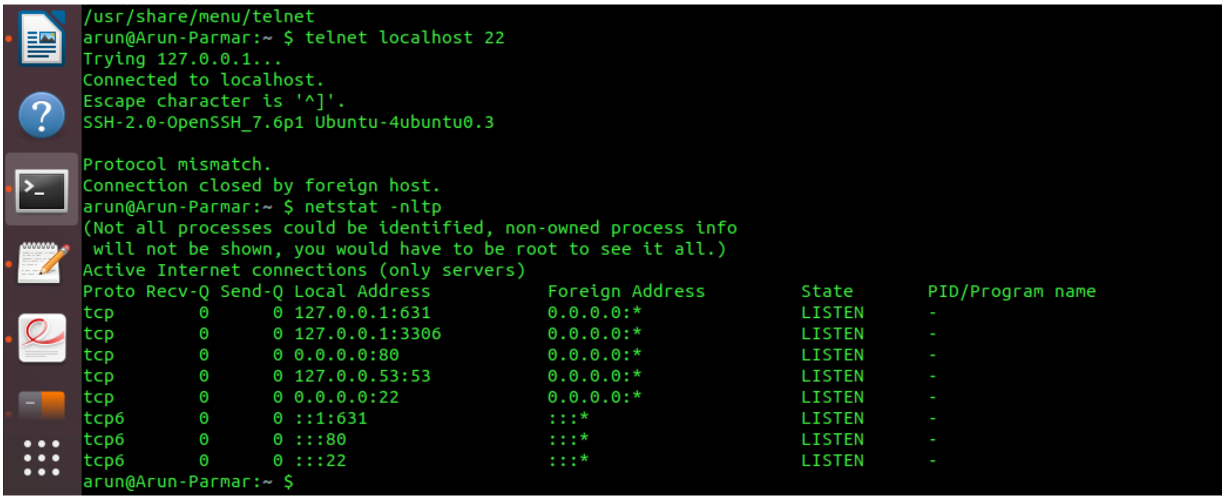
```
 2861 tty2     00:00:03 gedit
 2879 tty2     00:39:15 firefox
 3021 tty2     00:00:16 WebExtensions
 3834 tty2     00:00:01 update-notifier
 3837 tty2     00:00:10 gnome-software
 4287 tty2     00:00:00 RDD Process
 5417 tty2     00:00:02 gnome-calculato
 5463 tty2     00:00:00 deja-dup-monito
12934 pts/0    00:00:00 ps
18361 tty2     00:09:26 Web Content
18681 tty2     00:01:19 Web Content
18778 tty2     00:11:06 Web Content
18822 tty2     00:20:29 Web Content
20963 tty2     00:05:39 Web Content
21013 tty2     00:04:11 Web Content
23183 tty2     00:05:40 Web Content
25427 tty2     00:05:04 Web Content
arun@Arun-Parmar:~ $ sudo renice -n -1 -p 2879
2879 (process ID) old priority 0, new priority -1
arun@Arun-Parmar:~ $ sudo renice -n -0 -p 2879
2879 (process ID) old priority -1, new priority 0
arun@Arun-Parmar:~ $
```

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



```
2879 (process ID) old priority -1, new priority 0
arun@Arun-Parmar:~ $ 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
arun@Arun-Parmar:~ $
```

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



```
/usr/share/menu/telnet
arun@Arun-Parmar:~ $ telnet localhost 22
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3

Protocol mismatch.
Connection closed by foreign host.
arun@Arun-Parmar:~ $ netstat -nltp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
arun@Arun-Parmar:~ $
```

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

Cron Job: 45 23 * * 0

17.Difference between dig and traceroute

Dig: Dig stands for domain name groper. It is a network administration command-line tool for querying Domain Name System (DNS) name servers. It is useful for verifying and troubleshooting DNS problems and also to perform DNS lookups and displays the answers that are returned from the name server that were queried.

Traceroute: It is a command in Linux that prints the route that a packet takes to reach the host.It shows the hops it takes to reach a particular host.