1. How are devices represented in UNIX?
Ans :- All devices are represented by files called special files that are located in/dev directory. Thus, device files and other files are named and accessed in the same way. A 'regular file' is just an ordinary data file in the disk. A 'block special file' represents a device with characteristics similar to a disk (data transfer in terms of blocks). A 'character special file' represents a device with characteristics similar to a keyboard (data transfer is by stream of bits in sequential order).

2. What is 'inode'?
Ans :- All UNIX files have its description stored in a structure called 'inode'. The inode contains info about the file-size, its location, time of last access, time of last modification, permission and so on. Directories are also represented as files and have an associated inode. In addition to descriptions about the file, the inode contains pointers to the data blocks of the file. If the file is large, inode has indirect pointer to a block of pointers to additional data blocks (this further aggregates for larger files). A block is typically 8k.
Inode consists of the following fields: File owner identifier,File type,File access permissions,File access times,Number of links,File size and Location of the file data.

3. Brief about the directory representation in UNIX
Ans :- A Unix directory is a file containing a correspondence between filenames and inodes. A directory is a special file that the kernel maintains. Only kernel modifies directories, but processes can read directories. The contents of a directory are a list of filename and inode number pairs. When new directories are created, kernel makes two entries named '.' (refers to the directory itself) and '..' (refers to parent directory). System call for creating directory is mkdir (pathname, mode).

4. How do you change File Access Permissions?
Ans :- Every file has following attributes:
owner's user ID (16 bit integer)
owner's group ID (16 bit integer)
File access mode word

'r w x -r w x- r w x'

(user permission-group permission-others permission)
r-read, w-write, x-execute
To change the access mode, we use chmod(filename,mode).
Example 1:
To change mode of myfile to 'rw-rw-r--' (ie. read, write permission for user - read,write permission for group - only read permission for others) we give the args as:

chmod(myfile,0664) .
Each operation is represented by discrete values

'r' is 4
'w' is 2
'x' is 1

Therefore, for 'rw' the value is 6(4+2).
Example 2:
To change mode of myfile to 'rwxr–r–' we give the args as:
chmod(myfile,0744).

5. What are links and symbolic links in UNIX file system?
Ans :- A link is a second name (not a file) for a file. Links can be used to assign more than one name to a file, but cannot be used to assign a directory more than one name or link filenames on different computers.
Symbolic link 'is' a file that only contains the name of another file.Operation on the symbolic link is directed to the file pointed by the it.Both the limitations of links are eliminated in symbolic links.
Commands for linking files are:

Link ln filename1 filename2
Symbolic link ln -s filename1 filename2

6. What is a FIFO?
Ans :- FIFO are otherwise called as 'named pipes'. FIFO (first-in-first-out) is a special file which is said to be data transient. Once data is read from named pipe, it cannot be read again. Also, data can be read only in the order written. It is used in interprocess communication where a process writes to one end of the pipe (producer) and the other reads from the other end (consumer).

7. How do you create special files like named pipes and device files?
Ans :- The system call mknod creates special files in the following sequence.
1. kernel assigns new inode,
2. sets the file type to indicate that the file is a pipe, directory or special file,
3. If it is a device file, it makes the other entries like major, minor device numbers.
For example:
If the device is a disk, major device number refers to the disk controller and minor device number is the disk.

8. Discuss the mount and unmount system calls
Ans :- The privileged mount system call is used to attach a file system to a directory of another file system; the unmount system call detaches a file system. When you mount another file system on to your directory, you are essentially splicing one directory tree onto a branch in another directory tree. The first argument to mount call is the mount point, that is , a directory in the current file naming system. The second argument is the file system to mount to that point. When you insert a cdrom to your unix system's drive, the file system in the cdrom automatically mounts to /dev/cdrom in your system.

9. How does the inode map to data block of a file?
Ans :- Inode has 13 block addresses. The first 10 are direct block addresses of the first 10 data blocks in the file. The 11th address points to a one-level index block. The 12th address points to a two-level (double in-direction) index block. The 13th address points to a three-level(triple in-direction)index block. This provides a very large maximum file size with efficient access to large files, but also small files are accessed directly in one disk read.

10. What is a shell?
Ans :- A shell is an interactive user interface to an operating system services that allows an user to enter commands as character strings or through a graphical user interface. The shell converts them to system calls to the OS or forks off a process to execute the command. System call results and other information from the OS are presented to the user through an interactive interface. Commonly used shells are sh,csh,ks etc.

11. Brief about the initial process sequence while the system boots up.
Ans :- While booting, special process called the 'swapper' or 'scheduler' is created with Process-ID 0. The swapper manages memory allocation for processes and influences CPU allocation. The swapper inturn creates 3 children:

the process dispatcher,
vhand and
dbflush

with IDs 1,2 and 3 respectively.
This is done by executing the file /etc/init. Process dispatcher gives birth to the shell. Unix keeps track of all the processes in an internal data structure called the Process Table (listing command is ps -el).

12. What are various IDs associated with a process**?**
Ans :- Unix identifies each process with a unique integer called ProcessID. The process that executes the request for creation of a process is called the 'parent process' whose PID is 'Parent Process ID'. Every process is associated with a particular user called the 'owner' who has privileges over the process. The identification for the user is 'UserID'. Owner is the user who executes the process. Process also has 'Effective User ID' which determines the access privileges for accessing resources like files.

getpid() -process id
getppid() -parent process id
getuid() -user id
geteuid() -effective user id

18. How can a parent and child process communicate**?**
Ans :- A parent and child can communicate through any of the normal inter-process communication schemes (pipes, sockets, message queues, shared memory), but also have some special ways to communicate that take advantage of their relationship as a parent and child. One of the most obvious is that the parent can get the exit status of the child.

19. What is a zombie**?**
Ans :- When a program forks and the child finishes before the parent, the kernel still keeps some of its information about the child in case the parent might need it - for example, the parent may need to check the child's exit status. To be able to get this information, the parent calls `wait()'; In the interval between the child terminating and the parent calling `wait()', the child is said to be a `zombie' (If you do `ps', the child will have a `Z' in its status field to indicate this.)

20. What are the process states in Unix**?**
Ans :- As a process executes it changes state according to its circumstances. Unix processes have the following states:
Running : The process is either running or it is ready to run .
Waiting : The process is waiting for an event or for a resource.
Stopped : The process has been stopped, usually by receiving a signal.
Zombie : The process is dead but have not been removed from the process table.

21. What are the Unix system calls for I/O?
Ans :-

open(pathname,flag,mode) - open file
creat(pathname,mode) - create file
close(filedes) - close an open file
read(filedes,buffer,bytes) - read data from an open file
write(filedes,buffer,bytes) - write data to an open file
lseek(filedes,offset,from) - position an open file
dup(filedes) - duplicate an existing file descriptor
dup2(oldfd,newfd) - duplicate to a desired file descriptor
fcntl(filedes,cmd,arg) - change properties of an open file
ioctl(filedes,request,arg) - change the behaviour of an open file

The difference between fcntl anf ioctl is that the former is intended for any open file, while the latter is for device-specific operations.

22.When using rpmbuild how do you create a patch?
Ans :- diff -uNr package-1.0/ package-1.0.orig/ > ../SOURCES/package-1.0-my.patch

23.What tools would you use to investigate CPU and Memory bottlenecks?
Ans :-
- top, htop, atop, iftop, iotop
- getconf PAGESIZE
- vmstat 3 (processes, memory, paging, IO, traps, and cpu activity)
- vmstat –m (mem utilization slabinfo)
- vmstat –a (active/inactive memory pages)
- uptime
- free –m (MBs of total amount of free and used physical mem and swap, as well as buffers used by kernel)
- mpstat –P ALL (activities for each available cpu)
- pmap –d PID (reports memory map of a process, last line is very important: memory mapped to files/private address space/shared address space)
- strace -p
- lsof -p
- dstat (combines vmstat, iostat, ifstat, netstat)

LTTng (Linux Text Toolset Next Generation)
collectl

24.What tools would you use to investigate network bottlenecks?
Ans :-
- tcpdump –i eth0
- wireshark

- ethtool -i eth0
- nc (netcat for constructing raw tcp connections)
- sar –n NFS
- ss –s (list currently est, closed, orphaned and waiting TCP sockets)
- netstat -atun | awk '{print $5}' | cut -d: -f1 | sed -e '/^$/d' |sort | uniq -c | sort –n (is ur box under dos attack)
- iptraf (interactive colourful IP monitor)
- nmap (port scanner)
- ntop
- mtr
- nethogs
- jnettop
- apachetop
- Munin/Cacti
- Performance Co-Pilot (PCP)
- nmon
- trafmon
- zenoss

27.What is LVM layout ?

Ans :-

You have one or more physical volumes (/dev/sdb1 – /dev/sde1), and on these physical volumes you create one or more volume groups (e.g. fileserver), and in each volume group you can create one or more logical volumes (/dev/fileserver/share; /dev/fileserver/backup; etc).

If you use multiple physical volumes, each logical volume can be bigger than one of the underlying physical volumes (but of course the sum of the logical volumes cannot exceed the total space offered by the physical volumes).

It is a good practice to not allocate the full space to logical volumes, but leave some space unused. That way you can enlarge one or more logical volumes later on if you feel the need for it.

28.What is the difference between sector and blocks?

Ans :- Mass storage devices (hard disks, CD-ROMs, tapes) operate on chunks of data, usually called sectors. The size of these device sectors varies, but is fixed for any one device. Hard disks and floppies usually use 512 bytes, while data CDs and DVDs use 2048 bytes. Today, it is customary to number all sectors sequentially and leave the details to the device.

File systems also operate on chunks at a time, but they don't need to be the same size as the device's sectors. The chunks used by the file system are usually called blocks.

Ext3 supports block sizes up to 64 KB, but in x86 and x64 architectures, 4 KB is the maximum (and also default for filesystems over 512MB). This block size corresponds

to that of the kernel's memory pages in RAM, which makes paging easier for the operating system.

With large block sizes, small files have a large overhead. Some file systems were extended to compensate for this. BSD has 'fragment', raiserfs has 'tail': pieces of data from several files are packed into a single block, improving efficiency.

29.What tools do you use to troubleshoot memory?
Ans :-
cat /proc/meminfo
free -k
ipcs -lm
sysctl -a
blockdev –report
getconf -a
slabtop

30.How DNS resolution works?
Ans :- A client application requests an IP address from the nameserver usually by connecting to UDP port 53. The nameserver will attempt to resolve the FQDN based on its resolver library, which may contain authoritative information about the host requested or cached data about that name from an earlier query.
If the nameserver does not already have the answer in its resolver library, it will turn to root nameservers, to determine which nameservers are authoritative for the FQDN in question. Then, with that information, it will query the authoritative nameservers for that name to determine the IP address.

31.What is FQDN and secondary name server?
Ans :- FQDN of a host can be broken down into sections organized in a tree hierarchy. Except for the hostname, every section divided by "." is a called a zone.

Zones are defined on authoritative nameservers in zone files. Zone files are stored on primary nameservers (also called master nameservers), which are truly authoritative and where changes are made to the files.
Secondary nameservers (also called slave nameservers) receive their zone files from the primary nameservers. Any nameserver can be a primary and secondary nameserver for different zones at the same time, and they may also be considered authoritative for multiple zones. It all depends on the nameserver's particular configuration.
Every second level domain should have one primary and one secondary nameserver running on different physical machines for redundancy.
There are four nameserver configuration types:

master — Stores original and authoritative zone records for a certain zone, answering questions from other nameservers searching for answers concerning that namespace.
slave — Also answers queries from other nameservers concerning namespaces for which it is considered an authority. However, slave nameservers get their namespace information from master nameservers via a zone transfer, where the slave sends the master a NOTIFY request for a particular zone and the master responds with the information, if the slave is authorized to receive the transfer.
caching-only — Offers name to IP resolution services but is not authoritative for any zones. Answers for all resolutions are usually cached in a database stored in memory for a fixed period of time, usually specified by the retrieved zone record, for quicker resolution for other DNS clients after the first resolution.
forwarding — Forwards requests to a specific list of nameservers to be resolved. If none of the specified nameservers can perform the resolution, the process stops and the resolution fails.

32.What is the default Window system / Windows manager used in Linux?
Ans :-
Code:

X.org

33.What command is used to list the contents of directory?
Ans :-
Code:

ls
ls -l

34.What command is used to list the top 10 files / directories size wise?
Ans :-
Code:

for X in $(du -s * | sort -nr | cut -f 2); do du -hs $X ; done

35.What command is used to display a list of currently running processes?
Ans :-
Code:

ps
top

pstree
pgrep
/proc file system

36.What is a login shell?
Ans :- A program get executed when a user logs into UNIX box. E.g. bash, sh, ksh, csh

37.What is UID?
Ans :- User identification number which is assigned to each UNIX / Linux user; it may or may not be unique (unique number is recommended to avoid security related issues). UID and user relationship defined in /etc/passswd file.
Code:

man id
man users
man groups

38.Explain Unix User security concept?
Ans :- Permissions - chmod and chown
User groups - group management - user management
Read su, sudo man page

39.What PID?
Ans :- Process identification number; use ps command to see PID. It is a number used by Unix kernels and Windows operating systems to identify a process.

40.Explain process ID zero and process ID 1?
Ans :- All the idle task has process ID zero, and never exits.
The init process, with process ID 1, which does nothing but wait around for its child processes to die. Usually started for /etc/inittab

41.Explain wheel group usage along with an example?
Ans :-
Code:

man su

42.What command is used to check a file system for errors?
Ans :-

Code:

```
fsck
fsck.ext3
fsck.nfs
fsck.ext2
fsck.vfat
fsck.reiserfs
fsck.msdos
```

43.Is Linux / UNIX file system case sensitive? Give one example
Ans :- Yes, test.txt and TEST.txt are two different files

44.What file contains the list of drives that are mounted at boot?
Ans :-
/etc/fstab - Linux / Other UNIX version
/etc/vfstab - Solaris UNIX

45.Explain the usage of the fourth field in /etc/fstab?
Ans :- It is formatted as a comma separated list of options. Read mount command man page for all the option.

46.What is /etc/inittab file? In what file is the default run level defined?
Ans :- System V init examines the '/etc/inittab' file for an 'initdefault' entry, which tells init whether there is a default runlevel. init is the program on Unix that spawns all other processes. It runs as a daemon and typically has PID 1.
Code:

```
man init
cat /etc/inittab
```

Common runlevle values on RHEL
Code:

0. Halt
1. Single user mode
6. Reboot
3. Default text
5. Default GUI

To check the current runlevel:

Code:

```
who -r
runlevel
```

47.What command is used to get help about command? What command is used to read manual page for a given command?
Ans :-
Code:

```
info command-name
man command-name
command-name -h
command-name --help
```

48.What command form or symbol used to redirect output to a file?
Ans :-
Use the > symbol
Use the < symbol to read input from a file
Code:

```
command-name > output.txt
```

49.What is ssh? Specify ssh command syntax to execute command over a TCP/IP network?
Ans :- SSH is Application layer protocol which allows data to be exchanged over a secure channel between two computers.
Code:

```
ssh user@remote.box command-name
```

50.Explain steps for password less login? How do you set-up SSH with DSA / RSA public key authentication?
Ans :-
Howto Linux / UNIX setup SSH with DSA public key authentication (password less login)

55.Explain Raw device and command s to configure Raw device?
Ans :- Block device file that allows accessing a storage device such as a hard drive directly. For example /dev/hda. Use commands

Code:

mknod
fdisk
mkfs
mkfs.ext3

57.Explain Unix file types?
Ans : -
Directory
Pipes
Fifo
Symbolic link
Named pipe
Socket
Device file
Door
Regular file

58.Explain inode, superblock and hard links?
Ans : -
Understanding UNIX / Linux file system

59.Explain Unix domain socket?
Ans : - Unix Sockets
MySQL and many programs uses domain socket to make client / server communication. Usually fast as compare to TCP/IP

60.Explain UNIX software pipeline concept?
See shell or bash man page
Ans : -
Code:

cat /etc/passwd | grep username
mount | grep cdrom

61.Explain XYZ Unix daemons?
Where XYZ can be any one of the following:
Ans : -

init
httpd
dhcpd
lpd
nfsd
ntpd
syslogd
ypbind
ftpd
telnetd
sshd
named

62.Explain udev in Kernel 2.6?
Ans : -
udev is a device manager for the Linux kernel. Primarily, it manages device nodes in /dev. It is the successor of devfs and hotplug, which means that it handles the /dev directory and all user space actions when adding/removing devices, including firmware load.

*udev supports persistent device naming, which does not depend on, for example, the order in which the devices are plugged into the system. The default udev setup provides persistent names for storage devices. Any hard disk is recognized by its unique filesystem id, the name of the disk and the physical location on the hardware it is connected to

*udev executes entirely in user space, as opposed to devfs' kernel space. One consequence is that udev moved the naming policy out of the kernel and can run arbitrary programs to compose a name for the device from the device's properties, before the node is created; there, the whole process is also interruptible and it runs with a lower priority

63.Explain Process management and related commands?
Ans : -
top
htop
ps
pstree
kill
pgrep

pkill & killall
renice
xkill

64.Explain Memory management and related commands?
Ans : -
top
vmstat
free
ps

65.Secify special usage for each one of the following file
Ans : -
/dev/null - Send unwanted output
/dev/random - Random number generation
/dev/zero – Cache or Destroy data on a partition - dd if=/dev/zero of=/dev/sda98

66.Explain Linux Exec Shield?
Ans : -
Exec Shield is a project started at Red Hat, with the aim of
reducing the risk of worm or other automated remote attacks on Linux system

67.What is SELinux?
Ans : -
Security-Enhanced Linux (SELinux) is a Linux kernel security module that
provides the mechanism for supporting access control security policies,
including mandatory access controls
(MAC).
*Clean separation of policy from enforcement
*Well-defined policy interfaces
*Support for applications querying the policy and enforcing access control (for example, crond running jobs in the correct context)
*Independent of specific policies and policy languages
*Independent of specific security label formats and contents
*Individual labels and controls for kernel objects and services
*Support for policy changes
*Separate measures for protecting system integrity (domain-type) and data confidentiality (multilevel security)
*Flexible policy
*Controls over process initialization and inheritance and program execution
*Controls over file systems, directories, files, and open file descriptors

*Controls over sockets, messages, and network interfaces
*Controls over use of "capabilities"
*Cached information on access-decisions via the AVC (Access Vector Cache

68.Write a command to find all of the files which have been accessed within the last 10 days.
Ans : -
#find * -mtime -10

69.What is LILO?
Ans : - LILO (LInux LOader) is a boot loader for Linux

70.What is Grub?
Ans : - GRUB is a Linux based MultiBoot Loader. GRand Unified Boot Loader.

71.Explain the difference between LILO and Grub
Ans : - LILO has no interactive command interface, whereas GRUB does.

LILO does not support booting from a network, whereas GRUB does.

LILO stores information regarding the location of the operating systems it can to load physically on the MBR. If you change your LILO config file, you have to rewrite the LILO stage one boot loader to the MBR. Compared with GRUB, this is a much more risky option since a misconfigured MBR could leave the system unbootable. With GRUB, if the configuration file is configured incorrectly, it will simply default to the GRUB command-line interface.

LILO only loads linux and other boot loaders. and GRUB loads a large number of OS's.

LILO works by loading itself into a space that will fit on the MBR. Grub has two stages (because it's too overcomplicated to work as well, err I mean as easily as lilo). It loads stage 1 off the MBR (usually) and stage 2 out of /boot, along with it's config.

71.What is NFS?
Ans : - NFS stands for Network File System, a file system developed by Sun Microsystems, Inc. It is a client/server system that allows users to access files across a network and treat them as if they resided in a local file directory. For example, if you were using a computer linked to a second computer via NFS, you could access files on the second computer as if they

resided in a directory on the first computer. This is accomplished through the processes of exporting (the process by which an NFS server provides remote clients with access to its files) and mounting (the process by which file systems are made available to the operating system and the user

72. What is NAMED**?**

Ans : - Named services are defined by named service bindings. Named service bindings
enable applications to locate a service based on the name that is bound to the registry

73. Why You Shouldn't Use the root Login for everyday work**?**

Ans : - As we know that root is superuser in linux, having unlimited power to manipulate the system: when logged as root, you can read,modify or delete at any file,change into any directory,modify configration of the system & perform almostany task on system.
AS root user you can do virtually unlimited damage to the system, corrupting oor deleting all files. So,it is essential that you not log in as root user unless it is absolutely necessary.
Other reason for it for secuirty purpose,if you work on a linux server & if it is hacked by a hacker in this case if you log as root,hacker can acquire the power of root user & may try to damage your system. So during first login of the day try to login as normal user rather then root user, after that you may login as root user.

74. Describe the default partition scheme in Redhat Linux**?**

Ans : -

* swap partition
* /boot partition
* / partition
* home partition

75. What is boot block**?**

Ans : - boot sector or boot block is a region of a hard disk, floppy disk, optical disc, or other data storage device that contains machine code to be loaded into random-access memory (RAM) by a computer system's built-in firmware. The purpose of a boot sector is to allow the boot process of a computer to load a program (usually, but not necessarily, an operating system) stored on the same storage device. The location and size of the boot sector (perhaps

corresponding to a logical disk sector) is specified by the design of the computing platform.

76. What is logical block**?**
Ans : -
Logical block addressing (LBA) is a common scheme used for specifying the location of blocks of data stored on computer storage devices, generally secondary storage systems such as hard disks.
In logical block addressing, only one number is used to address data, and each linear base address describes a single block.

90. How do you lock and unlock user account **/** password**?**
Ans : - To lock, you can use the follow command:

```
# passwd -l username
```

To Unlock the same account
Following command re-enables an account by changing the password back to its previous value i.e. to value before using -l option.

```
# passwd -u username
```

91. Describe RPM and command to install **/** remove **/** update Linux system**?**
Ans : - RPM stand for Red Hat Package Manager
to install -# rpm -ivh packagename
to remove -# rpm -e <Packagename(s)>
to update -# rpm -uvh Packagename

94. Explain difference between rpm and yum command.
Ans : - RPM is the extraction **/** installation component. YUM is the downloader. If RPM
is run to install a package without its dependencies already installed, it will fail. YUM's job is to download all necessary dependencies.

96.How do you find files on UNIX or Linux system?
Ans : - Linux and Unix and their variants have several different ways of locating files. See each of the below commands for additional information about the command and how they can be used to locate files.

find
locate
wheris
which

98.Explain chkconfig command
Ans : -

1. Check Service Startup status from Shell Script
2. View Current Status of Startup Services
3. Add a new Service to the Startup
4. Remove a Service From Startup List
5. Turn-on or Turn-off a Service for a Selected Run Level
6. Script Files under rc.d Subdirectories
7. rcx.d Directory Changes for Add Operation

100.What is the purpose of the command?
Ans : -
grep
sed
awk
ifconfig
netstat
df
du
prtvtoc
fdisk -l
umaks
getfacl
setfacl
sudo
fsck
probe-scsi
vmstat

101.Explain LVM
Ans : -
LVM is a logical volume manager for the Linux kernel; it manages disk drives and similar mass-storage devices
LVM is commonly used for the following purposes:
Managing large hard disk farms by allowing disks to be added and replaced without downtimes and services disruption, in combination with hot swapping.
On small systems (like a desktop at home), instead of having to estimate at installation time how big a partition might need to be in the future, LVM allows file systems to be easily resized later as needed.
Performing consistent backups by taking snapshots of the logical volumes.
Creating single logical volumes of multiple physical volumes or entire hard disks (somewhat similar to RAID 0,), allowing for dynamic volume resizing.
LVM can be considered as a thin software layer on top of the hard disks and partitions, which creates an abstraction of continuity and ease-of-use for managing hard drive replacement, re-partitioning, and backup

102.What are the services required for nfs ?
Ans : -
*An NFS server on linux requires 3 services to be running in order to share files:

/etc/rc.d/init.d/portmap
/etc/rc.d/init.d/nfslock
/etc/rc.d/init.d/nfs

103.What is the best way to check the status of any service?
Ans : -
#service –status-all

105.Explain Linux Boot process especially kernel and initrd.
Kernel
Mounts the root file system as specified in the “root=” in grub.conf
Kernel executes the /sbin/init program
Since init was the 1st program to be executed by Linux Kernel, it has the process id (PID) of 1. Do a ‘ps -ef | grep init’ and check the pid.
initrd stands for Initial RAM Disk.
initrd is used by kernel as temporary root file system until kernel is booted and the real root file system is mounted. It also contains necessary drivers compiled inside, which helps it to access the hard drive partitions, and other hardware.
Init
Looks at the /etc/inittab file to decide the Linux run level.
Following are the available run levels
0 – halt
1 – Single user mode

2 – Multiuser, without NFS
3 – Full multiuser mode
4 – unused
5 – X11
6 – reboot
Init identifies the default initlevel from /etc/inittab and uses that to load all appropriate program.
Execute 'grep initdefault /etc/inittab' on your system to identify the default run level
If you want to get into trouble, you can set the default run level to 0 or 6. Since you know what 0 and 6 means, probably you might not do that.
Typically you would set the default run level to either 3 or 5.

106.Why we do have two commands useradd and adduser when their functialnality is same?
Ans : - adduser is just a symbolic link to useradd, but may try to copy the script from a Debian system to the CentOS one, I have never tried it, and may need to modify it a little before using it.

107.Can we have two apache servers having diff versions?
Ans : - Yes, you can have two different apache servers on one server, but they can't listen to the same port at the same time. Normally Apache listens to port 80 which is the default HTTP port. The second Apache version should listen to another port with the Listen option in httpd.conf, for example to port 81.

108.Which command is used to check the number of files and disk space used and the each user's defined quota?
Ans : - repquota

The repquota command is used to get a report on the status of the quotas you have set including the amount of allocated space and amount of used space.

109.What is the name and path of the main system log?
Ans : - /var/log/messages

By default, the main system log is /var/log/messages.

110.How secured is Linux? Explain.?

Ans : - In order to ensure safeness for an operating system, the most important aspect taken care is the security. Because of its authentication module. Linux is known as an operating system having absolute security than other ones.

Linux has Pluggable Authentication Modules (PAM) which provides a layer between applications and actual authentication mechanism. The PAM is a documentation store of loadable modules called by the application for authentication. It is controlled using the configuration file or the configuration directory. All PAM applications are configured in the directory "/etc/pam.d" or in a file "/etc/pam.conf". Using this operating system administrators are made assurance in control whenever a user can log in.

111.Can Linux computer be made a router so that several machines may share a single Internet connection? How?

Ans : - Yes, a Linux machine can be made a router. This is called "IP Masquerade." IPMasquerade is a networking function in Linux similar to the one-to-many (1: Many) NAT (Network Address Translation) servers found in many commercial firewalls and network routers. The IP Masquerade feature allows other "internal computers connected to this Linux box (via PPP, Ethernet, etc.) to also reachthe Internet as well. Linux IP Masquerading allows this functionality even ifthe internal computers do not have IP addresses.

112.What is the minimum number of partitions you need to install Linux?

Ans : -

Two

1. /
2. /boot

113.Which command is used to review boot messages?

Ans : - dmesg

The dmesg command displays the system messages contained in the kernel ring buffer. By using this command immediately after booting your computer, you will see the boot messages.

114.Which utility is used to make automate rotation of a log?
Ans : - logrotate command is used to make automate rotation of log.
Syntax of the command is:
logrotate [-dv] [-f|] [-s|] config_file+
It allows automatic rotation, compression, removal, and mailing of log files. This command is mainly used for rotating and compressing log files. This job is done every day when a log file becomes too large. This command can also be run by giving on command line. We can done force rotation by giving –f option with this command in command line. This command is also used for mailing. We can give –m option for mailing with this command. This option takes two arguments one is subject and other is recipient name.

116.What are the fields in the/etc/passwd file?
Ans : - 1. Username: It is used when user logs in. It should be between 1 and 32 characters in length.
2. Password: An x character indicates that encrypted password is stored in /etc/shadow file.
3. User ID (UID): Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.
4. Group ID (GID): The primary group ID (stored in /etc/group file)
5. User ID Info: The comment field. It allow you to add extra information about the users such as user's full name, phone number etc. This field use by finger command.
6. Home directory: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes /
7. Command/shell: The absolute path of a command or shell (/bin/bash). Typically, this is a shell. Please note that it does not have to be a shell.

117.Which commands are used to set a processor-intensive job to use less CPU time?
Ans : - The nice command is used to change a job's priority level, so that it runs slower or faster.

120.How shadow passwords are given?
Ans : - In the purpose giving shadow passwords the pwcony command is helpful for you. This will secure the system better. The pwconv command creates the file /etc/shadow and can change all passwords to “x” in the file /etc/passwd. And how to give the shadow passwords? Firstly, remove entries in the shadowed file left the

main file. Secondly, update the shadowed entries which do not have “x” the password in the main file. Next, add some missing shadowed entries. Finally, replace passwords in the main file with “x”. You can use these programs to take initial conversion and update the shadowed file in case the main file is edited in manua

121. How do you create a new user account**?**
Ans : - By using #useradd or #adduser command

122. Which password package is installed for the security of central password**?**
Ans : - The shadow password package moves the central password file to a more secure location

123. Which shell do you assign to a POP3 mail-only account**?**
Ans : - /sbin/nologin

124. Which daemon is responsible for tracking events on Linux system**?**
Ans : - syslogd is responsible for tracking system information and save it to the desired log files

125. Which daemon is used for scheduling of the commands**?**
Ans : - crond

127. What is Linux and why is it so popular**?**
Ans : -
Linux is an operating system that uses UNIX like Operating system. However, unlike UNIX, Linux is an open source and free software. Linux was originally created by Linus Torvalds and commonly used in servers.
Popularity of Linux is because of the following reasons

It is free and open source. We can download Linux for free and customize it as per our needs.

It is very robust and adaptable.

Immense amount of libraries and utilities

Linux is a multiuser, multitask GUI based open source operating system developed by Linus Torvalds Torvalds has invited the community to enhance the Linux kernel and thousands of system programmers worked on to enhance.

Prior to Linux, there is UNIX. The desktop work stations from various companies were based on UNIX. Later a numerous companies entered and each one of them had their own UNIX version. As the proprietary authority is owned by each company and the lack of central authority weaken UNIX. As Linux is free and runs on any PC platform it gained the popularity very quickly. The following are few more reasons for its popularity:

- People who are familiar with UNIX can work on Linux with ease and comfort.
- People who want great control over network security and on operating system

128.What is LILO?

Ans : - - LILO is Linux Loader is a boot loader for Linux. It is used to load Linux into the memory and start the Operating system. LILO can be configured to boot other operating systems as well. LILO is customizable, which means that if the default configuration is not correct, it can be changed. Config file for LILO is lilo.conf.

LILO stands for Linux Loader which is a bootstrap program. LILO is a code snippet which loads PC BIOS into the main memory at the time of starting the computer system. LILO handles the following tasks:

-Locating Linux kernel

-Identifying other supporting programs and loading them in the memory

-Staring Kernel

The selection of various kernel images and boot routines is supported by LILO. For this reason, LILO is known as boot manager.

129.What is the difference between home directory and working directory?

Ans : - Home directory is the default working directory when a user logs in. On the other hand, working directory is the user's current directory. Working directory can be changed. It can be changed using cd command.

Home directory in Linux contains user's personal data, configuration files, settings of a software etc. The content of home directory is private and the user has a complete control of it.

Home Directory: Every user will have one home directory and will have complete control over it. On login, home is the default working directory for the user. It contains the configuration files and responsible for login and logout of the user.

Working directory: The directory in which the user is working currently is known as working directory. The home may also be the working directory, if the user is working in it.

130. What is the difference between internal and external commands**?**
Ans : - Internal commands are commands that are already loaded in the system. They can be executed any time and are independent. On the other hand, external commands are loaded when the user requests for them. Internal commands don't require a separate process to execute them. External commands will have an individual process. Internal commands are a part of the shell while external commands require a Path. If the files for the command are not present in the path, the external command won't execute.

The commands that are directly executed by the shell are known as internal commands. No separate process is there to run these commands.
The commands that are executed by the kernel are knows as external commands. Each command has its unique process id.

131. Explain the difference between a static library and a dynamic library.

Ans : - Static libraries are loaded when the program is compiled and dynamically-linked libraries are loaded in while the program is running. Dynamic libraries save the RAM space as against the static library because linking to static libraries includes the actual code for the library function(s)/procedure(s) with the executable. DLL code is kept at one location and is usually shared among all the processes that use the DLL.
Static library has functionality that bound to a static program at compile time. Every static program has its own copy of library.
Dynamic libraries are loaded into the memory and binds at run time. The external functionality is accessed at runtime. This process reduces the overall footprint of memory.

132. What is LD_LIBRARY_PATH**?**

Ans : - -D_LIBRARY_PATH is an environment variable. It is used for debugging a new library or a non standard library. It is also used for which directories to search. Path to search for directories needs to given. The variable can be set by using setenv —LD_LIBRARY_PATH--$PATH

133. What is the file server in Linux server**?**
Ans : - File server is used for file sharing. It enables the processes required fro

sharing. All the files can be stored at a centralized location. Linux uses Samba to view the files on the server. Files on this server are backed up on a regular basis. Rights can be also assigned for the files on a file server.A file server is dedicated for persisting files in a location from which the networked systems can access. Certain access privileges can be set for files.
Linux has software named as 'samba' which allows the files to be shared, viewed and edited on any remote system which may has Windows 9 x/ME/2000/NT or Macintosh computer systems. These files on the file server are backed up from time to time. If a file is deleted inadvertently, the file can be recovered from the backup tape.

134.What is NFS? What is its purpose?
Ans : - NFS is Network File system. It is a file system used for sharing of files over a network. Other resources like printers and storage devices can also be shared. This means that using NFS files can be accessed remotely. Nfs command in linux can be used to achieve this.
Purpose of NFS:

NFS can be used for sharing of files remotely.

Data can be stored on a single machine and still remain accessible to others over the network.

Reduction of the number of removable media drives throughout the network since they can be shared.

NFS stands for Network File System. NFS is used to partition a disk on a remote machine disk. NFS allows a quick way of file sharing.

The unwanted people access potential is provided by NFS to access hard drive in a network. So that an unauthorized user can not access one's email, delete the files. File services from windows can be accessed. In other words files from one operating system can be shared by another using NFS.

135.w do I send email with linux?
Ans : - mail can be sent in Linux using the mail command.
Mail [options] [users]
Options include: -s for subject, -c for carbon copy, -b for blind carbon copy
Linux supports to work with sending mails using a set of commands called as mail commands. The command to send email is 'mail'. The 'mail' command is used to send and receive emails.
Syntax:
mail [options] [users]
Options are: -s,-c,-b
Where –s for subject, -c for copy and –b for blind carbon copy

Ex: mail username –s “Reports are needed”

It prompts displays the subject as “Reports are needed”.
Similarly if –c and –b is given the mail will be sent to the corresponding recipients.

136.Explain RPM (Red Hat Package Manager) features.
Ans : - RPM is a package managing system (collection of tools to manage software packages).
Features:

RPM can verify software packages.
RPM can be served as a powerful search engine to search for software’s.
Components, software’s etc can be upgraded using RPM without having to reinstall them
Installing, reinstalling can be done with ease using RPM
During updates RPM handles configuration files carefully, so that the customization is not lost .RPM is a powerful software management tool for installing, uninstalling, verifying, querying and updating software packages. RPM is a straight forward program to perform the above software management tasks. It is available with Fedora, Suse, CentOS, Mandriva Linux and other version of Linux.

137.What is Kernel? Explain the task it performs.
Ans : - Kernel is used in UNIX like systems and is considered to be the heart of the operating system. It is responsible for communication between hardware and software components. It is primarily used for managing the systems resources as well.
Kernel Activities:

The Kernel task manager allows tasks to run concurrently.
Managing the computer resources: Kernel allows the other programs to run and use the resources. Resources include i/o devices, CPU, memory.
Kernel is responsible for Process management. It allows multiple processes to run simultaneously allowing user to multitask.
Kernel has an access to the systems memory and allows the processes to access the memory when required.
Processes may also need to access the devices attached to the system. Kernel assists the processes in doing so.
For the processes to access and make use of these services, system calls are used.

138. What is Linux Shell**?** What is Shell Script**?**

Ans : - Linux shell is a user interface used for executing the commands. Shell is a program the user uses for executing the commands. In UNIX, any program can be the users shell. Shell categories in Linux are:
Bourne shell compatible, C shell compatible, nontraditional, and historical.
A shell script, as the name suggests, is a script written for the shell. Script here means a programming language used to control the application. The shell script allows different commands entered in the shell to be executed. Shell script is easy to debug, quicker as compared to writing big programs. However the execution speed is slow because it launches a new process for every shell command executed. Examples of commands are cp, cn, cd. Linux shell is the user interface to communicate with Linux operating system. Shell interprets the user requests, executes them. Shell may use kernel to execute certain programs. Shell Script: A shell script is a program file in which certain Linux commands are placed to execute one after another. A shell script is a flat text file. Shell scripts are useful to accept inputs and provide output to the user. Everyday automation process can be simplified by a shell script.

139. What are Pipes**?** Explain use of pipes.

Ans : - A pipe is a chain of processes so that output of one process (stdout) is fed an input (stdin) to another. UNIX shell has a special syntax for creation of pipelines. The commands are written in sequence separated by |. Different filters are used for Pipes like AWK, GREP.
e.g. sort file | lpr (sort the file and send it to printer)
Uses of Pipe

Several powerful functions can be in a single statement
Streams of processes can be redirected to user specified locations using >

Pipe is a symbol used to provide output of one command as input to another command. The output of the command to the left of the pipe is sent as input to the command to the right of the pipe. The symbol is |.
For example:
$ cat apple.txt | wc
In the above example the output of apple.txt file will be sent as input for wc command which counts the no. of words in a file. The file for which the no. of words counts is the file apple.txt.
Pipes are useful to chain up several programs, so that multiple commands can execute at once without using a shell script.

10.Explain trap command; shift Command, getopts command of linux.

Ans : - Trap command: controls the action to be taken by the shell when a signal is received.
Trap [OPTIONS] [[arg] signspec..]
Arg is the action to be taken or executed on receiving a signal specified in signspec.
e.g. trap "rm $FILE; exit" // exit (signal) and remove file (action)
Shift Command: Using shift command, command line arguments can be accessed. The command causes the positional parameters shift to the left. Shift [n] where n defaults to 1. It is useful when several parameters need to be tested.
Getopts command: this command is used to parse arguments passed. It examines the next command line argument and determines whether it is a valid option
Getopts {optstring} {variable1}. Here, optsring contains letters to be recognized if a letter is followed by a colon, an argument should be specified. E.g (whether the argument begins with a minus sign and is followed by any single letter contained inside options) If not, diagnostic messages are shown. It is usually executed inside a loop.
trap command is used to catch a signal that is sent to a process. An action is taken based on the signal by using the action which is defined in the trap command instead of taking the default effect on the process.
Example:
$ trap "echo 'interrupt signal received' " INT.
shift command is used to replace the parameters that were sent from command line. For example
$ shift will replace $1 by $2
getopts command is used for the purpose of parsing positional parameters.

141.What Stateless Linux server? What feature it offers?
Ans : - A stateless Linux server is a centralized server in which no state exists on the single workstations. There may be scenarios when a state of a partilcuar system is meaningful (A snap shot is taken then) and the user wants all the other machines to be in that state. This is where the stateless Linux server comes into picture.
Features:

It stores the prototypes of every machine
It stores snapshots taken for those systems
It stores home directories for those systems
Uses LDAP containing information of all systems to assist in finding out which snapshot (of state) should be running on which system.

Stateless linux is a way how a system is to run and be managed. Being a stateless system, a system should be able to be replaced at any time with or without local

storage media. In case of hard drive crash, the command resync can be used to a new drive. If server goes offline, a new virtual instance that is running the OS image off of the network storage.

142.What does nslookup do? Explain its two modes.

Ans : - Nslookup is used to find details related to a Domain name server. Details like IP addresses of a machine, MX records, servers etc. It sends a domain name query packet to the corresponding DNS.
Nslookup has two modes. Interactive and non interactive. Interactive mode allows the user to interact by querying information about different hosts and domains.
Non interactive mode is used to fetch information about the specified host or domain.
Interactive mode:
Nslookup [options] [server]
Nslookup is a program used to find information about internet Domain Name server. The two modes of nslookup are: Interactive and non-interactive.
Using 'interactive mode' user can query the name servers for the information pertaining to hosts and domains.
Using 'non-interactive mode' the user can just print the name and requested information of a host.

143.What is Bash Shell?
Ans : - Bash is a free shell for UNIX. It is the default shell for most UNIX systems. It has a combination of the C and Korn shell features. Bash shell is not portable. any Bash-specific feature will not function on a system using the Bourne shell or one of its replacements, unless bash is installed as a secondary shell and the script begins with #!/bin/bash. It supports regular and expressions. When bash script starts, it executes commands of different scripts. Bash stands for "Bourne Again Shell". A shell is the user interface. Bash is more convenient shell for users among others. The scripts written in Bash are portable among machines, distributions and even operating systems.

144.Explain some Network-Monitoring Tools in Linux: ping, traceroute, tcpdump, ntop

Ans : - Network monitoring tools are used to monitor the network, systems present on the network, traffic etc.
Ping: Ping command is used to check if the system is in the network or not. To check if the host is operating.
e.g. ping ip_address
When the command is executed, it returns a detailed summary of the host. Packets

sent, received, lost by estimating the round trip time.
Traceroute: the command is used to trace the path taken by the packet across a network. Tracing the path here means finding out the hosts visited by the packet to reach its destination. This information is useful in debugging. Roundtrip time in ms is shown for every visit to a host.
Tcpdump: commonly used to monitor network traffic. Tcdump captures and displays packet headers and matching them against criteria or all. It interprets Boolean operators and accepts host names, ip address, network names as arguments.
Ntop: Network top shows the network usage. It displays summary of network usage by machines on the network in a format as of UNIX top utility. It can also be run in web mode, which allows the display to be browsed with a web browser. It can display network traffic statistics, identify host etc. Interfaces are available to view such information.

145. How does the linux file system work**?**

Ans : - Linux file structure is a tree like structure. It starts from the root directory, represented by '**/**', and then expands into sub-directories. All the partitions are under the root directory. If a partition is mounted (The mount point defines the place of a particular data set in the file system) anywhere apart from a **"**device**"**, the system is not aware of the existence of that partition or device. Directories that are only one level below the root directory are often preceded by a slash, to indicate their position. Root "/" file system: The kernel needs a root file system to mount at start up. The root file system is generally small and should not be changed often as it may interrupt in booting. The root directory usually does not have the critical files. Instead sub directories are created. E.g. **/**bin (commands needed during bootup), **/**etc (config files) , **/**lib(shared libraries).
/usr filesystem : this file system is generally large as it contains the executable files to be shared amongst different machines. Files are usually the ones installed while installing Linux. This makes it possible to update the system from a new version of the distribution, or even a completely new distribution, without having to install all programs again. Sub directories include **/**bin, **/**include, **/**lib, **/**local (for local executables)
/var filesystem : this file system is specific to local systems. It is called as var because the data keeps changing. The sub directories include **/**cache**/**man (A cache for man pages), **/**games (any variable data belong to games), **/**lib (files that change), **/**log (log from different programs), **/**tmp (for temporary files)
/home filesystem: - this file system differs from host to host. User specific configuration files for applications are stored in the user's home directory in a file. UNIX creates directories for all users directory. E.g **/**home**/**my_name. Once the user is logged in ; he is placed in his home directory.
/proc filesystem : this file system does not exist on the hard disk. It is created by the kernel in its memory to provide information about the system. This information is

usually about the processes. Contains a hierarchy of special files which represent the current state of the kernel .Few of the Directories include /1 (directory with information about process num 1, where 1 is the identification number), /cpuinfo (information about cpu), /devices (information about devices installed), /filesystem (file systems configured), /net (information about network protocols), /mem (memory usage) At the time of installation of Linux, a file system is assigned and persists in the hard disk. This file system structure resembles a tree.
A file can be a list of names and numbers or executable programs. Linux treats every program as a file. Linux treats directories and computer components also as files.
A file could be a list of names and numbers, a cheesecake recipe, or an executable program. But under Linux, everything is a file. In addition to data and executable files, Linux treats directories and even the various components of your computer as files. It could be a keyboard, console, and printer, RAM or ROM. These are referred as special files known as devices. These files are available in /dev directory. Linux performs the communication with these devices by simply reading from or writing to these special files.

146. What are the process states in Linux**?**

Ans : - Process states in Linux:

Running: Process is either running or ready to run
Interruptible: a Blocked state of a process and waiting for an event or signal from another process
Uninterruptible: a blocked state. Process waits for a hardware condition and cannot handle any signal
Stopped: Process is stopped or halted and can be restarted by some other process
Zombie: process terminated, but information is still there in the process table.

147. What is a zombie**?**

Ans : - Zombie is a process state when the child dies before the parent process. In this case the structural information of the process is still in the process table.....

148. Explain each system calls used for process management in linux.

Answer - System calls used for Process management.....

149.Which command is used to check the number of files and disk space used and the each user's defined quota?
Ans : -
repquota command is used to check the status of the user's quota along with the disk space and number of files used. This command gives a summary of the user's quota that how much space and files are left for the user. Every user has a defined quota in Linux. This is done mainly for the security, as some users have only limited access to files. This provides a security to the files from unwanted access. The quota can be given to a single user or to a group of users.

150.What is the name and path of the main system log?
Ans : -
By default the main system log is /var/log/messages. This file contains all the messages and the script written by the user. By default all scripts are saved in this file. This is the standard system log file, which contains messages from all system software, non-kernel boot issues, and messages that go to 'dmesg'. dmesg is a system file that is written upon system boot.

151.How secured is Linux? Explain.
Ans : -
Security is the most important aspect of an operating system. Due to its unique authentication module, Linux is considered as more secured than other operating systems. Linux consists of PAM. PAM is Pluggable Authentication Modules. It provides a layer between applications and actual authentication mechanism. It is a library of loadable modules which are called by the application for authentication. It also allows the administrator to control when a user can log in. All PAM applications are configured in the directory "/etc/pam.d" or in a file "/etc/pam.conf". PAM is controlled using the configuration file or the configuration directory.

152.Can Linux computer be made a router so that several machines may share a single Internet connection? How?
Ans : -
Yes a Linux machine can be made a router. This is called "IP Masquerade." IP Masquerade is a networking function in Linux similar to the one-to-many (1: Many) NAT (Network Address Translation) servers found in many commercial firewalls and network routers. The IP Masquerade feature allows other "internal" computers connected to this Linux box (via PPP, Ethernet, etc.) to also reach the Internet as

well. Linux IP Masquerading allows this functionality even if the internal computers do not have IP addresses.
The IP masquerading can be done by the following steps:

1. The Linux PC must have an internet connection and a connection to LAN. Typically, the Linux PC has two network interfaces-an Ethernet card for the LAN and a dial-up PPP connection to the Internet (through an ISP).

2. All other systems on your LAN use the Linux PC as the default gateway for TCP/IP networking. Use the same ISP-provided DNS addresses on all systems.

3. Enable IP forwarding in the kernel. By default the IP forwarding is not enabled. To ensure that IP forwarding is enabled when you reboot your system, place this command in the /etc/rc.d/rc.local file.

4. Run /sbin/iptables-the IP packet filter administration program-to set up the rules that enable the Linux PC to masquerade for your LAN.

153.What is the minimum number of partitions you need to install Linux?
Ans : -
Minimum 2 partitions are needed for installing Linux. The one is / or root which contains all the files and the other is swap. Linux file system is function specific which means that files and folders are organized according to their functionality. For example, all executables are in one folder, all devices in another, all libraries in another and so on. / or 'root' is the base of this file system. All the other folders are under this one. / can be consider as C: .Swap is a partition that will be used as virtual memory. If there is no more available RAM a Linux computer will use an area of the hard disk, called swap, to temporarily store data. In other words it is a way of expanding your computers RAM.

154.Which command is used to review boot messages?
Ans : -
dmesg command is used to review boot messages. This command will display system messages contained in the kernel ring buffer. We can use this command immediately after booting to see boot messages. A ring buffer is a buffer of fixed size for which any new data added to it overwrites the oldest data in it. Its basic syntax is

dmesg [options]

Invoking dmesg without any of its options causes it to write all the kernel messages to standard output. This usually produces far too many lines to fit into the display screen all at once, and thus only the final messages are visible. However, the output can be redirected to the less command through the use of a pipe, thereby allowing the startup messages to be viewed on one screen at a time

dmesg | less

155.Which utility is used to make automate rotation of a log?
Ans : -
logrotate command is used to make automate rotation of log.
Syntax of the command is:
logrotate [-dv] [-f|] [-s|] config_file+
It allows automatic rotation, compression, removal, and mailing of log files. This command is mainly used for rotating and compressing log files. This job is done every day when a log file becomes too large. This command can also be run by giving on command line. We can done force rotation by giving –f option with this command in command line. This command is also used for mailing. We can give –m option for mailing with this command. This option takes two arguments one is subject and other is recipient name.

156.What are the partitions created on the mail server hard drive?
Ans : -
The main partitions are done firstly which are root, swap and boot partition. But for the mail server three different partitions are also done which are as follows:
1. /var/spool- This is done so that if something goes wrong with the mail server or spool than the output cannot overrun the file system.
2. /tmp- putting this on its own partition prevents any user item or software from overrunning the system files.
3. /home- putting this on its own is useful for system upgrades or reinstalls. It allow not to wipe off the /home hierarchy along with other areas.

157.What are the fields in the/etc/passwd file?
Ans : -
It contains all the information of the users who log into the system. It contains a list of the system's accounts, giving for each account some useful information like user ID, group ID, home directory, shell, etc. It should have general read permission as many utilities, like ls use it to map user IDs to user names, but write access only for the superuser (root). The main fields of /etc/passwd file are:
1. Username: It is used when user logs in. It should be between 1 and 32 characters in length.
2. Password: An x character indicates that encrypted password is stored in /etc/shadow file.
3. User ID (UID): Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.

4. Group ID (GID): The primary group ID (stored in /etc/group file)
5. User ID Info: The comment field. It allow you to add extra information about the users such as user's full name, phone number etc. This field use by finger command.
6. Home directory: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes /
7. Command/shell: The absolute path of a command or shell (/bin/bash). Typically, this is a shell.

158.Which commands are used to set a processor-intensive job to use less CPU time?
Ans : -
nice command is used for changing priority of the jobs.
Syntax: nice [OPTION] [COMMAND [ARG]...]
Range of priority goes from -20 (highest priority) to 19 (lowest).Priority is given to a job so that the most important job is executed first by the kernel and then the other least important jobs. This takes less CPU times as the jobs are scheduled and are given priorities so the CPU executes fast. The priority is given by numbers like -20 describe the highest priority and 19 describe the least priority.

159.How to change window manager by editing your home directory?
Ans : -
/.xinitrc file allows changing the window manager we want to use when logging into X from that account. The dot in the file name shows you that the file is a hidden file and doesn't show when you do a normal directory listing. For setting a window manager we have to save a command in this file. The syntax of command is: exec windowmanager.After this, save the file. Next time when you run a startx a new window manager will open and become default. The commands for starting some popular window managers and desktop environments are:
-KDE = startkde
-Gnome = gnome-session
-Blackbox = blackbox
-FVWM = fvwm
-Window Maker = wmaker
-IceWM = icewm

160.How documentation of an application is stored?
Ans : -
When a new application is installed its documentation is also installed. This documentation is stored under the directory named for application. For example if my application name is App1 then the path of the documentation will be

/user/doc/App1. It contains all the information about the application. It contains date of creating application, name of application and other important module of the application. We can get the basic information of application from the documentation.

161. How shadow passwords are given**?**

Ans : -

pwconv command is used for giving shadow passwords. Shadow passwords are given for better system security. The pwconv command creates the file /etc/shadow and changes all passwords to 'x' in the /etc/passwd file. First, entries in the shadowed file which don't exist in the main file are removed. Then, shadowed entries which don't have `x' as the password in the main file are updated. Any missing shadowed entries are added. Finally, passwords in the main file are replaced with `x'. These programs can be used for initial conversion as well to update the shadowed file if the main file is edited by hand.

162. How do you create a new user account**?**

Ans : -

useradd command is used for creating a new user account. When invoked without the

-D option, the useradd command creates a new user account using the values specified on the command line and the default values from the system. The new user account will be entered into the system files as needed, and initial files copied, depending on the command line options. This command uses the system default as home directory. If –m option is given then the home directory is made.

163. Which password package is installed for the security of central password**?**

Ans : -

Shadow password packages are used for security of central passwords. Security is the most important aspect of every operating system. When this package is not installed the user information including passwords is stored in the /etc/passwd file. The password is stored in an encoded format. These encoded forms can be easily identified by the System crackers by randomly encoding the passwords from dictionaries. The Shadow Package solves the problem by relocating the passwords to another file (usually /etc/shadow). The /etc/shadow file is set so that it cannot be read by just anyone. Only root will be able to read and write to the /etc/shadow file.

164. Which shell do you assign to a POP3 mail-only account**?**
Ans : -
POP3 mail only account is assigned to the /bin/false shell. However, assigning bash shell to a POP3 mail only gives user login access, which is avoided. /bin/nologin can also be used. This shell is provided to the user when we don't want to give shell access to the user. The user cannot access the shell and it reject shell login on the server like on telnet. It is mainly for the security of the shells. POP3 is basically used for downloading mail to mail program. So for illegal downloading of emails on the shell this account is assigned to the /bin/false shell or /bin/nologin. These both shells are same they both do the same work of rejecting the user login to the shell. The main difference between these two shells is that false shell shows the incorrect code and any unusual coding when user login with it. But the nologin shell simply tells that no such account is available. So nologin shell is used mostly in Linux.

165. Which daemon is responsible for tracking events on Linux system**?**
Ans : -
syslogd is responsible for tracking system information and save it to the desired log files. It provides two system utilities which provide system logging and kernel message trapping. Internet and UNIX domain sockets support enable this utility package to support both local and remote logging. Every logged message contains at least a time and a hostname field, normally a program name field, too. So to track these information this daemon is used. syslogd mainly reacts to the set of signals given by the user. These are the signals given to syslogd: SIGHUP: This lets syslogd perform a re-initialization. All open files are closed, the configuration file (default is /etc/syslog.conf) will be reread and the syslog facility is started again. SIGTERM: The syslogd will die. SIGINT, SIGQUIT: If debugging is enabled these are ignored, otherwise syslogd will die. SIGUSR1: Switch debugging on/off. This option can only be used if syslogd is started with the - d debug option. SIGCHLD: Wait for Childs if some were born, because of waiting messages.

166. Which daemon is used for scheduling of the commands**?**
Ans : -
The crontab command is used for scheduling of the commands to run at a later time.
SYNTAX
crontab [-u user] file
crontab [-u user] { -l | -r | -e }

Options
-l List - display the current crontab entries.

-r Remove the current crontab.

-e Edit the current crontab using the editor specified by the VISUAL or EDITOR environment variables.

When user exits from the editor, the modified crontab will be installed automatically. Each user can have their own crontab, and though these are files in /var, they are not intended to be edited directly. If the –u option is given than the crontab gives the name of the user whose crontab is to be tweaked. If it is given without this then it will display the crontab of the user who is executing the command.

167. How environment variable is set so that the file permission can be automatically set to the newly created files**?**

Ans : -

umask command is used to set file permission on newly created files automatically.

Syntax

umask [-p] [-S] [mode]

It is represented in octal numbers. We can simply use this command without arguments to see the current file permissions. To change the permissions, mode is given in the arguments. The default umask used for normal user is **0002.** The default umask for the root user is **0022.** For calculating the original values, the values shown by the umask must be subtracted by the default values. It is mainly used for masking of the file and directory permission. The /etc/profile script is where the umask command is usually set for all users. The –S option can be used to see the current default permissions displayed in the alpha symbolic format.

For example, umask **022** ensures that new files will have at most **755** permissions (**777** NAND **022**).

The permissions can be calculated by taking the NAND of original value with the default values of files and directories.