Q.1 Attempt the following (any TWO) **[10]**

Q.1(a) Enumerate the duties of Linux System Administrator. **[5]**

(A) Duties of a system administrator

The duties of a system administrator are wide-ranging, and vary widely from one organization to another.

- Installing and configuring servers
- Installing and configuring application software
- Creating and maintaining user accounts
- Backing up and restoring files
- Monitoring and tuning performance
- Configuring a secure system
- Using tools to monitor security

Installing and Configuring Servers

- The standard Red Hat graphical user interface (GUI) requires a graphical layer called XFree86. This is a server. It runs even on a standalone machine with one user account. It must be configured.
- One cannot have a graphical desktop without a server.
- Likewise, printing in Linux takes place only after a print server is configured.
- There are different servers like, Web server, FTP server, and mail server.
- This duty falls to the system administrator. He needs to know exactly which servers he needs and how to employ them, and to be aware that it is bad practice and a potential security nightmare to enable services that the system isn't using and doesn't need.

Installing and Configuring Application Software

- Although it is possible for individual users to install some applications in their home directories, these applications are not available to other users without the intervention of the system administrator.
- Besides, if an application is to be used by more than one user, it needs to be installed higher up in the Linux file hierarchy, which is a job that only the system administrator can perform.
- "Skeleton" configurations — administrator-determined default configurations — set the baseline for user employment of applications.

Creating and Maintaining User Accounts

- An account must be created for each user in Linux system and only system administrator can do this.
- S. Administrator might want to let users select their own passwords or he creates the passwords for the users.
- Old accounts which are not required anymore are blocked by the system admin.
- It might be that there are aspects of the business that make Web access desirable, but S admin doesn't want everyone spending their working hours surfing the Web.

Backing Up and Restoring Files

- There is considerable need to back up important files so that the system can be up and running again with minimal disruption in the event of hardware failure, security, or administration failure.
- Only the system administrator may do this.
- Because of its built-in security features, Linux doesn't allow users even to back up their own files to removable disks.
- He needs to formulate a strategy for making sure system is not vulnerable to catastrophic disruption.
- He might make a full system backup every few days.

- Restoring files also has an equal importance. He makes it certain that he can restores the files if the need arises by the your restore process at least once during a noncritical time.

Monitoring and Tuning Performance

- System tuning is an ongoing process aided by a variety of diagnostic and monitoring tools.
- Proper monitoring allows you to detect a misbehaving application that consumes more resources than it should or fails to exit completely upon closing.
- To squeeze the best performance from your equipment, monitor your system carefully.

Configuring a Secure System

- If there is a common threat in Linux system administration, it is the security of the computer and data integrity.
- The system administrator's important task, is to make certain that no data on the machine or network are likely to become corrupted whether by power failure, by misconfiguration or user error or by malicious or inadvertent intrusion from elsewhere.

Using Tools to Monitor Security

- Security is monitored by the system admin.
- He makes sure that whenever a security advisory is issued, he downloads and installs the repaired package.
- Preventing the use of your machine for malicious purposes and guarding against intrusion are, in the end, is his responsibility alone.

Q.1(b) Explain GRUB.conf file in details. [5]

(A) When the system boots, GRUB presents a graphical screen showing the operating systems that you can boot. The */boot/grub/grub.conf* file controls what information is displayed on the graphical screen. This file even controls whether you see the graphical screen at all. Listing shows a typical GRUB Configuration file.

```
# grub.conf generated by anaconda
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root  (hd0,0)
#          kernel /vmlinuz-version ro root = /dev/VolGroup00/LogVol00
#          initrd /initrd-version.img
# boot = /dev/had
    default = 0
timeout = 5
splashimage = (hd0, 0)/grub/splash.xpm.gz
hiddenmenu
title Fedora Core (2.6.9-1.667)
    root  (hd0, 0)
    kernel /vmlinuz-2.6.9-1.667 ro root=/dev/VolGroup00/LogVol00 rhgb quiet
    initrd /initrd-2.6.9-1.667.img
```

Listing : The /boot/grub/grub.conf GRUB configuration file.

All lines beginning with a # (hash character) are comments and will be ignored. GRUB also ignores blank lines.

The lines following the lines beginning with the hash character and before the line beginning with title are the menu interface commands that GRUB uses to display the menu. These lines have the following meanings:

- default = 0 — This command tells GRUB to boot the first listing beginning with title. If you had two entries beginning with title, you could set this number to 1 to boot the second entry.

- timeout = 5 — This command tells GRUB to boot the default entry after five seconds. To change the time, increase or decrease the number as desired.
- splashimage = (hd0,0)/grub/splash.xpm.gz — This command tells GRUB where to look for the splash image it displays for the menu. You can create your own images if you desire. Just be sure to follow the same format as shown here.
- **hiddenmenu** — This command tells GRUB not to display the menu and to boot the default after the timeout expires. You can still see the menu by pressing any key.
- **title** — This command tells GRUB to list a boot name on the menu using the name following the title command. In this example the title is Fedora Core (2.6.9-1.667), which is the name of the operating system and the kernel version number.

The lines following the title are explained here:

- **root (hd0,0)** — This line tells GRUB to boot the system from the first partition of the first hard drive.
- **kernel**... — This line tells GRUB the location of the kernel, as well as passes kernel parameters to the kernel. All locations are relative to the boot partition, so the listing here indicates that the kernel is in the root of the boot partition. If you want to pass kernel parameters to the kernel before it loads, this is the line to add them to. There are already two options shown here. The *rhgb* on the kernel line tells the system to use a graphical boot. Finally, the quiet option tells the system not to display detailed information about system booting.
- **initrd**... — This line tells GRUB the location of the initial ramdisk image that is used to load special drivers for the system. All locations are relative to the boot partition, so the listing here indicates that the initial ramdisk image is in the root of the boot partition.

Q.1(c) State the advantages of using hierarchical method for system organization. [5]

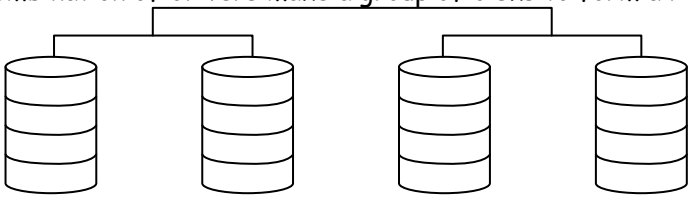
(A) The file system is organized in a flat, hierarchical file system. Linux's method of mounting its file systems in a flat, logical, hierarchical method has advantages over the file system mounting method used by window.

- Linux references everything relative to the root file system point /, whereas Windows has a different root mount point for every drive.
- If one has a /partition that fills up in Linux, one can create another file system called /usr/local and move the data from /usr/local in the original file system to the new file system definition.
- This practice frees up space on the /partition, and is an easy way to bring the system back to a fully functional state.
- This trick wouldn't work on a Windows machine, because Windows maps its file locations to static device disk definitions.

Q.1(d) What is RAID? Write and explain the different levels of RAID. [5]

(A) RAID stands for Redundant array of inexpensive / Independent Disks

- RAID contains a group or set or Arrays.
- A combination of drivers make a group of disks to form a RAID array or RAID set.



- It can be a minimum of 2 numbers of disk connected to a raid controller & make a logical volume or more drives can be in a group.
- There are 2 types of RAID
  (1) Software Raid
  (2) Hardware Raid

Raid Levels

(i) Raid 1

- Also known as disk mirroring
- Redundant Raid disk mode.
- A mirror of the first disk is kept on other disks
- If all disks crash but one all data can still be recovered.
- To work properly, RAID 1 needs two or more disks, & zero or spare disks.

(ii) RAID 5

- This levels combines the ability to use a large number of disks while still maintaining some redundancy.
- It uses there or more disks & space disks are optional.
- The final RAID 5 array contains combined file size of all disks except one.
- It can survive one disk loss, but if more than one disk fails, all data is lost.

Raid in Hardware :

- The principles of software RAID levels also apply to hardware RAID setups.
- The main difference is that in hardware RAID the disks have their own RAID controller with built-in software that handles RAID disk setup & I/O.

Q.2 Attempt the following (any TWO) [10]

Q.2(a) What are the files required to be changed when we setup a new system or move the system from one loction to another? [5]

(A) Whenever a new system is set up to work on a new network, a set of files needs to be modified to get it working on new network.

1) Setting up the IP Address-/etc/sysconfig/network-scripts/ifcfg-eth0

- To set up the IP address on the network interface, the following file has to be changed
  /etc/sysconfig/network-scripts/ifcfg-eth0
- Setting up the IP address on the network interface identifies the computer on the network.
- Open the file /etc/sysconfig/network-scripts/ifcfg-eth0.
- Insert the interface's IP address on the line that says
  IPADDR= " "
- Check the following lines also.
  BROADCAST=192.168.1.255"
  NETMASK="255.255.255.0"
  DEVICE ="eth0"
  BOOTPROTO="static"
  BROADCAST=192.168.1.255"
  NETASK="255.255.255.0"
  NETWORK="192.168.1.0"
  ONBOOT="yes"
  USERCTL=no
- Once, the IP address is added, restart the network service by the command – "service network restart".
- Then check the changed ipaddress with the command - ifconfig.

2) Setting up the Hostname - Choose the host name.

It has to be added in two different places
/etc/sysconfig/network
/etc/hosts

In /etc/sysconfig/network -
HOSTNAME = "JERRY"
/etc/hosts -

Change the first line in the file by adding the host name

127.0.0.1 JERRY localhost:localdomain

And reboot the machine.

3) Setting up the DNS Name resolution - resolv.conf.

- The program that resolves hostnames to IP addresses reads a file called resolv.conf.
- In this file DNS server's IP address can be put with the name given to the server.
- Multiple name servers can be added in this file. If one doesn't respond , the control shifts to the other host.
  - nameserver1.2.3.4
  - nameserver1.2.3.5
  - nameserver1.2.3.6
- On the local machine, try this with the ping command.
- If the local machine's address is 192.168.0.1 and the name given to it is "MyServer", then try to ping MyServer by the following command.

  ping MyServer

4) Starting up network service from xinetd -

- In computer networking, xinetd (extended Internet daemon) is an open-source super-server daemon which runs on many Unix-like systems and manages Internet-based connectivity.
- Xinetd is started on bootup and listens on ports designated in the /etc/xinetd.conf for incoming network connections.
- Multiple network services, for ex, telnet, talk, etc. are stored in the file xinetd.d.
- One should disable any unnecessary services from being started from xinetd as a part of securing the system. For example : telnet
- For example to disable telnet service, look in /etc/xinetd.d for a file telnet. And change the following line

  disable = no, and make it to yes to disable the telnet service.
- After the changes are saved, the xinetd service should be restarted by the following command.
- Service xinetd restart

5) Starting up network services from the rc Scripts – /etc/rc3.d directory.

- Network services that are not started out of xinetd are started out of the rc scripts at boot time.
- Network services started at the default boot level 3 are started out of the /etc/rc3.d directory.
- This file has the names of the services to start or stop.
- The script to start the service starts either an S and the kill script starts with a K.
- For example, SSH is started from /etc/rc3.d/S55sshd and killed upon shutdown from /etc/rc6/d/K25sshd.

Q.2(b) What is DHCP? Explain its configuration file. [5]

(A) Using DHCP, a client computer can have IP address & other information automatically assigned over the network.

The configuration file is /etc/dhcpd.conf

```
default lease-time 36000;
# amt of time in seconds that the host can keep the IP address
maximum lense-time 100000;
# maximum time the host can keep the IP address domain name
# the domain name of the DHCP server.
option domain name "example.com"';
option domain name server 192.168.1.1;
```

```
#nameservers
option routers 1.2.3.4, 1.2.3.5;
option routers 192.168.1.2;
# gateway/routers
option subnet mask 255.155.255.0;
# netmask (subnet mask of network)
option broadcast address 192.168.1.255;
# broadcast addr of network
subnet 192.168.1.0 netmask 255.255.255.0;
# subnet no gets assigned in range 192.168.1.3 192.168.1.126;
# define which addresses can be used.
```

Q.2(c) What are the advantages and disadvantages of NFS? Explain. [5]

(A) Advantages :

1) Biggest advantage NFS provides is centeralized control, maintenance and administration. Backup file system should be stored on a single server than to backup directories scattered.
2) NFS makes it trivial to provide access to shared disk space, or limit access to sensitive data.
3) NFS can also conserve disk space and prevent duplication of resources.
4) NFS when combined with NFS, users can log in any system, even remotely and still have access to their home directories and see a uniform view of shared data.

Disadvantages :

1) NFS is sensitive to network congestion, heavy network traffic shows down NFS performance similarly, heavy disk activity on the NFS server adversely affects NFS's performance.
2) If an exported file system is not available when a client attempts to mount it, the client system can hang.
3) Exported file system represents a single point of failure; if the disk or system exporting vital data or application becomes unavailable for any reason. Such as disk crash or server failure, no one can access that resource.
4) NFS suffers from potential security problems because its design assumes a trusted network, not a hostile environment in which systems are constantly being probed and attack.
5) The primary weakness of most NFS implementations based on protocol versions 1, 2 and 3, is that they are based on standard (unencrypted) RPC (Remote Procedure Call).

Q.2(d) Explain the concept of supernetting with suitable example. [5]

(A) With supernetting the class subnet marks are extended so that a network address & subnet mark could, for e.g. specify multiple class C subnets with one address.

for e.g.: if a thousand address are needed, you could supernet four class C networks together.

192.60.128.0
192.60.129.0
192.60.130.0
192.60.131.0
} Class C subnet address

192.60.128.0 → supernetted subnet address
255.255.252.0 → subnet mask
192.60.131.255 → Broadcast address

Here, subnet 192.60.128.0 includes all addresses from 192.60.128.0 to 192.60.131.255.
The network portion (Net ID) is 22 bits long, host portion is 10 bits long.

Q.3 Attempt the following (any TWO) [10]

Q.3(a) What are the different sections on smb.conf file? Explain. [5]

(A) Structure of the smb.conf file :

The smb.conf file is separated into several logical sections. A keyword surrounded by brackets [ ] denotes each section.

- **[global]**
  This is the first section which defines global parameters.

  Setting are as follows :
  1) Workgroup – MYGROUP, the name of the server. If a user accesses My network places on a windows machine, this server appears as MYGROUP.
  2) Server string = Samba server, it's a description field
  3) Security = user. This parameter indicates that samba will run in the user mode. That is each user must be an authorised user and verifies at the initial login time of file sharing.(different values are – share, server, domain)
  4) Log file=/var/log/samba/log – this of the location of the log file.
  5) smb passwd file = /etc/samba/smbpasswd – this shows the path to the location of the Samba users information file.

- **[homes]**
  This section is used to enable the server to give users quick access to their Home directories.
  1) comment = Home Directories – A comment line.
  2) browsable = yes - means that the directory will appear in the Windows file browser.
  3) writable = yes – means that the user can write to their directories.
  4) create mode = 0664 – sets the default permissions for files created in the directory.
  5) directory mode = 0775 – sets the default permissions for created directories.
  6) max connections = 1 – the maximum number of the simultaneous connections allowed. Setting this number to 1 prevents a user from logging in to the server from more than one location.

- **[printers]**
  This section sets the options for printing.
  1) path = /var/spool/samba – the location of the printer spool directory
  2) printable = yes - enables clients to send print jobs to the specified directory. This option must be checked otherwise printing does not work.
  3) browsable = yes - means that the printer appears in the browse list.

Q.3(b) What are the tasks to be performed to setup Timeserver? Explain the steps to configure NTP Server and NTP client. [5]

(A) Selecting a time server –

- There are three categories of time servers
  1) Hardware 2) Software 3) Both

Set up a Time server –

- The Network Time Protocol (NTP) is a protocol used to help coordinate the Linux system clock with an accurate time source.

  Download and install NTP package –
  Download and install with RPM.
  NTP rpm's filename starts with word ntp followed by version number as in Ntp-4.1.2.i386.rpm
  The /etc/ntp.conf file

- Is the configuration file for Linux NTP?

File :

```
server 0 rhel.pool.ntp.org
server 1 rhel.pool.ntp.org
server 2 rhel.pool.ntp.org
server 127.127.1.0
fudge 127.127.1.0.stratum 10

#restrict default ignore
#restrict 127.0.0.1
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap nopeer
```

Blocking Unauthorized Access

- If your ntpd is publicly accessible, do you really need to block all connections from unauthorized hosts?
- If "Yes", use the following default restriction (and keep in mind that you will have to add restrict lines for every authorized server and client host/subnet

To deny all machines from accessing the NTP server, add the following line to /etc/ntp.conf:

```
restrict default ignore
```

Add the following line to allow unrestricted access from the localhost restrict 127.0.0.1

The following line allows a subnet to receive time service and query server statistics:

```
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap nopeer
```

Access Control Option

There are numerous Access Control options which may be used on the restrict lines in your ntp.conf. Some of the more commonly used options are -

- **nomodify** -- "Do not allow this host/subnet to modify the ntpd settings even if they have the correct keys."
- **noserve** -- "Do not serve time to this host/subnet." This option is really intended to be used when you want to allow a host/subnet to access your ntpd only for monitoring and/or remote configuration.
- **notrust** -- "Ignore all NTP packets that are not cryptographically authenticated." This option tells ntpd to ignore all packets which are not crytographically authenticated.
- **noquery** -- "Do not allow this host/subnet to query your ntpd status." The ntpd status query features provided by ntpq/ntpdc will reveal some information about the system running ntpd (e.g. OS version, ntpd version) that you many not wish others to know. Restrict otherntp.server.org mask 255.255.255.255 nomodify notrap noquery
- **notrap**
- **nopeer**

  ```
  server 0 rhel.pool.ntp.org
  server 1 rhel.pool.ntp.org
  server 2 rhel.pool.ntp.org
  ```

  It says that the ntp clients to use public server form the rhel.pool.ntp.org project.

  ```
  server 127.127.1.0
  fudge 127.127.1.0.stratum 10
  ```

  Server says that the local system clock is a timeserver.

  If you are disconnected from the Internet then they are unavailable and you're left with the local clock. Using fudge to say that the local clock is stratum 10 makes ntp use the local clock when no timeservers are available. This is good because it makes sure you can disconnect your box from the Internet without getting your clock screwed.
- Save the ntp.conf file and restart NTP server.

How to get NTP started?

To get NTP configured to begin at boot, use the line-

```
#chkconfig ntpd on
```

To begin.stop and restart NTP after booting,

#service ntpd start
#service ntpd stop
#service ntpd restart

Configuring an NTP client

- Select the server to use a reference clock, start the NTP daemon, ntpd.
- Using GUI – Select system Settings – Date & time.
- Using command interface – type system-config-date
- The Date-Time properties window will get open
- Click the Network Time Protocol tab to configure NTP. Check the check box – enable network time protocol.
- Doing so NTP server pane gets enabled.
- Red Hat ships with two server configured: clock.redhat.com and clock2.redhat.com.
- Select any one and click on Add.
- To add the different server, type the name or IP address of the server.

Restart the ntpd.

- #service ntpd restart.

Q.3(c) How are reference clocks configured? Explain. [5]

(A) For timer server to keep and thus to serve accurate time, local time server needs to be synchronized against one or more master or reference clock.

NTP is a distributed application, meaning that server and client are dispersed, that any given client can request a time check from any given server and that the application continues to function inspite of one or even many of the server.

NTP is also hierarchical and organizes time servers into several stratum to reduce the wood on any given server or set of servers stratum 1 servers are referred to as primary server, stratum 2 servers as secondary server and so on.

There are far more secondary server than primary server and client sync to secondary or tertiary servers.

Q.3(d) On a Linux machine a directory named/home/newusr/TYIT is to be accessed from windows machine. Write the configuration to carry out this task. [5]

(A)

```
[global]
   workgroup = METRAN
   encrypt passwords = yes
   wins support = yes
   log level = 1
   max log size = 1000
   read only = no
[homes]
   browsable = no
   map archive = yes
[printers]
   path = /var/tmp
   printable = yes
   min print space = 2000

[test]
   browsable = yes
   read only = yes
   path = /home/newusr/TYIT
```

Q.4 Attempt the following (any TWO) [10]

Q.4(a) Explain use of ssh, scp, sftp services. [5]

(A) ssh

- It is a secure shell program.
- It is used for logging into a remoter machine and executing commands in a remote machine.
- It provides secure, encryptes communications between hosts.
- The host name to login should be specified.
- When the username is specified in the ssh command line, it demands for the password.

Example :

ssh node5

Log on securely to node5.

sshuser1@mylab.textra.edu

Log on to mylab.testra.edu as user user1.

scp

- This command securely copies files over the network.

Example : Putting of a single file –

scp myfile1.dat mylab.textra.edu:data1.txt

Getting of a single file -

scp mylab.textra.edu:data1.txt ./

It copiesnfile data1.text form your home directory of node4 to your current working directory on your local server.

sftp

- Is used to transfer files to and from a remote computer.
- It is interactive and secure.
- Once connected to the remote computer, giving a password if necessary, you can type the following interactive commands to change directories and to transfer files between your local computer and the remote computer.

get filename	Retrieves remote file and stores it to local computer.
put filename	Upload local file to store on remote computer.
cd path	Change remote directory to path
Ls	List remote files
Lls	List local files
lcd path	Change local directory to path
Quit	Quit sftp
Help	Display help text

Example :

sftp 192.156.1.0

Enter password :

sftp> use the above commands.

#sftp user1@mylab.textra.edu

Connect to mylab.testra.edu using username user1.

Q.4(b) What are the types of domain servers? Explain in brief. [5]

(A) The three types of local domain name servers are :

1) Master or Primary 2) Slave or Secondary 3) Caching

Master

The master contains all the information about the domain and supplies this information when requested. A master server is listed as an authoritative server when it contains the information you are seeking and it can provide that information.

Slave

The slave is intended as a backup in case the master server goes down or is not available. This server contains the same information as the master and provides it when requested if the master server cannot be contacted.

Caching

A caching server does not provide information to outside sources; it is used to provide domain information to other servers and workstations on the local network. The caching server remembers the domains that have been accessed. Use of a caching server speeds up searches since the domain information is already stored in memory, and the server knows exactly where to go rather than having to send out a request for domain information.

Q.4(c) Explain the two programs used to check the DNS configuration. [5]

(A)

- The command **dig** is a tool for querying DNS nameservers for information about host addresses, mail exchangers, nameservers and related information.

  Example : dig mt-example.com
  The output tells the technical details about the answer received from DNS server.
  Finally it tells the ip address of mt-example.com as

  ;; ANSWWER SECTION
  Mt-example.com 28626 IN A 205.190.150.66

  The quick way to get the answer only is : dig mtiexamplke.com +short

- **host** – is a simple utility for performing DNS lookup. It is normally used to convert names to IP addresses and vice versa.

  host [name] [server]

  name is a domain name that is to be looked up. It can also be an ip address. In which case host will by default perform a reverse lookup for the address.

  Server is an optional argument which is either the name or IP address of the name server that host should query instead of the server or servers listed in /etc/resolv.conf

Q.4(d) What are zone statement? Explain the different values for the zone statement. [5]

(A) The listings in /etc/ named.conf are zone statements.

- The zone statements refers to the file that are called zone files.
- Each zone statement begins with the word zone followed by the domain name and the data class.
- The four data class are in, hs, hesiod and chaos.
- If no type specified the default is in for internet.

Different values for zone statements :

1) allow query : Accepts queries only from hosts in the address list.
2) allow transfer : Zone transfers are accepted only by hosts in the address list.
3) allow – update : Hosts in the address list are allowed to update the database.
4) also-notify : Servers in the address list are sent a notify message when the zone updated.
5) check-names : Host name are checked for compliance with the RFC.
6) Max. transfer-time-in : specifies the time the slave waits for a zone transfer.
7) notify : when zone files are updated, this option when set to yes, sends DNS notify messages.

Q.5 Attempt the following (any TWO) [10]

Q.5(a) Why aliases are required while configuring send mail? What are the changes that are required for creating an alias? [5]

(A)

- Using mail alises, distribution list can be created.
- It becomes easy to access users more conveniently.
- If someone's spelling is difficult, an alias can be created for the name, and the mail still reaches to the intended person, if the name is misspelled.
- The alises file id /etc/alises

```
mailer-daemon postmaster
postmaster    root
#general redirections for pseudo accounts
daemon        root
lp            root
shutdown      root
usenet        root
ftpadm        ftp
ftpadmin      ftp
ftp-adm       ftp
ftp-admin     ftp

#trap decode to catch security attacks
decode        root

#person who should get root's mail
#root         marc
#users
bob:          marc
```

- To create an entry in the alises file, type username followed by a colon, followed by space, followed by alias.
- Multiple usernames can be specified on the left side of the colo to create a primitive distribution list.

Q.5(b) Explain SMTP, POP3 and IMAP4 protocols. [5]

(A) **SMTP -** (pronounced as separate letters) Short for *Simple Mail Transfer Protocol,* a protocol_for sending e-mail_messages between servers. Most e-mail systems that send mail over the Internet_use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client_using either POP_or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure_your e-mail application.

POP3

- The full form is Post Office Protocol.
- This protocol is a part of email process.
- POP3 was developed to solve the problem of what happens to messages when the recipient is not connected to the network.
- POP3 runs on a server that is connected to a network and that continuously sends and receives mail.
- The POP3 server stores any messages it receives until the message recipient request them.
- Without POP3, MUA and MTA cannot communicate.
- If one wants to read the mail, he needs POP3 to retrieve messages that arrive at his MTA while he is offline.
- POP3 uses the MTA's storage to hold messages until they are requested.

- When users want to check their email, they connect to the POP3 server and retrieve messages that were stored by the server.
- After retrieval, the messages are stored locally and one can his MUA on his PC to read them at his leisure.

IMAP4

- Full form – **Internet Massage Access Protocol version 4.**
- It provides much more sophisticated email-handling functionality than POP3 does.
- IMAP4 enables one to store email on a networked mail server.
- IMAP4 enables mail to reside permanently on a remote server, from which one can access his mail.
- Mail retrieval can be done from any device, office PC, PDA, cell phone etc.
- The usual mail delivery process involves three components, a mail user agent (MUA), a mail transfer agent (MTA) and a mail delivery agent (MDA).

Q.5(c) Write the purpose of the following parameters of vsftpd.conf file [5]
(i) anonymous_enable (ii) write _enable (iii) chown_username
(iv) ftpd_banner (v) dirmessage_enable

(A) anonymous_enable

If yes, allows anonymous FTP access.

write_enable

If YES, enables all variations of the FTP commands that allows

chown_username

specifies the name of user to set ownership of uploaded files.

ftpd_banner

allows you to display a site_specific banner message when users connect to the server.

dirmessage_enable

If set to YES, first time user enters a new directory, vsftpd displays contents of a file named message.

Q.5(d) Explain how to disable anonymous FTP. [5]

(A) Easiest way is to remove ftp user from /etc/ password & /etc/group.
The problem with this method is that later if you decide to permit anonymous FTP, you have to recreate user ftp & group & reconfigure vsftpd doesn't allow any FTP login if user ftp is not present in password file. Hence it's advisable to backup the two files.

Another approach is to add ftp to /etc/vsftpd/user_list and set user list deny = YES and anonymous enable = NO in /etc/vsftpd/vsftpd.conf. Do not just comment out anonymous_enable_YES

Q.6 Attempt the following (any TWO) [10]

Q.6(a) Explain the working of Apache web server. [5]

(A)

Directive	Description
ServerRoot	Name of the log files or additional configuration files are appended.
PidFile	It stores the name of the file containing the PId of master server process. By default its value is set to /var/run/httpd.pid
TimeOut	Defines the maximum time in seconds Apache waits for packet send and receive operations to complete. It likes defined in seconds. Default value is 120. Per connection

KeepAlive	Default value is Off. Sets the connection to a remote client in the absence of direct contact for the time specified by KeepAliveTimeOut directive.
MaxKeepAliveRequests	Sets the number of requests permitted. By default 100 requests.

Q.6(b) Explain the <Files><Files> and <IfModule></IFModule>blocks. [5]

(A) The <Files> </Files> block specifies that access to all files beginning with .ht is denied unconditionally to all clients, preventing clients from viewing their contents, an important measure considering that access file can contain security sensitive information.

```
<Files ~ " ^\.ht">
Order allow. deny
Deny from all
</ Files>
```

All directives inside an <if Module>
</if Module> block are evaluated only if the indicated module is loaded.

The default configuration file has a number of sub blocks.

```
<If Module mod mine-magnic.c>
    MIMEMagicfile conf IMagic
    <11EModule>
```

If the mod mime-magic module is loaded, the MIMEMagic file directive causes Apache to read the contents of the configuration file named letc/htpd/conf/magic.
This file enables Apache 10 determine their MIME type by reading the first few bytes of a file.

Q.6(c) Explain the shadow password system. [5]

(A)

- Shadow passwords are an enhancement to login security on Unix systems. Traditionally, passwords are kept in encrypted form in a world-readable table (/etc/passwd).
- To test a password, a program encrypts the given password with the same "key" that was used to encrypt the password stored in the/etc/passwd file If the /etc/passwd/ file password matches the encrypted login password, the user is granted access.
- To reduce the vulnerability of a world-readable password file, many newer Unix systems utilize shadow password files. The traditional password file is maintained in /etc/passwd (as it contains more than just password information), **/etc/passwd and /etc/shadow**
- Each line in both the files consists of colon-separated fields one line per user.
- The format of /etc/passwd is :

  Username : password : uid : gid : gecos : directory : shell

Fields in Password file

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(gecos)**: 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.

Example :

kiran : x : 502 : 502 : Kiran Sathe : /home/kiran : /bin/bash

- **/etc/shadow file**
  In addition to storing the encrypted password, /etc/shadow stores password expiration information.

The fields in /etc/shadow

1) User name : It is your login name
2) Password : It your encrypted password. The password should be minimum 6-8 characters long including special characters/digits
3) Last password change (lastchanged) : Days since Jan 1, 1970 that password was last changed
4) Minimum : The minimum number of days required between password changes i.e. the number of days left before the user is allowed to change his/her password
5) Maximum : The maximum number of days the password is valid (after that user is forced to change his/her password)
6) Warn : The number of days before password is to expire that user is warned that his/her password must be changed
7) Inactive : The number of days after password expires that account is disabled
8) Expire : days since Jan 1, 1970 that account is disabled i.e. an absolute date specifying when the login may no longer be used

Example :

vivek:1fnfffc$pGteyHdicpGOffXX4ow#5:13064:0:99999:7:::

↓ ↓ ↓ ↓ ↓ ↓

1 2 3 4 5 6

Q.6(d) Which command is used to change the expiration policy for a user's password? Explain with example. [5]

(A) The change command changes the expiration policy for a user's password.

Change [– ℓ] [–m mindays] [–M maxdays] [–d lastday]
[– I inactive] [–E expire date] [–w warndays] username

eg. Change – ℓ logon – m 60 – M75 – W5

will set the minimum days for the password as 60

75 days is the period (maximum) till when it can used.

A warning will be issued 5 days prior to expiry.

Q.7 Attempt the following (any THREE) [15]

Q.7(a) Write a note on GNU and Linux Distribution. [5]

(A) Debian GNU/Linux is a distribution that emphasizes free software. It supports many hardware platforms.

Distribution	Description
64 Studio	Attempts to specialize in audio and video production on x86-64 workstations.
Ubuntu	A distribution sponsored by Canonical Ltd. and receiving major funding from South African Mark Shuttleworth. Aims to offer a complete and polished desktop on a single DVD.
Damn Small Linux	It is a small distro designed to run on older hardware. It is commonly used on virtual machines due to low memory requirements.
Feather Linux	It boots from either a CD or a USB flash drive. Uses Knoppix-based hardware detection and the Fluxbox window manager.
Edubuntu	A complete Linux-based operating system targeted for primary and secondary education. It is freely available with community based support. The Edubuntu community is built on the ideas enshrined in the Edubuntu Manifesto: that software, especially for education, should be available free of charge and that software tools should be usable by people in their local language and despite any disabilities.

Q.7(b) How are NFSv4 client and server configured? Explain [5]

(A) Configuring an NFSv4 client :

NFSV4 specific mount options includes :

1) clientaddr = n → causes a clinet on a multi homed system to used the IP address specified by n to communicate with an NFSV4 server.
2) proto-type → Tells the client to use the network protocol specified by type which can be tcp or udp.
3) rsize = n → sets the read buffer size to n bytes maximum 32678.
4) sec = mode → set the security model to mode which can be sys, krb5i or krb5p.
5) wsize = n → set the write buffer size to n bytes. Maximum values is 32678.

Configurating on NESV4 Server :

- The /etc/exports file is the main NFS configuration file.
- It lists the file systems, the server exports, the system permitted to mount the exported file systems, and the mount options for each export.
- The two export file systems are /home/media.

The corresponding entry in /etc/ exports are :

/home 192.168.0.0/24 (rw, async)
/media 192.168.0.0/24 (ro)

With the exports configured, start (or restart) the daemons (the portmapper) using initialization scripts

service nfs start
service nfswork start

Use rpcinfo. P to make sure the necessary daemons are running.

rpcinfo – p

Showmount – a (or exportsfs – v) to list the server's NFS exports.
The final step in preparing an NFS server is to ensure that NFS services are started at boot time.

Q.7(c) Distinguish between NFS and SAMBA Server. [5]

(A) Easiest way is to remove ftp user from /etc/ password & /etc/group.
The problem with this method is that later if you decide to permit anonymous FTP, you have to recreate user ftp & group & reconfigure vsftpd doesn't allow any FTP login if user ftp is not present in password file. Hence it's advisable to backup the two files.

Another approach is to add ftp to /etc/vsftpd/user_list and set user list deny = YES and anonymous enable = NO in /etc/vsftpd/vsftpd.conf. Do not just comment out anonymous_enable_YES

Q.7(d) Compare inted and xinted services. Explain standalone services of xinetd. [5]

(A) Xinetd services are started from xinetd. Each of these services should ideally have its own file in the /etc/xinetd.d directory so should look in that directory to find the appropriate file and open the file to check whether it is enables or disabled.
Inetd and xinetd both help to restart and reload services but to restart service in inetd we use---
#service dhcpd start
but in xinetd we use----
#service xinetd start

Note: in inetd we give name of that service it means if you want to start dhcpd then you will have to give name service

dhcpd start
but in xinetd service we don't type that service telnet
start to start telnet we type service xinetd start

Standalone services of xinted

from apache	-	Web server
sshd	-	SSH server
sendmail	-	mail server
qmail	-	Mail server
postfix	-	Mail server
thttpd	-	Semilightweight web server
boa	-	Lightweight web server
named	-	DNS server
xfs	-	X font server
xdm	-	X display manager
portmap	-	maps RPC services to ports
rpc.quotad	-	serves quota information
knfsd	-	userspace portion of the NFS daemon
rpc.mountd	-	NFS mount server
squid	-	Web proxy server
mysql	-	database server
oracle	-	database server

Q.7(e) Explain the following : Mail User Agent, Mail Delivery Agent and Mail Transfer Agent. [5]

(A) Mail User Agent

- Provides an interface for reading and writing email messages
- MUA sends a composed email message to mail
- Transfer Agent (MTA), which transmits the message across the network.

Mail Transfer Agent

- MTA works without any intervention by the user.
  MTA determines the IP address of the recipients mail server.
- Receving MTA passes the message to yet another program the MDA.

Mail Delivery Agent

- MDA receives the message from the MTA
- It stores the new message in the recipients mailbox file

Q.7(f) Write an SSI page that will display the long listing of the directory/home/tyit. [5]

(A)

```
<html>
<head>
<title> SSI test page </title>
<link rel = "stylesheet" type="text/css" href="rhlnsa3.css">
</head>
<body>
<h1> SSI Test Page </h1>
<div id="content">
<pre>
<!-- # execcmd = "/s–1/home/tyit – –">
</pre>
</div> <!-- content – – >
</body>
</html>
```

❑ ❑ ❑ ❑ ❑