Question 8 (a)

What is backup? What are the strategies followed in Linux for backup?

BACKUP :-

Backup is the process of making a copy of system files, configuration and settings so that in case of emergency such as OS gets corrupt or hard disk crashes, the backup can be used to rebuild the system so that services can be resumed.

Strategies followed in Linux for backup :-

There are mainly three strategies followed in Linux for backup.

① Incremental backup

② Differential backup

③ Full backup

A full backup is a complete backup of an installation or a part of its file system.

If there is a complete crash, one can restore user data from the full back up. But the operating system files are also sometimes one produces over a period of time and with considerable effort. A full back up is easy to restore from, but given the large disk capabilities of today, the amount of time taken to make a full backup can be non-trivial. So one can think of a full backup at periodic intervals and daily or more frequent incremental backups, where only files that have changed since the last backup are copied. But it can be difficult to locate a needed file in an incremental backup, so the concept of differential backups was

In differential backup, all files that have changed since the last full backup are backed up. So the amount of backing up required is in between that of a full backup and an incremental backup.

It is important to consider what the backup media should be as well. Very often it is a tape of some kind, but a USB disk or network backup to a data centre can also be considered. One has to look at the reliability of a backup and make sure that one do not use media beyond their useful life. A backup is pointless if one cannot restore it. One cannot afford a single failure in a backup. One can also consider taking multiple backups each time.

Depending upon the criticality of the business, one might keep different copies of backup at different locations. But whatever the company characteristics, one has to make sure to have atleast one backup offsite that is geographically sufficiently distant from the site.

There are several different kinds of backup tools. Some are sophisticated commercial offerings while at the other end we have the basic linux commands such as tar and cpio. Both of them work quite well and one can decide what to use.

The tar command allows to take a backup of all or selected files in a directory hierarchy onto tape, floppy disk or the hard disk itself. Tar knows about directories and links, and maintain headers, checksums and file permissions and answers. To take a backup of all files under /home/khanz,

```
tar cvbf 40/dev/rmt0 /home/khanz
```

We can use cpio command for creating and restoring from archives. It reads the list of files from the standard output and copies them to whatever we specify.

For generating the list of filenames, we can use a program like find.

```
[khanz@linux khanz] $ find /home/khanz | cpio -o >
    /dev/rmt0
```

We can use the many options of the find command to choose files that satisfy specific conditions so that only those files are backed up.

Question 8(b)

What encryption function is used by windows 2000 operating system?

From windows 2000 onwards, the Encrypting File System (EFS) function is used for filesystem-level encryption. The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer. By default, no files are encrypted, but encryption can be enabled by users on a per-file, the file. Because the encryption and decryption operations are performed at a layer below NTFS, it is transparent to the user and all their applications.