Question 5(a)

Explain the role and importance of following tools for quota management in Linux:

- quotacheck
- repquota
- quota

quotacheck

quotacheck examines each filesystem, builds a table of current disk usage, and compares this table against that recorded in the disk quota file for the filesystem. If any inconsistencies are detected, both the quota file and the current system copy

of the incorrect quotas are updated. By default, only user quotas are checked. quotacheck expects each file system to be checked to have quota files named [a] quota.user and [a].quota.group located at the root of the associated filesystem. If a file is not present, quotacheck will create it. If the quotacheck file is corrupted, quotacheck will create it and tries to save as much as data possible. Rescuing data may need user intervention. With no additional options, quotacheck will simply exit in such a situation. When in interactive mode (option -i), the user is asked for advice.

repquota

repquota prints a summary of the disc usage and quotas for the specified file systems. For each user the current number of files and amount of space (in kilobytes) is printed, along with any quotas created with edquota. As repquota

tries to detect (by reading /etc/nsswitch.conf) whether entries are stored in standard plain text file or in database and either translates chunks of 1024 names or each name individually. One can override this autodetection by -c or -C option. Only the superuser can see quotas which are not their own.

quota

quota generates a report listing quota roots, giving their limits and usage. If the -f option is given, quota will first fix any inconsistencies in the quota subsystem, such as mail boxes with the wrong quota root or quota roots with the wrong quota usage reported. If an optional domain is given, the quota listing (and inconsistency fixing) is limited to quota roots with names that starts with one of the given prefixes.

Running quotas with both the -f option and mailbox-prefix arguments is not recommended.

Question 5(b)

Compare the security features / mechanism of Windows 2000 and Linux operating systems.

Physical Security Management

The main problem or issue of computer security is unauthorized physical access to a secure computer system and it is breach of computer security. If a computer has BIOS password enabled, it adds an extra layer of security. Physical security management is not dependent on the operating system. We can enable BIOS password on any Personal computer irrespective of the operating system.

Logon Security Management

When a user logs on to a window machine,

he is presented with an oscreen password prompt if enabled by the user. The login prompt will ensure the security of the data. Unauthorized access will be prevented with the use of logon security mechanism. The logon security feature is available in both windows 2000 as well as Linux operating system.

Users and group management :-

In windows 2000 and Linux operating system, every unique user of the system has a unique user account and is provided a security Identifier or SID at the time when account is used. Windows provides multiple levels of user accounts with the most powerful user account the Administrator. In Linux operating system, the most powerful account is root. These administrative accounts have the power to manage all the settings on each

One should set the minimum standards set for strengthening the password of user accounts. One should set length of password, number of failed attempts for locking out the user account in order to ensure security.

Domain management feature

Both windows 2000 and linux provides domain management feature through which the administrator has the full control on the users who can access the network PCs and also on the PCs. This model also provides for a single sign on (SSO) to all resources, that is the user is not requi to provide credentials for each computer that the user wishes to access.