Question 6 (a)

Why is the audit view limited to specific users only in Windows 2000?

Windows 2000 auditing is a facility responsible for tracking user activities, keeps a track of

system and as a result this is the account that must be properly secured. Thus, it is recommended that the administrator account must not be used for day-to-day work at the network.

Local and Global Group Management Feature

In both linux and window 2000, users are classified as local and global user groups. Local groups are applied to a single computer and are used to control access to resources on the local computer. Global groups apply to an entire domain, or group of computers.

We can combine groups together but the only allowed combination is to put a global group into a local group.

User Account Management Feature

Both Linux and window 2000 operating systems provide control on user account management.

them. Windows 2000 maintains a security log. User events are written onto their security log. All the events related actions are entered onto security log. An audit entry in security log not only comprises action that takes place, but also the user and success or failure of the event and when the action occured. Thus whatever event takes place in Windows 2000, security log has an entry for the same.

An audit group policy is configured for all domains and domain controllers. Auditing is assigned to parent container and it passes to Parent container and it passes it down the hierarchy to the child containers. However, if explicitly a child container is assigned a group Policy then child container group overrides Parent container settings.

To plan an audit policy, computers must identify on

which auditing is to be applied. By default, auditing option is turned off.

Following events can be audited on computers:

1. User logging on and off
2. User accounts and group changes
3. Changes to Active Directory objects
4. Files access
5. Shutting down Windows 2000 server
6. Restarting Windows 2000 server.

Keeping in view of the sensitivity of the auditing, the auditing view is limited to specific users only in Windows 2000.

If every user has access to audit view, then the information can be misutilized or modified by the users who want to gain unauthorized access. Thus, the audit view is limited to specific users in windows 2000.

Question 6(b)

Explain the purpose and features of registry management. Also, explain the uses of it.

The Windows 2000 Registry stores the configuration data for the computer, and as such is obviously a critical item to secure properly. The Registry in Windows 2000 can be directly updated with the tools like Regedit.exe and Regedt32.exe. It is recommended that Regedt32.exe be used as permissions can by applied to individual keys as one sees fit.

The following lists are the permissions that are available for Registry:

① Query value - Ask for and receive the value of a key.

② Set value - change a key value.

③ Create subkey - Create a subkey

④ Enumerate subkey - List the subkey

⑤ Notify - set Auditing

⑥ Create link - Link this key to some other key.

⑦ Write DAC - Change permissions

⑧ Read control - Find the owner of a key

⑨ Write owner - Change ownership of a key

⑩ Delete - Delete the key.

With the help of windows 2000 registry, the administrator can enforce desired rules and regulations. The registry feature of windows operating system also allows the administrator to audit the system and its user's activities. Through registry, the administrator can set what all the devices that can be plugged in for use and also he can deny certain type of devices. This will increase the security of the operating system.