Question 1(a)

Write the purpose of VPN and name the VPN technologies supported by Windows 2000.

VPN stands for Virtual Private Network. VPN provides a secure network connection between two remote machines. Virtual Private Network (VPN) is an extension of private network that involves encapsulation, encryption and authentication to links across shared or private networks.

A VPN uses tunneling to transfer data on a VPN using dedicated lines or dial up lines. A VPN mimics the properties of a dedicated Private network through internet; allowing data transfer between two computers in a network.

VPN's tunneling is a secure method of using an inter-network infrastructure to transfer a payload. A tunneling protocol comprises of tunnel maintenance protocol and tunnel data transfer protocols.

The two basic types are:

① Voluntary tunnels

② Compulsory tunnels

VPN management involves managing addresses, server access, authentication, and encryption. Troubleshooting VPN involves checking connectivity, remote access connection establishment, routing, IPsec.

VPN Technologies supported by Windows 2000 :-

Windows 2000 supports the following VPN technologies:

① Point to Point Tunnel Protocol (PPTP)

② Layer 2 Transfer Protocol (L2TP)

Question 1(b)

List the main contents of Password files and where are they located in windows? Also, explain the concept of shadow passwords?

Following are the main contents of Password files:

① Username : Stores login name i.e., username.

② Information used to validate a user's password.

③ User identifier number which is used by the operating system for internal purpose.

④ Group identifier number, which identifies the primary group of the user.

⑤ Gecos field, commentary that described the person or account.

⑥ Path to the user's home directory.

⑦ Program that is started every time the user logs into the system.

In windows, the password file is stored in C:\Windows\System32\SAM.

Shadow File:-

Shadow file is used to increase the security level of password by restricting all but highly privileged user's access to hashed password data. Typically, that data is kept in files owned by and accessible only by the super user.