Course Code : MCS-022

Course Title : Operating System Concepts And Networking Management

Last Date of Submission : 15th October, 2018 (For July, 2018 Session)

15th April, 2019 (For January, 2019 Session)

Question 1:

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

Ans:

A Virtual Private Network is a connection method used to add security and privacy to private and public networks, like WiFi Hotspots and the Internet. Virtual Private Networks are most often used by corporations to protect sensitive data. However, using a personal VPN is increasingly becoming more popular as more interactions that were previously face-to-face transition to the Internet. Privacy is increased with a Virtual Private Network because the user's initial IP address is replaced with one from the Virtual Private Network provider. Subscribers can obtain an IP address from any gateway city the VPN service provides. For instance, you may live in San Francisco, but with a Virtual Private Network, you can appear to live in Amsterdam, New York, or any number of gateway cities.

Protocols used by WIN 2000 for VPN are PPTP (Print to print tunnel Protocol), L2TP (Layer 2 Transfer Protocol), IPSec (IP security), IP-IP.

VPN management involves managing user addresses, servers access, authentication and encryption. Troubleshooting VPN involves checking connectivity, remote access connection establishment, routing, IPSec.

(b) List the main contents of Password files and where are they located in Windows? Also, explain the concept of Shadow passwords?

Ans

Windows stores its passwords in **Security Accounts Manager** database, or SAM database. This is a file that exists in the registry and access to it is tightly controlled while windows is running; however, local administrators who can run processes as NT AUTHORITY\SYSTEM can access it.

In the entire SAM database, the main contents of the account are under the node of /Domain/Account/Users. Each account following two sub-items, F and V. Saved in the project F

is the account registry records, such as the last login time, lockout time, the failed login count, total logins since creation and so on. Project V saves the basic information of the account, like user name, full name, contents, group ownership, password hash, etc.

Concept of Shadow Password

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). Although this scheme is reasonably secure, it is still subject to break-in attempts, such as the "dictionary attack", where common or likely passwords are encrypted and tested against the /etc/passwd file until a match is found. For a good password, these types of attacks can take a long time (since, on most systems, there are literally over 10,000 trillion possible passwords). However, many users choose common words, combinations of common words, or variants on personal data for their passwords. These are easily cracked, often within a few hours.

To reduce the vulnerability of a world-readable password file, many newer Unix systems use shadow password files. The traditional password file is maintained in /etc/passwd (as it contains more than just password information), but the actual encrypted passwords, along with expiration data, are kept in a file that can only be read or used by root (the Unix Administrator account). Processes which require access to the shadow password file must be owned by root or be granted root level permissions before access is obtained, which provides much greater security against password snooping.