Course 3 Week 3

Introduction to Windows Administration

User & Kernel Mode:-

File Systems - NTFS 1993
FAT 80s

Role-Based Access Control and Permissions.

Windows access control --> ACL's list. Permissions.

Privileged Accounts.

Privileged Accounts like Administrators of Window Services have direct or indirect access to most or all

assets in an IT organization.

→ Administrators will configure Windows to manage access control to provide security for multiple roles and users.

Principle of least Privileges.

↳ Giving a user account or process only those privileges which are essential to perform its intended function.

↳ Better system stability
↳ Better system security.
↳ Ease of Deployment.

Access Control:-

- Permissions
- Inheritance of permissions

→ ownership of objects — User rights
Object Auditi

Local User Accounts.

→ Local User Accounts are stored locally on the Windows workstation or server

Default Local User Acount.

- → Administrator account
- → Guest Acount
- → HelpAssistant account
- → Default Acount.

Default local system accounts.

- → SYSTEM
- → NETWORK SERVICE
- → LOCAL SERVICE.

Windows 10 Security App. (1703)

→ Virus & threat Protection

→ Account Protection
→ Firewall & network protection
→ App Browser control
→ Device security.
→ Device performance & Health
→ Family options.

Features of Active Directory

What is Active Directory.

Active Directory Domain Service (AD DS) store info about objects on the network and making this information easy for administrators and users to find and use.

↳ shared Resources, Servers, volumes, printers, network users,

Computer Accounts.

Active Directory Groups.

→ Security Groups are used to collect user accounts, computer accounts, and other groups into manageable units.

→ Server Administrators
→ Data Administrators.

Distribution Groups. → used to create email distribution lists.

Security Groups → used to assign permissions to shared resources.

Kerberos Authentication & logs.

↳ Is an authentication protocol used to verify the identity of a user or host.

The Kerberos Key Distribution Center

is integrated with other Windows
Server Security Service and uses
the domain Active Directory Domain
Service Database.

The key Benefits of Kerberos
include: Delegated Authentication,
Single sign on,
Interoperability, More efficient
authentication to servers.
Mutual Authentication.

Windows Server Logs.
Logging Server Logs.
Windows Event Logs.

Windows Auditing Overview.

Account Logon Events
Account Management.

Directory Servie Acces.

Audit Policy

1. Logon Events
2. Object Access
3. Policy Change
4. Privilege use
5. Process Tracking
6. System Events