Course 3 Week 3

Introduction to Windows Administration

User & Kernel Mode:-

File Systems. ⎰ NTFS 1443
⎱ FAT 80S

Role - Based Access Control and
Permissions.

Windows access control --> ALC's list.
Permission.

Privileged Accounts.
Privileged Accounts like Administrator
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 uses.

Principle of least Priviledges:

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

    ↳ Better System stability
    ↳ Better System Security.
    ↳ Ease of Deployment.

Access Control:-
- Permissions   - Inheritance of permissio

    - User rights an

→ Ownership of objects   → User rights an
                                Object Auditi

Local User Accounts.

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

Default Local User Account:
→ Administrator account
→ Guest Account
→ HelpAssistant account
→ Default Account.

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 Performane & Health
→ Family options.

Features of Active Directory

What is Active Directory.

Active Directory Domain Server

(AD DS) store info about objects on the network and makes this information easy for administrations 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.

→ Service Administration
→ 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 domains Active Directory Domain
Services Database.

The Key Benefits of KerbServer
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 Service Access.

Audit Policy

1.) Logon Events

2.) Object Access

3.) Policy Change

4.) Privilege Use

5.) Process Tracking

6.) System Events