CYBER LANCERS
The Frontline of Digital Security

Active Directory Domain Services (AD DS) Implementation Project

Problem Statement - HR & IT Department Focus

1. PROJECT OBJECTIVE

Primary Goal:
Design and deploy a functional Active Directory environment for a small organization with HR and IT departments that demonstrates:

- Centralized user authentication
- Department-based access control using security groups
- Group Policy enforcement for security basics
- File share permissions based on department roles
- Basic audit logging of important activities

2. SCOPE

What You'll Do:

Task	Description
Install AD DS + DNS	Set up Windows Server as Domain Controller for `corp.local`
Create OU Structure	Users (HR, IT), Computers (Workstations, Servers), Groups
Create Users & Groups	10-15 users split between HR and IT departments
Setup File Shares	HR Share, IT Share, Common Share with proper permissions
Create GPOs	Password policy, firewall, screen lock, drive mapping
Enable Auditing	Track failed logins, account lockouts, admin changes
Test & Document	Join client, verify access, capture screenshots

What You WON'T Do:

- Multiple domains or forests
- Certificate Authority or advanced features
- Complex delegation models
- Enterprise-scale monitoring
- Cloud/Azure integration

3. TECHNICAL REQUIREMENTS

3.1 AD Infrastructure Setup

Domain: corp.local
Domain Controller: Windows Server 2019/2022
Clients: Windows 10/11 (2-3 machines)
File Server: Same as DC or separate member server

3.2 OU Structure (Simple)

```
corp.local
├── Users
│   ├── HR (5-8 users)
│   └── IT (5-8 users)
├── Computers
│   ├── Workstations
│   └── Servers
└── Groups
```

3.3 Users to Create

HR Department:

- hr.manager (Manager)
- hr.staff.1 (Staff)
- hr.staff.2 (Staff)
- hr.service (Service Account - optional)

IT Department:

- it.admin (Administrator)
- it.sup

CYBER LANCERS

The Frontline of Digital Security