Active Directory Basics Lab Documentation

Platform: TryHackMe
Room: Active Directory Basics
Focus: Windows Active Directory fundamentals, user & system management, authentication

---

Lab Overview

This lab introduces **Active Directory (AD)**, a centralized system used to manage users, computers, and policies in enterprise environments. It demonstrates how organizations control access, enforce security, and manage infrastructure at scale.

Objectives

- Understand **Windows Domains & Domain Controllers**
- Learn **Active Directory structure (Users, Groups, OUs)**
- Perform **user & computer management**
- Apply **Group Policy Objects (GPOs)**
- Explore **authentication methods (Kerberos & NTLM)**
- Understand **Trees, Forests, and Trust relationships**

Key Concepts

1. Windows Domain & Domain Controller

- A **domain** centralizes authentication and resource management
- A **Domain Controller (DC)** runs Active Directory services
- Credentials are stored centrally in AD

This allows organizations to enforce **security policies across all machines**

---

2. Active Directory Structure

Active Directory is a **hierarchical database** that stores:

- Users
- Computers
- Groups
- Policies

It enables:

- Authentication (login validation)
- Authorization (access control)
- Centralized management

---

3. Organizational Units (OUs)

- Logical containers used to organize users and devices
- Used to apply policies and delegate control

✔ Example:

- Separate OUs for **Workstations vs Servers**

Hands-On Tasks

Task 1–2: Domain Fundamentals

- Identified:
    - Active Directory = credential storage
    - Domain Controller = AD service host

Task 3: AD Objects & Groups

- Key findings:
    - Admin group: **Domain Admins**
    - Machine accounts format: `COMPUTERNAME$`

    - OUs used for structured management

Task 4: Managing Users (Help Desk Simulation)

Performed:

- Logged in via **RDP**
- Reset user password using PowerShell:

Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password')

- Forced password reset on next login:

Set-ADUser -ChangePasswordAtLogon $true -Identity sophie

💡 Demonstrates real-world **help desk / IT support tasks**

Task 5: Managing Computers

- Organized devices into OUs:
    - Workstations
    - Servers

✔ Best practice: Separate OUs for better policy control

Task 6: Group Policy (GPO)

- GPOs used to enforce:
    - Security settings
    - Software installs
    - User restrictions
- Key share:
    - `SYSVOL` → distributes policies across domain

Task 7: Authentication Methods

Kerberos (Default)

- Uses:
    - TGT (Ticket Granting Ticket)
    - TGS (Service Tickets)

✔ Secure, no password sent over network

NTLM (Legacy)

- Uses challenge-response authentication
- Password hash never transmitted

Task 8: Trees, Forests, Trusts

- **Tree:** Domains sharing same namespace
- **Forest:** Multiple domain trees
- **Trust Relationship:** Allows cross-domain access

✔ Example:

- User in Domain A can access resources in Domain B

Key Security Insights

- Centralized authentication reduces attack surface
- Kerberos prevents password exposure
- GPOs enforce organization-wide security
- Delegation allows controlled privilege assignment

Real-World Relevance

This lab directly maps to:

- Help Desk (password resets, account management)
- System Administration (AD structure, GPOs)
- SOC / Security roles (authentication & access control)

Skills Demonstrated

- Active Directory navigation
- User & computer administration
- PowerShell command usage
- Authentication mechanisms
- Enterprise network structure understanding

Conclusion

This lab builds a strong foundation in **Active Directory**, which is a core technology used in almost every corporate IT environment. Mastery of these concepts is essential for **IT support, cybersecurity, and system administration roles**.