Active Directory Basics and Functionality

Introduction

This room introduces the basic concepts and functionality provided by Active Directory.

Task 2: Windows Domains

In a Windows domain, credentials are stored in a centralized repository called:
Answer: Active Directory

The server in charge of running the Active Directory services is called:
Answer: Domain Controller

What is AD?

Active Directory is a directory database/server that stores users' information such as usernames, phone numbers, emails, and many other credentials. The same network user's things can be managed from Active Directory, including privileges.

The server that runs the Active Directory services is known as a Domain Controller (DC).

A Windows domain helps centralize administration and overcomes limitations like manually creating users on individual computers. It allows for centralized management of security policies and other resources.

A Real-World Example

In schools or universities, you are usually provided with a username and password to log in to any computer on campus. This works because your credentials are validated by Active Directory, eliminating the need to store them on each machine. Policies applied through AD also control your access to features such as the Control Panel.

Task 3: Active Directory

Which group normally administrates all computers and resources in a domain?
Answer: Domain Admin

What would be the name of the machine account associated with a machine named TOM-PC?
Answer: TOM-PC$

What type of containers should we use to group all Quality Assurance users?
Answer: Organizational Unit

Core Components of Active Directory

1. Users: Represent employees or services with access to the network.
2. Machines: Every computer joining the domain has a machine account.
3. Security Groups: Used to assign access permissions over resources.
4. Organizational Units (OUs): Container objects used to group users and computers for policy application.

Delegation

Delegation allows administrators to grant specific privileges to users. For example, IT support staff can be given permission to reset passwords of lower-privilege users.

Task 4: Managing Users in AD

What was the flag found on Sophie's desktop?
Answer: THM{thanks_for_contacting_support}

Password Reset and Delegation

1. Use the RDP port to access the Phillip account.
2. Open a Command Prompt, switch to PowerShell, and reset Sophie's password.
   Command: Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password') -Verbose
3. Enforce password reset on login: Set-ADUser -ChangePasswordAtLogon $true -Identity sophie -Verbose.

Task 5: Managing Computers in AD

How many computers ended up in the Workstations OU?
Answer: 7

Is it recommendable to create separate OUs for Servers and Workstations?
Answer: yay

Task 6: Group Policies

What is the name of the network share used to distribute GPOs?
Answer: SYSVOL

Can a GPO be used to apply settings to users and computers?
Answer: yay

Task 7: Authentication Methods

Will a current version of Windows use NetNTLM by default?
Answer: nay

What ticket allows us to request further tickets in Kerberos?
Answer: Ticket Granting Ticket

Is a user's password transmitted over the network in NetNTLM?
Answer: nay

Task 8: Trees, Forests, and Trusts

What is a group of Windows domains with the same namespace called?
Answer: Tree

What should be configured between two domains to access each other's resources?
Answer: 2 trust relationship