Active Directory Lab – Cybersecurity Home Lab Project

# Overview

This lab focused on setting up an Active Directory Domain Services (AD DS) environment on Windows Server, joined a Windows client to the domain, and configured a Group Policy Object (GPO). The goal was to simulate enterprise domain infrastructure management and group-based policy enforcement.

# Objectives

* Install and configure Active Directory Domain Services (AD DS) and DNS on Windows Server.
* Create and configure a domain: luis.local.
* Troubleshoot and resolve DNS resolution issues between Ubuntu DNS and Windows clients.
* Successfully join a Windows 10 client to the luis.local domain.
* Create Organizational Units (OUs) and user accounts within Active Directory.
* Create and apply a Group Policy Object (GPO) to set a custom desktop background.

# Environment

* Domain Controller: Windows Server 2022 (win-dc.luis.local)
* DNS: Initially Ubuntu BIND9 (192.168.1.10), later replaced with Windows DNS (192.168.1.5)
* Client: Windows 10
* Network: Internal VirtualBox network with static IPs and gateway through Ubuntu Server

# Steps Taken

1. Installed Active Directory Domain Services (AD DS) and DNS roles on Windows Server.

2. Promoted the server to a Domain Controller with the domain name luis.local.

3. Identified and resolved DNS delegation, resolution, and SRV record issues.

4. Switched DNS responsibilities from BIND9 (Ubuntu) to Windows DNS for better AD integration.

5. Set DNS forwarding to Ubuntu and Google DNS for internet access.

6. Successfully joined a Windows 10 client to the domain.

7. Created users and Organizational Units (OUs): Cybersecurity, Accounting, and Admins.

8. Created a Group Policy Object to enforce a desktop background for the Cybersecurity OU.

9. Downloaded and imported updated ADMX templates to support policy configurations.

10. Verified GPO was applied correctly via Group Policy Result tools.

# Results

The Windows client successfully joined the luis.local domain, users were managed under their respective OUs, and the GPO was enforced on the Cybersecurity group, setting a custom desktop background. This demonstrates a full AD DS deployment with DNS integration, client domain join, and group policy application.

# Future Enhancements

* Configure login scripts and audit policies via GPO.
* Set up mapped drives for different OUs.
* Restrict USB access with Group Policies.
* Deploy software through Group Policy.
* Implement centralized logging and monitoring for AD events.