Active Directory Threat Detection Lab — Level 1 Workbook

LEVEL 1 — FOUNDATION: 'WHAT IS AD AND WHY DO WE CARE'

# 📘 Overview

Active Directory (AD) is Microsoft’s directory service that provides centralized authentication, authorization, and policy management for Windows networks. AD DS uses a hierarchical database (the “directory”) to store objects such as user and computer accounts, groups, and other resources. Each object has attributes (like name, password hash, group memberships) and is protected by Access Control Lists (ACLs).

AD integrates security via single sign-on: users sign in once and can access authorized resources across the domain using one set of credentials.

# 🔑 Key Concepts

**Domain, Forest, and OU:** *https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/understanding-active-directory-domain-services*

**DNS and SRV Records:** *https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/service-location-srv-records*

**Netlogon and SYSVOL:** *https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/netlogon-and-sysvol-share-not-created*

**Kerberos and NTLM Authentication:** *https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview*

**Group Policy (GPO):** *https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/group-policy-overview*

**Event ID Reference:** *https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-audit-events*

# ✅ Checklist

* ☐ Identify Domain and Forest names.
* ☐ Find all Domain Controllers and their roles (FSMO, Global Catalog).
* ☐ Verify DNS SRV record registration for LDAP.
* ☐ Access and review Netlogon and SYSVOL shares.
* ☐ List privileged groups and document members (Domain Admins, etc.).
* ☐ Find and document the structure of Organizational Units (OUs).
* ☐ Review Default Domain and Domain Controller policies.
* ☐ Verify Kerberos ticket issuance with `klist` and `whoami /all`.
* ☐ Document logon-related event IDs on a Domain Controller.

# 🧪 Exercises

Use PowerShell and built-in Windows tools to perform the following:

* 🔹 Use `nltest /dclist:<yourdomain>` to list DCs and record them.
* 🔹 Run `nslookup -type=SRV \_ldap.\_tcp.dc.\_msdcs.<yourdomain>` and interpret results.
* 🔹 Log in with a domain account, then run `klist` and `whoami /groups`.
* 🔹 Connect to `\\<DC>\NETLOGON` and `\\<DC>\SYSVOL` and list files.
* 🔹 Document the password policy using `net accounts` or GPMC.
* 🔹 Determine which DCs are Global Catalogs using `Get-ADDomainController`.
* 🔹 Research the differences between Kerberos and NTLM.
* 🔹 Generate a sample Event ID (4624) and locate it in Event Viewer.

# 📝 Documentation Prompts

Answer and record the following in your workbook or lab notebook:

* 🖊️ What is your domain and forest name?
* 🖊️ What are the hostnames and roles of your Domain Controllers?
* 🖊️ What are the key settings in your Default Domain Policy?
* 🖊️ What groups does your test user belong to?
* 🖊️ What files are present in NETLOGON and SYSVOL shares?
* 🖊️ Which DCs are Global Catalog servers and why?
* 🖊️ What is one main difference between Kerberos and NTLM?
* 🖊️ What event logs did you observe during your tests?