Active Directory 101
for CySec Pro & Red Teamers

OBJECTS:

- 00 – Active Directory (AD) - Simplified Overview
- 01 – Active Directory (AD) - Total breakdown
- 02 – Active Directory (AD) - Importance, Components & Pentester's Guide
- 03 – Authentications Methods: NTLM, Kerberos, OAuth, LDAP
- 04 – RBAC in Active Directory (AD) Domain Controllers (DC)
- 05 – Modern Technologies: PAM and Importance of usage

VulnCorp & CSC
Abbas Aghayev
In/aghayev2a
Update_may_19_2025_v1.2a

OBJECT 00 - Active Directory (AD) - Simplified Overview

1. What is Active Directory?

Active Directory (AD) is Microsoft's directory service that helps organizations manage users, computers, and other resources in a networked environment. It provides:

- Centralized authentication (who can log in?)
- Authorization (what can they access?)
- Policy enforcement (security rules, configurations)

It's like a phonebook for a company's IT infrastructure, storing details about users, groups, computers, and permissions.

2. Why Do Companies Use Active Directory?

✅ Single Sign-On (SSO) – Users log in once to access multiple services.
✅ Centralized User Management – Admins control all accounts from one place.
✅ Security Policies (GPOs) – Enforce password rules, firewall settings, etc.
✅ Scalability – Supports thousands of users and devices.
✅ Integration with Microsoft Products – Works seamlessly with Windows, Office 365, Exchange, etc.

Example: When an employee logs into their workstation, AD checks their credentials and determines what files, servers, or apps they can access.

3. Key Components of Active Directory

Component	Description
Domain (e.g., `corp.local`)	A logical group of users, computers, and resources under the same security policies.
Domain Controller (DC)	The server that runs AD and authenticates users.
Active Directory Database (`NTDS.dit`)	Stores all user passwords (hashed), group memberships, and permissions.
Organizational Units (OUs)	Folders to organize users, groups, and computers (e.g., `HR`, `Finance`).
Group Policy Objects (GPOs)	Rules applied to users/computers (e.g., "Force password changes every 30 days").
Kerberos	Default authentication protocol (replaces insecure NTLM).
LDAP (Lightweight Directory Access Protocol)	Used to query and modify AD data (e.g., "Find all users in the Sales group").
Trusts	Allows users from one domain to access resources in another.

4. What is a Domain Controller (DC)?

- The "brain" of Active Directory – authenticates users and enforces security policies.
- Stores the AD database (`NTDS.dit`) – contains password hashes, group memberships, etc.
- Uses Kerberos for authentication (more secure than NTLM).
- Multi-DC environments – Companies often have backup DCs for redundancy.

Why is the DC a Prime Target for Hackers?

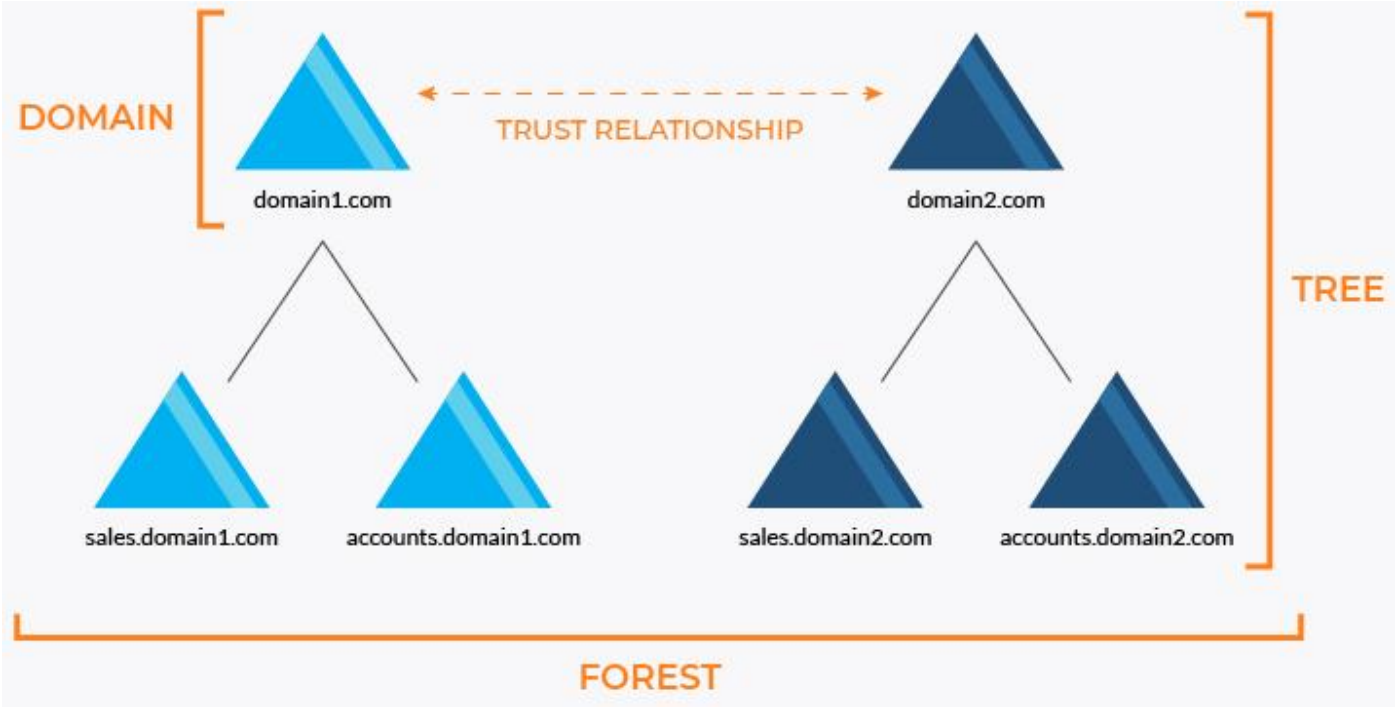
- If compromised, attackers can:
  - Steal all user passwords (DCSync attack).
  - Create fake admin accounts (Golden Ticket attack).
  - Control the entire network.

Summary

- AD = Microsoft's user & resource management system.
- Used by companies for centralized security & access control.
- Domain Controllers (DCs) are critical servers that run AD.
- Major components: Domains, OUs, GPOs, Kerberos, LDAP.

OBJECT 01 - Active Directory (AD) is structured in a hierarchical model—like a company's org chart. Here's the breakdown:

https://learn.microsoft.com/en-us/entra/identity/domain-services/concepts-forest-trust



1. Domain	2. Tree	3. Forest
- The core unit of AD (e.g., `corp.local`). - Contains users, computers, groups, and policies. Key Features: ✓ Single security boundary (authentication happens here). ✓ Uses a Domain Controller (DC) to manage it. ✓ Stores data in `NTDS.dit` (password hashes, Kerberos keys). Attack Relevance: • Compromising one domain doesn't automatically compromise others (unless trusts exist). • Golden Ticket attacks forge Kerberos tickets for domain persistence.	- A collection of domains sharing a contiguous namespace. - Example: - Root: `corp.local` - Child: `us.corp.local` - Child: `eu.corp.local` Key Features: ✓ Automatic two-way trust between parent/child domains. ✓ Uses Kerberos transitive trusts. Attack Relevance: - If you compromise the root domain, you can exploit trusts to access child domains (cross-domain attacks).	- The highest-level container in AD. - Contains one or more domain trees with a shared: - Global Catalog (searchable directory of all objects). - Schema (rules for object types). Example: - Forest: `corp.com` - Tree 1: `corp.com` → `us.corp.com` - Tree 2: `devops.net` → `cloud.devops.net` Key Features: ✓ Security boundary (compromising the forest = full control). ✓ Enterprise Admins group has forest-wide privileges. Attack Relevance: - Forest Trusts can be abused for lateral movement. - Privilege Escalation Path: - Compromise a child domain → Exploit trust → Attack the forest root.

4. Trusts (How Domains/Forests Communicate)

Trust Type	Description	Attack Potential
Transitive Trust	Automatically flows across domains in a forest.	Golden Ticket attacks can cross trusts.
Non-Transitive Trust	Manually configured, limited scope.	Harder to exploit (but not impossible).
Forest Trust	Links two separate forests.	If misconfigured, can lead to forest compromise.
External Trust	Connects to non-AD domains (e.g., MIT Kerberos).	Risk of trust poisoning.

Real-World Attack Example:

1. Hacker compromises `dev.corp.com`.
2. Exploits transitive trust to attack `corp.com`.
3. Uses DCSync to dump hashes from the root domain.

5. Organizational Units (OUs) vs. Domains

Ous	**Domains**
Used for grouping objects (users, computers).	Security boundary (authentication).
No separate security policies (inherits from domain).	Has its own password policies, admins.
Example: `OU=Finance, DC=corp, DC=local`	Example: `corp.local`

Why It Matters for Pentesters:
- GPOs are applied at OU level → Misconfigurations = privilege escalation.
- OUs help map the AD structure for targeted attacks.

6. Attack Paths in AD Hierarchy
1. Initial Access → Compromise a low-priv user/workstation.
2. Enumeration → Map trusts with `nltest /domain_trusts` or BloodHound.
3. Lateral Movement → Exploit trusts to jump domains.
4. Privilege Escalation → Target Enterprise Admins in the forest root.

Tools to Exploit AD Structure:
- BloodHound → Visualizes attack paths.
- Mimikatz → Dumps hashes, forges tickets.
- PowerView → Maps trusts, OUs, and groups.

Final Thoughts
- Domains = Security boundaries.
- Trees = Group of domains with shared naming.
- Forests = The ultimate AD container (Enterprise Admins rule here).
- Trusts = Can be abused for cross-domain attacks.

For Hackers: AD's hierarchy is a goldmine for privilege escalation.
For Defenders: Monitor trusts, Enterprise Admins, and cross-domain logins.

OBJECT 02 - Active Directory (AD) - Importance, Components & Pentester's Guide

1. Key Components of Active Directory:

Component	Description	Why It Matters
Domain Controller (DC)	Server that authenticates users and enforces security policies	Compromising a DC = Full domain takeover.
Active Directory Database (NTDS.dit)	Stores all user credentials, hashes, and group memberships.	Attackers target this for credential theft (DCSync attack).
Kerberos Authentication	Default authentication protocol (replaces NTLM).	Golden/Silver Ticket attacks exploit Kerberos.
LDAP (Lightweight Directory Access Protocol)	Used to query/modify AD objects (users, groups, etc.).	LDAP injection & insecure binds can leak data.
Group Policy Objects (GPOs)	Policies applied to users/computers (password rules, firewall settings).	Misconfigured GPOs can lead to privilege escalation.
Organizational Units (OUs)	Containers for organizing users, groups, and computers.	Helps in lateral movement by mapping the AD structure.
Trusts	Defines relationships between domains/forests.	Attackers abuse trusts for cross-domain attacks.

2. What a Pentester Must Know About Active Directory

A. Enumeration & Reconnaissance

- Tools:
  - `PowerView` (PowerShell)
  - `BloodHound` (visualizes attack paths)
  - `ldapsearch` (LDAP queries)
- Key Commands:

powershell
Get-NetUser -Domain <domain> List all users
Get-NetGroup -Domain <domain> List all groups
Get-NetComputer -Domain <domain> List all machines

B. Common Attack Vectors

Attack	Description	Impact
Kerberoasting	Stealing service account hashes (TGS tickets)	Privilege escalation.
AS-REP Roasting	Exploiting users with "Do not require Kerberos pre-auth".	Password cracking.
DCSync Attack	Mimicking a DC to extract password hashes.	Domain admin compromise.
Pass-the-Hash (PtH)	Using NTLM hashes to authenticate without plaintext passwords	Lateral movement.
Golden Ticket Attack	Forging Kerberos TGT tickets with KRBTGT hash	Persistent admin access.
GPO Abuse	Modifying GPOs to execute malicious scripts	Mass compromise.

C. Post-Exploitation & Lateral Movement

- Techniques:
  - Overpass-the-Hash (Convert hashes to Kerberos tickets)
  - Pass-the-Ticket (Use stolen Kerberos tickets)
  - RDP Hijacking (Stealing sessions)
  - Tools: `Mimikatz` (Credential dumping), `CrackMapExec` (Automates lateral movement) , `Impacket` (Python-based AD exploitation)

D. Defensive Evasion

- Avoiding Detection With: Clearing Windows Event Logs, LOLBAS (Using built-in tools like `PsExec`, `WMI`) , Kerberos Delegation Abuse (Stealth Op)

E. Privilege Escalation Paths

1. From Low-Priv User → Domain Admin
   - Find users in privileged groups (`Domain Admins`, `Enterprise Admins`).
   - Exploit misconfigured service accounts.
   - Abuse ACLs (Access Control Lists) on AD objects.

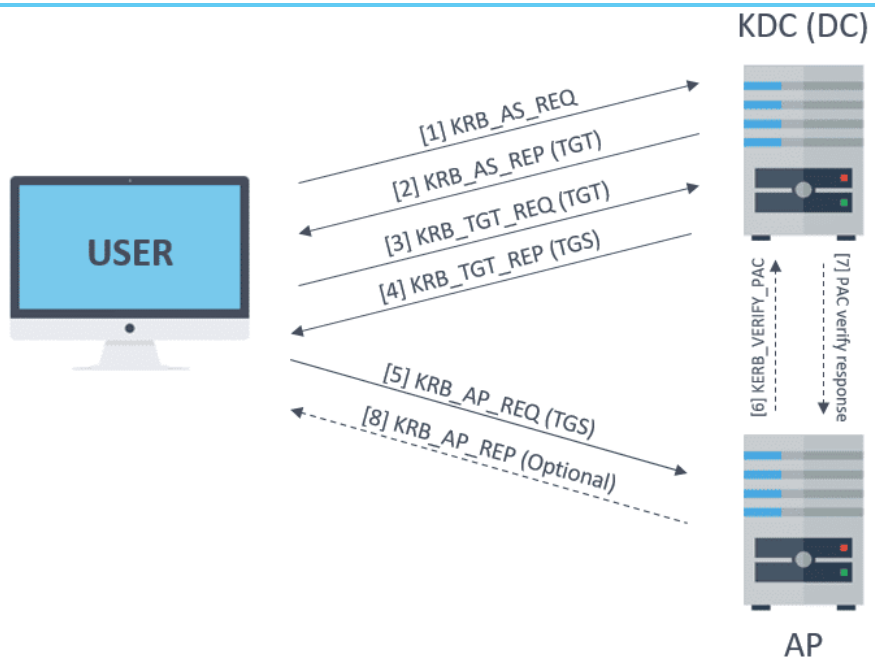
2. BloodHound Analysis
   - Shows shortest path to Domain Admin via graph-based attacks.

Final Thoughts for Pentesters

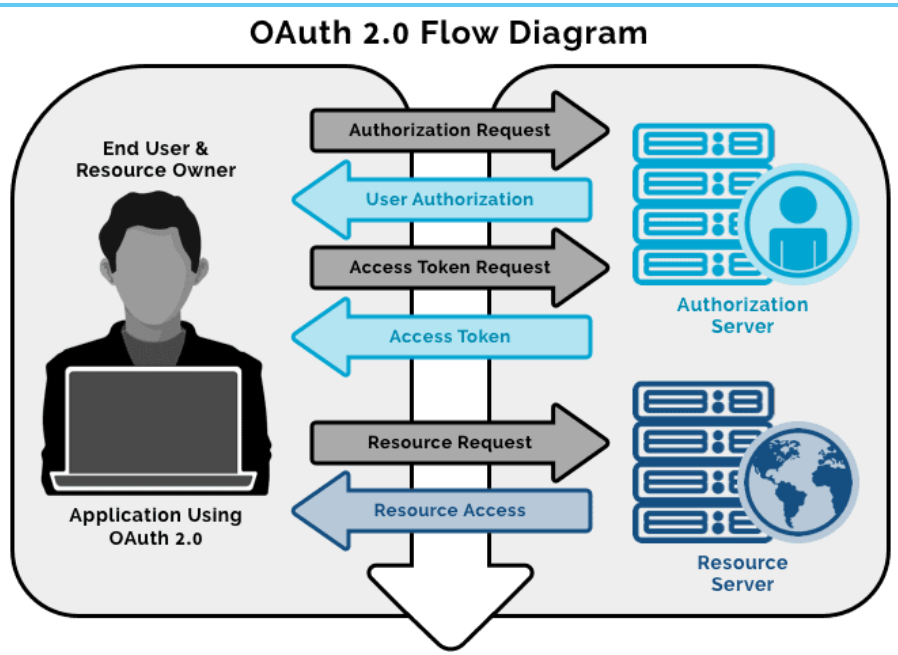
- AD is the crown jewel in most corporate networks.
- Most breaches happen due to misconfigurations, not zero-days.
- Learn BloodHound & Mimikatz—they are essential for AD pentesting.

OBJECT 03 – Authentications

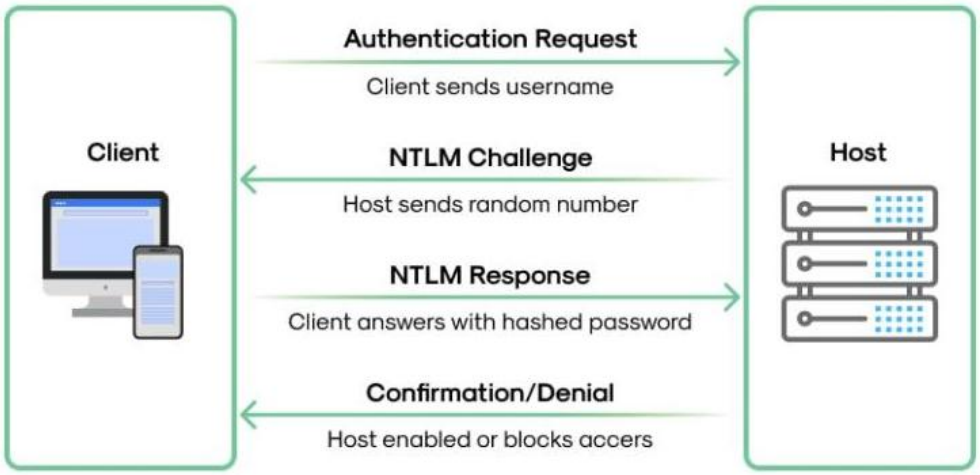
This is how Kerberos works



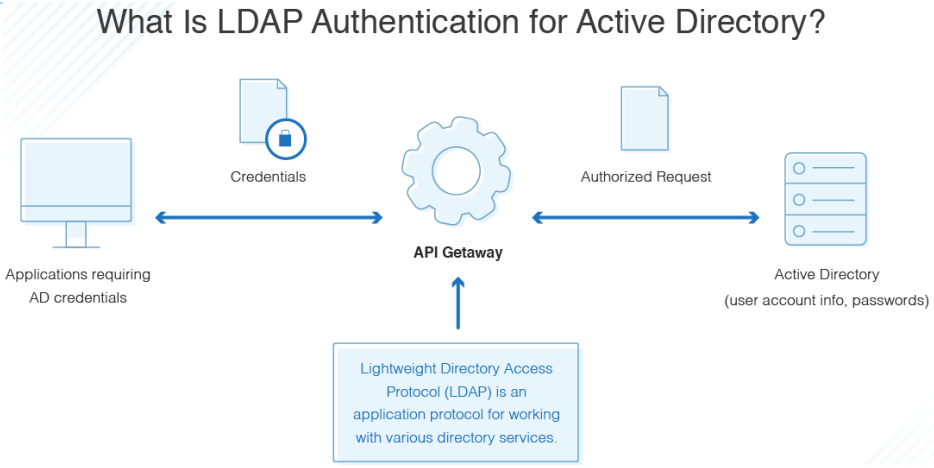
This is how OAuth works



This is how NTLM Works



This is how LDAP works



VulnCorp & CSC
Abbas Aghayev
In/aghayev2a
Update_may_19_2025_v1.2a

Here's a breakdown of the key differences between Kerberos, NTLM, OAuth, and LDAP:

Feature	Kerberos	NTLM	OAuth	LDAP
Purpose	Authentication protocol (uses tickets)	Authentication protocol (challenge-response)	Authorization framework (delegated access)	Directory access protocol (query & manage users/groups)
Protocol Type	Network authentication (ticket-based)	Microsoft's old authentication (obsolete)	Token-based authorization (for APIs/web)	Directory services protocol (hierarchical data)
Security	Strong (mutual auth, encryption)	Weak (vulnerable to attacks like Pass-the-Hash)	Depends on implementation (OAuth 2.0 + PKCE recommended)	No built-in security (relies on TLS/SASL)
Usage	Enterprise networks (Active Directory)	Legacy Windows systems	Modern web apps (Google, Facebook logins)	User/group management (Active Directory, OpenLDAP)
Mechanism	Uses symmetric-key cryptography (TGT & service tickets)	Challenge-response (NTLM hash)	Tokens (Access Token, Refresh Token)	Queries (Bind, Search, Modify operations)
Delegation	Supports delegation (constrained/unconstrained)	No delegation	Supports delegated access (scoped permissions)	Not applicable
Standard	RFC 4120	Microsoft proprietary	RFC 6749 (OAuth 2.0)	RFC 4511 (LDAPv3)

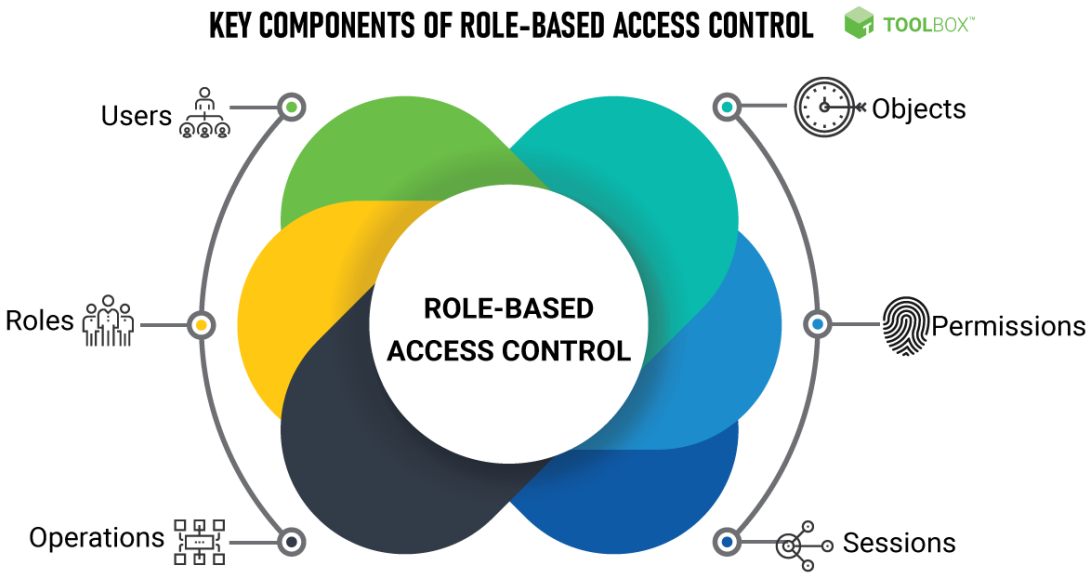
Key Differences:

1. Kerberos vs NTLM
   - Kerberos is more secure, uses tickets, and is the default in modern Active Directory.
   - NTLM is older, less secure, and used only for backward compatibility.
2. Kerberos vs OAuth
   - Kerberos is for authentication (proving identity).
   - OAuth is for authorization (granting access to resources).
3. LDAP vs Kerberos/NTLM/OAuth
   - LDAP is not an authentication protocol but a way to query directories (like Active Directory).
   - Kerberos/NTLM can use LDAP to fetch user details.
4. OAuth vs Others
   - OAuth is mainly for web/API access (e.g., "Login with Google").
   - Kerberos/NTLM are for internal network authentication.

When to Use Which?

- Kerberos → Best for enterprise networks (Windows AD, Linux via MIT Kerberos).
- NTLM → Avoid (only for legacy systems).
- OAuth → Modern web/mobile apps (SSO, API access).
- LDAP → Managing user directories (often paired with Kerberos for auth).

OBJECT 04 - Role-Based Access Control (RBAC) in Active Directory (AD) Domain Controllers (DC)



RBAC (Role-Based Access Control) is a security model used in Active Directory (AD) to manage permissions based on user roles rather than individual accounts. It simplifies administration by assigning privileges to groups (roles) rather than individual users.

1. How RBAC Works in Active Directory
- Instead of assigning permissions to each user, admins define roles (like "HR Manager," "Helpdesk," "Finance Auditor").
- Users are added to security groups, and permissions are granted to these groups.
- Example:
  - Role: "Helpdesk Technician"
  - Permissions: Reset passwords, unlock accounts
  - Assigned via: AD Security Group (`Helpdesk_Group`)

2. Key Components of RBAC in AD

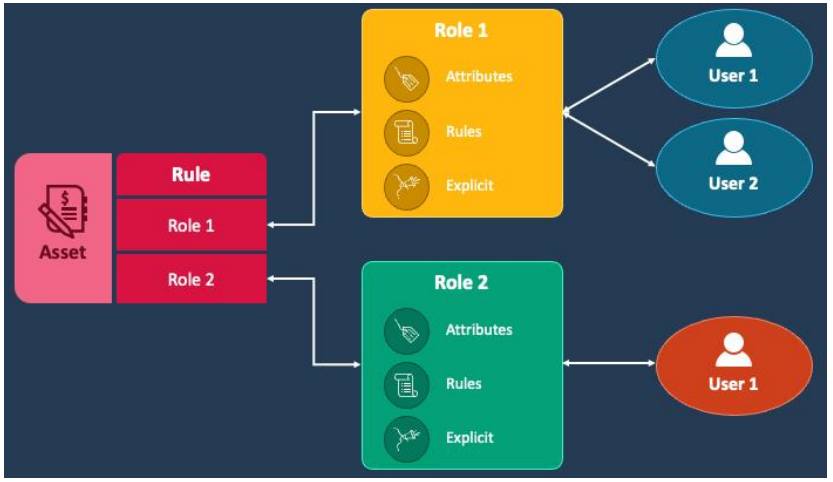
Component	Description	Example
Security Groups	Groups that define roles (e.g., `Finance_Team`, `Admins`).	`Helpdesk_Group` can reset passwords.
Permissions (ACLs)	Access rights assigned to groups (e.g., "Modify user objects").	`HR_Group` can edit employee details.
Organizational Units (OUs)	Containers for applying role-based policies.	`OU=Finance` has special GPOs.
Group Policy Objects (GPOs)	Enforce role-specific settings (e.g., "Finance users get encrypted drives").	`GPO_Finance_Secure` applies BitLocker.

3. Benefits of RBAC in AD

- ✅ Simplified Management – Admins manage groups, not individual users.
- ✅ Least Privilege – Users get only the access they need.
- ✅ Auditability – Easier to track who has what permissions.
- ✅ Security – Reduces risk of excessive privileges.

4. Common RBAC Roles in AD

Role	*Permissions*	*Security Group Examples*
Domain Admin	Full control over AD.	`Domain Admins`
Helpdesk	Reset passwords, manage workstations.	`Helpdesk_Team`
HR Manager	Modify employee records.	`HR_Managers`
Auditor	Read-only access to logs.	`Auditors_Group`



5. How Attackers Exploit Weak RBAC

- Privilege Escalation: If a low-priv user is added to `Domain Admins`, attackers gain full control.
- Group Spoofing: If a compromised account is in `Enterprise Admins`, attackers can take over the forest.
- Permission Misconfigurations: Overly permissive groups lead to lateral movement.

Example Attack:

1. Attacker compromises a `Helpdesk_Group` member.
2. Exploits password reset privileges to hijack an admin account.
3. Moves laterally to Domain Controller via `DCSync`.

Final Thoughts

- RBAC in AD = Assign permissions to groups, not users.
- Critical for security & compliance (e.g., SOX, HIPAA).
- Weak RBAC = Easy path for attackers to escalate privileges.

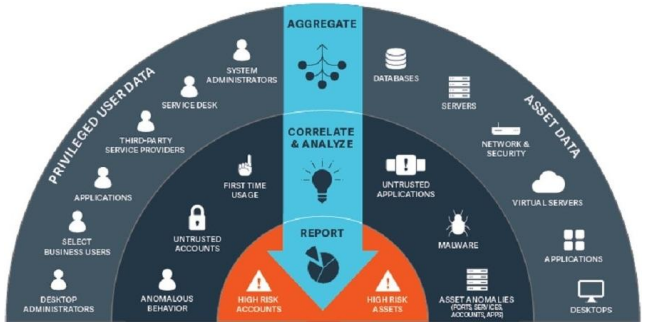
6. Practices for RBAC in AD
- Follow Least Privilege – Only grant necessary permissions.
- Use Nested Groups – Example: `Helpdesk_Group` → `IT_Staff` → `All_Employees`.
- Regularly Audit Group Membership – Remove stale accounts.
- Disable Legacy Protocols (NTLM) – Enforce Kerberos for role-based auth.
- Monitor Sensitive Groups (e.g., `Domain Admins`, `Enterprise Admins`).

If you have eyes to see, if you have minds to go through, if you have mouth for silent then thank me later.

VulnCorp & CSC
Abbas Aghayev
In/aghayev2a
Update_may_19_2025_v1.2a

OBJECT 05 - Privileged Access Management (PAM) in Active Directory

(And why it's critical for security!)



PAM (**Privileged Access Management**) is a security framework that controls, monitors, and secures access to privileged accounts (like **Domain Admins, Service Accounts, and Local Admins**) in AD and other systems:

1. Why PAM Matters in AD

- Privileged accounts = 1 target for attackers (e.g., `**Domain Admins**`, `**Enterprise Admins**`).
- A single compromised admin account can lead to full domain takeover.
- PAM enforces Zero Trust principles:
  - **Just-In-Time (JIT) Access** – Admins get temporary privileges, not permanent.
  - **Least Privilege** – Limits unnecessary access.
  - **Audit & Monitoring** – Tracks who used what and when.

2. Key PAM Concepts in Active Directory

A. Privileged Accounts in AD

Account Type	Risk if Compromised
Domain Admins	Full control over AD (disaster!).
Enterprise Admins	Control over the entire forest.
Service Accounts	Often have excessive permissions
Local Admins	Can escalate to Domain Admin in misconfigured environments.

B. PAM Strategies for AD

1. Separate Privileged & Non-Privileged Accounts
   - Admins should have two accounts:
     - Regular account (for email, browsing).
     - Admin account (only used for elevated tasks).

2. Password Vaulting
   - Store privileged passwords in a secure vault (e.g., CyberArk, Thycotic).
   - Rotate passwords automatically.

3. Just-In-Time (JIT) Access
   - Admins request temporary access (approved via workflow).
   - Example: Microsoft PIM (Privileged Identity Management).

4. Session Monitoring & Recording
   - Log all actions taken by admins (e.g., Microsoft LAPS for local admin passwords).

VulnCorp & CSC
Abbas Aghayev
In/aghayev2a
Update_may_19_2025_v1.2a

5. Multi-Factor Authentication (MFA) Enforcement
   - Require MFA for all privileged logins.

3. Microsoft's PAM Solutions for AD

A. Microsoft LAPS (Local Administrator Password Solution)
- Randomizes & manages local admin passwords on workstations.
- Prevents Pass-the-Hash attacks.

B. Azure AD Privileged Identity Management (PIM)
- Provides temporary role activation (e.g., "Become Domain Admin for 1 hour").
- Requires approval & MFA.

C. Microsoft Defender for Identity
- Detects malicious privilege escalation (e.g., Golden Ticket attacks).

4. How Attackers Bypass Weak PAM

- Pass-the-Hash (PtH) – Steals hashes from admin accounts.
- Golden Ticket – Forges Kerberos tickets for persistent access.
- DCSync Attack – Mimics a DC to dump all passwords.
- Kerberoasting – Cracks service account passwords.

Example Attack Flow:
Hacker phishes a low-priv user → Gets local admin → Dumps LSASS → Steals Domain Admin hash → Owns the domain.

Final Thoughts
- PAM = Locking down the "keys to the kingdom" (privileged accounts).
- Without PAM, AD is a hacker's playground.
- Tools like CyberArk, Thycotic, and Microsoft PIM help enforce PAM.

*Microsoft LAPS **(Local Administrator Password Solution)***
*Microsoft PIM **(Privileged Identity Management)** (Azure AD & Hybrid AD)*