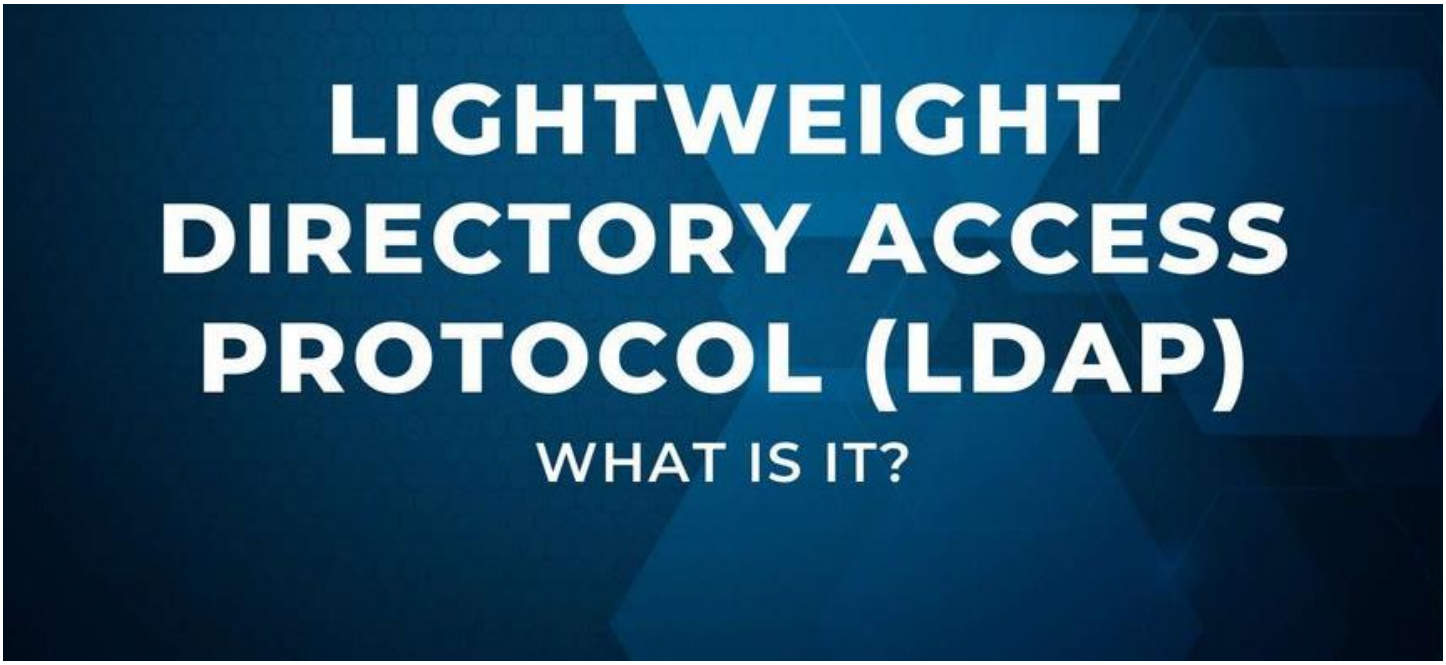

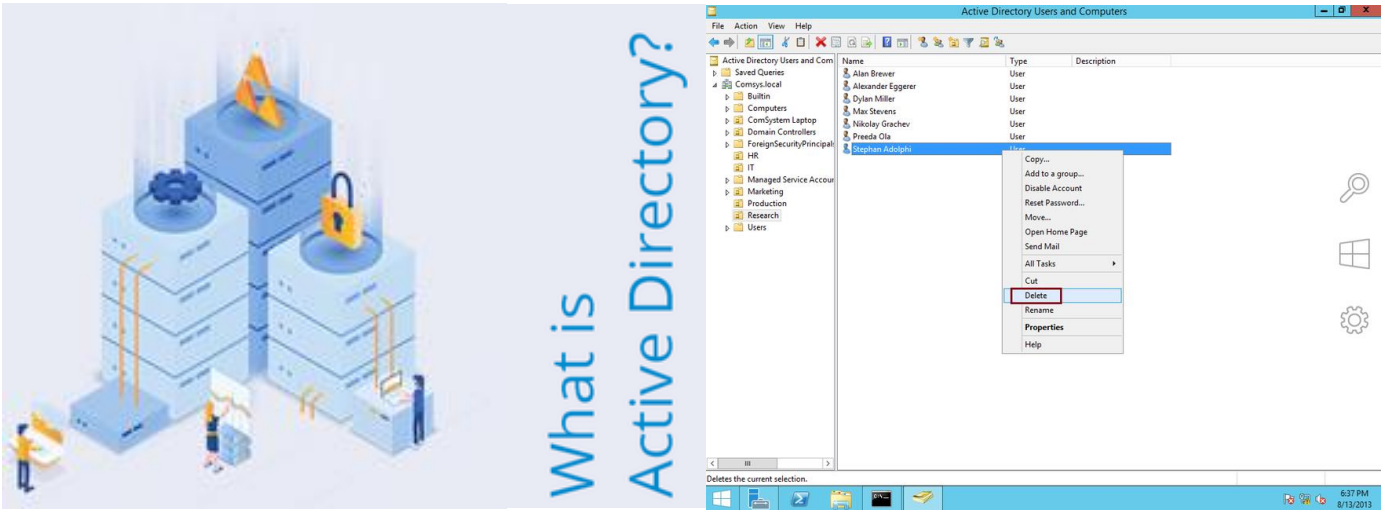

LDAP (Lightweight Directory Access Protocol)

EMRR Ekanayaka 11/2/25

Table of Contents

LDAP (Lightweight Directory Access Protocol)

This is an open, vendor-neutral protocol used to access and manage directory information services over a network. It's commonly used for storing and retrieving data such as user accounts, passwords, and permissions in centralized directories.

🔑 Key Features of LDAP: -

1. Centralized Authentication
    1. Manages user credentials in one place (e.g., Active Directory)
    2. Supports Single Sign-On (SSO) systems.

2. Hierarchical Structure

    Data is organized like a tree, called the Directory Information Tree (DIT).

```
dc=company,dc=com
├── ou=users
│   ├── cn=John Doe
│   └── cn=Jane Smith
└── ou=groups
    └── cn=Admins
```

3. Platform-Independent: - Works on Linux, Windows, and other systems.

4. Common Protocol: - Used with Active Directory, OpenLDAP, etc.

⚙️ How LDAP Works: -

1. Client-Server Model

    Clients send requests (like login attempts) to the LDAP server.

2. LDAP Server

    Stores data (users, groups, etc.) and responds to client queries.

3. Operations

    Bind: Authenticate users.

    Search: Look up data in the directory.

    Modify: Add, delete, or update data.

LDAP in Security: -

Used in penetration testing to

- Enumerate users/groups.
- Bypass weak authentication mechanisms.
- Exploit misconfigurations.

Ports: -

- ✓ Port 389 = LDAP (unencrypted or with STARTTLS)
- ✓ Port 636 = LDAPS (secure communication)

For penetration testing, you can use tools like Nmap to detect LDAP services:

```
nmap -p 389,636 -sV <target-ip>
```

Centralized Authentication (CA) Explained: -

Centralized Authentication is a method where all user credentials (like usernames and passwords) are stored and managed in one central location. This makes it easier to control access, manage users, and improve security across an organization.

✅ Key Benefits: -

1. Single Point of Management

   Admins can create, modify, or delete user accounts from one place.

Example: When an employee leaves, disabling their account centrally cuts off all access.

2. Single Sign-On (SSO)

   Users log in once and gain access to multiple systems without re-entering credentials.

3. Stronger Security Controls

   Centralized policies for password complexity, multi-factor authentication (MFA), etc.

4. Audit and Monitoring

   Easy to track login activities and detect suspicious behavior.

📁 Example Systems Using CA: -

1. Active Directory (AD): Uses LDAP for directory services and Kerberos for authentication.
2. FreeIPA (Linux environments): Combines LDAP, Kerberos, and other services.
3. RADIUS: Common in network authentication, especially Wi-Fi.

🔐 LDAP + Active Directory: -

When you log into your company's email, intranet, or internal apps

- Your credentials are sent to the Active Directory (AD) server over LDAP (port 389) or LDAPS (port 636).
- AD checks your credentials.
- If valid, it authenticates you, granting access to multiple resources without re-login (SSO).

📁 Active Directory (AD): -

Active Directory (AD) is a Microsoft-developed directory service used for managing users, computers, and resources in a network. It handles authentication, authorization, and access control, making it essential for enterprise environments.

🚀 Core Functions of Active Directory: -

1. Authentication

   Authentication is the process of verifying that a user, application or other identity is who they claim to be, for example, by checking their user ID and password.

   ✓ Verifies user credentials when logging into systems.
   ✓ Uses protocols like LDAP (port 389 - unsecure, port 636 - secure) and Kerberos (port 88).

2. Authorization

   Authorization is the process of determining whether the identity has the proper permissions to access the service or resource that it has requested.

   ✓ Determines what resources a user can access after authentication.
   ✓ Example: Read-only access to files vs. admin privileges.

3. Resource Management
   ✓ Centralized control over user accounts, computers, printers, servers, etc.
   ✓ Simplifies tasks like adding new users or deploying security policies.

Active Directory Structure: -

1. Domain
    - ✓ A collection of objects (users, computers, etc.) sharing the same AD database.
    - ✓ Example: company.local

A domain is a collection of AD objects, such as users, computers, groups and Organizational Units, that are stored in a shared database. An Active Directory domain is a management boundary, which means the objects in it can be managed together.

2. Organizational Units (OUs)
    - ✓ Subdivisions within domains to organize objects (like folders).
    - ✓ Example: OU=IT, OU=HR

An AD domain can be further organized into organizational units. Administrators often use OUs to group users, computers and users into units that mirror the organization's structure to easily apply relevant policies to each group.

3. Forest
    - ✓ The top-level container holding one or more domains.
    - ✓ Represents the entire AD environment.

A forest is a set of one or more domains. Many organizations have a single forest, but organizations with multiple divisions, service providers, and companies in the process of a merger or acquisition often have multiple forests.

4. Tree
    - ✓ A collection of domains connected in a hierarchical structure within a forest.

5. Group Policy Objects (GPOs)
    - ✓ Rules and settings applied to users and computers (like password policies, desktop restrictions).

Protocols Used in AD: -

1. LDAP (Port 389/636): For querying and modifying directory data.
2. Kerberos (Port 88): For secure authentication.
3. DNS (Port 53): AD relies heavily on DNS for name resolution.
4. SMB (Port 445): For file sharing and domain-related communication.

🎯 Active Directory in Penetration Testing: -

1. Enumeration

Identify domain users, groups, computers, and trust relationships using tools like ldapsearch, enum4linux, or BloodHound.

2. Privilege Escalation

Exploit weak configurations, like misconfigured permissions or outdated software.

3. Pass-the-Hash & Kerberoasting

Steal hashed credentials or service tickets to gain unauthorized access.

ldapsearch -x -h <AD_IP> -b "dc=company,dc=com"

🔐 Active Directory (AD) Authentication Methods: -

Active Directory supports multiple authentication protocols to verify user identities. The most common methods are Kerberos, NTLM, and LDAP Bind.\

🚀 **1. Kerberos Authentication (Default Method)**

Kerberos is the default and most secure authentication protocol in Active Directory. It uses tickets to allow secure, password-less access after the initial login.

🔗 How Kerberos Works: -

1. User Login:

The user enters their username and password

2. AS-REQ (Authentication Service Request)

The client sends a request to the Key Distribution Center (KDC) (usually the Domain Controller).

3. AS-REP (Authentication Service Reply)

   The KDC responds with a Ticket-Granting Ticket (TGT) encrypted with the user's password hash.

4. TGS-REQ (Ticket-Granting Service Request)

   The client uses the TGT to request access to specific services.

5. TGS-REP

   The KDC issues a Service Ticket.

6. Access Granted

   The client presents the Service Ticket to the target service (like a file server) for access.

Kerberos Authentication Command (Linux):

kinit username@DOMAIN.COM

Then verify the ticket:

klist

🚪 2. NTLM (NT LAN Manager) Authentication

NTLM is an older, less secure protocol but still used in legacy systems. It relies on hash-based authentication and is vulnerable to attacks like Pass-the-Hash.

🔗 How NTLM Works:

1. User Login

The client sends the username to the server.

2. Challenge

The server responds with a random challenge.

3. Response

The client encrypts the challenge with the user's password hash and sends it back.

4. Validation

The server validates the response by comparing it with its own calculation.

⚡ NTLM Authentication Test (Linux): -

Using smbclient:

smbclient //192.168.1.10/share -U username

Or enumerate users via NTLM with enum4linux →

enum4linux -u username -p password <target-ip>

🌐 3. LDAP Bind Authentication

LDAP can authenticate users in AD using two methods:

1. Simple Bind

   Sends credentials in plain text (use with SSL/TLS on port 636).

2. SASL Bind

   Uses Kerberos or NTLM for more secure authentication.

⚡ LDAP Simple Bind Example

ldapsearch -x -H ldap://192.168.1.10 -D "cn=admin,dc=example,dc=com" -w password -b "dc=example,dc=com"

🛡️ Which Method to Use?

✅ Kerberos: Preferred for secure environments.

⚠️ NTLM: Avoid unless needed for legacy systems.

🔐 LDAP Bind: Use with SSL/TLS for directory queries.

Refer →

1. LDAP - https://www.youtube.com/watch?v=SK8Yw-CiRHk
2. Active Directory
    - https://www.youtube.com/watch?v=mH48U0PlLKI&pp=ygUXaG93IEFEIHdvcmtzIGluIHdpbmRvd3M%3D
    - https://www.youtube.com/watch?v=GfqsFtmJQg0
    - https://www.youtube.com/watch?v=OfXJlmuoc20&pp=ygUQQWN0aXZlIERpcmVjdG9yeQ%3D%3D
    - https://www.youtube.com/watch?v=Yb__4XttW7g&pp=ygUXaG93IEFEIHdvcmtzIGluIHdpbmRvd3M%3D
3. Kerberos - https://www.youtube.com/watch?v=1yWW7VQUX0A
4. Blogs - https://blog.netwrix.com/active-directory-basics/