Lab 3: Perform LDAP Enumeration

Lab Scenario

As a professional ethical hacker or penetration tester, the next step after SNMP enumeration is to perform LDAP enumeration to access directory listings within Active Directory or other directory services. Directory services provide hierarchically and logically structured information about the components of a network, from lists of printers to corporate email directories. In this sense, they are similar to a company's org chart.

LDAP enumeration allows you to gather information about usernames, addresses, departmental details, server names, etc.

Lab Objectives

- Perform LDAP enumeration using Active Directory Explorer (AD Explorer)

Overview of LDAP Enumeration

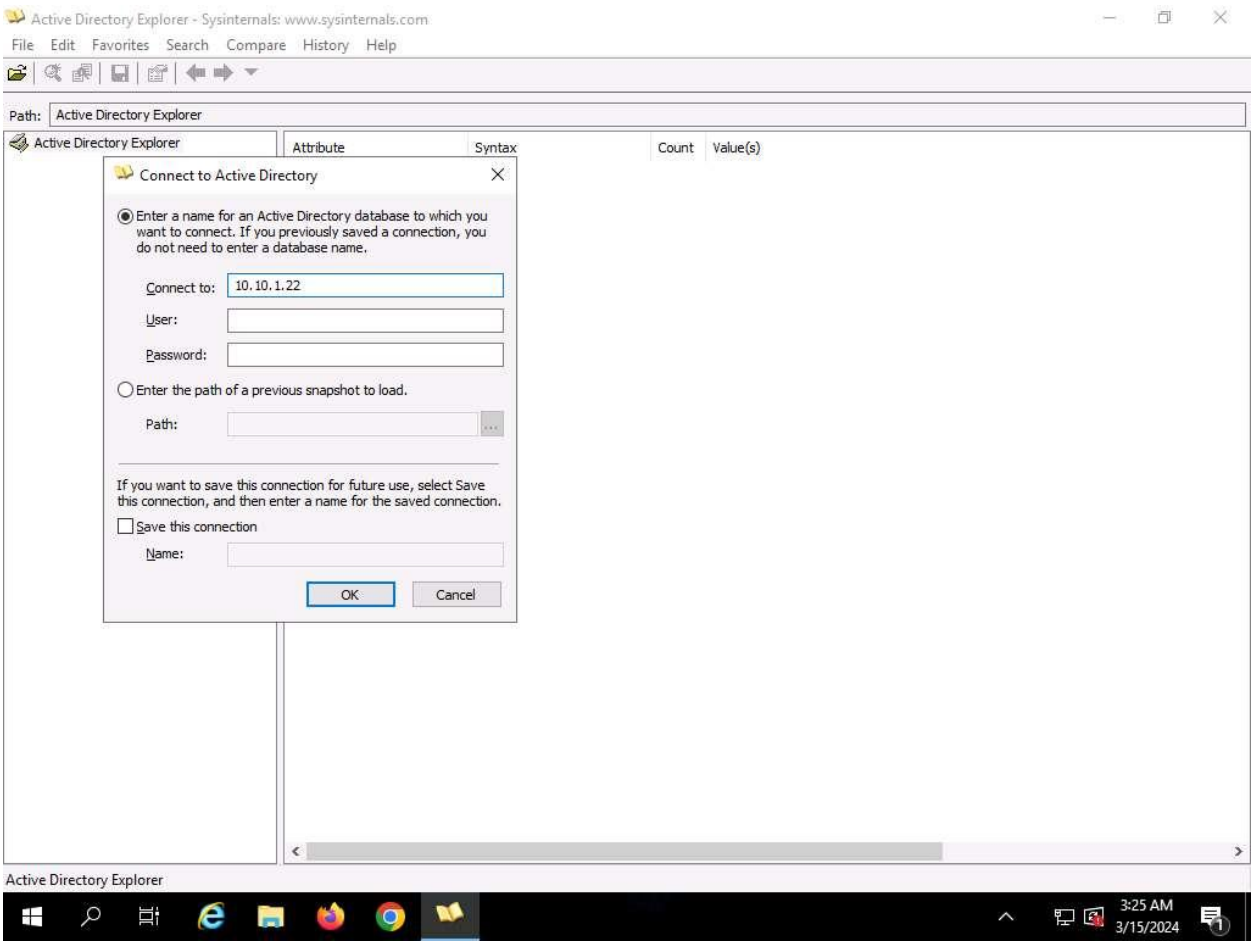
LDAP (Lightweight Directory Access Protocol) is an Internet protocol for accessing distributed directory services over a network. LDAP uses DNS (Domain Name System) for quick lookups and fast resolution of queries. A client starts an LDAP session by connecting to a DSA (Directory System Agent), typically on TCP port 389, and sends an operation request to the DSA, which then responds. BER (Basic Encoding Rules) is used to transmit information between the client and the server. One can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names.

Task 1: Perform LDAP Enumeration using Active Directory Explorer (AD Explorer)

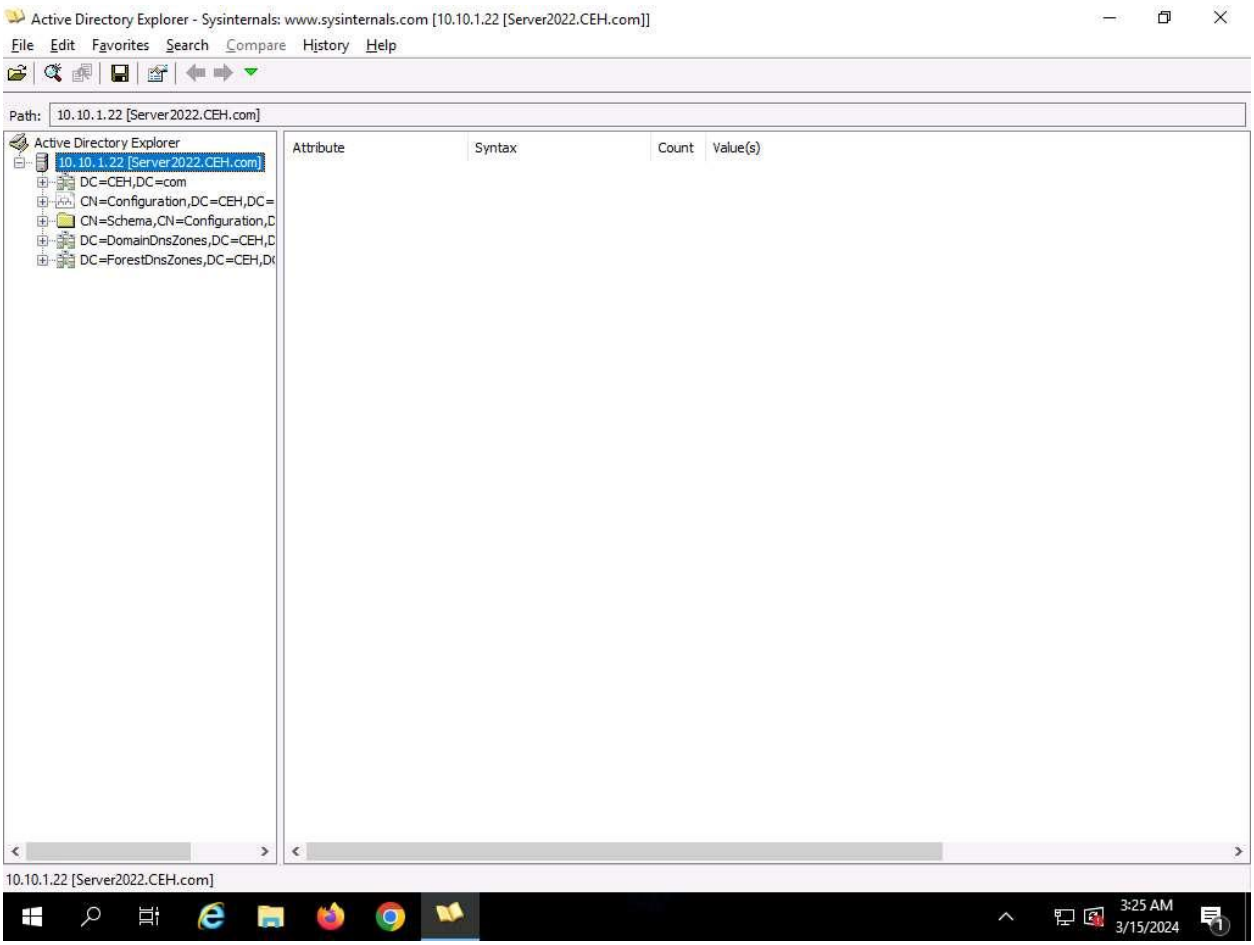
Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that can be saved and re-executed.

Here, we will use the AD Explorer to perform LDAP enumeration on an AD domain and modify the domain user accounts.

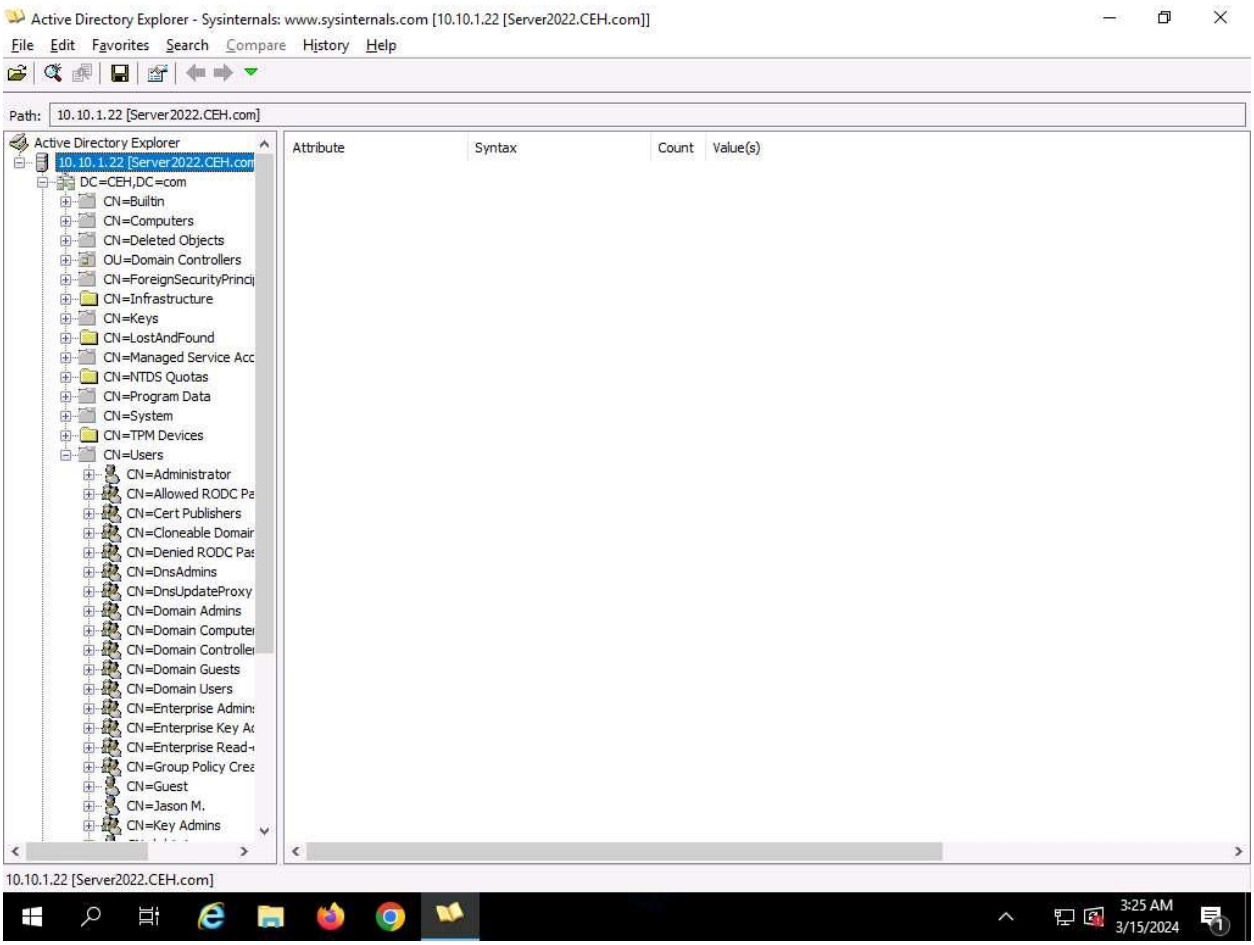
1. Click Windows Server 2019 to switch to the **Windows Server 2019** machine and click Ctrl+Alt+Delete to activate the machine. Login with **Administrator**/**Pa$$w0rd**.
2. Navigate to **Z:\CEHv13 Module 04 Enumeration\LDAP Enumeration Tools\Active Directory Explorer** and double-click **ADExplorer.exe**.
3. The **Active Directory Explorer License Agreement** window appears; click **Agree**.
4. The **Connect to Active Directory** pop-up appears; type the IP address of the target in the **Connect to** field (here, we are targeting the **Windows Server 2022** machine: **10.10.1.22**) and click **OK**.



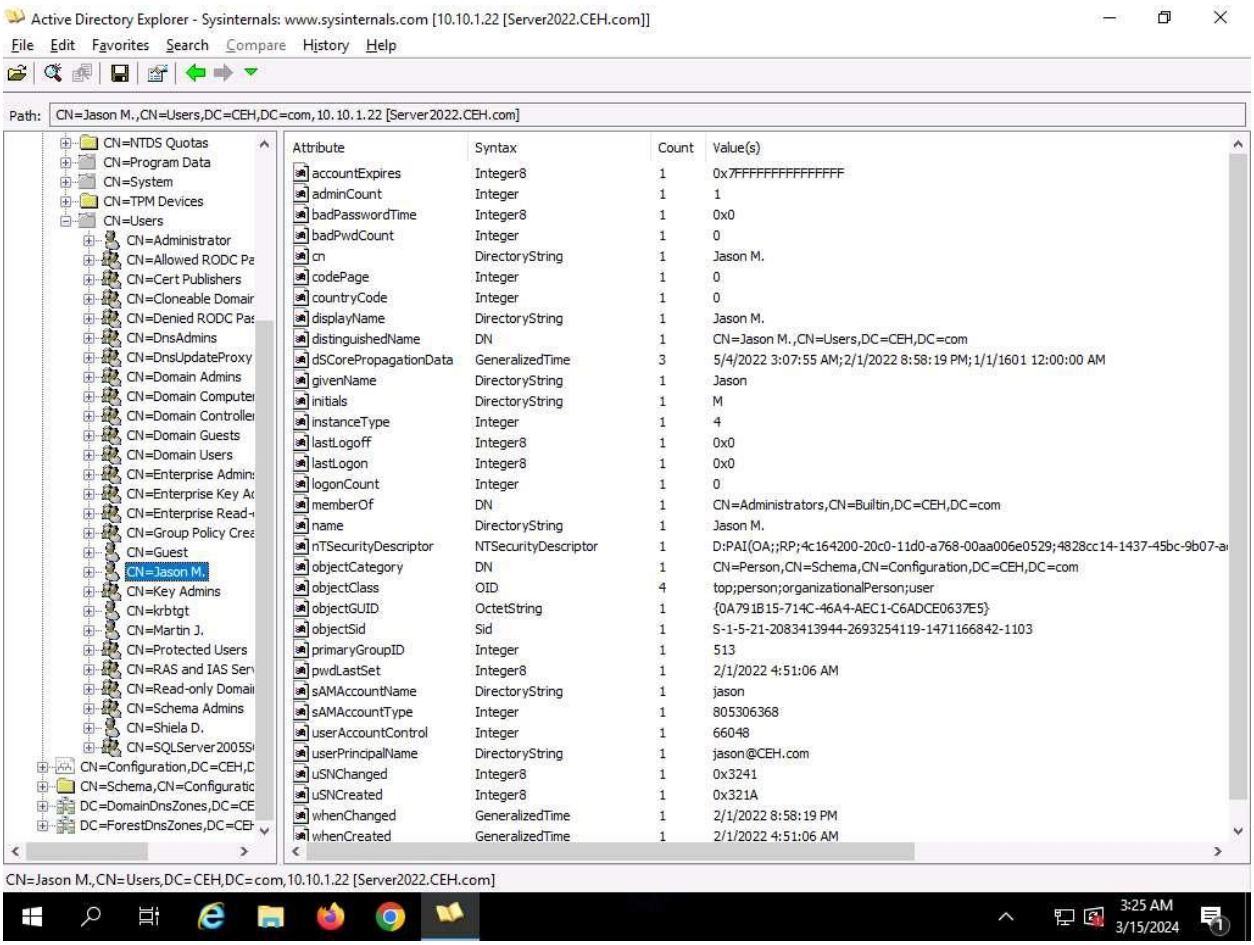
5. The **Active Directory Explorer** displays the active directory structure in the left pane, as shown in the screenshot.



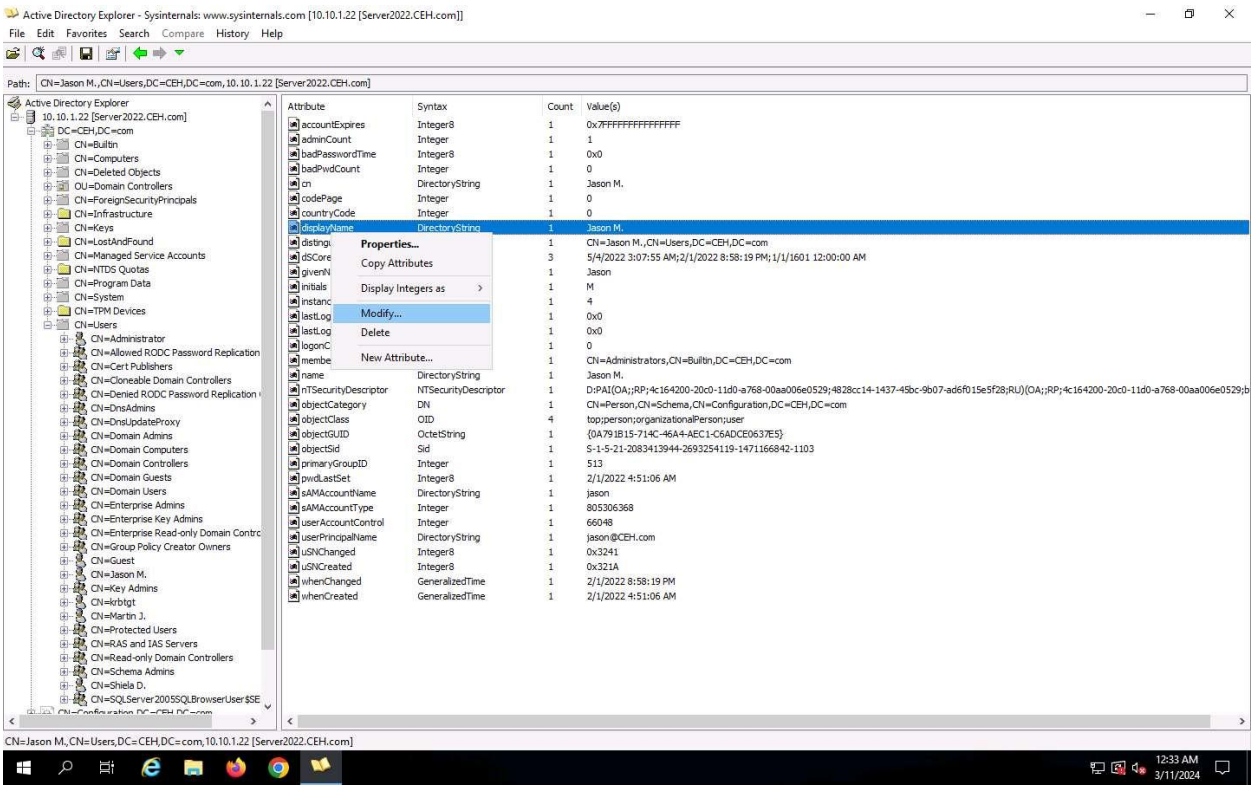
6. Now, expand **DC=CEH**, **DC=com**, and **CN=Users** by clicking "**+**" to explore domain user details.



7. Click any **username** (in the left pane) to display its properties in the right pane.



8. Right-click any attribute in the right pane (here, **displayName**) and click **Modify…** from the context menu to modify the user's profile.



9. The **Modify Attribute** window appears. First, select the username under the **Value** section, and then click the **Modify…** button. The **Edit Value** pop-up appears. Rename the username in the **Value data** field and click **OK** to save the changes.
10. You can read and modify other user profile attributes in the same way.
11. This concludes the demonstration of performing LDAP enumeration using AD Explorer.
12. You can also use other LDAP enumeration tools such as **Softerra LDAP Administrator** (https://www.ldapadministrator.com), **LDAP Admin Tool** (https://www.ldapsoft.com), **LDAP Account Manager** (https://www.ldap-account-manager.org), and **LDAP Search** (https://securityxploded.com) to perform LDAP enumeration on the target.
13. Close all open windows and document all the acquired information.

Question 4.3.1.1

Perform LDAP Enumeration using Active Directory Explorer (AD Explorer) and find the Domain Controller machine's IP address.

Question 4.3.1.2

Perform LDAP enumeration using Active Directory Explorer (AD Explorer) and find the userPrincipalName for the user named Jason M.