Lab #1 - LDAP and Active Directory

Overview

LDAP is a method that can be used for authentication, and potential data access (such as groups for authorization). Microsoft Active Directory implements and extends the LDAP standard, and can be accessed using LDAP browsers. In this lab, you will access both the College and your cas-dc01 template directory controller and review the information stored. You will answer questions about authentication and security.

Preparation

Download the Open Source (free) Apache Directory Studio; this will be used to browse existing LDAP servers to see the information available: https://directory.apache.org/studio/downloads.html

Part 1

For part 1, you will access the Conestoga College Active Directory server and authenticate with your own user credentials. Start Apache Directory Studio and choose Workbench -> LDAP -> Connection. Use the following settings:

Hostname: AD05D.conestogac.on.ca **Port**: 389 **Encryption**: None

Check Network Parameters – should pass the test

Auth Method: Simple Authentication **Bind DN or user:** <*username*>@conestogac.on.ca
Bind Password: <*Your Password***>**

Check Authentication – it should succeed

Base DN: DC=conestogac,DC=on,DC=ca No modification changes, leave at default

Trust the certificate for AD05D.conestogac.on.ca

Once connected, use the interface to browser the information in Active Directory. The bind itself was enough to confirm authentication, and is a practice used by many applications for authentication. Active Directory itself does contain information in the directory, particularly around users and groups. Pick some area of it at random and include it in your screenshot to prove you connected.

Screenshots

Show a screenshot or screenshots that are identifiable as yourself that show the work was completed.

Reflection

Write a reflection with this part of the lab. What kind of data is stored in the directory? What are the various attributes for an entry? How can one search the directory? How are objects uniquely identified in the directory? Any other observations or questions as you look at this? Use some or all of these questions to inspire your reflection on the work done.

Part 2

For part 2, you will access your own Active Directory server and authenticate with user credentials that you create in your own directory server. Start Apache Directory Studio and choose Workbench -> LDAP -> Connection. Use the following settings:

Hostname: *<IP ADDRESS>* **Port**: 389 **Encryption**: None

Check Network Parameters – should pass the test

Auth Method: Simple Authentication **Bind DN or user:** *<username>*
Bind Password: <*Your Password>*

Check Authentication – it should succeed

Base DN: *<BASE DN>* No modification changes, leave at default

Trust the certificate for your AD server

Once connected, use the interface to browser the information in Active Directory. The bind itself was enough to confirm authentication, and is a practice used by many applications for authentication. Active Directory itself does contain information in the directory, particularly around users and groups. Pick some area of it at random and include it in your screenshot to prove you connected.

Screenshots

Show a screenshot or screenshots that are identifiable as yourself that show the work was completed.

Reflection

Write a reflection with this part of the lab. How does the data differ from entries in the College directory service? What can you observe about the *userPassword* and the data stored within it? Why is this service important within the realm of enterprise application security? Considering the value of the data stored within directory services, what are the various ways of ensuring its security? Use some or all of these questions to inspire your reflection on the work done.