Connecting a Client to OpenLDAP

LPIC-2: Linux Engineer (202-450)

Objectives:

At the end of this episode, I will be able to:

1. Pluggable Authentication Modules (PAM) and how clients use them with OpenLDAP.
2. Configure a Linux client to authenticate with OpenLDAP.

> Additional resources used during the episode can be obtained using the download link on the overview episode.

- Connecting a Client to OpenLDAP

    - How Clients Connect
    - Configuring a Client
    - Testing Authentication

    - How Clients Connect

    - OpenLDAP is not supported by default
    - Pluggable Authentication Modules (PAM)

        - Extensions to Linux that allow alternative login methods

    - PAM Examples

        - SmartCard
        - RADIUS
        - Active Directory
        - MFA
        - OpenLDAP

    - Name Service LDAP Connection Daemon (NSLCD)

        - Interfaces OpenLDAP with PAM

- Configuring a Client

    1. Install required packages

        - `sudo apt install libnss-ldapd libpam-ldapd ldap-utils`

            1. ldap://10.222.0.53/
            2. dc=lab,dc=itpro,dc=tv
            3. Select passwd, group, and shadow

    2. Enable home directories in PAM

        - `sudoedit /etc/pam.d/common-session`

            - `session optional pam_mkhomedir.so skel=/etc/skel umask=077`

    3. Enable TLS in *nslcd*

        - `sudoedit /etc/nslcd.conf`

            - `ssl start_tls`
            - `tls_reqcert allow`

    4. Reboot

- Testing Authentication

    - Login with an OpenLDAP user
    - Verify UID and GUID
    - Verify creation of their home directory