- Filename: eccouncil-ceh31250-v12-4-4-1-ldap-enumeration.md
- Show Name: CEHv12 (312-50)
- Topic Name: Recon Techniques - Enumeration
- Episode Name: LDAP Enumeration
  ==

LDAP Enumeration

Objectives:

- Define LDAP Enumeration
- Enumerate target info with LDAP Enumeration tools

- What is LDAP and how is it used?
  - Lightweight Directory Access Protocol
    - Kinda like a 'phone book' of network resource attributes
      - User names
      - Email addresses
      - Phone numbers
      - Groups
  - Uses Port 389
    - Secure ldap use 636
- So LDAP is just full of possibly useful info, but how do we access it?
  - Windows server admins
    - Server Admin Tools
    - AD Explorer (Sysinternals)
  - 3rd-Party
  - Softerra LDAP Admin
    - https://www.ldapadministrator.com/
  - ldapsearch
    - `ldapsearch -LLL -x -H ldap://192.168.241.200 -b '' -s base'(objectclass=*)'`
  - Python
    - https://ldap3.readthedocs.io/en/latest/
  - Nmap
    - https://nmap.org/nsedoc/scripts/ldap-search.html