LDAP Enumeration

Agasthya P - CH.EN.U4CYS22004

#### What is LDAP?

Lightweight Directory Access Protocol (LDAP) is a protocol designed to help users locate data such as organizational details, user accounts, and network resources like files and devices. It also serves as a central authentication server, making it a critical component in network security. LDAP operates on port 389 by default.

#### What Information Does LDAP Enumeration Reveal?

By performing LDAP enumeration, attackers or penetration testers can gather sensitive information such as:

* Valid usernames
* Email addresses
* Organizational structure
* Group memberships

This information can be leveraged to further penetrate the network or plan advanced attacks.

### LDAP Enumeration

#### 1: Using Nmap with the LDAP Search Script

The Nmap "ldap-search" script allows you to query the LDAP server for specific attributes. Below is an example command:

nmap -p 389 --script ldap-search --script-args 'ldap.username="cn=ldaptest,cn=users,dc=cqure,dc=net",ldap.password=ldaptest,ldap.qfilter=users,ldap.attrib=sAMAccountName' 61.221.84.77

**Explanation:**

* -p 389: Specifies the LDAP port.
* --script ldap-search: Calls the Nmap script to perform LDAP queries.
* --script-args: Passes arguments to the script, including the username, password, query filter, and the attribute (e.g., sAMAccountName).
* 61.221.84.77: The target LDAP server IP address.

#### 2: Using Enum4Linux for Enumeration

Enum4Linux is another powerful tool for enumerating LDAP servers. You can extract data like account information and domain details with the following command:

enum4linux 61.221.84.77 | egrep "Account|Domain|Lockout|group"

**Explanation:**

* enum4linux: Initiates the enumeration process.
* 61.221.84.77: Specifies the target server.
* egrep: Filters output to display key details related to accounts, domains, lockout policies, and groups.

#### 3: Nmap with Multiple LDAP Scripts

To leverage multiple LDAP-related scripts without brute-forcing, use the following command:

nmap -n -sV --script "ldap\* and not brute" -p 389 61.221.84.77

**Explanation:**

* -n: Disables DNS resolution.
* -sV: Enables service version detection.
* --script "ldap\* and not brute": Executes all LDAP scripts except brute force.
* -p 389: Specifies the LDAP port.
* 61.221.84.77: The target server.

