LDAP Enumeration

Lightweight Directory Access Protocol (LDAP) is a widely used protocol for accessing and managing directory services, such as Active Directory in Windows environments. LDAP servers often contain sensitive information about users, groups, and other resources within an organization.

Before going further with the LDAP Enumeration techniques, one thing i want to clear out that the LDAP works mostly with Windows Active Directory. As this course is a rolling-release one, that means we will be adding Active Directory modules in the near future. Going too deep into the LDAP enumeration techniques at this time will only confuse you more. So, i will only discuss one or two techniques related to LDAP Enumeration here. Rest will be covered thoroughly when we will discuss Active Directory enumeration.

Enumeration with nmap

Just like every other service, we will start off our enumeration with nmap.

```
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' <target IP>
```

```
nmap -p 389 --script ldap-search --script-args
'ldap.username="cn=ldaptest,cn=users,
dc=cqure,dc=net",ldap.password=ldaptest,
ldap.qfilter=custom,ldap.searchattrib="operatingSystem",
ldap.searchvalue="Windows *Server*",ldap.attrib=
{operatingSystem,whencreated,OperatingSystemServicePack}' <host>
```

Enumeration with Enum4linux

Enum4linux is also useful while performing LDAP Enumeration. We can perform the same full scan using it but can use egrep to get the result relevant to us.

```
python3 enum4linux-ng.py -A 192.168.29.141 | egrep
"Account|Domain|Lockout|group"
```