ONDOKUZ MAYIS ÜNİVERSİTESİ MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

**OpenID Connect Tabanlı Tek Oturum Açma (SSO) Sağlayıcısı**

**Yard. Doç. Dr. Recai Oktaş**
**13061066 – Meryem Saka**

**RAPOR 5**

**Bu hafta proje için;**

- ✓ OpenLDAP Kurulumu ve Kullanımı

**konusunda çalışıldı.**

**Kurulum;**

OpenLDAP birçok Linux dağıtımının deposunda bulunabilir ve kolayca kurulur. Kaynak koddan da kurulum yapmak mümkündür.

1. **apt-get install slapd ldap-utils**

Bu komutla Debian deposundaki OpenLDAP sunucu programını kurulumu yapılır ve istemci için gerekli programlar (ldapsearch, ldapadd, vb.) kurulmuş olur. **ROOT** parolasını girdikten sonra kurulum tamamlanır.

OpenLDAP paketi kurulduktan sonra ilk olarak **"/etc/ldap/slapd.conf"** dosyasını düzenlemek ve bir kök girdi (base entry) oluşturmak gerekir.

2. **# vi /etc/ldap/slapd.conf**

```
# Schema and objectClass definitions
  include       /etc/ldap/schema/core.schema
  include       /etc/ldap/schema/cosine.schema
  include       /etc/ldap/schema/nis.schema
  include       /etc/ldap/schema/inetorgperson.schema
  database bdb
  suffix "dc=omu,dc=edu,dc=tr"
  rootdn "cn=manager,dc=omu,dc=edu,dc=tr"
  rootpw {SSHA}XyZmHH1RlnSVXTj87UvxOAOCZA8oxNCT
  directory /usr/local/var/openldap-data
```

Burada sırasıyla veri tabanı türünü, kuruluma uygun sonek yapısını, yetkili kullanıcının ismini ve parolasını, son olarak da verilerin tutulacağı yol belirtilir. Parola düz metin olarak tutabileceği gibi **"slappasswd"** komutuyla şifrelenmiş olarak da üretebilir.

Sırada kök girdi oluşturma var.

3. **# vi base.ldif**

```
  dn: dc=nodomain
  objectclass: dcObject
  objectclass: organization
  o: OMU
  dc: omu.edu.tr
  dn: cn=root,dc=omu,dc=edu,dc=tr
  objectclass: organizationalRole
  cn: root
#ldapadd -x -D "cn=root,dc=omu,dc=edu,dc=tr" -W -f base.ldif
```

Burada önce içinde kök girdi bilgileri olan bir ldif dosyası yaratılır. Sonra **"ldapadd"** komutuyla sunucuya eklenir. **-D** parametresi ile bir kullanıcı işlemi yapılacağı, **-W** ile parola girileceği, **-X** ile parola şifrelemesi belirtilir. Temel kurulum tamamlanır.

Kurulum **"ldapsearch"** komutuyla test edilir:

4. **ldapsearch -x -b 'dc=omu,dc=edu,dc=tr' '(objectclass=*)'**

```
# extended LDIF
# LDAPv3
# base with scope subtree
# filter: (objectclass=*)
# requesting: ALL

# nodomain
  dn: dc=omu,dc=edu,dc=tr
  objectClass: top
  objectClass: dcObject
  objectClass: organization
  o: OMU
  dc: nodomain

# root, nodomain
  dn: cn=manager,dc=omu,dc=edu,dc=tr
  objectClass: simpleSecurityObject
  objectClass: organizationalRole
  cn: root
  description: LDAP rootistrator

# search result
  search: 2
  result: 0 Success
# numResponses: 3
# numEntries: 2
```

**LDAP erişim yetkilerinin yapılandırılması;**
**access to attrs=userPassword, shadowLastChange**

- **by dn="manager,dc=omu,dc=edu,dc=tr"** // Bu kullanıcı herkesin userPassword, shadowLastChange'e yazma hakkına sahiptir.
- **by anonymous auth** //Anonim kullanıcı sadece kanıtlama yapabilir.
- **by self write** //Herkes kendi userPassword, shadowLastChange değiştirme hakkına sahiptir.
- **by * none** // Kimse hiçbir şey yapamaz (!)

Bu şekildekullanıcı izinleri düzenlenebilir.

**Proje için gelecek haftada;**

1. OpenLDAP Kullanımı ve Geliştirilmesi
**araştırması yapılacaktır.**

Meryem Saka
13061066
11 Kasım 2016