

# 网络对抗原理 大作业

## 实验二



学    院    网络与信息安全学院

专    业    信息安全

姓    名    任旭杰 15180110034

## 1. 安装并配置 openldap

修改/etc/hosts

```
renxujie2@ubuntu: /etc/apt
```

```
# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0      ip6-localnet
ff00::0      ip6-mcastprefix
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
~
~
~
~
~
~
~
~
~
~
~
"/etc/hosts" [只读] 10L, 280C
```

## 使用 apt-get 下载安装 ldap 并修改配置文件

```

#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
#BASE      dc=ldapdomain,dc=com
#URI        ldap://192.168.5.180:389
#SIZELIMIT  12
#TIMELIMIT  15
#DEREF      never

# TLS certificates (needed for GnuTLS)
TLS_CACERT  /etc/ssl/certs/ca-certificates.crt

~
~
~
~
~
~
"/etc/ldap/ldap.conf" 17L, 301C

```

配置完成。使用 ldapsearch 测试

```
root@ubuntu: /etc
root@ubuntu:/etc# ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config dn:
dn: cn=config
dn: cn=module{0},cn=config
dn: cn=schema,cn=config
dn: cn={0}core,cn=schema,cn=config
dn: cn={1}cosine,cn=schema,cn=config
dn: cn={2}nis,cn=schema,cn=config
dn: cn={3}inetorgperson,cn=schema,cn=config
dn: olcBackend={0}mdb,cn=config
dn: olcDatabase={-1}frontend,cn=config
dn: olcDatabase={0}config,cn=config
dn: olcDatabase={1}mdb,cn=config
root@ubuntu:/etc#
```

向 ldap 中插入数据

```
root@ubuntu: /etc/ldap
root@ubuntu:/etc/ldap# vi shiyan2.ldif
root@ubuntu:/etc/ldap# ldapadd -x -D cn=admin,dc=example,dc=com -W -f shiyan2.ldif
Enter LDAP Password:
adding new entry "ou=students,dc=example,dc=com"
ldap_add: Object class violation (65)
        additional info: object class 'organizationalPerson' requires attribute 'sn'

root@ubuntu:/etc/ldap# ldapadd -x -D cn=admin,dc=example,dc=com -W -f add_content.ldif
Enter LDAP Password:
adding new entry "ou=Groups,dc=example,dc=com"
ldap_add: Already exists (68)

root@ubuntu:/etc/ldap# ldapsearch -x -LLL -b dc=example,dc=com '' cn gidNumber
dn: dc=example,dc=com
dn: cn=admin,dc=example,dc=com
cn: admin
dn: ou=Groups,dc=example,dc=com
root@ubuntu:/etc/ldap#
```

下载安装 phpldapadmin，并修改配置文件

```
renxujie2@ubuntu: /etc/apt
GNU nano 2.5.3      文件: /etc/phpldapadmin/config.php

/* Examples:
'ldap.example.com',
'ldaps://ldap.example.com/',
'ldapi://%2fusr%2flocal%2fvar%2frun%2fldapi'
(Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','127.0.0.1');

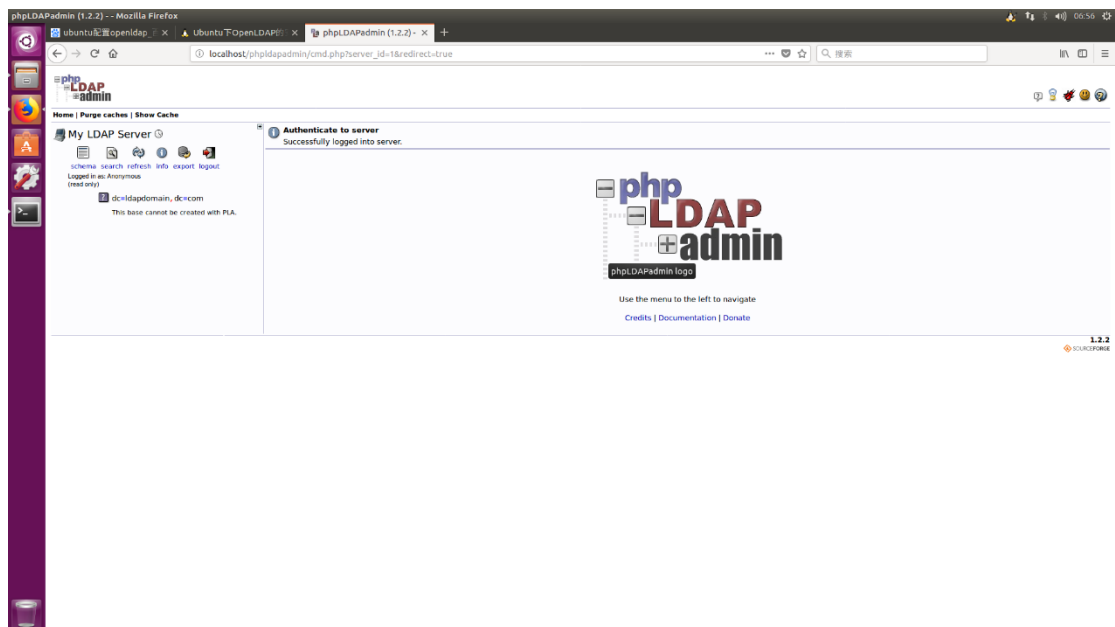
/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

/* Array of base DN's of your LDAP server. Leave this blank to have phpldapadmin
auto-detect it for you. */
$servers->setValue('server','base',array('dc=ldapdomain,dc=com'));

/* Five options for auth_type:
1. 'cookie': you will login via a web form, and a client-side cookie will
store your login dn and password.
2. 'session': same as cookie but your login dn and password are stored on the
server.

^G 求助      ^O 写入      ^W 搜索      ^K 剪切文字      ^J 对齐      ^C 光标位置
^X 离开      ^R 读档      ^R 替换      ^U 还原剪切      ^T 拼写检查      ^_ 跳行
```

成功登陆 phpldapadmin



## 2. 配置 Apache 服务器及 Basic 认证模块

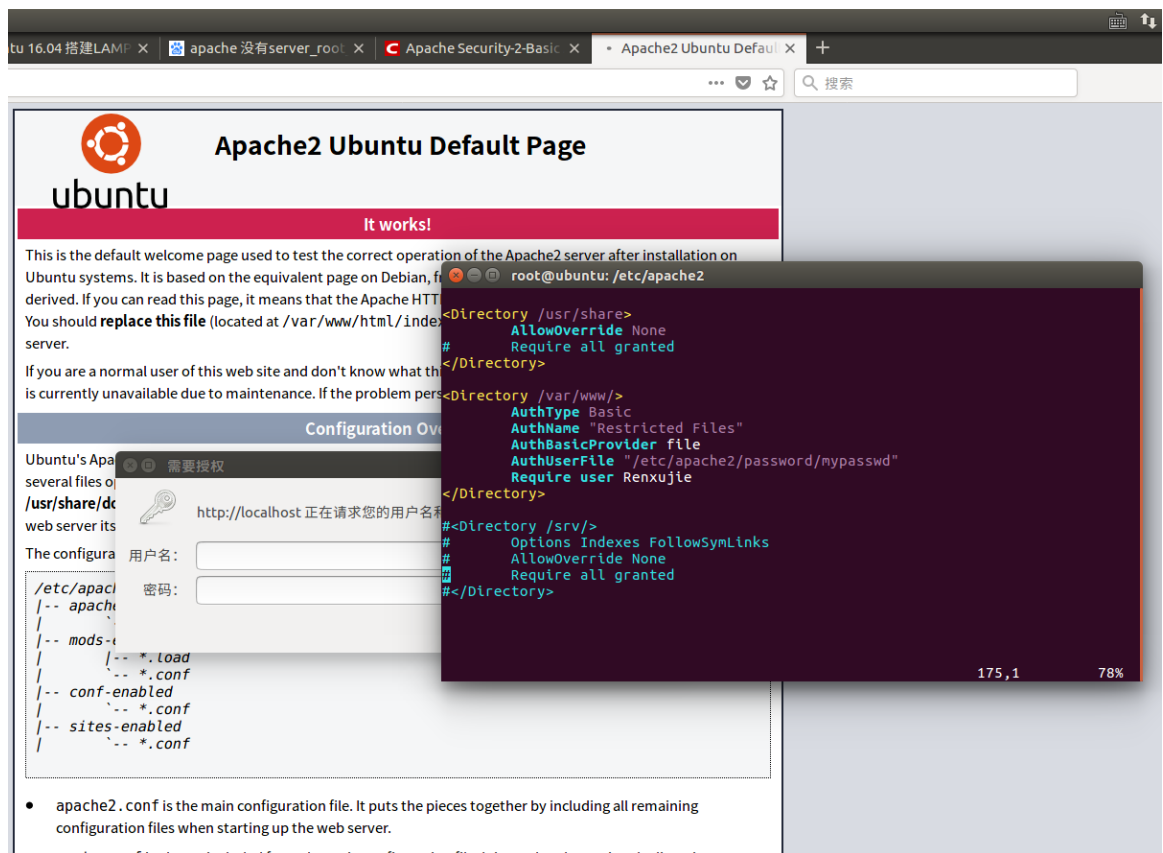
配置完 Apache 服务器后，新建密码文件

```
root@ubuntu: /etc/apache2/mods-available
-rw-r--r-- 1 root root 78 Jun 11 07:24 socache_shmcb.load
-rw-r--r-- 1 root root 66 Jun 11 07:24 spelling.load
-rw-r--r-- 1 root root 3110 Jun 11 07:24 ssl.conf
-rw-r--r-- 1 root root 97 Jun 11 07:24 ssl.load
-rw-r--r-- 1 root root 749 Jun 11 07:24 status.conf
-rw-r--r-- 1 root root 64 Jun 11 07:24 status.load
-rw-r--r-- 1 root root 72 Jun 11 07:24 substitute.load
-rw-r--r-- 1 root root 64 Jun 11 07:24 suexec.load
-rw-r--r-- 1 root root 70 Jun 11 07:24 unique_id.load
-rw-r--r-- 1 root root 423 Jun 11 07:24 userdir.conf
-rw-r--r-- 1 root root 66 Jun 11 07:24 userdir.load
-rw-r--r-- 1 root root 70 Jun 11 07:24 usertrack.load
-rw-r--r-- 1 root root 74 Jun 11 07:24 vhost_alias.load
-rw-r--r-- 1 root root 66 Jun 11 07:24 xml2enc.load
root@ubuntu:/etc/apache2/mods-available# a2enmod auth_basic.load
Considering dependency authn_core for auth_basic:
Module authn_core already enabled
Module auth_basic already enabled
root@ubuntu:/etc/apache2/mods-available# htpasswd -c /etc/apache2/password/mypas
swd Renxujie
New password:
Re-type new password:
Adding password for user Renxujie
root@ubuntu:/etc/apache2/mods-available#
```

开启 Basic 模块

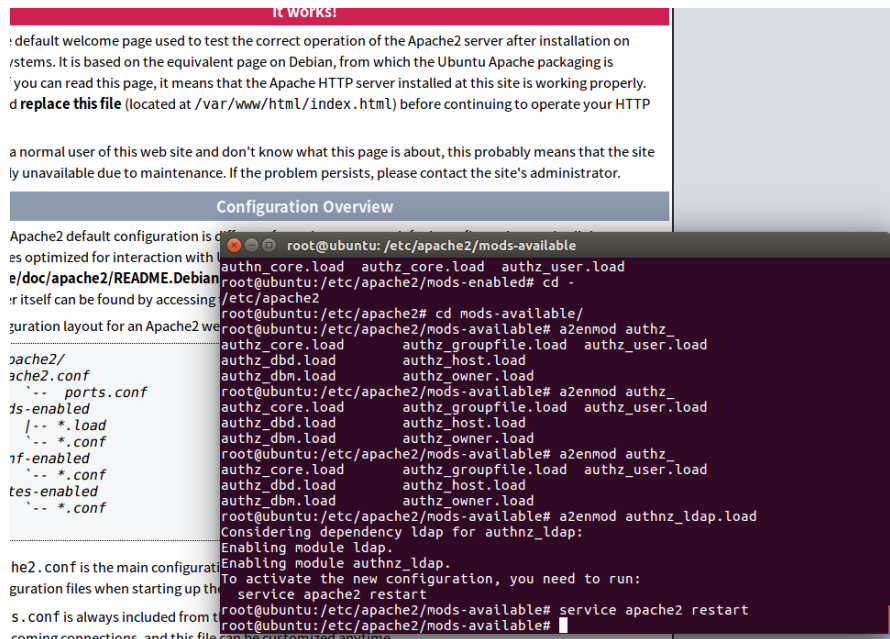
```
root@ubuntu: /etc/apache2/mods-available
-rw-r--r-- 1 root root 68 Jun 11 07:24 setenvif.load
-rw-r--r-- 1 root root 78 Jun 11 07:24 slotmem_plain.load
-rw-r--r-- 1 root root 74 Jun 11 07:24 slotmem_shm.load
-rw-r--r-- 1 root root 74 Jun 11 07:24 socache_dbm.load
-rw-r--r-- 1 root root 84 Jun 11 07:24 socache_memcache.load
-rw-r--r-- 1 root root 78 Jun 11 07:24 socache_shmcb.load
-rw-r--r-- 1 root root 66 Jun 11 07:24 spelling.load
-rw-r--r-- 1 root root 3110 Jun 11 07:24 ssl.conf
-rw-r--r-- 1 root root 97 Jun 11 07:24 ssl.load
-rw-r--r-- 1 root root 749 Jun 11 07:24 status.conf
-rw-r--r-- 1 root root 64 Jun 11 07:24 status.load
-rw-r--r-- 1 root root 72 Jun 11 07:24 substitute.load
-rw-r--r-- 1 root root 64 Jun 11 07:24 suexec.load
-rw-r--r-- 1 root root 70 Jun 11 07:24 unique_id.load
-rw-r--r-- 1 root root 423 Jun 11 07:24 userdir.conf
-rw-r--r-- 1 root root 66 Jun 11 07:24 userdir.load
-rw-r--r-- 1 root root 70 Jun 11 07:24 usertrack.load
-rw-r--r-- 1 root root 74 Jun 11 07:24 vhost_alias.load
-rw-r--r-- 1 root root 66 Jun 11 07:24 xml2enc.load
root@ubuntu:/etc/apache2/mods-available# a2enmod auth_basic.load
Considering dependency authn_core for auth_basic:
Module authn_core already enabled
Module auth_basic already enabled
root@ubuntu:/etc/apache2/mods-available#
```

修改 Apache2.conf 配置文件并导入密码文件，重启 Apache 服务，需要进行认证才能登陆。

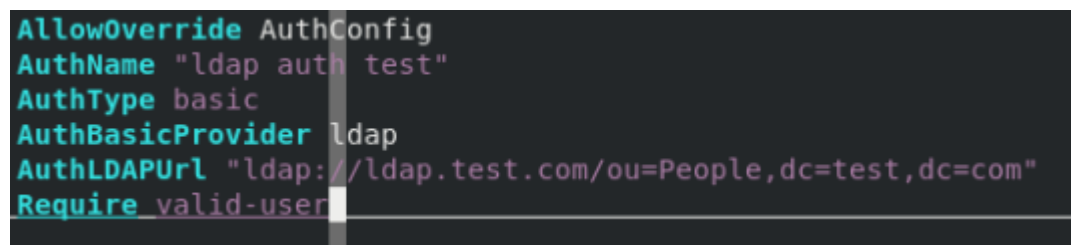


### 3. 配置 ldap 模块

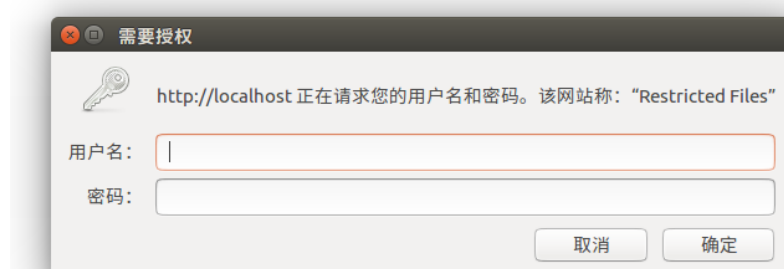
#### 启动 ldap 模块



#### 启动 ldap 模块后，修改 Apache2.conf



#### 需要认证





#### 4. 搭建 RADIUS 服务器

安装 freeradius 后，使用命令 `freeradius -X` 检测安装是否成功

```
root@ubuntu: /etc/apache2
root@ubuntu:/etc/apache2# sudo service freeradius start
root@ubuntu:/etc/apache2# sudo freeradius -X
freeradius: FreeRADIUS Version 2.2.8, for host x86_64-pc-linux-gnu, built on Jul
 26 2017 at 15:27:21
Copyright (C) 1999-2015 The FreeRADIUS server project and contributors.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License.
For more information about these matters, see the file named COPYRIGHT.
Starting - reading configuration files ...
including configuration file /etc/freeradius/radiusd.conf
including configuration file /etc/freeradius/proxy.conf
including configuration file /etc/freeradius/clients.conf
including files in directory /etc/freeradius/modules/
including configuration file /etc/freeradius/modules/pap
including configuration file /etc/freeradius/modules/attr_rewrite
including configuration file /etc/freeradius/modules/mschap
including configuration file /etc/freeradius/modules/sradutmp
including configuration file /etc/freeradius/modules/etc_group
including configuration file /etc/freeradius/modules/unix
including configuration file /etc/freeradius/modules/opendirectory
including configuration file /etc/freeradius/modules/detail.log
including configuration file /etc/freeradius/modules/digest
```

成功使用 `radtest` 验证

```
renxujie2@ubuntu: /etc/ldap
renxujie2@ubuntu:/etc/ldap$ ldapsearch -x -LLL -b dc=example,dc=com 'uid=john' c
n gidNumber
renxujie2@ubuntu:/etc/ldap$ ldapsearch -x -LLL -b dc=example,dc=com '' cn gidNum
ber
dn: dc=example,dc=com

dn: cn=admin,dc=example,dc=com
cn: admin

dn: ou=Groups,dc=example,dc=com

renxujie2@ubuntu:/etc/ldap$ vi
add_content.ldif  ldap.conf          schema/          shiyan2.ldif
dd_content.ldif   sasl2/          shiyan2.ldif    slapd.d/
renxujie2@ubuntu:/etc/ldap$ vi add_content.ldif
renxujie2@ubuntu:/etc/ldap$ radtest steve testing localhost 1812 testing123
Sending Access-Request of id 97 to 127.0.0.1 port 1812
  User-Name = "steve"
  User-Password = "testing"
  NAS-IP-Address = 127.0.0.1
  NAS-Port = 1812
  Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=97, length=20
renxujie2@ubuntu:/etc/ldap$
```



5. 在之前 Apache 的 RADIUS 认证模块的配置下,不改变配置,切换到使用 LDAP 存放的学生用户名密码认证

修改/etc/raddb/mods-available/ldap

```
server = 'localhost'
server = 'ldap.rrdns.example.org'
server = 'ldap.rrdns.example.org'

# Port to connect on, defaults to 389, will be ignored for LDAP URIs.
port = 389

# Administrator account for searching and possibly modifying.
# If using SASL + KRB5 these should be commented out.
identity = 'cn=admin,dc=example,dc=org'
password = mypass

# Unless overridden in another section, the dn from which all
# searches will start from.
base_dn = 'dc=example,dc=org'
```

进入/etc/raddb/sites-available, 修改 default

```
526 Auth-Type LDAP {
527     ldap
528 }
```

修改同一目录下的 ldap 文件

```
server site ldap {
    listen {
        ipaddr = *
        port = 1833
        type = auth
    }
    authorize {
        #
        #       update {
        #           control:Auth-Type := ldap
        #       }
        #       update control {
        #           &Auth-Type := LDAP
        #       }
        #   }
    authenticate {
        Auth-Type LDAP {
            ldap
        }
    }
    post-auth {
        Post-Auth-Type Reject {
        }
    }
}
```

使用 radtest 测试如下：

```
Sent Access-Request Id 165 from 0.0.0.0:42134 to 127.0.0.1:1833 length 80
  User-Name = "test"
  User-Password = "bin"
  NAS-IP-Address = 192.168.43.116
  NAS-Port = 0
  Message-Authenticator = 0x00
  Framed-Protocol = PPP
  Cleartext-Password = "bin"
```

成功。