实验10 Linux文件系统运维实验

实验目的

掌握Linux文件系统访问权限的查看、修改、定义等基本运维技能。

实验内容

- 1.使用ls命令查看文件及其属性
- 2.使用chmod命令改变文件访问权限
- 3.使用访问控制列表
- 4.使用mv命令处理文件（文件移动和重命名）
- 5.安装并配置一个基本的LDAP服务器
- 6.设置文件其它安全属性

实验前提

本实验指导建立在ubuntu server 1604基础上。

实验步骤

一.使用ls命令查看文件及其属性

1.选定某个目录，例如根目录或用户主目录。 `cd \` 或 `cd ~` 。

2.运行 `ls -l` 命令（如有必要，在ls之前加上sudo）来获取更多的关于文件和目录的信息，如：创建时间、所有者、访问权限等。

3.运行 `ls -a` 命令来查看包括隐藏文件在内的所有当前目录下文件。

二.使用chmod命令改变文件访问权限

chmod命令种的参数含义：

- u代表文件或目录的所有者
- g文件或目录所属的组

- o除了文件或目录的所有者或所属组之外，其他用户均属于此范围。

1.进入用户主目录。

```
cd ~
```

2.新建文件notes.txt。

```
vi notes.txt
```

键入任意内容后保存退出。

3.为该文件设立访问权限，尝试执行下列命令并观察文件属性。

```
chmod u+x notes.txt

ls notes.txt

chmod g+x, o+x notes.txt

ls notes.txt
```

4.删除用户某些权限。

```
chmod o-x notes.txt
```

5.移除所有者对该文件的读权限

```
chmod a-r notes.txt
```

6.利用八进制表示法的数字来设置对文件的访问权限.

```
chmod 754 notes.txt
```

请问上述命令对notes.txt设置了何种权限？

7.参考其它文件属性设置当前文件属性

```
# 新建文件并保存
vi file2.txt

chmod --reference=notes.txt file2.txt
```

查看当前file2.txt的读写权限设置。

三.使用访问控制列表

这个实验目的是使用acl控制用户访问权限。

1.测试是否能连接互联网

```
ping www.baidu.com

# 若不能，则考虑重设网络连接
```

2.安装acl模块

```
sudo apt install acl
```

3.新建一个实验文件，名为mykeys.txt

`nano mykeys.txt` ， 内容任意。

4.查看acl默认设置。

```
getfacl mykeys.txt
```

5.创建3个用户，分别为命名为user1, user2和user3

```
sudo useradd user1
sudo passwd -d user1
# 注：上述命令是为了user1能免密码登录。
<p class="mume-header " id="注上述命令是为了user1能免密码登录"></p>


sudo useradd user2
sudo passwd -d user2

sudo useradd user3
sudo passwd -d user3
```

6.增加一个用户组，将user1，user2,user3加入组

```
sudo addgroup usergroup1

sudo usermod -G usergroup1 user1
sudo usermod -G usergroup1 user2
sudo usermod -G usergroup1 user3
```

7.创建访问目标。

```
sudo mkdir -p /example/accounts
```

8.将user1设置为/example的所有者

```
sudo chown user1 /example
```

假设用户user1仅希望在accounts目录中赋予用户user2写权限。如果利用上面的chmod命令，那么用户user1只能通过为组group1设置写权限完成操作。但同时也会赋予用户user3写权限，而这是用户user1不希望发生的。所以，用户user1可以通过使用ACL来仅赋予用户user2写权限。

9.设置acl，并查看结果。

```
setfacl -m u:user1:rwx accounts
setfacl -m u:user2:rwx accounts
setfacl -m other:--- accounts
getfacl /example/accounts
```

注：以上操作均为特权用户leo或root执行。

10.在虚拟机终端上，将用户leo或root登出。

```
logout
```

11.以user1登录（即用户名为user1），然后查看能否进入accouts。

```
cd /example/accounts
```

如果能够成功，logout即可。

12.以user3登录，然后查看能否进入accouts。

```
cd /example/accounts
```

user3 应该被禁止进入accounts目录。

四.使用mv命令处理文件（文件移动和重命名）

1.建立实验用目录和文件

```
sudo mkdir -p /home/leo/example

nano mykeys1.txt
#键入任意内容后保存

nano mykeys2.txt
#键入任意内容后保存

nano mykeys3.txt
#键入任意内容后保存
```

2.移动单个文件至目标目录。

```
mv mykeys1.txt  /home/leo/example
```

3.移动多个文件至目标目录。

```
mv mykeys2.txt  mykeys3.txt /home/leo/example
```

4.对文件和文件夹进行重命名

```
cd /home/leo/example/

mv mykeys2.txt  yourkeys1.txt
```

5.有关mv命令的其它选项，都比较简单，可以自行练习。

五.安装并配置一个基本的LDAP服务器

1.确保联网的情况下，安装slapd软件包：

```
sudo apt-get install slapd
```

2.在安装过程中，会被提示输入并确认管理员（administrator）的密码，该密码用于LDAP管理员账户（administrator）。这里统一设置为123456.

3.安装LDAP需要的一些其他实用工具：

```
sudo apt install ldap-utils
```

4.启动并按照需要重新配置LDAP软件包。

输入如下命令启动配置工具:

```
sudo dpkg-reconfigure slapd
```

5.在配置过程中会出现一系列的问题提示，按照需要逐个选择合适的配置。

- 首先，会弹出关于省略OpenLDAPserver 服务器配置的提示,选择No并继续。
- 下一步，需要输入域名（Domain name）。可以使用服务器上已有的域名也可以重新创建。本实验中使用example.com。
- 根据提示输入组织名（Organization Name），本实验用xxx。
- 当出现Database backend to use?提示时。选择HDB选项（一种层次数据库）。
- 当询问删除slapd时是否移除数据库时，选择No。
- 当出现提示是否移动旧数据库时，选择Yes从而允许配置程序创建一个新的数据库。
- 当询问是否允许LDAPv2协议时，选择No。
- 当配置完成后。

注：上述设置大多数采用了默认配置。

6.测试与ldapwhoami的LDAP连接，该连接应该返回我们连接的用户名：

```
ldapwhoami -H ldap:// -x
```

上述命令返回应该是anonymous

7.开始安装phpldapadmin软件包。

它可以让管理员使用web管理接口管理LDAP服务。

```
sudo apt-get install phpldapadmin
```

8.打开phpldapadmin的配置文件设定一些参数值：

```
sudo  nano  /etc/phpldapadmin/config.php
```

9.搜索下面给定的部分，修改为Ubuntu服务器的域名或IP地址(本例中为10.10.10.128，自己使用ifconfig检查)：

```
$servers->setValue('server','host','127.0.0.1');

# 修改样例:
$servers->setValue('server','host','10.10.10.128');
```

10.接下来编辑下面这个条目，输入之前重新配置slapd软件包时所给的域名：

```
$servers->setValue('server','base',array('dc=example,dc=com'));
```

按照上面命令行的格式将域名赋值给dc属性。因为当前的域名是example.com，所以上面命令行中的输入应该是：dc=example, dc=com。

11.找到下面这行，再次将域名作为dc属性输入。关于cn属性，其值应为admin：
$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');

12.找到和下面这段代码中内容相似的部分，首先取消前面的备注，然后将其值设置为true：

```
$config->custom->appearance['hide_template_warning'] = true;
```

13.完成所有这些配置更改之后，保存并关闭文件。

14.当完成phpldapadmin的配置之后，在自己的windows中打开浏览器。地址为 http://10.10.10.128/phpldapadmin 。

15.当phpldapadmin页面打开之后，在页面左边可以找到login（登录）链接，点击它会出现一个登陆提示。

16.如果phpldapadmin已经被正确配置了，那么在登录界面会出现正确的Login DN信息。在本例中应该是：cn=admin,dc=example,dc=com。如果正确输入了管理员密码，则管理界面会打开。

17.在管理界面左边你可以看见域组件的地方（dc=example,dc=co），点击旁边的+号。将会显示目前正在使用的登录账户。

六.设置文件其它安全属性

1.在用户主目录下，新建一个文本文件，名为mykeys.txt.

```
leo@ubuntu:~$ vi mykeys.txt
```

之后在文件中键入任意内容，保存退出。

2.查看当前文件属性

```
leo@ubuntu:~$ lsattr mykeys.txt
```

3.锁定文件并查看属性。

锁定文件可以给文件赋予 i 属性。

```
leo@ubuntu:~$ sudo chattr +i  mykeys.txt

leo@ubuntu:~$ lsattr mykeys.txt
```

4.尝试删除或更改 mykeys.txt,是否能够成功？ 如果使用root 用户能否删除和修改mykeys.txt数据？

```
leo@ubuntu:~$ sudo rm -rf mykeys.txt
```

5.取消文件锁定。

```
leo@ubuntu:~$ sudo chattr -i  mykeys.txt

leo@ubuntu:~$ lsattr mykeys.txt
```

6.再次尝试删除或更改 mykeys.txt,是否能够成功？

7.设置文件属性，使mykeys.txt仅能增加数据，不能删减数据。

这种操作常用于日志文件或备份目录的设置，只可增加内容、创建文件而不可删除。

```
# 建立一个实验目录并备份一些日志
leo@ubuntu:~$ mkdir mydir
leo@ubuntu:~$ lsattr mylogs -a
leo@ubuntu:~$ sudo chattr +a mylogs
leo@ubuntu:~$ lsattr mylogs -a
leo@ubuntu:~$ cd mylogs/
leo@ubuntu:~/mylogs$ cp  /var/log/*.log  .
leo@ubuntu:~/mylogs$ ls


# 尝试删除文件
leo@ubuntu:~/mylogs$ sudo rm -rf vmware-*
```

8.思考如何能删除掉mylogs中的前缀为vmware的文件？