

Лабораторная работа №2 Лабораторная работа Дискреционное разграничение прав в Linux. Основные атрибуты

фio:ван яо

группа:НПМбд-02-21

билет:1032215430

Содержание

- Цель работы
- Выполнение лабораторной работы
- таблицы прав доступа
- Выводы

1. Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

2. Выполнение лабораторной работы

- 1 В установленной при выполнении предыдущей лабораторной работы операционной системе создайте учётную запись пользователя guest (используя учётную запись администратора):
useradd guest

- 2 Задайте пароль для пользователя guest (используя учётную запись администратора):
passwd guest

```
root@wangyao:~  
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)  
[ root@wangyao ~] # useradd guest  
[ root@wangyao ~] # passwd guest  
更改用户 guest 的密码。  
新的 密码：  
无效的密码： 密码少于 8 个字符  
重新输入新的 密码：  
抱歉，密码不匹配。  
新的 密码：  
无效的密码： 密码未通过字典检查 - 过于简单化/系统化  
重新输入新的 密码：  
抱歉，密码不匹配。  
新的 密码：  
重新输入新的 密码：  
passwd: 所有的身份验证令牌已经成功更新。  
[ root@wangyao ~] #
```

- 3 Войдите в систему от имени пользователя guest

```
[ root@wangyao ~] # su - guest  
[ guest@wangyao ~] $
```

- 4 Определите директорию, в которой вы находитесь, командой pwd. Сравните её с приглашением командной строки. Определите, является ли она вашей домашней директорией? Если нет, зайдите в домашнюю директорию

```
[ guest@wangyao ~] $ pwd  
/home/guest  
[ guest@wangyao ~] $
```

- 5 Уточните имя вашего пользователя командой whoami

```
[ guest@wangyao ~] $ whoami  
guest
```

- 6 Уточните имя вашего пользователя, его группу, а также группы, куда входит пользователь, командой id. Выведенные значения uid, gid и др. запомните. Сравните вывод id с выводом команды groups.

```
[ guest@wangyao ~] $ id  
uid=1001(guest) gid=1001(guest) 组=1001(guest) 环境=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[ guest@wangyao ~] $ groups  
guest  
[ guest@wangyao ~] $
```

- 7 Сравните полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки

```
[guest@wangyao ~]$ whoami
guest
[guest@wangyao ~]$ echo $USER
guest
[guest@wangyao ~]$ echo "Current username: $(whoami)"
Current username: guest
[guest@wangyao ~]$
```

- 8 Просмотрите файл /etc/passwd командой
cat /etc/passwd

Найдите в нём свою учётную запись. Определите uid пользователя.

Определите gid пользователя. Сравните найденные значения с полученными в предыдущих пунктах

```
[guest@wangyao ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-bus-proxy:x:999:998:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:998:997:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:996:User for polkitd:/:/sbin/nologin
abrt:x:173:173:/:etc/abrt:/sbin/nologin
unbound:x:996:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
colord:x:995:993:User for colord:/var/lib/colord:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
geoclue:x:994:991:User for geoclue:/var/lib/geoclue:/sbin/nologin
```

```
[guest@wangyao ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001:/:/home/guest:/bin/bash
```

- 9 Определите существующие в системе директории командой
ls -l /home/

Удалось ли вам получить список поддиректорий директории /home? Какие права установлены на директориях?

```
guest:x:1001:1001:/:/home/guest:/bin/bash
[guest@wangyao ~]$ ls -l /home
总用量 8
drwx-----. 5 guest guest 4096 9月 9 14:30 guest
drwx-----. 14 wangyao wangyao 4096 9月 9 14:21 wangyao
[guest@wangyao ~]$
```

- 10 Проверьте, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой:

lsattr /home

Удалось ли вам увидеть расширенные атрибуты директории?

Удалось ли вам увидеть расширенные атрибуты директорий других пользователей?

```
[ root@wangyao ~] # lsattr /home
----- /home/wangyao
----- /home/guest
[ root@wangyao ~] # getfattr /home
[ root@wangyao ~] # getfattr /var/log
[ root@wangyao ~] #
```

- 11 Создайте в домашней директории поддиректорию dir1 командой `mkdir dir1`

Определите командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию dir1.

```
[ root@wangyao ~] # lsattr /home
----- /home/wangyao
----- /home/guest
[ root@wangyao ~] # getfattr /home
[ root@wangyao ~] # getfattr /var/log
[ root@wangyao ~] #
```

- 12 Снимите с директории dir1 все атрибуты командой `chmod 000 dir1`

и проверьте с её помощью правильность выполнения команды `ls -l`

```
[ root@wangyao ~] # chmod 000 dir1
[ root@wangyao ~] # ls -ld dir1
d----- . 2 root root 6 9月  9 15:05 dir1
[ root@wangyao ~] # setfattr -x user.example dir1
[ root@wangyao ~] # getfattr dir1
[ root@wangyao ~] #
```

- 13 Попробуйте создать в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`

Объясните, почему вы получили отказ в выполнении операции по созданию файла?

Оцените, как сообщение об ошибке отразилось на создании файла? Проверьте командой `ls -l /home/guest/dir1`

действительно ли файл file1 не находится внутри директории dir1

```
[root@wangyao ~]# chmod 755 dir1
[root@wangyao ~]# echo "echo" > /dir1/file1
-bash: /dir1/file1: 没有那个文件或目录
[root@wangyao ~]# echo "echo" > /home/dir1/file1
-bash: /home/dir1/file1: 没有那个文件或目录
[root@wangyao ~]# ls -ld dir1
drwxr-xr-x. 2 root root 6 9月  9 15:05 dir1
[root@wangyao ~]# ls -ld /home/dir1
ls: 无法访问/home/dir1: 没有那个文件或目录
[root@wangyao ~]# echo "test" > /root/dir1/file1
[root@wangyao ~]# ls -l /root/dir1
总用量 4
-rw-r--r--. 1 root root 5 9月  9 15:17 file1
[root@wangyao ~]# █
```

3. таблицы прав доступа

- 14 Заполните таблицу «Установленные права и разрешённые действия» (см. табл. 2.1), выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-». Замечание 1: при

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
|------------------|-------------|----------------|----------------|---------------|--------------|------------------|------------------------------|----------------------|-----------------------|
| d (000) (0) | 0 | - | - | - | - | - | - | - | - |
| d-x (001) (1) | 0 | - | - | - | - | + | - | - | - |
| d--x (001) (1) | 0 | - | - | - | - | + | - | - | - |
| d---x (001) (1) | 0 | - | - | - | - | + | - | - | - |
| d r (100) (4) | 0 | - | - | - | + | - | + | - | - |
| d r-x (101) (5) | 0 | - | - | - | + | + | + | - | - |
| d rw (110) (6) | 0 | - | - | + | + | - | + | - | - |
| d rw-x (111) (7) | 0 | - | - | + | + | + | + | - | - |
| d rwx (111) (7) | 0 | + | + | + | + | + | + | + | + |
| d (000) (0) | 100 | - | - | - | + | - | + | - | - |
| d-x (001) (1) | 100 | - | - | - | + | + | + | - | - |
| d--x (001) (1) | 100 | - | - | - | + | + | + | - | - |
| d---x (001) (1) | 100 | - | - | - | + | + | + | - | - |
| d r (100) (4) | 100 | - | - | - | + | - | + | - | - |
| d r-x (101) (5) | 100 | - | - | - | + | + | + | - | - |
| d rw (110) (6) | 100 | - | - | + | + | - | + | - | - |
| d rw-x (111) (7) | 100 | - | - | + | + | + | + | - | - |
| d rwx (111) (7) | 100 | + | + | + | + | + | + | + | + |
| d (000) (0) | 200 | - | - | - | + | - | + | - | - |
| d-x (001) (1) | 200 | - | - | - | + | + | + | - | - |

| Права директории | Права файла | Создание файла | Удаление файла | Запись в файл | Чтение файла | Смена директории | Просмотр файлов в директории | Переименование файла | Смена атрибутов файла |
|------------------|-------------|----------------|----------------|---------------|--------------|------------------|------------------------------|----------------------|-----------------------|
| d --x (001) (1) | 200 | - | - | - | + | + | + | - | - |
| d ---x (001) (1) | 200 | - | - | - | + | + | + | - | - |
| d r (100) (4) | 200 | - | - | - | + | - | + | - | - |
| d r-x (101) (5) | 200 | - | - | - | + | + | + | - | - |
| d rw (110) (6) | 200 | - | - | + | + | - | + | - | - |
| d rw-x (111) (7) | 200 | - | - | + | + | + | + | - | - |
| d rwx (111) (7) | 200 | + | + | + | + | + | + | + | + |

- 15 На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения операций внутри директории dir1, заполните табл. 2.2

| Операция | Минимальные права на директорию | Минимальные права на файл |
|------------------------|---------------------------------|---------------------------|
| Создание файла | d -wx | 000 |
| Удаление файла | d -wx | 000 |
| Чтение файла | d -x | 400 (1) |
| Запись в файл | d -x | 200 (2) |
| Переименование файла | d -wx | 000 |
| Создание поддиректории | d -wx | 000 |
| Удаление поддиректории | d -wx | 000 |

4. Выводы

Получил практические навыки работы с атрибутами файлов в консоли и закрепите теоретические основы дискреционного контроля доступа в современных системах с открытым исходным кодом на базе операционной системы Linux.