

Отчет по лабораторной работе №2

Дискреционные разграничения прав в Linux. Основные атрибуты

Евсеева Дарья Олеговна

17 сентября, 2022

Содержание

Цель работы	4
Задание	5
Теоретическое введение	6
Выполнение лабораторной работы	7
1. Создание пользователя	7
2. Работа с директориями	9
3. Заполнение таблиц прав доступа.	11
Выводы	16
Список литературы	17

Список иллюстраций

1	Создание пользователя guest	7
2	Установка пароля для пользователя guest	7
3	Вход в систему через пользователя guest	7
4	Определение текущей директории	8
5	Уточнение имени пользователя	8
6	Просмотр информации о пользователе	8
7	Просмотр файла /etc/passwd (1)	9
8	Просмотр файла /etc/passwd (2)	9
9	Просмотр директорий в системе	9
10	Просмотр расширенных атрибутов	10
11	Создание поддиректории dir1	10
12	Проверка прав доступа и расширенных атрибутов dir1	10
13	Снятие атрибутов с директории	10
14	Проверка возможности создания файла	10
15	Проверка наличия файла в директории	11
16	Создание файла и проверка прав и действий	11
17	Проверка прав и действий (1)	12
18	Проверка прав и действий (2)	12
19	Проверка прав и действий (3)	12
20	Проверка прав и действий (4)	13
21	Установленные права и действия (1)	13
22	Установленные права и действия (2)	14
23	Установленные права и действия (3)	14
24	Установленные права и действия (4)	15
25	Минимальные права для совершения операций	15

Цель работы

Целью данной работы является 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.

Задание

1. Создать гостевого пользователя.
2. Провести работу с директориями от имени гостевого пользователя.
3. Заполнить таблицы прав доступа.

Теоретическое введение

Дискреционное разграничение доступа — подход к разграничению доступа, предполагающий назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей.

Выполнение лабораторной работы

Выполнять работу будем в операционной системе, установленной при выполнении предыдущей лабораторной работы.

1. Создание пользователя

Для начала, используя учетную запись администратора, создадим пользователя guest с помощью команды useradd.

```
[doevseeva@doevseeva ~]$ su
Password:
[root@doevseeva doevseeva]# useradd guest
```

Рис. 1: Создание пользователя guest

Далее установим пароль для созданного пользователя.

```
[root@doevseeva doevseeva]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password fails the dictionary check - it does not contain enough DIFFERENT characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@doevseeva doevseeva]#
```

Рис. 2: Установка пароля для пользователя guest

Войдем в систему от имени созданного пользователя guest.

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

Рис. 3: Вход в систему через пользователя guest

Выполним команду `pwd`, чтобы определить текущую директорию.

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

Рис. 4: Определение текущей директории

Мы видим, что директория является домашней директорией для пользователя `guest` и совпадает с приглашением командной строки.

Выполним команду `whoami` для уточнения имени пользователя.

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

Рис. 5: Уточнение имени пользователя

Далее выполним команду `id` для просмотра информации о пользователе. Также проверим вывод команды `groups`.

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

Рис. 6: Просмотр информации о пользователе

Здесь мы видим, что имя пользователя — `guest`, значение `uid` равняется `1001(guest)`, значение `gid` равняется `1001(guest)`, также пользователь входит в единственную группу — `1001(guest)`. Выводы обеих команд соотносятся друг с другом.

Полученные данные также соответствуют данным в приглашении командной строки.

Посмотрим содержимое файла `/etc/passwd`.


```
[guest@doevseeva ~]$
[guest@doevseeva ~]$ 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
```

Рис. 7: Просмотр файла /etc/passwd (1)

```
doevseeva:x:1000:1000:doevseeva:/home/doevseeva:/bin/bash
vboxadd:x:976:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
[guest@doevseeva ~]$
```

Рис. 8: Просмотр файла /etc/passwd (2)

Мы видим, что в последней строке вывода содержится информация о текущем пользователе guest. Значение uid равняется 1001 и значение gid равняется 1001, что совпадает с данными, полученными ранее.

2. Работа с директориями

Определим существующие в системе директории.

```
[guest@doevseeva ~]$ ls -l /home/
total 4
drwx-----. 14 doevseeva doevseeva 4096 Sep 17 13:52 doevseeva
drwx-----.  4 guest      guest      92 Sep 17 14:11 guest
[guest@doevseeva ~]$
```

Рис. 9: Просмотр директорий в системе

Нам удалось получить список поддиректорий директории /home, и мы видим, что в системе есть домашние директории пользователей doevseeva и guest. У обеих директорий установлены права на чтение, запись и исполнение для пользователя.

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home.

```
[guest@doevseeva ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/doevseeva
----- /home/guest
[guest@doevseeva ~]$
```

Рис. 10: Просмотр расширенных атрибутов

Нам удалось получить только данные о домашней директории текущего пользователя `guest`, и можно видеть, что установленных расширенных атрибутов нет. Данные о домашней директории пользователя `doevseeva` не были получены.

Создадим в домашней директории поддиректорию `dir1`.

```
[guest@doevseeva ~]$ mkdir dir1
[guest@doevseeva ~]$ ls
dir1
[guest@doevseeva ~]$
```

Рис. 11: Создание поддиректории `dir1`

Далее определим, какие права доступа и расширенные атрибуты были выставлены на созданную директорию.

```
[guest@doevseeva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 17 14:19 dir1
[guest@doevseeva ~]$ lsattr
----- ./dir1
[guest@doevseeva ~]$
```

Рис. 12: Проверка прав доступа и расширенных атрибутов `dir1`

Снимем с созданной директории все атрибуты.

```
[guest@doevseeva ~]$ chmod 000 dir1
[guest@doevseeva ~]$ ls -l
total 0
d----- . 2 guest guest 6 Sep 17 14:19 dir1
[guest@doevseeva ~]$
```

Рис. 13: Снятие атрибутов с директории

Далее попытаемся создать внутри директории файл.

```
[guest@doevseeva ~]$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
[guest@doevseeva ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
```

Рис. 14: Проверка возможности создания файла

Как мы видим, в доступе было отказано, так как мы сняли все атрибуты с директории, также из-за этого мы не можем увидеть, действительно ли не создан файл.

Добавим к директории право на чтение и проверим список файлов в ней.

```
[guest@doevseeva ~]$ chmod u+r dir1
[guest@doevseeva ~]$ ls -l /home/guest/dir1
total 0
[guest@doevseeva ~]$
```

Рис. 15: Проверка наличия файла в директории

Мы видим, что директория действительно пуста.

3. Заполнение таблиц прав доступа.

Заполним таблицу “Установленные права и разрешенные действия”, выполняя действия от имени владельца директории (файлов), определив опытным путем, какие операции разрешены, а какие нет.

Для начала вернем директории все права доступа для пользователя и создадим в ней файл для дальнейшей проверки действий. Затем приступим к заполнению таблицы.

```
[guest@doevseeva ~]$ chmod 700 dir1
[guest@doevseeva ~]$ ls
dir1
[guest@doevseeva ~]$ echo "test" > /home/guest/dir1/file1
[guest@doevseeva ~]$ ls -l /home/guest/dir1
ls: cannot access '/home/guest/dir1': No such file or directory
[guest@doevseeva ~]$ ls -l /home/guest/dir1
total 4
-rw-r--r--. 1 guest guest 5 Sep 17 14:40 file1
[guest@doevseeva ~]$ chmod 000 dir1/file1
[guest@doevseeva ~]$ ls -l /home/guest/dir1
total 4
----- 1 guest guest 5 Sep 17 14:40 file1
[guest@doevseeva ~]$
[guest@doevseeva ~]$ chmod 200 dir1
[guest@doevseeva ~]$ ls -l
total 0
d-w----- 2 guest guest 19 Sep 17 14:40 dir1
[guest@doevseeva ~]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest@doevseeva ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
```

Рис. 16: Создание файла и проверка прав и действий

```
[guest@doevseeva ~]$ chmod 500 dir1/
[guest@doevseeva ~]$ ls -l
total 0
dr-x-----. 2 guest guest 19 Sep 17 15:45 dir1
[guest@doevseeva ~]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest@doevseeva ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@doevseeva ~]$ echo "dddd" > dir1/file1
[guest@doevseeva ~]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest@doevseeva ~]$ cd dir1/
[guest@doevseeva dir1]$ ls
file1
[guest@doevseeva dir1]$ cd ..
[guest@doevseeva ~]$ mv dir1/file1 dir1/file2
mv: cannot move 'dir1/file1' to 'dir1/file2': Permission denied
[guest@doevseeva ~]$
[guest@doevseeva ~]$ chmod 100 dir1/file1
[guest@doevseeva ~]$ chmod 200 dir1/file1
```

Рис. 17: Проверка прав и действий (1)

```
[guest@doevseeva ~]$ chmod 300 dir1/file1
[guest@doevseeva ~]$ ls -l dir1/
total 4
--wx-----. 1 guest guest 8 Sep 17 15:51 file1
[guest@doevseeva ~]$
[guest@doevseeva ~]$
[guest@doevseeva ~]$ chmod 000 dir1/
[guest@doevseeva ~]$ ls -l
total 0
d-----.. 2 guest guest 19 Sep 17 15:51 dir1
[guest@doevseeva ~]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest@doevseeva ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@doevseeva ~]$ echo "sss" > dir1/file1
-bash: dir1/file1: Permission denied
[guest@doevseeva ~]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest@doevseeva ~]$ cd dir1/
-bash: cd: dir1/: Permission denied
```

Рис. 18: Проверка прав и действий (2)

```
[guest@doevseeva ~]$ cd dir1/
-bash: cd: dir1/: Permission denied
[guest@doevseeva ~]$ ls dir1/
ls: cannot open directory 'dir1/': Permission denied
[guest@doevseeva ~]$ mv dir1/file1 dir1/file2
mv: failed to access 'dir1/file2': Permission denied
[guest@doevseeva ~]$ chmod 000 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
```

Рис. 19: Проверка прав и действий (3)

```
[guest@doevseeva ~]$ chmod 700 dir1/
[guest@doevseeva ~]$ ls -l
total 0
drwx-----. 2 guest guest 19 Sep 17 16:51 dir1
[guest@doevseeva ~]$ touch dir1/file2
[guest@doevseeva ~]$ rm dir1/file2
[guest@doevseeva ~]$ echo "ooooool" > dir1/file1
[guest@doevseeva ~]$ cat dir1/file1
ooooool
[guest@doevseeva ~]$ cd dir1/
[guest@doevseeva dir1]$ ls
file1
[guest@doevseeva dir1]$ cd ..
[guest@doevseeva ~]$ mv dir1/file1 dir1/file2
[guest@doevseeva ~]$ mv dir1/file2 dir1/file1
[guest@doevseeva ~]$ chmod 000 dir1/file1
[guest@doevseeva ~]$
```

Рис. 20: Проверка прав и действий (4)

Итак, закончим заполнение таблицы “Установленные права и действия”.

Установленные права и разрешенные действия									
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)	- - - - - (000)	-	-	-	-	-	-	-	-
d--x----- (100)	- - - - - (000)	-	-	-	-	+	-	-	+
d-w----- (200)	- - - - - (000)	-	-	-	-	-	-	-	-
d-wx----- (300)	- - - - - (000)	+	+	-	-	+	-	+	+
dr----- (400)	- - - - - (000)	-	-	-	-	-	+	-	-
d-x----- (500)	- - - - - (000)	+	-	-	-	+	+	-	+
drw----- (600)	- - - - - (000)	-	-	-	-	-	+	-	-
drwx----- (700)	- - - - - (000)	+	+	-	-	+	+	+	+
d----- (000)	- --x----- (100)	-	-	-	-	-	-	-	-
d--x----- (100)	- --x----- (100)	-	-	-	-	+	-	-	+
d-w----- (200)	- --x----- (100)	-	-	-	-	-	-	-	-
d-wx----- (300)	- --x----- (100)	+	+	-	-	+	-	+	+
dr----- (400)	- --x----- (100)	-	-	-	-	-	+	-	-
d-x----- (500)	- --x----- (100)	-	-	-	-	+	+	-	+
drw----- (600)	- --x----- (100)	-	-	-	-	-	+	-	-
drwx----- (700)	- --x----- (100)	+	+	-	-	+	+	+	+

Рис. 21: Установленные права и действия (1)

d----- (000)	- -w----- (200)	-	-	-	-	-	-	-	-
d-x----- (100)	- -w----- (200)	-	-	+	-	+	-	-	+
d-w----- (200)	- -w----- (200)	-	-	-	-	-	-	-	-
d-wx----- (300)	- -w----- (200)	+	+	+	+	+	-	+	+
dr----- (400)	- -w----- (200)	-	-	-	-	-	+	-	-
d-x----- (500)	- -w----- (200)	-	-	+	-	+	+	-	+
drw----- (600)	- -w----- (200)	-	-	-	-	-	+	-	-
drwx----- (700)	- -w----- (200)	+	+	+	-	+	+	+	+
d----- (000)	- -wx----- (300)	-	-	-	-	-	-	-	-
d-x----- (100)	- -wx----- (300)	-	-	+	-	+	-	-	+
d-w----- (200)	- -wx----- (300)	-	-	-	-	-	-	-	-
d-wx----- (300)	- -wx----- (300)	+	+	+	-	+	-	+	+
dr----- (400)	- -wx----- (300)	-	-	-	-	-	+	-	-
d-x----- (500)	- -wx----- (300)	-	-	+	-	+	+	-	+
drw----- (600)	- -wx----- (300)	-	-	-	-	-	+	-	-
drwx----- (700)	- -wx----- (300)	+	+	+	-	+	+	+	+
d----- (000)	- r----- (400)	-	-	-	-	-	-	-	-
d-x----- (100)	- r----- (400)	-	-	-	+	+	-	-	+

Рис. 22: Установленные права и действия (2)

d-w----- (200)	- r----- (400)	-	-	-	-	-	-	-	-
d-wx----- (300)	- r----- (400)	+	+	-	+	+	-	+	+
dr----- (400)	- r----- (400)	-	-	-	-	-	+	-	-
d-x----- (500)	- r----- (400)	-	-	-	+	+	+	-	+
drw----- (600)	- r----- (400)	-	-	-	-	-	+	-	-
drwx----- (700)	- r----- (400)	+	+	-	+	+	+	+	+
d----- (000)	- r-x----- (500)	-	-	-	-	-	-	-	-
d-x----- (100)	- r-x----- (500)	-	-	-	+	+	-	-	+
d-w----- (200)	- r-x----- (500)	-	-	-	-	-	-	-	-
d-wx----- (300)	- r-x----- (500)	+	+	-	+	+	-	+	+
dr----- (400)	- r-x----- (500)	-	-	-	-	-	+	-	-
d-x----- (500)	- r-x----- (500)	-	-	-	+	+	+	-	+
drw----- (600)	- r-x----- (500)	-	-	-	-	-	+	-	-
drwx----- (700)	- r-x----- (500)	+	+	-	+	+	+	+	+
d----- (000)	- rw----- (600)	-	-	-	-	-	-	-	-
d-x----- (100)	- rw----- (600)	-	-	+	+	+	-	-	+
d-w----- (200)	- rw----- (600)	-	-	-	-	-	-	-	-
d-wx----- (300)	- rw----- (600)	+	+	+	+	+	-	+	+

Рис. 23: Установленные права и действия (3)

dr----- (400)	- rw----- (600)	-	-	-	-	-	+	-	-
d-x----- (500)	- rw----- (600)	-	-	+	+	+	+	-	+
drw----- (600)	- rw----- (600)	-	-	-	-	-	+	-	-
drwx----- (700)	- rw----- (600)	+	+	+	+	+	+	+	+
d----- (000)	- rwx----- (700)	-	-	-	-	-	-	-	-
d--x----- (100)	- rwx----- (700)	-	-	+	+	+	-	-	+
d-w----- (200)	- rwx----- (700)	-	-	-	-	-	-	-	-
d-wx----- (300)	- rwx----- (700)	+	+	+	+	+	-	+	+
dr----- (400)	- rwx----- (700)	-	-	-	-	-	+	-	-
d-x----- (500)	- rwx----- (700)	-	-	+	+	+	+	-	+
drw----- (600)	- rwx----- (700)	-	-	-	-	-	+	-	-
drwx----- (700)	- rwx----- (700)	+	+	+	+	+	+	+	+

Рис. 24: Установленные права и действия (4)

Теперь, на основании заполненной таблицы определим те или иные минимально необходимые права для выполнения операций внутри директории и заполним таблицу “Минимальные права для совершения операций”.

Минимальные права для совершения операций

Операция	Минимальные права на директо- рию	Минимальные права на файл
Создание файла	300	000
Удаление файла	300	000
Чтение файла	100	200
Запись в файл	100	200
Переименование файла	300	000
Создание поддиректории	300	000
Удаление поддиректории	300	000

Рис. 25: Минимальные права для совершения операций

Выводы

В результате проделанной работы мы приобрели практические навыки работы в консоли с атрибутами файлов и закрепили теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

- Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” <https://esystem.rudn.ru/>