

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Аскеров Александр Эдуардович

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	15
	Список литературы	16

Список иллюстраций

2.1	Создание учётной записи guest	6
2.2	Указание пароля	6
2.3	Переключение на пользователя guest	6
2.4	Текущая директория	7
2.5	Переход в домашнюю директорию	7
2.6	Отображение имени пользователя	7
2.7	Команда id	7
2.8	Команда groups	8
2.9	Просмотр /etc/passwd	8
2.10	Существующие в системе директории	8
2.11	Просмотр расширенных атрибутов директории	9
2.12	Создание поддиректории dir1	9
2.13	Права на директорию dir1	10
2.14	Изменение доступа к dir1	10
2.15	Отображение прав доступа	10
2.16	Попытка создания файла в dir1	10
2.17	Попытка просмотреть содержимое dir1	11

Список таблиц

2.1	Установленные права и разрешённые действия	11
2.2	Минимальные права для совершения операций	13

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

В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора).

```
[root@aeaskerov ~]# useradd guest  
[root@aeaskerov ~]#
```

Рис. 2.1: Создание учётной записи guest

Зададим пароль для пользователя guest.

```
[root@aeaskerov ~]# passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@aeaskerov ~]#
```

Рис. 2.2: Указание пароля

Войдём в систему от имени пользователя guest.

```
[root@aeaskerov ~]# su guest  
[guest@aeaskerov root]$
```

Рис. 2.3: Переключение на пользователя guest

Определим директорию, в которой находимся, командой pwd.

```
[guest@aeaskerov root]$ pwd
/root
[guest@aeaskerov root]$
```

Рис. 2.4: Текущая директория

Отображённая директория не является домашней, поэтому теперь перейдём в домашнюю.

```
[guest@aeaskerov root]$ cd
[guest@aeaskerov ~]$
```

Рис. 2.5: Переход в домашнюю директорию

Уточним имя пользователя командой `whoami`.

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

Рис. 2.6: Отображение имени пользователя

Уточним имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`.

```
[guest@aeaskerov ~]$ id
uid=1007(guest) gid=100(users) groups=100(users) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@aeaskerov ~]$
```

Рис. 2.7: Команда `id`

Выполним команду `groups`.

```
[guest@aeaskerov ~]$ groups
users
[guest@aeaskerov ~]$
```

Рис. 2.8: Команда groups

Команда groups просто показывает, к каким группам относится текущий пользователь. А команда id используется для определения имен пользователей и групп, а также числовых идентификаторов (UID или идентификатор группы) пользователя.

Полученная информация об имени пользователя и данные, выводимые в приглашении командной строки, совпадают.

Посмотрим информацию о guest в файле /etc/passwd.

```
[guest@aeaskerov ~]$ cat /etc/passwd | grep guest
guest:x:1007:100::/home/guest:/bin/bash
[guest@aeaskerov ~]$
```

Рис. 2.9: Просмотр /etc/passwd

UID равен 1007, GID равен 100. Эти значения совпадают со значениями, показанными командой id.

Определим существующие в системе директории.

```
[guest@aeaskerov ~]$ ls -l /home/
total 4
drwx-----. 15 aeaskerov aeaskerov 4096 Mar  2 16:25 aeaskerov
drwx-----.  6 alice      users      146 Sep 20 18:54 alice
drwx-----.  6 bob       users      146 Sep 24 18:58 bob
drwx-----.  6 carol     users      146 Sep 20 18:54 carol
drwx-----.  5 dan       users      111 Sep 20 12:35 dan
drwx-----.  5 dave      users      111 Sep 20 12:35 dave
drwx-----.  5 david     users      111 Sep 20 12:36 david
drwx-----.  6 guest     users      125 Mar  2 16:46 guest
drwx-----.  3 alice     alice      78 Sep  9 16:57 Hope
drwx-----.  3 bob       bob        78 Sep  9 21:00 Tom
drwxr-xr-x.  2 root      root        6 Sep 24 19:55 users
[guest@aeaskerov ~]$
```

Рис. 2.10: Существующие в системе директории

Список поддиректорий директории /home получить не удалось. Установленные права (read, write, execute) позволяют только владельцам взаимодействовать с директориями.

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

```
[guest@aeaskerov ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/aeaskerov
lsattr: Permission denied While reading flags on /home/Hope
lsattr: Permission denied While reading flags on /home/Tom
lsattr: Permission denied While reading flags on /home/alice
lsattr: Permission denied While reading flags on /home/bob
lsattr: Permission denied While reading flags on /home/carol
lsattr: Permission denied While reading flags on /home/dan
lsattr: Permission denied While reading flags on /home/dave
lsattr: Permission denied While reading flags on /home/david
----- /home/users
----- /home/guest
[guest@aeaskerov ~]$
```

Рис. 2.11: Просмотр расширенных атрибутов директории

Их не удалось посмотреть из-за отказа в доступе как у guest, так и у других пользователей.

Создадим в домашней директории поддиректорию dir1.

```
[guest@aeaskerov ~]$ mkdir dir1
[guest@aeaskerov ~]$
```

Рис. 2.12: Создание поддиректории dir1

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

```
[guest@aeaskerov ~]$ ls -l
total 0
drwxr-xr-x. 2 guest users 6 Mar  2 16:50 dir1
drwxr-xr-x. 2 guest users 6 Sep 12 10:17 Documents
drwxr-xr-x. 2 guest users 6 Sep 12 10:17 Pictures
[guest@aeaskerov ~]$ lsattr
----- ./Pictures
----- ./Documents
----- ./dir1
[guest@aeaskerov ~]$
```

Рис. 2.13: Права на директорию dir1

Снимем с директории dir1 все атрибуты.

```
[guest@aeaskerov ~]$ chmod 000 dir1
[guest@aeaskerov ~]$
```

Рис. 2.14: Изменение доступа к dir1

Отообразим права доступа к dir1.

```
[guest@aeaskerov ~]$ ls -l
total 0
d----- . 2 guest users 6 Mar  2 16:50 dir1
drwxr-xr-x. 2 guest users 6 Sep 12 10:17 Documents
drwxr-xr-x. 2 guest users 6 Sep 12 10:17 Pictures
[guest@aeaskerov ~]$
```

Рис. 2.15: Отображение прав доступа

Попытаемся создать в директории dir1 файл file1.

```
[guest@aeaskerov ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@aeaskerov ~]$
```

Рис. 2.16: Попытка создания файла в dir1

В доступе отказано, так как мы запретили запись в директорию dir1.

Оценим, как сообщение об ошибке отразилось на создании файла.

```
[guest@aeaskerov ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@aeaskerov ~]$
```

Рис. 2.17: Попытка посмотреть содержимое dir1

Заполним таблицу «Установленные права и разрешённые действия», выполняя действия от имени владельца директории (файлов), определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, внесём в таблицу знак «+», если не разрешена, знак «-».

Таблица 2.1: Установленные права и разрешённые действия

Права директории	Права файла	1	2	3	4	5	6	7	8
d------(000)	------(000)	-	-	-	-	-	-	-	-
d--x------(100)	------(000)	-	-	-	-	+	-	-	+
d-w------(200)	------(000)	-	-	-	-	-	-	-	-
d-wx------(300)	------(000)	+	+	-	-	+	-	+	+
dr------(400)	------(000)	-	-	-	-	-	-	-	-
dr-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)	-	-	-	-	-	-	-	-
dr-x------(500)	---x------(100)	-	-	-	-	+	+	-	+
drw------(600)	---x------(100)	-	-	-	-	-	-	-	-
drwx------(700)	---x------(100)	+	+	-	-	+	+	+	+
d------(000)	--w------(200)	-	-	-	-	-	-	-	-
d--x------(100)	--w------(200)	-	-	+	-	+	-	-	+

Права директории	Права файла	1	2	3	4	5	6	7	8
d-w------(200)	--w------(200)	-	-	-	-	-	-	-	-
d-wx------(300)	--w------(200)	+	+	+	-	+	-	+	+
dr------(400)	--w------(200)	-	-	-	-	-	-	-	-
dr-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)	-	-	-	-	-	-	-	-
dr-x------(500)	--wx------(300)	-	-	+	-	+	+	-	+
drw------(600)	--wx------(300)	-	-	-	-	-	-	-	-
drwx------(700)	--wx------(300)	+	+	+	-	+	+	+	+
d------(000)	-r------(400)	-	-	-	-	-	-	-	-
d--x------(100)	-r------(400)	-	-	-	+	+	-	-	+
d-w------(200)	-r------(400)	-	-	-	-	-	-	-	-
d-wx------(300)	-r------(400)	+	+	-	+	+	-	+	+
dr------(400)	-r------(400)	-	-	-	-	-	-	-	-
dr-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)	-	-	-	-	-	-	-	-

Права директории	Права файла	1	2	3	4	5	6	7	8
dr-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)	+	+	+	+	+	-	+	+
dr----- (400)	-rw----- (600)	-	-	-	-	-	-	-	-
dr-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)	-	-	-	-	-	-	-	-
dr-x----- (500)	-rwx----- (700)	-	-	+	+	+	+	-	+
drw----- (600)	-rwx----- (700)	-	-	-	-	-	-	-	-
drwx----- (700)	-rwx----- (700)	+	+	+	+	+	+	+	+

На основании заполненной таблицы определим минимально необходимые права для выполнения операций внутри директории dir1, заполним таблицу 2.2.

Таблица 2.2: Минимальные права для совершения операций

Операция	Права на директорию	Права на файл
Создание файла	d-wx----- (300)	----- (000)
Удаление файла	d-wx----- (300)	----- (000)
Чтение файла	d--x----- (100)	-r----- (400)

Операция	Права на директорию	Права на файл
Запись в файл	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)
Удаление поддиректории	d-wx----- (300)	----- (000)

3 Выводы

Получены практические навыки работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. How to manage Linux permissions for users, groups, and others