

Лабораторная работа № 2

Дискреционное разграничение прав в Linux. Основные атрибуты

Беличева Дарья Михайловна

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	18
	Список литературы	19

Список иллюстраций

3.1	Создание учетной записи пользователя guest и задание пароля . .	8
3.2	Вход в систему от имени пользователя guest	9
3.3	Ввод пароля для пользователя guest	9
3.4	Определение директории, имени пользователя, группы и их идентификаторов	10
3.5	Просмотр файла /etc/passwd	10
3.6	Существующие в системе директории, их права и расширенные атрибуты	11
3.7	Создание директории dir1 и определение ее прав	11
3.8	Лишение всех прав директории dir1	12
3.9	Попытка создание файла в директории dir1	12
3.10	Определения разрешенных действий с различными правами . . .	13

Список таблиц

3.1	Установленные права и разрешённые действия	14
3.2	Минимальные права для совершения операций	17

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 Теоретическое введение

В Linux, как и в любой многопользовательской системе, абсолютно естественным образом возникает задача разграничения доступа субъектов — пользователей к объектам — файлам дерева каталогов.

Один из подходов к разграничению доступа — так называемый дискреционный (от англ. *discretion* — чье-либо усмотрение) — предполагает 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 в (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей [1].

Основная команда для работы с правами в Linux: `chmod`. Есть три основных вида прав:

- `r` – чтение;
- `w` – запись;
- `x` – выполнение;
- `s` – выполнение от имени суперпользователя (дополнительный);

Также есть три категории пользователей, для которых вы можете установить эти права на файл `linux`:

- `u` – владелец файла;
- `g` – группа файла;

- 0 – все остальные пользователи.

3 Выполнение лабораторной работы

В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest (используя учётную запись администратора) с помощью команды `useradd guest`. Зададим пароль для пользователя guest командой `passwd guest` (рис. 3.1).

```
[dmbelicheva@dmbelicheva ~]$ sudo -i
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for dmbelicheva:
[root@dmbelicheva ~]# useradd guest
[root@dmbelicheva ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
[root@dmbelicheva ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@dmbelicheva ~]#
```

Рис. 3.1: Создание учетной записи пользователя guest и задание пароля

Войдем в систему от имени пользователя guest (рис. 3.2, 3.3).

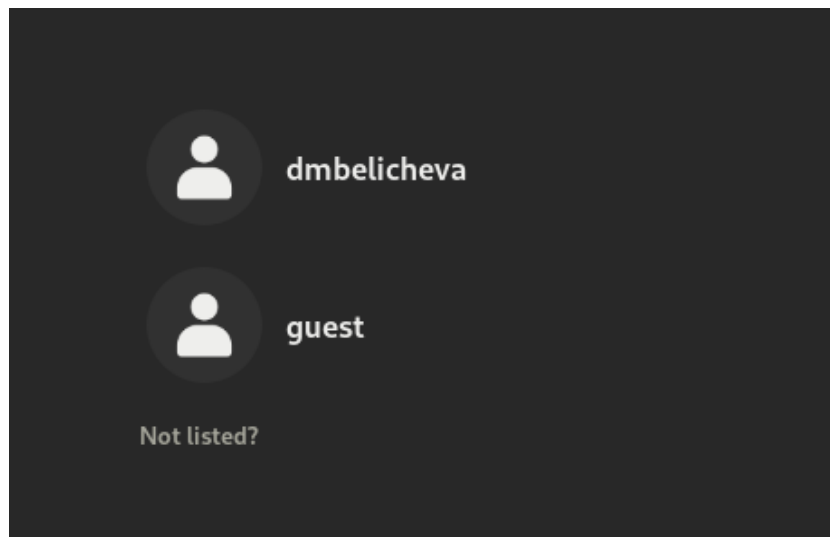


Рис. 3.2: Вход в систему от имени пользователя guest

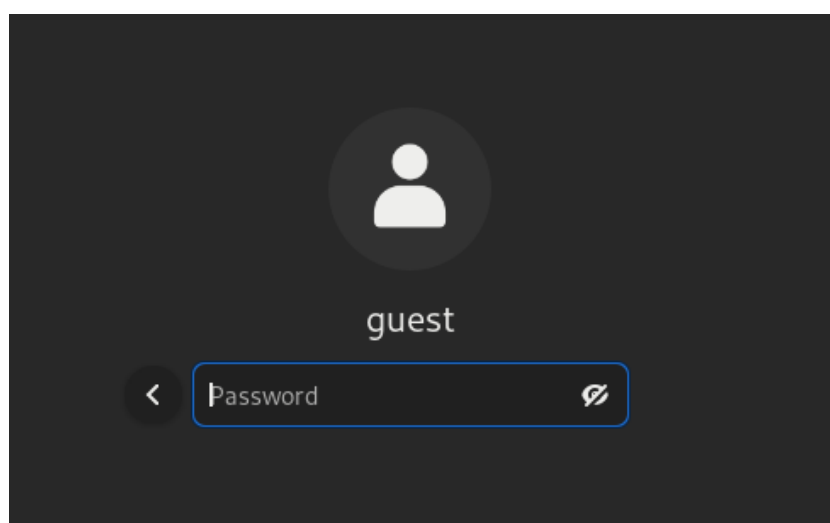


Рис. 3.3: Ввод пароля для пользователя guest

Определим директорию, в которой находимся, командой `pwd`. Мы находимся в директории `/home/guest`. Сравнив её с приглашением командной строки, увидим что они идентичны (`guest`). Также с помощью команды `cd ~` определим, что директория, в которой мы находимся, является домашней директорией. Уточним имя пользователя командой `whoami`, увидим имя `guest`. Уточним имя пользовате-

ля, его группу, а также группы, куда входит пользователь, командой `id` (рис. 3.4). Увидим, что имя пользователя `guest`, его `uid` - 1001, группа также называется `guest`, ее `gid` - 1001. Сравним вывод `id` с выводом команды `groups`, вывод идентичен.

```
[guest@dmbelicheva ~]$ pwd
/home/guest
[guest@dmbelicheva ~]$ cd
[guest@dmbelicheva ~]$ cd ~
[guest@dmbelicheva ~]$ whoami
guest
[guest@dmbelicheva ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@dmbelicheva ~]$ groups
guest
```

Рис. 3.4: Определение директории, имени пользователя, группы и их идентификаторов

Посмотрим файл `/etc/passwd` командой `cat /etc/passwd` (рис. 3.5). Найдем в нём свою учётную запись, определим `uid` пользователя и `gid` пользователя. Используем программу `grep` в качестве фильтра. Сравнив найденные значения с полученными в предыдущих пунктах, увидим, что они одинаковы.

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

Рис. 3.5: Просмотр файла `/etc/passwd`

Определим существующие в системе директории командой `ls -l /home/` (рис. 3.6). Нам удалось получить список поддиректорий `/home`, а именно там находится две директории `dmbelicheva` и `guest`. У этих поддиректорий есть все права (`rwX`) для пользователя, для групп и других прав нет.

Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой `lsattr /home`. Нам удалось увидеть расширенные атрибуты директории `guest` (их нет), но доступа к директории `dmbelicheva` у нас нет.

```
[guest@dmbelicheva ~]$ ls -l /home/
total 8
drwx-----. 14 dmbelicheva dmbelicheva 4096 Sep 13 18:43 dmbelicheva
drwx-----. 14 guest      guest      4096 Sep 13 18:49 guest
[guest@dmbelicheva ~]$ lsattr /home
lsattr: Permission denied while reading flags on /home/dmbelicheva
----- /home/guest
[guest@dmbelicheva ~]$
```

Рис. 3.6: Существующие в системе директории, их права и расширенные атрибуты

Создадим в домашней директории поддиректорию `dir1` командой `mkdir dir1`. Определим командами `ls -l` и `lsattr`, какие права доступа и расширенные атрибуты были выставлены на директорию `dir1` (рис. 3.7). На директорию `dir1` по умолчанию были выставлены права `drwxr-xr-x`, то есть для пользователя у нас доступны все права, для групп и других только чтение и выполнение.

```
[guest@dmbelicheva ~]$ mkdir dir1
[guest@dmbelicheva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Desktop
drwxr-xr-x. 2 guest guest 6 Sep 13 19:05 dir1
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Documents
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Music
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Public
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Templates
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Videos
[guest@dmbelicheva ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@dmbelicheva ~]$
```

Рис. 3.7: Создание директории `dir1` и определение ее прав

Теперь снимем с директории `dir1` все атрибуты командой `chmod 000 dir1` и

проверим правильность выполнения с помощью команды `ls -l` (рис. 3.8). Действительно, увидим, что у директории `dir1` теперь права `d---`, то есть нет прав.

```
[guest@dmbelicheva ~]$ chmod 000 dir1
[guest@dmbelicheva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Desktop
d------. 2 guest guest 6 Sep 13 19:05 dir1
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Documents
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Music
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Public
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Templates
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Videos
[guest@dmbelicheva ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@dmbelicheva ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@dmbelicheva ~]$
```

Рис. 3.8: Лишение всех прав директории `dir1`

При попытке создать в директории `dir1` файл `file1` командой `echo "test" > /home/guest/dir1/file1` мы получим отказ, так как у этой директории нет никаких прав, соответственно создавать в ней файлы мы не можем (рис. 3.9). Оценить, как сообщение об ошибке отразилось на создании файла командой `ls -l /home/guest/dir1`, так как мы не можем перейти в эту директории, нам отказано в доступе.

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

Рис. 3.9: Попытка создание файла в директории `dir1`

В табл. [3.1] приведены данные о том, какие операции разрешены, а какие нет для владельца данных.

Для заполнения таблицы, нам предлагалось опытным путем проверить, какие права позволяют выполнять те или иные действие (рис. 3.10).

```

[guest@dmbelicheva ~]$ cd /home/guest/dir1
[guest@dmbelicheva dir1]$ ls
[guest@dmbelicheva dir1]$ touch file1
[guest@dmbelicheva dir1]$ ls
file1
[guest@dmbelicheva dir1]$ echo "test" > /home/guest/dir1/file1
[guest@dmbelicheva dir1]$ cat file1
test
[guest@dmbelicheva dir1]$ lsattr file1
----- file1
[guest@dmbelicheva dir1]$ ls -l file1
-rw-r--r--. 1 guest guest 5 Sep 13 19:16 file1
[guest@dmbelicheva dir1]$ chmod +x file1
[guest@dmbelicheva dir1]$ ls -l file1
-rwxr-xr-x. 1 guest guest 5 Sep 13 19:16 file1
[guest@dmbelicheva dir1]$ chmod 000 file1
[guest@dmbelicheva dir1]$ cat file1
cat: file1: Permission denied
[guest@dmbelicheva dir1]$ echo "hello" > file1
bash: file1: Permission denied
[guest@dmbelicheva dir1]$ rm -r file1
rm: remove write-protected regular file 'file1'? y
[guest@dmbelicheva dir1]$ ls
[guest@dmbelicheva dir1]$ ls -l
total 0
[guest@dmbelicheva dir1]$ ls -l dir1
ls: cannot access 'dir1': No such file or directory
[guest@dmbelicheva dir1]$ cd ..
[guest@dmbelicheva ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Desktop
drwx-----. 2 guest guest 6 Sep 13 19:21 dir1
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Documents
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Music
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Public
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Templates
drwxr-xr-x. 2 guest guest 6 Sep 13 18:45 Videos
[guest@dmbelicheva ~]$ cd dir1
[guest@dmbelicheva dir1]$ touch file1
[guest@dmbelicheva dir1]$ ls

```

Рис. 3.10: Определения разрешенных действий с различными правами

Таблица 3.1: Установленные права и разрешённые действия

Права директории	Права файла	Про- Пе- Сме- смотр ре- на Сме- фай- име- ат- на лов в но- ри- зда- ле- За- Чте- ди- ди- ва- бу- ние ние пись ние рек- рек- ние тов фай- фай- в фай- то- то- фай- фай- ла ла файл ла рии рии ла ла							
		ла	ла	файл	ла	рии	рии	ла	ла
d(000)	(000)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	+	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(500)	(000)	-	-	-	-	+	+	-	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(600)	(000)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	+	+	+	+	+
d(000)	(100)	-	-	-	-	-	-	-	-
d(100)	(100)	-	-	-	-	+	-	-	+
d(200)	(100)	-	-	-	-	-	-	-	-
d(300)	(100)	+	+	-	-	+	-	+	+
d(400)	(100)	-	-	-	-	-	+	-	-
d(500)	(100)	-	-	-	-	+	+	-	+
d(600)	(100)	-	-	-	-	-	+	-	-
d(700)	(100)	+	+	-	-	+	+	+	+
d(000)	(200)	-	-	-	-	-	-	-	-
d(100)	(200)	-	-	+	-	+	-	-	+
d(200)	(200)	-	-	-	-	-	-	-	-

							Про- смотр	Пе- ре-	Сме- на	
							Сме- на	фай- лов в	име- но-	ат- ри-
							ди- рек-	ди- рек-	ва- ние	бу- тов
Права директории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	то- рии	то- рии	фай- ла	фай- ла	
d(300)	(200)	+	+	+	-	+	-	+	+	
d(400)	(200)	-	-	-	-	-	+	-	-	
d(500)	(200)	-	-	+	-	+	+	-	+	
d(600)	(200)	-	-	-	-	-	+	-	-	
d(700)	(200)	+	+	+	-	+	+	+	+	
d(000)	(300)	-	-	-	-	-	-	-	-	
d(100)	(300)	-	-	+	-	+	-	-	+	
d(200)	(300)	-	-	-	-	-	-	-	-	
d(300)	(300)	+	+	+	-	+	-	+	+	
d(400)	(300)	-	-	-	-	-	+	-	-	
d(500)	(300)	-	-	+	-	+	+	-	+	
d(600)	(300)	-	-	-	-	-	+	-	-	
d(700)	(300)	+	+	+	-	+	+	+	+	
d(000)	(400)	-	-	-	-	-	-	-	-	
d(100)	(400)	-	-	-	+	+	-	-	+	
d(200)	(400)	-	-	-	-	-	-	-	-	
d(300)	(400)	+	+	-	+	+	-	+	+	
d(400)	(400)	-	-	-	-	-	+	-	-	
d(500)	(400)	-	-	-	+	+	+	-	+	
d(600)	(400)	-	-	-	-	-	+	-	-	
d(700)	(400)	+	+	-	+	+	+	+	+	

Права директории	Права файла	<div> <div>Про- Пе- Сме-</div> <div>смотр ре- на</div> <div>Сме- фай- име- ат-</div> <div>на лов в но- ри-</div> <div>ди- ди- ва- бу-</div> <div>рек- рек- ние тов</div> </div>							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	ди- рек- то- рии	фай- ла	фай- ла
d(000)	(500)	-	-	-	-	-	-	-	-
d(100)	(500)	-	-	-	+	+	-	-	+
d(200)	(500)	-	-	-	-	-	-	-	-
d(300)	(500)	+	+	-	+	+	-	+	+
d(400)	(500)	-	-	-	-	-	+	-	-
d(500)	(500)	-	-	-	+	+	+	-	+
d(600)	(500)	-	-	-	-	-	+	-	-
d(700)	(500)	+	+	-	+	+	+	+	+
d(000)	(600)	-	-	-	-	-	-	-	-
d(100)	(600)	-	-	+	+	+	-	-	+
d(200)	(600)	-	-	-	-	-	-	-	-
d(300)	(600)	+	+	+	+	+	-	+	+
d(400)	(600)	-	-	-	-	-	+	-	-
d(500)	(600)	-	-	+	+	+	+	-	+
d(600)	(600)	-	-	-	-	-	+	-	-
d(700)	(600)	+	+	+	+	+	+	+	+
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(700)	-	-	-	-	-	+	-	-

Права директории	Права файла	Права на файлы				Права на директорию			
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Про- смотр фай- лов в ди- рек- то- рии	Пе- ре- име- но- ва- ние фай- ла	Сме- на ат- ри- бу- тов фай- ла
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(700)	+	+	+	+	+	+	+	+

В табл. [3.2] приведены данные о том, какие минимальные права должны быть для совершения различных действий.

Таблица 3.2: Минимальные права для совершения операций

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	(000)
Удаление файла	d(300)	(000)
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	(000)
Удаление поддиректории	d(300)	(000)

4 Выводы

В процессе выполнения данной лабораторной работы я получила практические навыки работы в консоли с атрибутами файлов, закрепила теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Дискреционное разграничение доступа Linux [Электронный ресурс]. 2023.
URL: <https://debianinstall.ru/diskretсионное-razgranichenie-dostupa-linux/>.