

Отчёт по лабораторной работе №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Абузярова Лейла Джамилевна НБИбд-01-19

Содержание

1	Цель работы	4
2	Выполнение лабораторной работы	5
3	Вывод	14
	Список литературы	15

List of Figures

2.1	Информация о пользователе guest	5
2.2	Определение директория	6
2.3	Сравнение выводов id и groups	6
2.4	Изучение файла /etc/passwd	7
2.5	Проверка на расширенные атрибуты	7
2.6	Проверка на расширенные атрибуты у dir1	8
2.7	Снятие атрибутов	8
2.8	Снятие атрибутов с директории	9
2.9	Заполнение таблицы	9

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.


```
guest@dabuziarova-
[1dabuziarova@dabuziarova ~]$ useradd guest
useradd: Permission denied.
[1dabuziarova@dabuziarova ~]$ su
[1dabuziarova@dabuziarova ~]$ useradd guest
[1dabuziarova@dabuziarova ~]$ passwd guest
Именем гостя:
Новый пароль:
Повторите еще раз пароль:
passwd: все данные аутентификации успешно обновлены.
[1dabuziarova@dabuziarova ~]$ su guest
[1dabuziarova@dabuziarova ~]$ pwd
/home/guest
[1dabuziarova@dabuziarova ~]$ cd
[1dabuziarova@dabuziarova ~]$ pwd
/home/guest
[1dabuziarova@dabuziarova ~]$ whoami
guest
[1dabuziarova@dabuziarova ~]$ id guest
uid=1001(guest) gid=1001(guest) rpynm=1001(guest)
[1dabuziarova@dabuziarova ~]$ groups guest
guest : guest
[1dabuziarova@dabuziarova ~]$ 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
```

Figure 2.2: Определение директория

Далее мы уточнили имя пользователя, его группу, а также группы, куда входит пользователь, командой `id`. Выведенные значения `uid`, `gid` и др. Сравнили вывод `id` с выводом команды `groups`. Видим, что `gid` и группы = 1001(guest)

```
guest@dabuziarova-
[1dabuziarova@dabuziarova ~]$ useradd guest
useradd: Permission denied.
[1dabuziarova@dabuziarova ~]$ su
[1dabuziarova@dabuziarova ~]$ useradd guest
[1dabuziarova@dabuziarova ~]$ passwd guest
Именем гостя:
Новый пароль:
Повторите еще раз пароль:
passwd: все данные аутентификации успешно обновлены.
[1dabuziarova@dabuziarova ~]$ su guest
[1dabuziarova@dabuziarova ~]$ pwd
/home/guest
[1dabuziarova@dabuziarova ~]$ cd
[1dabuziarova@dabuziarova ~]$ pwd
/home/guest
[1dabuziarova@dabuziarova ~]$ whoami
guest
[1dabuziarova@dabuziarova ~]$ id guest
uid=1001(guest) gid=1001(guest) rpynm=1001(guest)
[1dabuziarova@dabuziarova ~]$ groups guest
guest : guest
[1dabuziarova@dabuziarova ~]$ 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
```

Figure 2.3: Сравнение выводов `id` и `groups`

Сравним полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки и убедимся, что они совпадают. Просмотрим файл `/etc/passwd` командой: `cat /etc/passwd`. Найдем в нём свою учётную запись. Определим `uid` пользователя. Определим `gid` пользователя. Сравним найденные значения с полученными в предыдущих пунктах. Guest имеет те же идентификаторы 1001, наш пользователь под идентификатором 1002.

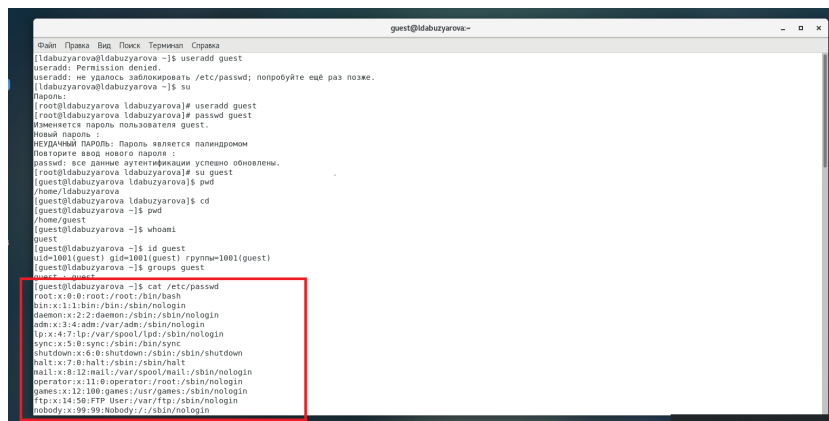


Figure 2.4: Изучение файла /etc/passwd

Определим существующие в системе директории командой `ls -l /home/`. Проверили, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`, командой: `lsattr /home`. Нам не удалось увидеть расширенные атрибуты директорий других пользователей, только своей домашней директории.

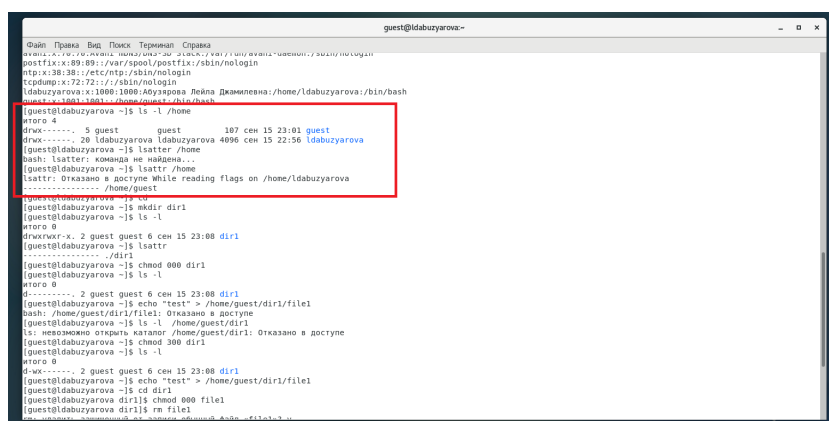


Figure 2.5: Проверка на расширенные атрибуты

Создали 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`.

```
guest@dabuzayrova:~$ ls -l /home
total 4
drwxr-xr-x. 5 guest guest 107 сен 15 23:01 guest
drwxr-xr-x. 2 dabuzayrova dabuzayrova 4096 сен 15 22:56 dabuzayrova
[guest@dabuzayrova ~]$ lsattr /home
bash: lsattr: команда не найдена...
[guest@dabuzayrova ~]$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/ldabuzayrova
[guest@dabuzayrova ~]$ cd
[guest@dabuzayrova ~]$ mkdir dir1
[guest@dabuzayrova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzayrova ~]$ lsattr
lsattr: Отказано в доступе
[guest@dabuzayrova ~]$ chmod 000 dir1
[guest@dabuzayrova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzayrova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@dabuzayrova ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@dabuzayrova ~]$ chmod 300 dir1
[guest@dabuzayrova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzayrova ~]$ echo "test" > /home/guest/dir1/file1
[guest@dabuzayrova ~]$ cd dir1
[guest@dabuzayrova dir1]$ chmod 000 file1
[guest@dabuzayrova dir1]$ rm file1
```

Figure 2.6: Проверка на расширенные атрибуты у dir1

Сняли с директории dir1 все атрибуты командой `chmod 000 dir1` и проверили с `ls -l` помощью правильность выполнения команды `chmod`.

```
guest@dabuzayrova:~$ ls -l /home
total 4
drwxr-xr-x. 5 guest guest 107 сен 15 23:01 guest
drwxr-xr-x. 2 dabuzayrova dabuzayrova 4096 сен 15 22:56 dabuzayrova
[guest@dabuzayrova ~]$ lsattr /home
bash: lsattr: команда не найдена...
[guest@dabuzayrova ~]$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/ldabuzayrova
[guest@dabuzayrova ~]$ cd
[guest@dabuzayrova ~]$ mkdir dir1
[guest@dabuzayrova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzayrova ~]$ lsattr
lsattr: Отказано в доступе
[guest@dabuzayrova ~]$ chmod 000 dir1
[guest@dabuzayrova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzayrova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@dabuzayrova ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@dabuzayrova ~]$ chmod 300 dir1
[guest@dabuzayrova ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzayrova ~]$ echo "test" > /home/guest/dir1/file1
[guest@dabuzayrova ~]$ cd dir1
[guest@dabuzayrova dir1]$ chmod 000 file1
[guest@dabuzayrova dir1]$ rm file1
```

Figure 2.7: Снятие атрибутов

Создали в директории dir1 файл file1 командой `echo "test" > /home/guest/dir1/file1`. Так как ранее мы отозвали все атрибуты, то тем самым лишили всех прав на взаимодействие с dir1.


```
guest@dabuzarova-
Файл Правка Вид Поиск Терминал Справка
guest@x:80:80:/var/spool/postfix:/sbin/nologin
http://x:38:/etc/ntp/sbin/nologin
guest@x:72:72:/:/sbin/nologin
ldabuzarova:x:1000:1000:Абузарова Лейла Джамилевна:/home/ldabuzarova:/bin/bash
guest@x:1001:1001:/home/guest:/bin/bash
[guest@dabuzarova ~]$ ls -l /home
иторо 4
drwxr-xr-x. 5 guest guest 107 сен 15 23:01 guest
drwxr-xr-x. 20 ldabuzarova ldabuzarova 4096 сен 15 22:56 ldabuzarova
[guest@dabuzarova ~]$ lsattr /home
bash: lsattr: команда не найдена...
[guest@dabuzarova ~]$ lsattr /home
lsattr: Отказано в доступе while reading flags on /home/ldabuzarova
----- /home/guest
[guest@dabuzarova ~]$ cd
[guest@dabuzarova ~]$ mkdir dir1
[guest@dabuzarova ~]$ ls -l
иторо 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzarova ~]$ lsattr
----- /dir1
[guest@dabuzarova ~]$ chmod 000 dir1
[guest@dabuzarova ~]$ ls -l
иторо 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzarova ~]$ lsattr
----- /dir1
[guest@dabuzarova ~]$ chmod 000 dir1
[guest@dabuzarova ~]$ ls -l
иторо 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzarova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@dabuzarova ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@dabuzarova ~]$ chmod 300 dir1
[guest@dabuzarova ~]$ ls -l
иторо 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzarova ~]$ echo "test" > /home/guest/dir1/file1
[guest@dabuzarova ~]$ cd dir1
[guest@dabuzarova dir1]$ chmod 000 file1
[guest@dabuzarova dir1]$ rm file1
```

Figure 2.8: Снятие атрибутов с директории

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

```
guest@dabuzarova-
Файл Правка Вид Поиск Терминал Справка
[guest@dabuzarova ~]$ ls -l
иторо 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzarova ~]$ lsattr
----- /dir1
[guest@dabuzarova ~]$ chmod 000 dir1
[guest@dabuzarova ~]$ ls -l
иторо 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzarova ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@dabuzarova ~]$ ls -l /home/guest/dir1
ls: невозможно открыть каталог /home/guest/dir1: Отказано в доступе
[guest@dabuzarova ~]$ chmod 300 dir1
[guest@dabuzarova ~]$ ls -l
иторо 0
drwxr-xr-x. 2 guest guest 6 сен 15 23:08 dir1
[guest@dabuzarova ~]$ echo "test" > /home/guest/dir1/file1
[guest@dabuzarova ~]$ cd dir1
[guest@dabuzarova dir1]$ chmod 000 file1
[guest@dabuzarova dir1]$ rm file1
rm: удалить записанный от записи обычный файл «file1»: y
[guest@dabuzarova dir1]$ ls -l
ls: невозможно открыть каталог -: Отказано в доступе
[guest@dabuzarova dir1]$ cd ..
[guest@dabuzarova ~]$ echo "test" > /home/guest/dir1/file1
[guest@dabuzarova ~]$ chmod 400 /home/guest/dir1/file1
[guest@dabuzarova ~]$ chmod 400 dir1
[guest@dabuzarova ~]$ chmod 100 dir1
[guest@dabuzarova ~]$ cat /home/guest/dir1/file1
test
[guest@dabuzarova ~]$ chmod 200 /home/guest/dir1/file1
[guest@dabuzarova ~]$ echo "test" > /home/guest/dir1/file1
[guest@dabuzarova ~]$ chmod 300 dir1
[guest@dabuzarova ~]$ mv /home/guest/dir1/file1 /home/guest/dir1/file2
[guest@dabuzarova ~]$ mkdir /home/guest/dir1/dir2
[guest@dabuzarova ~]$ mkdir /home/guest/dir1/dir2
[guest@dabuzarova ~]$
```

Figure 2.9: Заполнение таблицы

- 1 - Создание файла
- 2- Удаление файла
- 3- Запись в файл
- 4- Чтение файла
- 5- Смена директории
- 6- Просмотр файлов в директории

7 - Переименование файла

8- Смена атрибутов файла

Table 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)	-	-	+	-	+	-	-	+
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)	+	+	+	-	+	+	+	+

Права директории	Права файла	1	2	3	4	5	6	7	8
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)	-	-	-	-	-	-	-	-
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)	-	-	-	-	-	-	-	-

Права директории	Права файла	1	2	3	4	5	6	7	8
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 таблицы выше определили минимально необходимые права для выполнения операций внутри директории dir1 и заполнили таблицу 2.2. Для заполнения последних двух строк опытным путем проверили минимальные права.

Table 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)
Запись в файл	d--x----- (100)	--w----- (200)
Переименование файла	d-wx----- (300)	----- (000)
Создание поддиректории	d-wx----- (300)	----- (000)

Операция	Права на директорию	Права на файл
Удаление поддиректории	d-wx----- (300)	----- (000)

3 Вывод

В ходе выполнения лабораторной работы были получены практические навыки работы в консоли с атрибутами файлов, произошло закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

1. Теория разграничения прав пользователей
2. Разрешения доступа к файлам