

# Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Ли Тимофей Александрович

# Содержание

Цель работы	4
Выполнение лабораторной работы	5
Выводы	13

## Список иллюстраций

0.1	создание пользователя . . . . .	5
0.2	выполненные операции . . . . .	6
0.3	чтение файла <code>etc/passwd</code> . . . . .	6
0.4	выполненные операции . . . . .	7
0.5	выполненные операции . . . . .	8
0.6	проверка разрешений . . . . .	8
0.7	проверка создания поддиректории . . . . .	12

## 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.

# Выполнение лабораторной работы

Используя учетную запись root, создал нового пользователя guest1, установил для него пароль: (рис. @fig:001):

```
[tim@localhost ~]$ su root
Пароль:
[root@localhost tim]# useradd guest1
[root@localhost tim]# passwd guest1
Изменение пароля пользователя guest1.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль должен содержать не менее 8 символов
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@localhost tim]#
```

Рис. 0.1: создание пользователя

Затем, зашел в систему с новым пользователем, определил директорию, в которой нахожусь, командой pwd. Эта директория совпадает с приглашением командной строки, но не является домашней. Перешел в домашнюю директорию.

Уточнил имя пользователя командой whoami, далее, используя команду id, узнал uid (1002) и gid (1002). Ввел команду groups, получил группу guest1, что совпадает с выводом команды id.

Имя пользователя, выведенное командой id, совпадает с приглашением командной строки.

Далее посмотрел файл etc/passwd с помощью команды cat (все вышеперечисленные действия на рис. 2) (рис. @fig:002)

```

[guest1@localhost ~]$ pwd
/home/guest1
[guest1@localhost ~]$ cd ..
[guest1@localhost home]$ pwd
/home
[guest1@localhost home]$ whoami
guest1
[guest1@localhost home]$ id
uid=1002(guest1) gid=1002(guest1) rpyнны=1002(guest1) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest1@localhost home]$ groups
guest1
[guest1@localhost home]$ cat /etc/passwd
cat: /etc/passwd: Нет такого файла или каталога
[guest1@localhost home]$ 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:65534:65534:Kernel Overflow User:/sbin/nologin
dbus:x:81:81:system message bus:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/sbin/nologin
tss:x:59:59:Account used for TPM access:/dev/null:/sbin/nologin
polkitd:x:998:996:User for polkitd:/sbin/nologin
geoclue:x:997:995:User for geoclue:/var/lib/geoclue:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
pipewire:x:996:992:PipeWire System Daemon:/var/run/pipewire:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
libstoragemgmt:x:905:989:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
qemu:x:107:107:qemu user:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/sbin/nologin
unbound:x:994:988:Unbound DNS resolver:/etc/unbound:/sbin/nologin
gluster:x:993:987:GlusterFS daemons:/run/gluster:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
saslauthd:x:992:76:Saslauthd user:/run/saslauthd:/sbin/nologin
dnsmasq:x:985:985:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin

```

Рис. 0.2: выполненные операции

Нашел строку с данными о новом пользователе, также вывел только ее с помощью уточнения `grep guest1`: (рис. @fig:003)

```

radvd:x:75:75:radvd user:/sbin/nologin
sssd:x:984:984:User for sssd:/sbin/nologin
cockpit-ws:x:983:982:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:982:981:User for cockpit-ws instances:/nonexisting:/sbin/nologin
chrony:x:981:980::/var/lib/chrony:/sbin/nologin
colord:x:980:979:User for colord:/var/lib/colord:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
setroubleshoot:x:979:978::/var/lib/setroubleshoot:/sbin/nologin
flatpak:x:978:977:User for flatpak system helper:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
clevis:x:977:976:Clevis Decryption Framework unprivileged user:/var/cache/clevis:/sbin/nologin
gnome-initial-setup:x:976:975::/run/gnome-initial-setup:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
tim:x:1000:1000:Tim:/home/tim:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
guest1:x:1002:1002::/home/guest1:/bin/bash
[guest1@localhost home]$ cat /etc/passwd | grep guest1
guest1:x:1002:1002::/home/guest1:/bin/bash

```

Рис. 0.3: чтение файла `/etc/passwd`

Как видим, в файле указаны верные `uid` и `gid` (оба 1002).

Определил содержание директории home командой ls, получил список поддиректорий, на каждой из них установлены права на чтение, запись и выполнение только для владельцев.

С помощью команды lsattr посмотрел расширенные атрибуты поддиректорий. Для всех кроме guest1 мне отказано в доступе, а для guest1 никаких атрибутов не установлено.

Создал папку guest1/dir1, с помощью команд ls -l и lsattr посмотрел, какие права доступа и расширенные атрибуты у новой папки. Для нее права доступа полные, кроме записи для “прочих пользователей” и никаких расширенных атрибутов. (вышеперечисленные действия на рис. 4) (рис. @fig:004)

```
[guest1@localhost home]$ ls -l /home/
итого 12
drwx-----. 16 guest  guest  4096 сен 28 23:02 guest
drwx-----. 15 guest1 guest1 4096 окт  2 15:31 guest1
drwx-----. 15 tim    tim    4096 окт  2 15:30 tim
[guest1@localhost home]$ lsattr /home
lsattr: Отказано в доступе While reading flags on /home/tim
lsattr: Отказано в доступе While reading flags on /home/guest
----- /home/guest1
[guest1@localhost home]$ mkdir /quest1/dir1
mkdir: невозможно создать каталог «/quest1/dir1»: Нет такого файла или каталога
[guest1@localhost home]$ cd guest1
[guest1@localhost ~]$ mkdir dir1
[guest1@localhost ~]$ ls -l
итого 0
drwxrwxr-x. 2 guest1 guest1 6 окт  2 15:40 dir1
drwxr-xr-x. 2 guest1 guest1 6 окт  2 15:31 Видео
drwxr-xr-x. 2 guest1 guest1 6 окт  2 15:31 Документы
drwxr-xr-x. 2 guest1 guest1 6 окт  2 15:31 Загрузки
drwxr-xr-x. 2 guest1 guest1 6 окт  2 15:31 Изображения
drwxr-xr-x. 2 guest1 guest1 6 окт  2 15:31 Музыка
drwxr-xr-x. 2 guest1 guest1 6 окт  2 15:31 Общедоступные
drwxr-xr-x. 2 guest1 guest1 6 окт  2 15:31 'Рабочий стол'
drwxr-xr-x. 2 guest1 guest1 6 окт  2 15:31 Шаблоны
[guest1@localhost ~]$ lsattr
----- ./Рабочий стол
----- ./Загрузки
----- ./Шаблоны
----- ./Общедоступные
----- ./Документы
----- ./Музыка
----- ./Изображения
----- ./Видео
----- ./dir1
```

Рис. 0.4: выполненные операции

Далее я снял все права доступа с папки dir с помощью команды chmod и попытался создать в ней файл file1 с содержимым “test”. Я получил отказ, поскольку после обнуления прав доступа даже владелец не может создавать файлы в данной папке. После этого я проверил результат выполнения предыдущей операции командой ls, но

также получил отказ в доступе. В итоге я открыл файловый менеджер и убедился, что файл не создан. (вышеперечисленные действия на рис. 5) (рис. @fig:005)

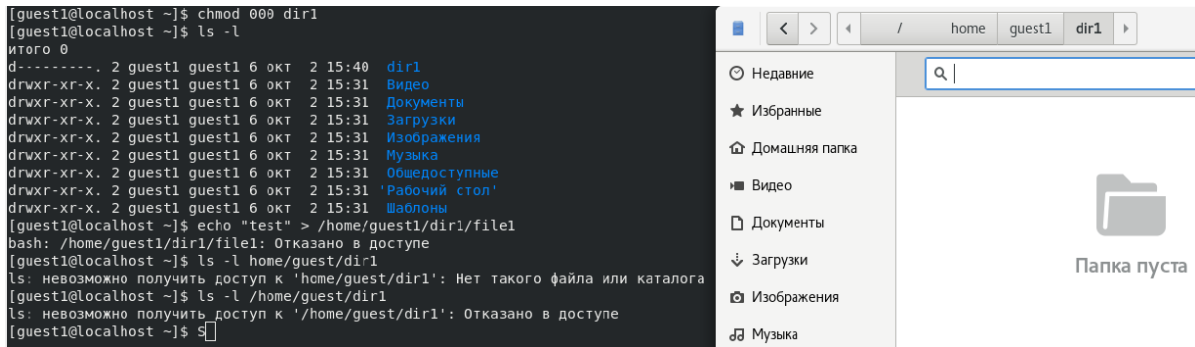


Рис. 0.5: выполненные операции

Затем, я создал в папке `dir1` файл `test` и от имени владельца опытным путем начал проверять, какие операции разрешены, а какие нет. Для этого использовал команды `cd` (смена директории), `touch` (создание файла), `rm` (удаление файла), `echo` (запись в файл), `cat` (чтение файла), `ls` (просмотр содержимого), `mv` (переименование файла), `chmod` (смена атрибутов): (рис. @fig:006)

```
[guest1@localhost ~]$ cd dir1
[guest1@localhost dir1]$ touch 1
[guest1@localhost dir1]$ rm 1
[guest1@localhost dir1]$ echo "finished" > test
[guest1@localhost dir1]$ cat test
finished
[guest1@localhost dir1]$ ls
test
[guest1@localhost dir1]$ mv test d
[guest1@localhost dir1]$ mv d test
[guest1@localhost dir1]$ chmod 500 test
[guest1@localhost dir1]$ chmod 700 test
```

Рис. 0.6: проверка разрешений

На основе полученных ответов заполнил таблицу (таб. 2.1)



Таблица 0.1: Установленные права и разрешённые действия

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переимено- вание файла	Смена атрибу- тов файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-
d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	+	-	-	+
d(100)	(300)	-	-	+	-	+	-	-	+
d(100)	(400)	-	-	-	+	+	-	-	+
d(100)	(500)	-	-	-	+	+	-	-	+
d(100)	(600)	-	-	+	+	+	-	-	+
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переимено- вание файла	Смена атрибу- тов файла
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	+
d(300)	(700)	+	+	+	+	+	-	+	+
d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(500)	(100)	-	-	-	-	+	+	-	+
d(500)	(200)	-	-	+	-	+	+	-	+
d(500)	(300)	-	-	+	-	+	+	-	+
d(500)	(400)	-	-	-	+	+	+	-	+
d(500)	(500)	-	-	-	+	+	+	-	+
d(500)	(600)	-	-	+	+	+	+	-	+
d(500)	(700)	-	-	+	+	+	+	-	+

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переимено- вание файла	Смена атрибу- тов файла
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-
d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(700)	(100)	+	+	-	-	+	+	+	+
d(700)	(200)	+	+	+	-	+	+	+	+
d(700)	(300)	+	+	+	-	+	+	+	+
d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

Затем, на основе полученных ответов заполнил таблицу 2.2. Также для заполнения этой таблицы проверил минимальные разрешения для создания/удаления поддиректории: (рис. @fig:007):

```

[guest1@localhost ~]$ chmod 000 dir1
[guest1@localhost ~]$ mkdir dir1/dir2
mkdir: невозможно создать каталог «dir1/dir2»: Отказано в доступе
[guest1@localhost ~]$ chmod 100 dir1
[guest1@localhost ~]$ mkdir dir1/dir2
mkdir: невозможно создать каталог «dir1/dir2»: Отказано в доступе
[guest1@localhost ~]$ chmod 200 dir1
[guest1@localhost ~]$ mkdir dir1/dir2
mkdir: невозможно создать каталог «dir1/dir2»: Отказано в доступе
[guest1@localhost ~]$ chmod 300 dir1
[guest1@localhost ~]$ chmod 300 dir1
[guest1@localhost ~]$ mkdir dir1/dir2
[guest1@localhost ~]$ █

```

Рис. 0.7: проверка создания поддиректории

В итоге получил следующую таблицу: (таб. 2.2)

Таблица 0.2: Минимальные права для совершения операций

Операция	min права на директорию	min 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)

## Выводы

Получил практические навыки работы в консоли с атрибутами файлов, закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.