

Лабараторная работа №3

Отчет

Славинский Владислав Вадимович

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
3	Выводы	18

Список иллюстраций

2.1	Открытие терминала с root	6
2.2	Создание каталогов main и third	7
2.3	Владелец каталогов	7
2.4	Смена владельцев	8
2.5	Установка разрешений	8
2.6	Переход на учетную запись bob	9
2.7	Создание файла под пользователем bob в каталоге /data/main . . .	9
2.8	Создание файла в каталоге /data/third	9
2.9	Переключение на пользователя alice	10
2.10	Создание alice1, alice2	10
2.11	Переход на пользователя bob	10
2.12	Удаление файлов	11
2.13	Создание bob1,bob2	11
2.14	Установка бит идентификатора группы и sticky-бит для общего каталога группы	11
2.15	Создание файлов	11
2.16	Проверка защиты sticky-bit	12
2.17	Переключимся на пользователя root	12
2.18	Установка прав на чтение и выполнение	12
2.19	Проверка разрешений	13
2.20	Полномочия файла newfile1	14
2.21	Полномочия файла newfile1 в каталоге third	14
2.22	Установка ACL для каталога /data/main	15
2.23	Добавление ACL для каталога /data/third	15
2.24	Проверка настроек	15
2.25	Проверка настроек	16
2.26	Вход в учетную запись carol	16
2.27	Проверка операций с файлами	17

Список таблиц

1 Цель работы

Получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

2 Выполнение лабораторной работы

Откроем терминал с учетной записью root(рис. 2.1)

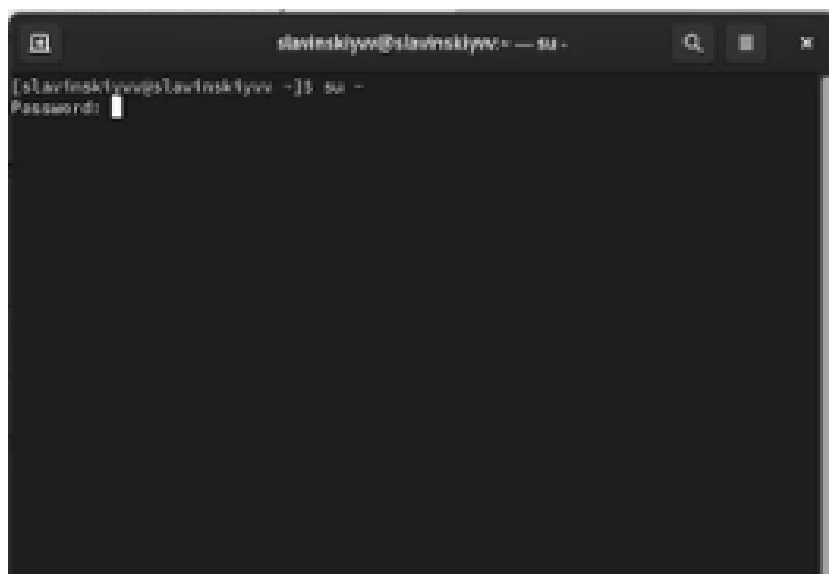


Рис. 2.1: Открытие терминала с root

В корневом каталоге создадим каталоги /data/main и /data/third с помощью mkdir. (рис. 2.2)

```

[olovinskiy@olovinskiy ~]$ su -
Password:
[root@olovinskiy ~]# mkdir -p /data/main /data/third
[root@olovinskiy ~]#

```

Рис. 2.2: Создание каталогов main и third

Посмотрим, кто является владельцем этих каталогов, для этого используем команду `ls -Al /data`. Владелец каталогов является root. (рис. 2.3)

```

[olovinskiy@olovinskiy ~]$ su -
Password:
[root@olovinskiy ~]# mkdir -p /data/main /data/third
[root@olovinskiy ~]# ls -Al /data
total 0
drwxr-xr-x. 2 root root 4 Sep 19 14:05 main
drwxr-xr-x. 2 root root 4 Sep 19 14:05 third
[root@olovinskiy ~]#

```

Рис. 2.3: Владелец каталогов

Изменим владельцев этих каталогов с root на main и third и посмотрим изменения. (рис. 2.4)

```
root@slavinskiy:~# su -
Password:
[root@slavinskiy ~]# mkdir -p /data/main /data/third
[root@slavinskiy ~]# ls -al /data
total 0
drwxr-xr-x. 3 root root 6 Sep 20 13:35 main
drwxr-xr-x. 3 root root 6 Sep 20 13:35 third
[root@slavinskiy ~]# chgrp main /data/main
[root@slavinskiy ~]# chgrp third /data/third
[root@slavinskiy ~]# ls -al /data
total 0
drwxr-xr-x. 3 root main 6 Sep 20 13:35 main
drwxr-xr-x. 3 root third 6 Sep 20 13:35 third
[root@slavinskiy ~]#
```

Рис. 2.4: Смена владельцев

Установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам. Проверяем изменения, как видим, у нас все применилось. (рис. 2.5)

```
total 0
drwxr-xr-x. 3 root main 6 Sep 20 13:35 main
drwxr-xr-x. 3 root third 6 Sep 20 13:35 third
[root@slavinskiy ~]# chmod 770 /data/main
[root@slavinskiy ~]# chmod 770 /data/third
[root@slavinskiy ~]# ls -al /data
total 0
drwxrwx---. 3 root main 6 Sep 20 13:35 main
drwxrwx---. 3 root third 6 Sep 20 13:35 third
[root@slavinskiy ~]#
```

Рис. 2.5: Установка разрешений

Далее перейдем на учетную запись bob. (рис. 2.6)


```
total 0
-rwxrwxrwx. 1 root main 0 Sep 20 13:35 mai
-rwxrwxrwx. 1 root third 0 Sep 20 13:35 thi
[root@slavinskiy ~]# su - bob
[bob@slavinskiy ~]#
```

Рис. 2.6: Переход на учетную запись bob

Под пользователем bob попробуем перейти в каталог /data/main и создать файл emptyfile в этом каталоге. Видим, что владельцем является bob и группа тоже bob. (рис. 2.7)

```
[root@slavinskiy ~]# su - bob
[bob@slavinskiy ~]# cd /data/main
[bob@slavinskiy main]# touch emptyfile
[bob@slavinskiy main]# ls -la
total 0
-rw-rw-rw. 1 bob bob 0 Sep 20 13:35 emptyfile
```

Рис. 2.7: Создание файла под пользователем bob в каталоге /data/main

Под пользователем bob попробуем перейти в каталог /data/third и создать файл emptyfile в этом каталоге. Как видим, нам выводится Permission denied или же отказано в доступе, все из-за того, что пользователь bob входил в группу main, а не в группе third. (рис. 2.8)

```
total 0
-rw-rw-rw. 1 bob bob 0 Sep 20 13:35 emptyfile
[bob@slavinskiy main]# cd /data/third/
-bash: cd: /data/third/: Permission denied
[bob@slavinskiy main]# cd /data/third/
-bash: cd: /data/third/: Permission denied
[bob@slavinskiy main]# cd
[bob@slavinskiy ~]# cd /data/third/
-bash: cd: /data/third/: Permission denied
[bob@slavinskiy ~]#
```

Рис. 2.8: Создание файла в каталоге /data/third

Переключимся на учётную запись пользователя alice(рис. 2.9)

```
[bob@alawinskiyyv main]$ cd  
[bob@alawinskiyyv ~]$ cd /data/third/  
-bash: cd: /data/third/: Permission denied  
[bob@alawinskiyyv ~]$ su - alice  
Password:  
[alice@alawinskiyyv ~]$
```

Рис. 2.9: Переключение на пользователя alice

Перейдем в каталог /data/main и создадим два файла, владельцем которых является alice. (рис. 2.10)

```
[alice@alawinskiyyv ~]$ su - alice  
Password:  
[alice@alawinskiyyv ~]$ cd /data/main  
[alice@alawinskiyyv main]$ touch alice1  
[alice@alawinskiyyv main]$ touch alice2  
[alice@alawinskiyyv main]$
```

Рис. 2.10: Создание alice1, alice2

Перейдем под учётную запись пользователя bob. (рис. 2.11)

```
[alice@alawinskiyyv main]$ su - bob  
Password:  
[bob@alawinskiyyv ~]$
```

Рис. 2.11: Переход на пользователя bob

Перейдем в каталог /data/main. Введем команду `ls -l`, чтобы увидеть файлы alice, и попробуем удалить файлы. Как видим, через пользователя bob, мы смогли удалить файлы alice в каталоге main (рис. 2.12)

```

bob@alvinackipov: main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 28 18:45 alice1
-rw-r--r--. 1 alice alice 0 Sep 28 18:45 alice2
-rw-r--r--. 1 bob  bob  0 Sep 28 18:33 emptyfile
bob@alvinackipov: main]$ rm -f alice*
bob@alvinackipov: main]$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Sep 28 18:39 emptyfile
bob@alvinackipov: main]$

```

Рис. 2.12: Удаление файлов

Создадим два файла, которые принадлежат пользователю bob. (рис. 2.13)

```

-rw-r--r--. 1 bob bob 0 Sep 28 18:19 empty
[bob@alvinackipov: main]$ touch? bob1
[bob@alvinackipov: main]$ touch? bob2
[bob@alvinackipov: main]$

```

Рис. 2.13: Создание bob1,bob2

Под пользователем root установим для каталога /data/main бит идентификатора группы, а также sticky-бит для разделяемого (общего) каталога группы.(рис. 2.14)

```

Password:
[root@alvinackipov ~]# chmod g+s,o+t /data/main
[root@alvinackipov ~]#

```

Рис. 2.14: Установка бит идентификатора группы и sticky-бит для общего каталога группы

Под пользователем alice создадим в каталоге /data/main файлы alice3 и alice4. Здесь мы видим, что два этих файла принадлежать группе main(рис. 2.15)

```

total 0
-rw-r--r--. 1 alice main 0 Sep 28 18:48 alice3
-rw-r--r--. 1 alice main 0 Sep 28 18:48 alice4
-rw-r--r--. 1 bob  bob  0 Sep 28 18:48 bob1
-rw-r--r--. 1 bob  bob  0 Sep 28 18:48 bob2
-rw-r--r--. 1 bob  bob  0 Sep 28 18:39 emptyfile
[alice@alvinackipov: main]$

```

Рис. 2.15: Создание файлов

Под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob с помощью команды: `rm -rf bob*`. Sticky-bit предотвратил удаление, поскольку alice не является создателем файлов, но alice является создателем каталога, поэтому все равно alice сможет все удалить.(рис. 2.16)

```
alice@alavinskiyye: /data/main$ ls -la
total 4
drwxr-xr-x 1 bob  bob  0 Sep 20 13:39 emptyfile
[alice@alavinskiyye: main]$ rm -rf bob*
rm: cannot remove 'bob/*': operation not permitted
rm: cannot remove 'bob/*': operation not permitted
[alice@alavinskiyye: main]$
```

Рис. 2.16: Проверка защиты sticky-bit

Переключимся в терминале на учётную запись пользователя root.(рис. 2.17)

```
[alice@alavinskiyye: main]$ su -
Password:
[root@alavinskiyye: ~]#
```

Рис. 2.17: Переключимся на пользователя root

Установим права на чтение и выполнение в каталоге /data/main для группы third и права на чтение и выполнение для группы main в каталоге /data/third.(рис. 2.18)

```
Password:
[root@alavinskiyye: ~]# setfacl -m g:third:rx /data/main
[root@alavinskiyye: ~]# setfacl -m g:main:rx /data/third
[root@alavinskiyye: ~]#
```

Рис. 2.18: Установка прав на чтение и выполнение

Используем команду `getfacl`, чтобы убедиться в правильности установки разрешений. Как видим, в каталоге main высвечивается third, а для third-main.(рис. 2.19)

```
root@slavinskiyy:~# getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# flags: -at
user::rw-
group::r-x
group:third:r-x
mask::rw-
other::---
```

```
root@slavinskiyy:~# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rw-
group::r-x
group:main:r-x
mask::rw-
other::---
```

```
root@slavinskiyy:~#
```

Рис. 2.19: Проверка разрешений

Создадим новый файл с именем newfile1 в каталоге /data/main и используем `getfacl /data/main/newfile1` для проверки текущих назначений полномочий. Видим, что для пользователя у нас полномочия для записи и чтения, а для группы только для чтения. Так же владельцами являются пользователь root и группа main.(рис. 2.20)

```

[root@slavinskiyev ~]# getfacl /data/third
getfacl: Removing leading '/' from absolute path names
# file: data/third
# owner: root
# group: third
user::rx
group::rx
mask::rx
other::---

[root@slavinskiyev ~]# cd /data/main
[root@slavinskiyev main]# touch /data/main/newfile1
[root@slavinskiyev main]# getfacl /data/main/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile1
# owner: root
# group: main
user::rw-
group::r--
other::r--

[root@slavinskiyev main]#

```

Рис. 2.20: Полномочия файла newfile1

Сделаем тоже самое, только в каталоге /data/third и видим, что владелец группы является уже не third, а root.(рис. 2.21)

```

# group: main
user::rw-
group::r--
other::r--

[root@slavinskiyev main]# cd
[root@slavinskiyev ~]# cd /data/third/
[root@slavinskiyev third]# touch /data/third/newfile1
[root@slavinskiyev third]# getfacl /data/third/newfile1
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile1
# owner: root
# group: root
user::rw-
group::r--
other::r--

[root@slavinskiyev third]#

```

Рис. 2.21: Полномочия файла newfile1 в каталоге third

Установим ACL по умолчанию для каталога /data/main.(рис. 2.22)

```
other:---

[root@alavinskijpv third]# cd
[root@alavinskijpv ~]# setfacl -m d:group:third:rwx /data/main
[root@alavinskijpv ~]#
```

Рис. 2.22: Установка ACL для каталога /data/main

Добавим ACL по умолчанию для каталога /data/third.(рис. 2.23)

```
[root@alavinskijpv third]# cd
[root@alavinskijpv ~]# setfacl -m d:group:third:rwx /data/main
[root@alavinskijpv ~]# setfacl -m d:group:main:rwx /data/third
[root@alavinskijpv ~]#
```

Рис. 2.23: Добавление ACL для каталога /data/third

Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main. Видим, что что настройки работают, полномочия для third тоже есть. (рис. 2.24)

```
[root@alavinskijpv ~]# setfacl -m d:group:main:rwx /data/third
[root@alavinskijpv ~]# touch /data/main/newfile2
[root@alavinskijpv ~]# getfacl /data/main/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/main/newfile2
# owner: root
# group: main
user::rwx
group::rwx
group:third:rwx
mask::rwx
other::---
```

Рис. 2.24: Проверка настроек

Сделаем те же действия только для каталога /data/third. Теперь у группы third есть полномочия в каталоге main.(рис. 2.25)

```

# daemon: root
# group: root
user::root
group::root                #effective:root
group::third:root          #effective:root
mask::root
other::---

[root@galaxinikey ~]# touch /data/third/newfile2
[root@galaxinikey ~]# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::root
group::root                #effective:root
group::third:root          #effective:root
mask::root
other::---
[root@galaxinikey ~]#

```

Рис. 2.25: Проверка настроек

Для проверки полномочий группы third войдем под учётной записью члена группы third.(рис. 2.26)

```

other::---

[root@galaxinikey ~]# su - carol
[carol@galaxinikey ~]#

```

Рис. 2.26: Вход в учетную запись carol

Попробуем удалить newfile1 и newfile2 и осуществить запись в эти файлы. Как видим, удалось записать только в newfile2, поскольку мы применили настройки для newfile2 для записи и чтения, а для newfile1 только для чтения.(рис. 2.27)


```
carel@slawinskiyy:~$  
[root@slawinskiyy:~]# touch /data/third/newfile2  
[root@slawinskiyy:~]# gkillact /data/third/newfile1  
warning: Removing leading '/' from absolute path names  
# files: data/third/newfile2  
# owner: root  
# group: root  
user:rwx-  
group:rwx- effective:rwx-  
mask:rwx-  
other:---  
[root@slawinskiyy:~]# su - carel  
carel@slawinskiyy:~$ rm /data/main/newfile1  
rm: remove write-protected regular empty file '/data/main/newfile1'? y  
rm: cannot remove '/data/main/newfile1': Permission denied  
carel@slawinskiyy:~$ rm /data/main/newfile2  
rm: cannot remove '/data/main/newfile2': Permission denied  
carel@slawinskiyy:~$ echo "hello, world!" >> /data/main/newfile1  
hello /data/main/newfile1: Permission denied  
carel@slawinskiyy:~$ echo "hello, world!" >> /data/main/newfile2  
carel@slawinskiyy:~$
```

Рис. 2.27: Проверка операций с файлами

3 Выводы

В ходе выполнения лабораторной работы были получены навыки настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux. # Ответы на контрольные вопросы

1. `chown :main /data/main/report.txt`
2. `find /data -user alice`
3. `chmod -R ug=rwx,o= /data.`
4. `chmod +x /data/main/script.sh.`
5. `chmod g+s /data/main.`
6. `chmod +t /data/main.`
7. `setfacl -R -m g:third:r /data/main`
8. `setfacl -R -m g:main:rx /data/third` - для файлов, которые уже есть `setfacl -R -m d:g:main:rx /data/main` - для будущих файлов
9. Значение `umask` должно быть 007. Пример: `umask 007, touch /data/main/1.txt.`
В этом случае файл будет иметь разрешение 660, и другие пользователи не смогут получать разрешения на новые файлы.
10. `chmod a-w /data/main/2.txt.`