Отчет по лабораторной работе №3

Настройка прав доступа

Сидорова Арина Валерьевна

Содержание

Список иллюстраций

1 Цель работы

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

2 Выполнение лабораторной работы

2.1 Управление базовыми разрешениями

Откроем терминал с учетной записью root. В корневом каталоге создадим каталоги /data/main/ и /data/third. Проверим, кто является владельцем этих каталогов. (рис. 2.1).

```
avsidorova@avsidorova:~$ sudo i
[sudo] пароль для avsidorova:
sudo: i: команда не найдена
avsidorova@avsidorova:~$ sudo -i
root@avsidorova:~# mkdir -p /data/main /data/third
root@avsidorova:~# ls -Al /data
итого 0
drwxr-xr-x. 2 root root 6 сен 19 07:32 main
drwxr-xr-x. 2 root root 6 сен 19 07:32 third
```

Рис. 2.1: main,third

Изменим владельцев этих каталогов с root на main и third соответственно. (рис. 2.2).

```
root@avsidorova:~# chgrp main /data/main
root@avsidorova:~# chgrp third /data/third
```

Рис. 2.2: изменим владельцев

Посмотрим, кто является владельцем этих каталогов (рис. 2.3)

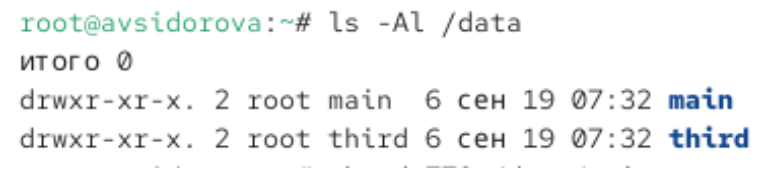

Рис. 2.3: проверям владельцев

Установим разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователями группам. После этого проверим установленные права. (рис. 2.4)

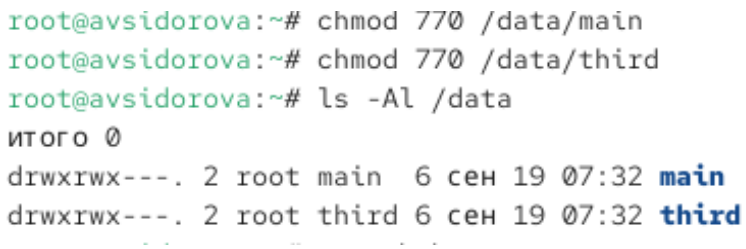

Рис. 2.4: chmod

Перейдем в другой терминал, под пользователем bob в каталоге /data/main создадим файл emptyfile. Создался файл под пользователем bob, так как у группы есть права доступа. Перейдем в каталог /data/third и создадим файл emptyfile, нам отказано в доступе, так как группа не имеет прав. (рис. 2.5)

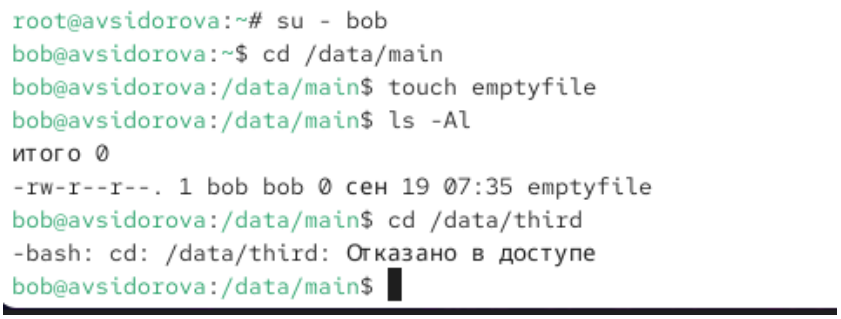

Рис. 2.5: emptyfile

2.2 Управление специальными разрешениями

Откроем новый терминал под пользователем Alice. Перейдем в каталог /data/main и создадим два файла alice1, alice2 (рис. 2.6)

```
avsidorova@avsidorova:~$ su alice
Пароль:
alice@avsidorova:/home/avsidorova$ cd /data/main
alice@avsidorova:/data/main$ touch alice1
alice@avsidorova:/data/main$ touch alice2
alice@avsidorova:/data/main$
```

Рис. 2.6: alice1, alice2

Видим два файла, созданные пользователем alice. Попробуем удалить файлы, принадлежащие пользователю alice. Создадим два файла, которые будут принадлежать пользователю bob (bob1, bob2) (рис. 2.7)

```
bob@avsidorova:/data/main$ ls -Al
итого 0
-rw-r--r--. 1 alice alice 0 сен 19 07:39 alice1
-rw-r--r--. 1 alice alice 0 сен 19 07:39 alice2
-rw-r--r--. 1 bob   bob   0 сен 19 07:35 emptyfile
bob@avsidorova:/data/main$ rm -f alice*
bob@avsidorova:/data/main$ ls -Al
итого 0
-rw-r--r--. 1 bob bob 0 сен 19 07:35 emptyfile
bob@avsidorova:/data/main$ touch bob1
bob@avsidorova:/data/main$ touch bob2
bob@avsidorova:/data/main$
```

Рис. 2.7: bob1, bob2

В терминале под пользователем root установим для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы (рис. 2.8)

```
avsidorova@avsidorova:~$ sudo -i
[sudo] пароль для avsidorova:
root@avsidorova:~# chmod g+s,o+t /data/main
root@avsidorova:~#
```

Рис. 2.8: chmod g+s o+t

Изменим содержимое файла .bashrc, добавив строку export EDITOR=/usr/bin/mceditor

В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4. Теперь мы увидели, что два созданных файла принадлежат группе main, которая является группой-владельцем каталога /data/main (рис. 2.9)

```
alice@avsidorova:/data/main$ touch alice3
alice@avsidorova:/data/main$ touch alice4
alice@avsidorova:/data/main$ ls-l
bash: ls-l: команда не найдена...
^[[A^Z
[1]+  Остановлен    ls-l
alice@avsidorova:/data/main$ ls -l
итого 0
-rw-r--r--. 1 alice main 0 сен 19 07:43 alice3
-rw-r--r--. 1 alice main 0 сен 19 07:43 alice4
-rw-r--r--. 1 bob   bob  0 сен 19 07:40 bob1
-rw-r--r--. 1 bob   bob  0 сен 19 07:40 bob2
-rw-r--r--. 1 bob   bob  0 сен 19 07:35 emptyfile
alice@avsidorova:/data/main$
```

Рис. 2.9: alice3, alice4

В терминале под пользователем alice попробуем удалить файлы, принадлежащие пользователю bob (Не получилось) (рис. 2.10)

```
alice@avsidorova:/data/main$ rm -rf bob*
rm: невозможно удалить 'bob1': Операция не позволена
rm: невозможно удалить 'bob2': Операция не позволена
alice@avsidorova:/data/main$
```

Рис. 2.10: rm -rf bob*

2.3 Управление расширенными разрешениями с использованием списков ACL

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.

Используем команду getfacl, чтобы убедиться в правильности установки разрешений. (рис. 2.11)

```
root@avsidorova:~# setfacl -m g:third:rx /data/main
root@avsidorova:~# setfacl -m g:main:rx /data/third
root@avsidorova:~# getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# flags: -st
user::rwx
group::rwx
group:third:r-x
mask::rwx
other::---

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

root@avsidorova:~#
```

Рис. 2.11: setfactl/getfactl

Создадим новый файл с именем newfile1 в каталоге /data/main и проверим текущие назначения полномочий (user - чтения и редактирование; group, other - чтение). (рис. 2.12)

```
root@avsidorova:~# touch /data/main/newfile1
root@avsidorova:~# 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@avsidorova:~#
```

Рис. 2.12: newfile1

Выполним аналогичные действия в /data/third (рис. 2.13)

```
root@avsidorova:~# touch /data/third/newfile1
root@avsidorova:~# 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@avsidorova:~#
```

Рис. 2.13: newfile1 - data/third/

Установим ACL по умолчанию для каталога /data/main. Добавим ACL по умолчанию для каталога /data/third. Убедимся, что настройки ACL работают, добавив новый файл в каталог /data/main. (рис. 2.14)

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

Рис. 2.14: ACL /data/main

Используем getfactl для проверки текущих назначений полномочий. Выполним аналогичные действия для каталога /data/third. (рис. 2.15)

Рис. 2.15: ACL /data/third

Для проверки полномочий группы third в каталоге /data/third войдем в другом терминале под учётной записью члена группы third.Проверим операции с файлами: rm /data/main/newfile1 - Успешно rm /data/main/newfile2 - Не хватает прав доступа Проверим, возможно ли осуществить запись в файл: echo “Hello, world” » /data/main/newfile1 - Не хватает прав доступа echo “Hello, world” » /data/main/newfile2 - Успешно (рис. 2.16)

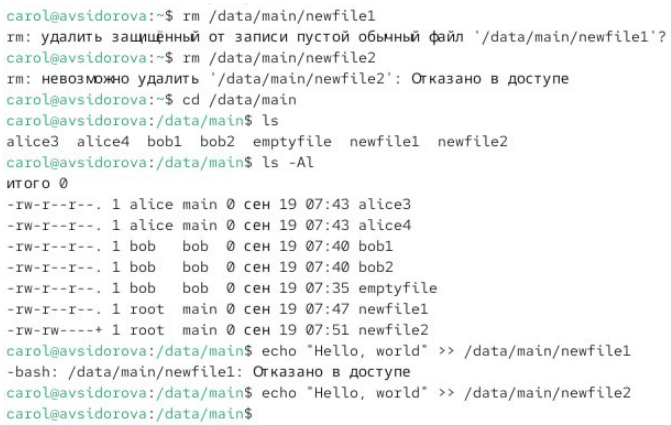

Рис. 2.16: echo

3 Выводы

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