Отчёт по лабораторной работе №3

Настройка прав доступа

Тукаев Тимур

Содержание

1 Цель работы **5**

2 Выполнение **6**
2.1 Управление базовыми разрешениями 6
2.2 Управление специальными разрешениями 9
2.3 Управление расширенными разрешениями (ACL) 13

3 Контрольные вопросы **18**

4 Заключение **20**

Список иллюстраций

2.1 Переход под root и создание каталогов 6
2.2 Работа пользователя bob в /data/main 8
2.3 Удаление файлов alice пользователем bob 10
2.4 SGID и sticky-bit в каталоге /data/main 12
2.5 ACL каталогов /data/main и /data/third 14
2.6 ACL файлов newfile1 в каталогах /data/main и /data/third 15
2.7 Наследование ACL по умолчанию для newfile2 16
2.8 Проверка прав пользователя carol 17

Список таблиц

1 Цель работы

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

2 Выполнение

2.1 Управление базовыми разрешениями

1. Получен доступ суперпользователя командой su. После ввода пароля открыт терминал с правами root.

```
titukaev@titukaev:~$ su
Password:
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# mkdir -p /data/main /data/third
root@titukaev:/home/titukaev# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Dec  9 11:54 main
drwxr-xr-x. 2 root root 6 Dec  9 11:54 third
root@titukaev:/home/titukaev# chgrp main /data/main/
root@titukaev:/home/titukaev# chgrp third /data/third/
root@titukaev:/home/titukaev# ls -Al /data
total 0
drwxr-xr-x. 2 root main  6 Dec  9 11:54 main
drwxr-xr-x. 2 root third 6 Dec  9 11:54 third
root@titukaev:/home/titukaev# chmod 770 /data/main/
root@titukaev:/home/titukaev# chmod 770 /data/third/
root@titukaev:/home/titukaev# ls -Al /data
total 0
drwxrwx---. 2 root main  6 Dec  9 11:54 main
drwxrwx---. 2 root third 6 Dec  9 11:54 third
root@titukaev:/home/titukaev# su bob
bob@titukaev:/home/titukaev$ cd /data/main/
bob@titukaev:/data/main$ touch emptyfile
bob@titukaev:/data/main$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Dec  9 11:56 emptyfile
bob@titukaev:/data/main$ cd /data/third/
bash: cd: /data/third/: Permission denied
bob@titukaev:/data/main$
```

Рис. 2.1: Переход под root и создание каталогов

2. В корневом каталоге созданы директории `/data/main` и `/data/third` с помощью `mkdir -p /data/main /data/third`.
   Командой `ls -Al /data` просмотрены их владельцы и права доступа: владельцем и группой обеих директорий является `root`.

3. Изменены группы-владельцы каталогов: для `/data/main` установлена группа `main`, для `/data/third` — группа `third` (`chgrp main /data/main`, `chgrp third /data/third`).
   Повторный вывод `ls -Al /data` показывает, что группы каталогов изменены на `main` и `third` соответственно.

4. Для каталогов `/data/main` и `/data/third` установлены права `770` (`rwxrwx---`). Это даёт владельцу и группе полный доступ к каталогам и полностью запрещает доступ всем остальным пользователям. Проверка `ls -Al /data` подтверждает установленные права.

5. В другом терминале выполнен вход под учётной записью пользователя `bob` с помощью `su bob`.

6. Пользователь `bob` перешёл в каталог `/data/main` (`cd /data/main`) и создал файл `emptyfile` (`touch emptyfile`). Команда `ls -Al` показала, что файл принадлежит пользователю `bob` и группе `bob`, но каталог доступен, так как `bob` входит в группу `main`, которая имеет полный доступ к каталогу.

```
titukaev@titukaev:~$ su
Password:
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# mkdir -p /data/main /data/third
root@titukaev:/home/titukaev# ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Dec  9 11:54 main
drwxr-xr-x. 2 root root 6 Dec  9 11:54 third
root@titukaev:/home/titukaev# chgrp main /data/main/
root@titukaev:/home/titukaev# chgrp third /data/third/
root@titukaev:/home/titukaev# ls -Al /data
total 0
drwxr-xr-x. 2 root main  6 Dec  9 11:54 main
drwxr-xr-x. 2 root third 6 Dec  9 11:54 third
root@titukaev:/home/titukaev# chmod 770 /data/main/
root@titukaev:/home/titukaev# chmod 770 /data/third/
root@titukaev:/home/titukaev# ls -Al /data
total 0
drwxrwx---. 2 root main  6 Dec  9 11:54 main
drwxrwx---. 2 root third 6 Dec  9 11:54 third
root@titukaev:/home/titukaev# su bob
bob@titukaev:/home/titukaev$ cd /data/main/
bob@titukaev:/data/main$ touch emptyfile
bob@titukaev:/data/main$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Dec  9 11:56 emptyfile
bob@titukaev:/data/main$ cd /data/third/
bash: cd: /data/third/: Permission denied
bob@titukaev:/data/main$
```

Рис. 2.2: Работа пользователя bob в /data/main

Пояснение: группа `main` имеет права `rwx` на каталог `/data/main`, поэтому любой пользователь из этой группы, включая `bob`, может создавать в нём файлы.

7. Далее пользователь `bob` попытался перейти в каталог `/data/third` (`cd /data/third`), однако получил сообщение *Permission denied*.
   Пояснение: группа-владелец каталога `/data/third` — `third`, права на каталог `rwx` установлены только для владельца и группы. Пользователь `bob` не состоит в группе `third`, поэтому доступ к каталогу ему запрещён.

2.2 Управление специальными разрешениями

1. В новом терминале выполнен вход под пользователем `alice`. Пользователь перешёл в каталог `/data/main` и создал там два файла `alice1` и `alice2` командами `touch alice1` и `touch alice2`.

2. В другом терминале выполнен вход под пользователем `bob`. Пользователь `bob` перешёл в `/data/main` и вывел список файлов (`ls -l`), где отобразились файлы `alice1` и `alice2`, принадлежащие пользователю `alice`.

3. Пользователь `bob` удалил файлы `alice1` и `alice2`, выполнив `rm -f alice*`.
   Пояснение: оба пользователя состоят в группе `main`, у которой есть права на запись в каталог `/data/main`. Так как sticky-bit ещё не установлен, любой пользователь с правом записи в каталог может удалять любые файлы в нём, даже не являясь их владельцем.

```
bob@titukaev:/data/main$
bob@titukaev:/data/main$ su alice
Password:
alice@titukaev:/data/main$ cd /data/main/
alice@titukaev:/data/main$ touch alice1
alice@titukaev:/data/main$ touch alice2
alice@titukaev:/data/main$
alice@titukaev:/data/main$ su bob
Password:
bob@titukaev:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Dec  9 11:59 alice1
-rw-r--r--. 1 alice alice 0 Dec  9 11:59 alice2
-rw-r--r--. 1 bob   bob   0 Dec  9 11:56 emptyfile
bob@titukaev:/data/main$ rm -f alice*
bob@titukaev:/data/main$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Dec  9 11:56 emptyfile
bob@titukaev:/data/main$ touch bob1
bob@titukaev:/data/main$ touch bob2
bob@titukaev:/data/main$ su
Password:
root@titukaev:/data/main# chmod g+s,o+t /data/main/
root@titukaev:/data/main#
exit
bob@titukaev:/data/main$
exit
alice@titukaev:/data/main$ touch alice3
alice@titukaev:/data/main$ touch alice4
alice@titukaev:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Dec  9 12:01 alice3
-rw-r--r--. 1 alice main 0 Dec  9 12:01 alice4
-rw-r--r--. 1 bob   bob  0 Dec  9 12:00 bob1
-rw-r--r--. 1 bob   bob  0 Dec  9 12:00 bob2
-rw-r--r--. 1 bob   bob  0 Dec  9 11:56 emptyfile
alice@titukaev:/data/main$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
alice@titukaev:/data/main$
```

Рис. 2.3: Удаление файлов alice пользователем bob

4. Затем пользователь `bob` создал в каталоге `/data/main` файлы `bob1` и `bob2`. Файлы принадлежат пользователю `bob` и группе `bob`.

5. В терминале root для каталога `/data/main` были установлены специальные биты: бит идентификатора группы (SGID) и sticky-bit: `chmod g+s,o+t`

`/data/main`.

SGID обеспечивает наследование группового владельца каталога, sticky-bit запрещает удаление файлов пользователями, не являющимися их владельцами.

6. После этого пользователь `alice` снова перешёл в каталог `/data/main`, создал файлы `alice3` и `alice4` и вывел список содержимого каталога (`ls -l`).

```
bob@titukaev:/data/main$
bob@titukaev:/data/main$ su alice
Password:
alice@titukaev:/data/main$ cd /data/main/
alice@titukaev:/data/main$ touch alice1
alice@titukaev:/data/main$ touch alice2
alice@titukaev:/data/main$
alice@titukaev:/data/main$ su bob
Password:
bob@titukaev:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Dec  9 11:59 alice1
-rw-r--r--. 1 alice alice 0 Dec  9 11:59 alice2
-rw-r--r--. 1 bob   bob   0 Dec  9 11:56 emptyfile
bob@titukaev:/data/main$ rm -f alice*
bob@titukaev:/data/main$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Dec  9 11:56 emptyfile
bob@titukaev:/data/main$ touch bob1
bob@titukaev:/data/main$ touch bob2
bob@titukaev:/data/main$ su
Password:
root@titukaev:/data/main# chmod g+s,o+t /data/main/
root@titukaev:/data/main#
exit
bob@titukaev:/data/main$
exit
alice@titukaev:/data/main$ touch alice3
alice@titukaev:/data/main$ touch alice4
alice@titukaev:/data/main$ ls -l
total 0
-rw-r--r--. 1 alice main 0 Dec  9 12:01 alice3
-rw-r--r--. 1 alice main 0 Dec  9 12:01 alice4
-rw-r--r--. 1 bob   bob  0 Dec  9 12:00 bob1
-rw-r--r--. 1 bob   bob  0 Dec  9 12:00 bob2
-rw-r--r--. 1 bob   bob  0 Dec  9 11:56 emptyfile
alice@titukaev:/data/main$ rm -rf bob*
rm: cannot remove 'bob1': Operation not permitted
rm: cannot remove 'bob2': Operation not permitted
alice@titukaev:/data/main$
```

Рис. 2.4: SGID и sticky-bit в каталоге /data/main

Пояснение: благодаря установленному SGID все новые файлы в каталоге `/data/main` теперь принадлежат группе `main`, независимо от личной основной группы пользователя, создавшего файлы.

7. Пользователь `alice` попытался удалить файлы `bob1` и `bob2`, выполнив `rm`

`-rf bob*`.

В ответ было выдано сообщение *Operation not permitted* для файлов `bob1` и `bob2`.

Пояснение: sticky-bit на каталоге `/data/main` запрещает удаление файлов, владельцем которых является другой пользователь. Поэтому `alice` не может удалить файлы `bob1` и `bob2`, хотя у неё есть права на запись в каталог. При этом `alice` по-прежнему может удалять собственные файлы в каталоге.

2.3 Управление расширенными разрешениями (ACL)

1. В терминале root выполнен вход (`su -`). Для групп были настроены расширенные права доступа с помощью ACL:
   - группе `third` даны права чтения и выполнения (`rx`) в каталоге `/data/main` командой `setfacl -m g:third:rx /data/main`;
   - группе `main` даны права чтения и выполнения (`rx`) в каталоге `/data/third` командой `setfacl -m g:main:rx /data/third`.
2. Командой `getfacl /data/main` выведены расширенные права каталога `/data/main`, а командой `getfacl /data/third` — каталога `/data/third`.

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# setfacl -m g:third:rx /data/main
root@titukaev:/home/titukaev# setfacl -m g:main:rx /data/third/
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev# 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@titukaev:/home/titukaev#
```

Рис. 2.5: ACL каталогов /data/main и /data/third

Пояснение: в выводе `getfacl` видно, что помимо обычных POSIX-прав появились записи для групп `third` и `main` соответственно, предоставляющие им доступ `r-x`.

3. Создан файл `/data/main/newfile1`. Команда `getfacl /data/main/newfile1` показала, что у файла установлены только стандартные права: владелец `root`, группа `main`, права `rw-` для владельца и группы, `r--` для остальных.

   Аналогично создан файл `/data/third/newfile1` и проверены его права.

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# touch /data/main/newfile1
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev# touch /data/third/newfile1
root@titukaev:/home/titukaev# 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@titukaev:/home/titukaev#
```

Рис. 2.6: ACL файлов newfile1 в каталогах /data/main и /data/third

Пояснение: так как ACL по умолчанию для каталогов ещё не были заданы, новые файлы получают только стандартные права, не наследуя дополнительных записей ACL.

4. Для каталогов были установлены ACL по умолчанию:
   - для `/data/main` — запись `d:g:third:rwx`, дающая группе `third` права `rwx` для всех новых объектов в каталоге (`setfacl -m d:g:third:rwx /data/main`);
   - для `/data/third` — запись `d:g:main:rwx`, дающая группе `main` права `rwx` для новых объектов (`setfacl -m d:g:main:rwx /data/third`).
5. Затем в каталоге `/data/main` создан новый файл `newfile2`. Команда `getfacl /data/main/newfile2` показала, что помимо стандартных прав у файла есть унаследованная запись ACL для группы `third` с правами `rwx`.

Аналогичные действия были выполнены для `/data/third/newfile2`, где файл унаследовал ACL для группы `main`.

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# setfacl -m d:g:third:rwx /data/main/
root@titukaev:/home/titukaev# setfacl -m d:g:main:rwx /data/third/
root@titukaev:/home/titukaev# touch /data/main/newfile2
root@titukaev:/home/titukaev# 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::---

root@titukaev:/home/titukaev# touch /data/third/newfile2
root@titukaev:/home/titukaev# getfacl /data/third/newfile2
getfacl: Removing leading '/' from absolute path names
# file: data/third/newfile2
# owner: root
# group: root
user::rw-
group::rwx                      #effective:rw-
group:main:rwx                  #effective:rw-
mask::rw-
other::---

root@titukaev:/home/titukaev#
```

Рис. 2.7: Наследование ACL по умолчанию для newfile2

Пояснение: теперь новые файлы наследуют ACL по умолчанию от родительских каталогов, поэтому соответствующие групповые права автоматически добавляются к каждому новому объекту.

6. Для проверки прав группы `third` выполнен вход под пользователем `carol` (член группы `third`).
   Пользователь `carol` попытался удалить файлы `/data/main/newfile1` и `/data/main/newfile2` командами `rm /data/main/newfile1` и `rm /data/main/newfile2`. Оба раза было выдано сообщение о невозможности удаления (*Permission denied*).

7. Затем пользователь `carol` попытался дозаписать данные в файлы:

- `echo "Hello world" >> /data/main/newfile1`
- `echo "Hello world" >> /data/main/newfile2`

Для обеих команд получено сообщение *Permission denied*.

```
root@titukaev:/home/titukaev#
root@titukaev:/home/titukaev# su carol
carol@titukaev:/home/titukaev$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'? y
rm: cannot remove '/data/main/newfile1': Permission denied
carol@titukaev:/home/titukaev$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
carol@titukaev:/home/titukaev$
carol@titukaev:/home/titukaev$ echo "Hello world" >> /data/main/newfile1
bash: /data/main/newfile1: Permission denied
carol@titukaev:/home/titukaev$ echo "Hello world" >> /data/main/newfile2
carol@titukaev:/home/titukaev$
```

Рис. 2.8: Проверка прав пользователя carol

Пояснение:

- Удаление файлов запрещено из-за установленного sticky-bit на каталоге `/data/main`: только владельцы файлов или суперпользователь могут их удалять.
- Попытка записи завершается неудачей, так как для существующих файлов `newfile1` и `newfile2` у группы, к которой принадлежит пользователь `carol`, нет прав на запись. В ACL для этих файлов группе `third` предоставлены права чтения и/или выполнения, но не права `w`. Поэтому, несмотря на наличие расширенных прав на каталог, пользователь не может изменять содержимое файлов.

3 Контрольные вопросы

1. Чтобы изменить владельца и группу файла, используют команду `chown` с указанием нового владельца и группы через двоеточие. Например: `chown user:group filename`.

2. Найти все файлы, принадлежащие конкретному пользователю, позволяет команда `find` с параметром `-user`. Например: `find / -user alice`.

3. Для применения прав чтения, записи и выполнения ко всем файлам каталога `/data` для владельца и группы, без предоставления прав другим пользователям, используют команду `chmod -R 770 /data`.

4. Добавить разрешение на выполнение для файла можно командой `chmod +x filename`.

5. Чтобы новые файлы автоматически наследовали групповую принадлежность каталога, применяется установка SGID-бита на каталог: `chmod g+s directory`.

6. Ограничить удаление файлов только их владельцами позволяет установка sticky-бита на каталог: `chmod +t directory`.

7. Добавить ACL, дающий группе права чтения для всех существующих файлов текущего каталога, можно командой `setfacl -m g:group:r *`.

8. Чтобы гарантировать группе права чтения на все текущие и будущие файлы, необходимо: • назначить ACL для существующих файлов: `setfacl -`

`m g:group:r *` • назначить ACL по умолчанию для каталога: `setfacl -m d:g:group:rx .`

9. Для того чтобы «другие» пользователи не получали никаких прав при создании файлов, маска umask должна запрещать все разрешения для категории “other”. Например: `umask 007`.

10. Чтобы предотвратить случайное удаление файла `myfile`, можно убрать для него разрешение на запись или установить immutable-атрибут. Например: `chattr +i myfile`.

4 Заключение

В ходе выполнения лабораторной работы были продемонстрированы различные механизмы управления правами доступа в Linux. Были изучены базовые разрешения, специальные атрибуты (SGID и sticky-bit), а также расширенные списки контроля доступа ACL.