РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

Презентация
по лабораторной работе
НАСТРОЙКА ПРАВ ДОСТУПА

дисциплина: Основы администрирования операционных систем

Студент: Павленко Сергей
Группа: НПИбд-02-23
№ ст. билета: 1032235465

МОСКВА

2024 г.

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

Выполнение лабораторной работы:

Откройте терминал с учётной записью root:

```
[spavlenko@spavlenko ~]$ su spavlenko
Password:
[spavlenko@spavlenko ~]$
```

В корневом каталоге создайте каталоги /data/main и /data/third: mkdir -p /data/main /data/third Посмотрите, кто является владельцем этих каталогов. Для этого используйте: ls -Al /data

```
[spavlenko@spavlenko ~]$ sudo mkdir -p /data/main /data/third
[sudo] password for spavlenko:
[spavlenko@spavlenko ~]$ ls -Al /data
total 0
drwxr-xr-x. 2 root root 6 Sep 21 19:47 main
drwxr-xr-x. 2 root root 6 Sep 21 19:47 third
[spavlenko@spavlenko ~]$
```

Прежде чем устанавливать разрешения, измените владельцев этих каталогов с root на main и third соответственно: chgrp main /data/main chgrp third /data/third Посмотрите, кто теперь является владельцем этих каталогов: ls -Al /data

```
[spavlenko@spavlenko ~]$ sudo chgrp main /data/main
[spavlenko@spavlenko ~]$ sudo chgrp third /data/third
[spavlenko@spavlenko ~]$ ls -Al /data
total 0
drwxr-xr-x. 2 root main  6 Sep 21 19:47 main
drwxr-xr-x. 2 root third 6 Sep 21 19:47 third
[spavlenko@spavlenko ~]$
```

Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам: chmod 770 /data/main chmod 770 /data/third Проверьте установленные права доступа.

```
[spavlenko@spavlenko ~]$ sudo chmod 770 /data/main
[spavlenko@spavlenko ~]$ sudo chmod 770 /data/third
[spavlenko@spavlenko ~]$ ls -Al /data
total 0
drwxrwx---. 2 root main  6 Sep 21 19:47 main
drwxrwx---. 2 root third 6 Sep 21 19:47 third
[spavlenko@spavlenko ~]$
```

В другом терминале перейдите под учётную запись пользователя bob: su – bob

```
[spavlenko@spavlenko ~]$ su bob
Password:
[bob@spavlenko spavlenko]$
```

Под пользователем bob попробуйте перейти в каталог /data/main и создать файл emptyfile в этом каталоге: cd /data/main

touch emptyfile

ls -Al

Опишите и поясните результат этого действия

Возможные результаты: **Успешное создание файла:** Если пользователь bob имеет права на запись в каталог /data/main, файл emptyfile будет успешно создан. Команда ls -Al покажет, что файл был создан с пустым содержимым (размер 0 байт), а также отобразит права доступа к нему или же **Ошибка "Permission denied":** Если у пользователя bob нет прав на запись в каталог /data/main, команда touch emptyfile вызовет ошибку:

```
[bob@spavlenko spavlenko]$ cd /data/main
[bob@spavlenko main]$ touch emptyfile
[bob@spavlenko main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 21 19:52 emptyfile
[bob@spavlenko main]$
```

Под пользователем bob попробуйте перейти в каталог /data/third и создать файл emptyfile в этом каталоге. Опишите и поясните результат этого действия.

Возможные результаты и их объяснение:

Успешное создание файла: если пользователь bob имеет права на запись в каталог /data/third, файл emptyfile будет создан без ошибок. Команда ls -Al покажет права доступа к этому файлу.

Ошибка "Permission denied": если у пользователя bob нет прав на запись в каталог /data/third, команда touch emptyfile вызовет ту же ошибку:

```
[bob@spavlenko main]$ cd /data/third/
bash: cd: /data/third/: Permission denied
[bob@spavlenko main]$ touch emptyfile
[bob@spavlenko main]$ ls -Al
total 0
-rw-r--r--. 1 bob bob 0 Sep 21 19:53 emptyfile
[bob@spavlenko main]$
```

Откройте новый терминал под пользователем alice.

Перейдите в каталог /data/main: cd /data/main Создайте два файла, владельцем которых является alice: touch alice1 touch alice2

```
[bob@spavlenko main]$ su alice
Password:
[alice@spavlenko main]$ cd /data/main/
[alice@spavlenko main]$ touch alice1
[alice@spavlenko main]$ touch alice2
[alice@spavlenko main]$
```

В другом терминале перейдите под учётную запись пользователя bob (пользователь bob является членом группы main, как и alice): su – bob

```
[spavlenko@spavlenko ~]$ su bob
Password:
[bob@spavlenko spavlenko]$
```

Перейдите в каталог /data/main: cd /data/main и в этом каталоге введите: ls -l Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice: rm -f alice* Убедитесь, что файлы будут удалены пользователем bob.

```
[bob@spavlenko spavlenko]$ cd /data/main/
[bob@spavlenko main]$ ls -l
total 0
-rw-r--r--. 1 alice alice 0 Sep 21 19:54 alice1
-rw-r--r--. 1 alice alice 0 Sep 21 19:54 alice2
-rw-r--r--. 1 bob   bob   0 Sep 21 19:53 emptyfile
[bob@spavlenko main]$ rm -f alice*
[bob@spavlenko main]$ ls -l
total 0
-rw-r--r--. 1 bob bob 0 Sep 21 19:53 emptyfile
[bob@spavlenko main]$
```

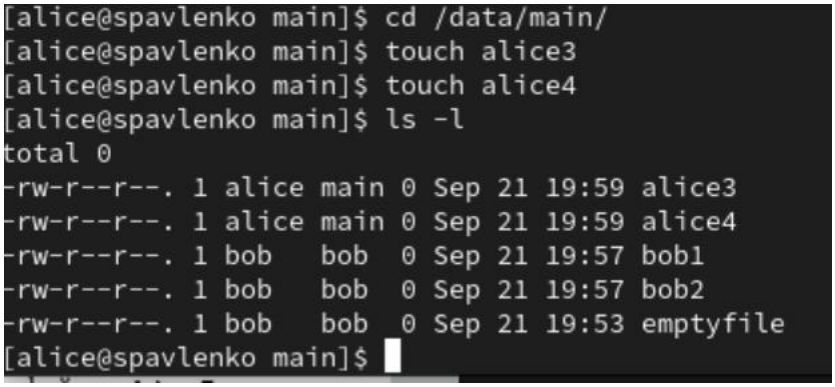
Создайте два файла, которые принадлежат пользователю bob: touch bob1 touch bob2

```
[bob@spavlenko main]$ touch bob1
[bob@spavlenko main]$ touch bob2
[bob@spavlenko main]$
```

В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также stiky-бит для разделяемого (общего) каталога группы: chmod g+s,o+t /data/main

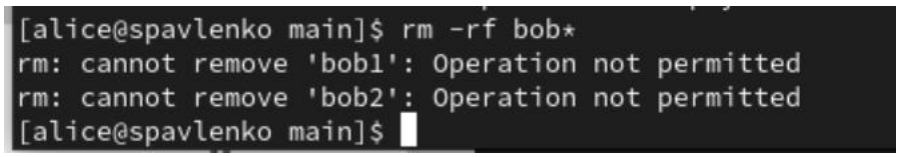
```
[spavlenko@spavlenko ~]$ sudo chmod g+s,o+t /data/main
[sudo] password for spavlenko:
[spavlenko@spavlenko ~]$
```

В терминале под пользователем alice создайте в каталоге /data/main файлы alice3 и alice4: touch alice3 touch alice4 ls -l Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.

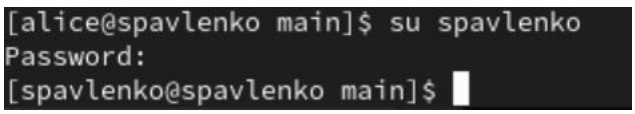


В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob: rm -rf bob*

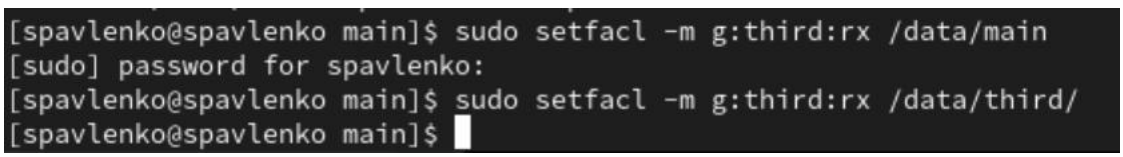
Убедитесь, что sticky-bit предотвратит удаление этих файлов пользователем alice, поскольку этот пользователь не является владельцем этих файлов. Обратите внимание: поскольку пользователь alice является владельцем каталога /data/main, то он может удалить все свои файлы в любом случае.



Откройте терминал с учётной записью root su



Установите 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: setfacl -m g:third:rx /data/main setfacl -m g:main:rx /data/third



Используйте команду getfacl, чтобы убедиться в правильности установки разрешений: getfacl /data/main getfacl /data/third

```
[spavlenko@spavlenko main]$ getfacl /data/main
getfacl: Removing leading '/' from absolute path names
# file: data/main
# owner: root
# group: main
# flags: -st
user::rwx
group::rwx
other::---

[spavlenko@spavlenko main]$ getfacl /data/third/
getfacl: Removing leading '/' from absolute path names
# file: data/third/
# owner: root
# group: third
user::rwx
group::rwx
other::---

[spavlenko@spavlenko main]$
```

Создайте новый файл с именем newfile1 в каталоге /data/main: touch /data/main/newfile1

Используйте getfacl /data/main/newfile1 для проверки текущих назначений полномочий. Какие права доступа у этого файла? Объясните, почему. Выполните аналогичные действия для каталога /data/third. Дайте пояснения.

Объяснение:

- **user::rw-**: Владелец файла (root) имеет права на чтение и запись (но не на выполнение).
- **group::r--**: Группа, к которой принадлежит файл (root), имеет только права на чтение.
- **other::r--**: Остальные пользователи также имеют только права на чтение.

```
[spavlenko@spavlenko main]$ touch /data/third/newfile1
touch: cannot touch '/data/third/newfile1': Permission denied
[spavlenko@spavlenko main]$ sudo touch /data/third/newfile1
[spavlenko@spavlenko main]$ sudo 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--

[spavlenko@spavlenko main]$
```

Установите ACL по умолчанию для каталога /data/main: setfacl -m d:g:third:rwx /data/main

Добавьте ACL по умолчанию для каталога /data/third:

```
[spavlenko@spavlenko main]$ sudo setfacl -m d:g:third:rwx /data/main
[spavlenko@spavlenko main]$ sudo setfacl -m d:g:main:rwx /data/third
```

Убедитесь, что настройки ACL работают, добавив новый файл в каталог /data/main: touch /data/main/newfile2

Используйте getfacl /data/main/newfile2 для проверки текущих назначений полномочий. Выполните аналогичные действия для каталога /data/third.

```
[spavlenko@spavlenko main]$ touch /data/main/newfile2
touch: cannot touch '/data/main/newfile2': Permission denied
[spavlenko@spavlenko main]$ sudo touch /data/main/newfile2
[spavlenko@spavlenko main]$ sudo 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::---

[spavlenko@spavlenko main]$ sudo touch /data/third/newfile2
[spavlenko@spavlenko main]$ sudo 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::---

[spavlenko@spavlenko main]$
```

Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third: su - carol Проверьте операции с файлами: rm /data/main/newfile1 rm /data/main/newfile2 Проверьте, возможно ли осуществить запись в файл: echo "Hello, world" >> /data/main/newfile1 echo "Hello, world" >> /data/main/newfile2 Объясните результат произведённых действий.

Удаление произошло только для файла newfile1, так как пользователю предоставлены права на запись в каталоге, в то время как для файла newfile2 у пользователя нет прав для этого

Запись невозможна для файла newfile1, так как произошло его удаление, а запись для файла newfile2 возможна так как у пользователя есть права на запись в файл и каталог

```
[spavlenko@spavlenko main]$ su carol
Password:
[carol@spavlenko main]$ rm /data/main/newfile1
rm: remove write-protected regular empty file '/data/main/newfile1'?
[carol@spavlenko main]$ rm /data/main/newfile2
rm: cannot remove '/data/main/newfile2': Permission denied
[carol@spavlenko main]$ echo "Hello, world" >> /data/main/newfile1
bash: /data/main/newfile1: Permission denied
[carol@spavlenko main]$ echo "Hello, world" >> /data/main/newfile2
[carol@spavlenko main]$
```

Вывод: в ходе выполнения лабораторной работы были получены практические навыки по настройке прав доступа в операционной системе Linux

Контрольные вопросы:

1. Как следует использовать команду chown, чтобы установить владельца группы для файла? Приведите пример.

Команда chown позволяет установить нового владельца и группу для файла. Для этого используется синтаксис chown user:group filename.

2. С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю? Приведите пример.

Для поиска всех файлов, принадлежащих конкретному пользователю, можно использовать команду find с параметром -user. Пример: find / -user alice

3. Как применить разрешения на чтение, запись и выполнение для всех файлов в каталоге /data для пользователей и владельцев групп, не устанавливая никаких прав для других? Приведите пример.

Для этого используется команда chmod с параметрами для пользователей (u) и групп (g), не устанавливая прав для остальных (o). Пример: chmod -R ug+rwx,o-rwx /data

4. Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?

Для этого используется команда chmod с флагом +x.

5. Какая команда позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога? Приведите пример.

Для этого используется установка SGID-бита на каталог с помощью команды chmod.

Пример: chmod g+s /directory

6. Необходимо, чтобы пользователи могли удалять только те файлы, владельцами которых они являются, или которые находятся в каталоге, владельцами которого они являются. С помощью какой команды можно это сделать? Приведите пример.

Для этого можно установить **Sticky bit** на каталог, чтобы пользователи могли удалять только свои файлы.

chmod +t /shared

7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге?

Для управления доступом через ACL (Access Control List) используется команда setfacl.

8. Что нужно сделать для гарантии того, что члены группы получат разрешения на чтение для всех файлов в текущем каталоге и во всех его подкаталогах, а также для всех файлов, которые будут созданы в этом каталоге в будущем? Приведите пример.

Чтобы обеспечить это, можно использовать рекурсивную установку ACL с флагом наследования для группы.

Пример: setfacl -R -m g:groupname:rx . && setfacl -d -m g:groupname:rx .

9. Какое значение umask нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы? Приведите пример.

Значение umask определяет права по умолчанию для создаваемых файлов. Чтобы "другие" пользователи не получали прав, нужно установить umask в 0077.

Пример: umask 0077

10. Какая команда гарантирует, что никто не сможет удалить файл myfile случайно?

Для защиты файла от удаления можно сделать его неизменяемым с помощью команды chattr (устанавливается атрибут immutable). chattr +i myfile