Лабараторная работа №3

Отчет

Славинский Владислав Вадимович

Содержание

Список иллюстраций

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 учетой записью root(рис. 2.1)

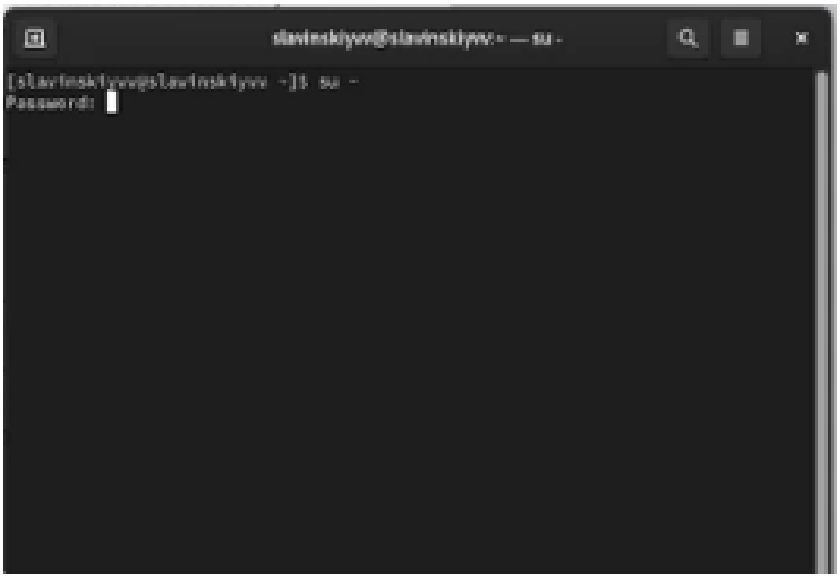

Рис. 2.1: Открытие терминала с root

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

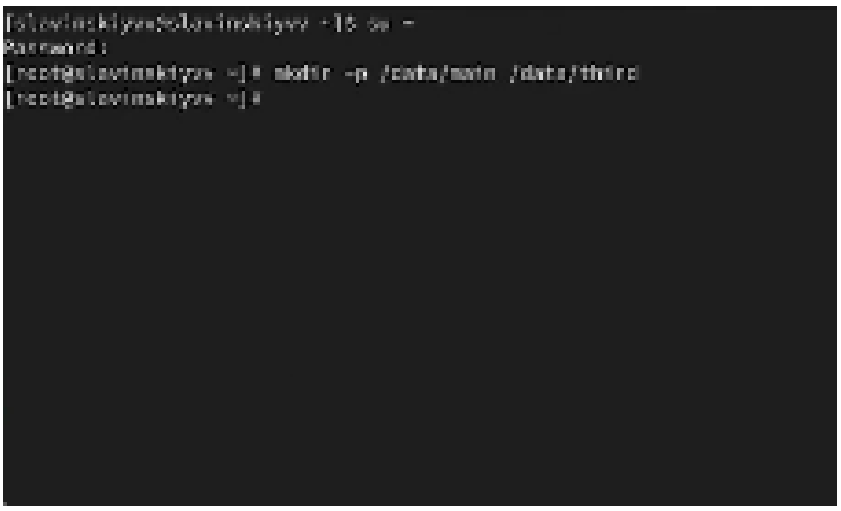

Рис. 2.2: Создание каталогов main и third

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

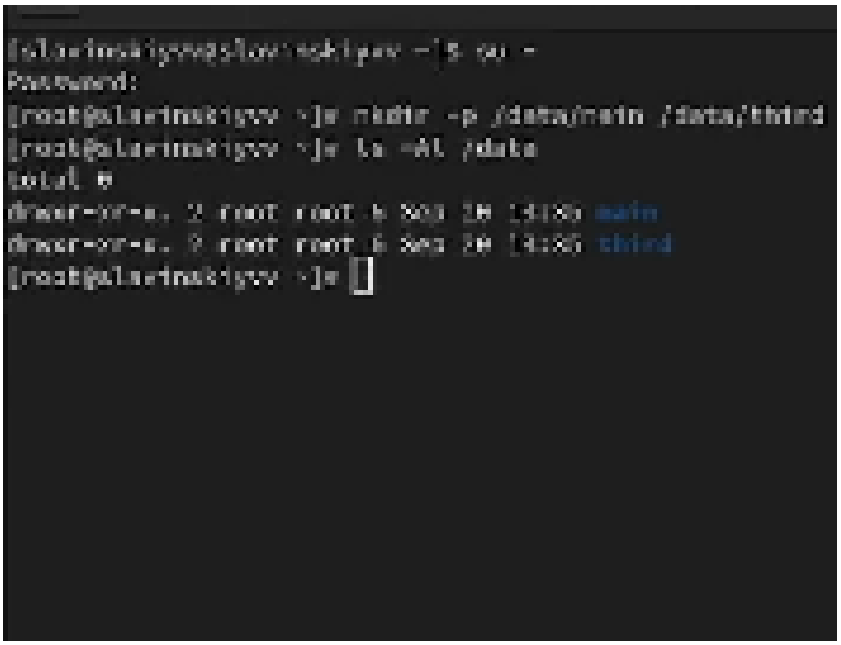

Рис. 2.3: Владелец каталогов

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

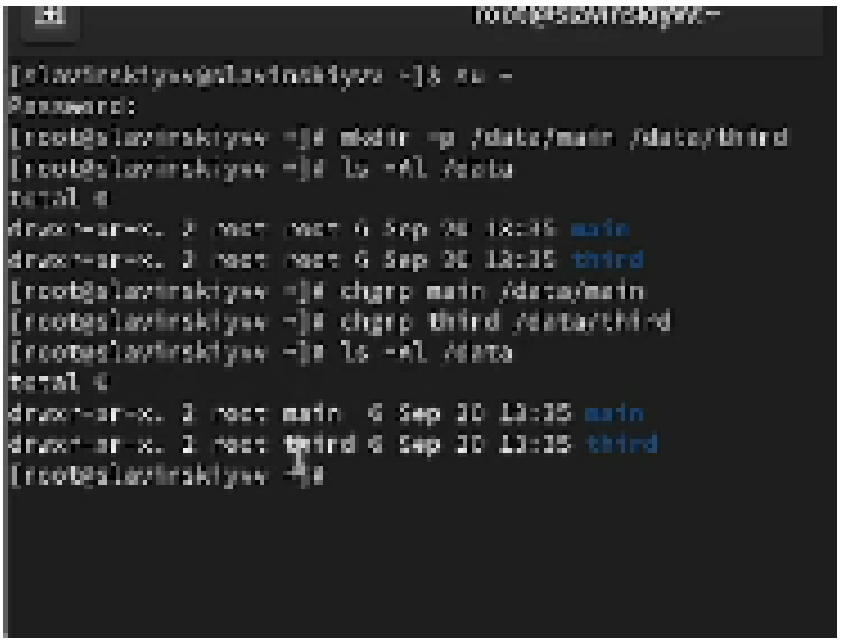

Рис. 2.4: Смена владельцев

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)

Рис. 2.5: Установка разрешений

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

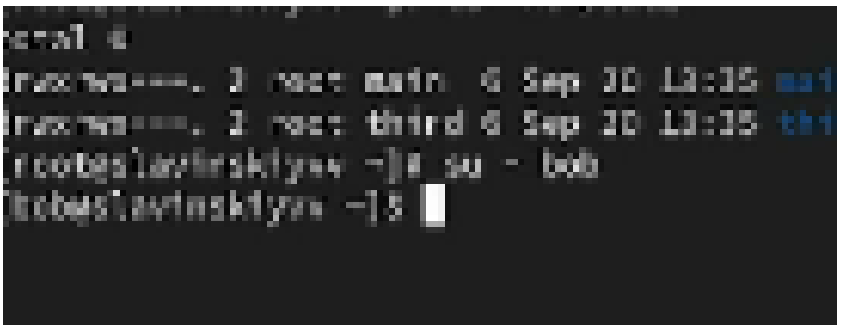

Рис. 2.6: Переход на учетную запись bob

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)

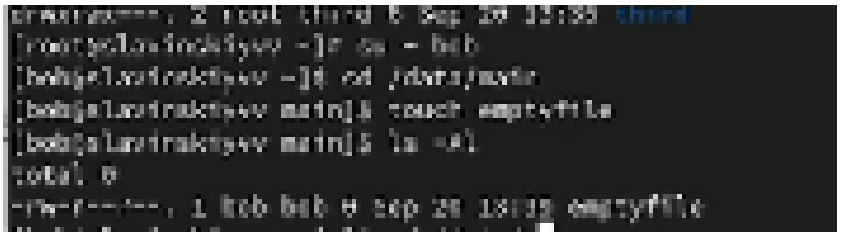

Рис. 2.7: Создание файла под пользователем bob в каталоге /data/main

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)

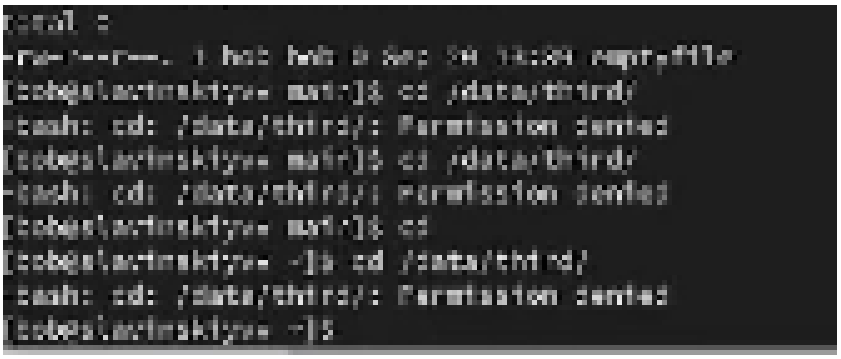

Рис. 2.8: Создание файла в каталоге /data/third

Переключимся на учётную запись пользователя alice(рис. 2.9)

Рис. 2.9: Переключение на пользователя alice

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

Рис. 2.10: Создание alice1, alice2

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

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)

Рис. 2.12: Удаление файлов

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

Рис. 2.13: Создание bob1,bob2

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

Рис. 2.14: Установка бит идентификатора группы и stiky-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)

Рис. 2.15: Создание файлов

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

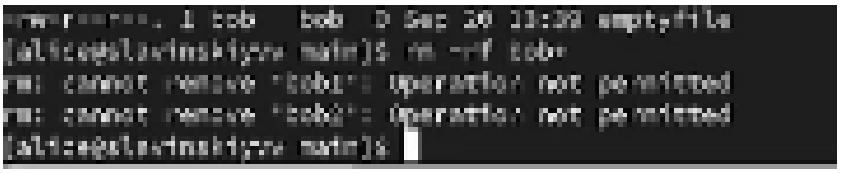

Рис. 2.16: Проверка защиты sticky-bit

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

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)

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)

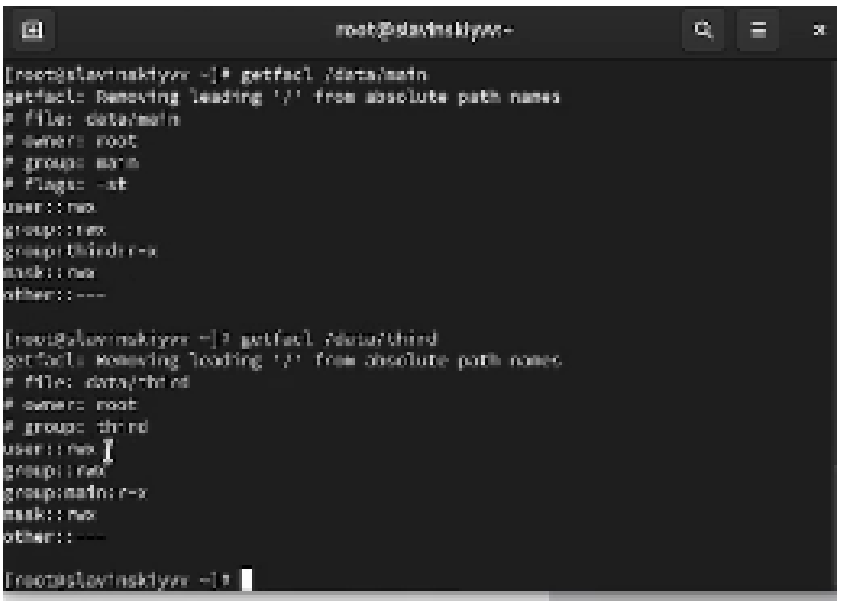

Рис. 2.19: Проверка разрешений

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)

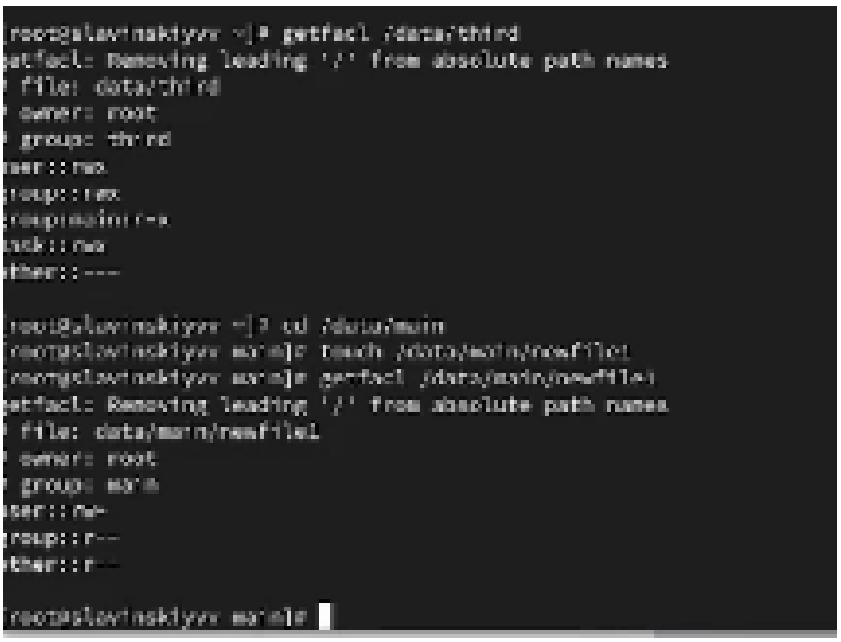

Рис. 2.20: Полномочия файла newfile1

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

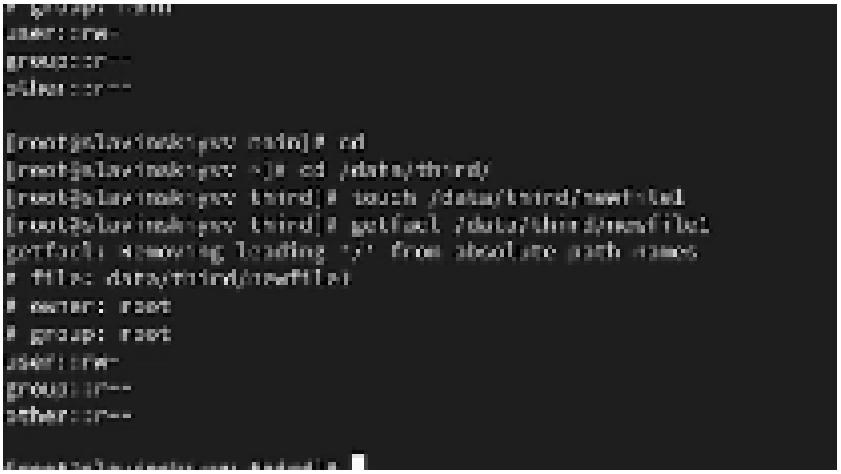

Рис. 2.21: Полномочия файла newfile1 в каталоге third

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

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

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

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)

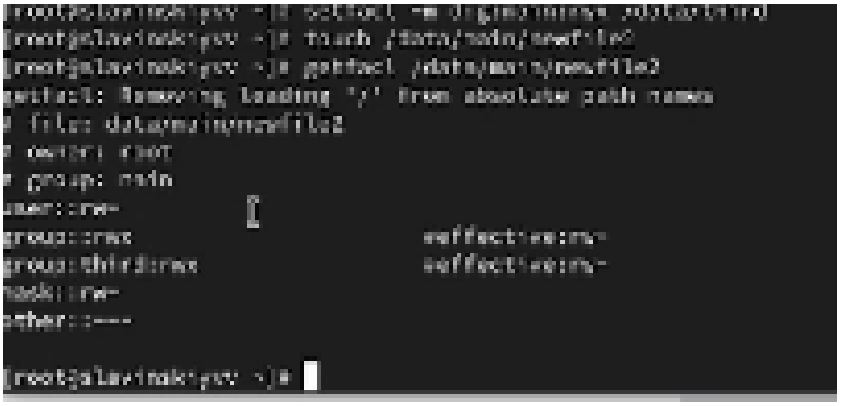

Рис. 2.24: Проверка настроек

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

Рис. 2.25: Проверка настроек

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

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)

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.