

Лабораторная работа 3

Дискреционное разграничение прав в Linux. Два пользователя

Смородова Дарья Владимировна

2022 Sep 22nd

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	8
4	Выводы	15
5	Список литературы	16

List of Tables

List of Figures

3.1	Создание пользователя guest2 и задание ему пароля	8
3.2	Добавление пользователя guest2 в группу guest	8
3.3	Вход в систему от двух пользователей на двух разных консолях .	9
3.4	Определение директории, в которой мы находимся	9
3.5	Проверка id	10
3.6	Файл /etc/passwd	11
3.7	Файл /etc/passwd	11
3.8	Регистрация пользователя guest2 в группе guest	12
3.9	Изменение прав директории /home/guest	12
3.10	Проверка правильности снятия атрибутов	12
3.11	Установленные права и разрешённые действия для групп 1	13
3.12	Установленные права и разрешённые действия для групп 2	13
3.13	Минимальные права для совершения операций от имени пользо- вателей входящих в группу	14

1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов для групп пользователей.

2 Теоретическое введение

В операционной системе Linux есть много отличных функций безопасности, но она из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо.

Изначально каждый файл имеет три параметра доступа:

- Чтение - разрешает получать содержимое файла, но на запись нет. Для каталога позволяет получить список файлов и каталогов, расположенных в нем;
- Запись - разрешает записывать новые данные в файл или изменять существующие, а также позволяет создавать и изменять файлы и каталоги;
- Выполнение - вы не можете выполнить программу, если у нее нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система может понять, что этот файл нужно запускать как программу.

Но все эти права были бы бессмысленными, если бы применялись сразу для всех пользователей. Поэтому каждый файл имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

- Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права, чтение, запись и выполнение.

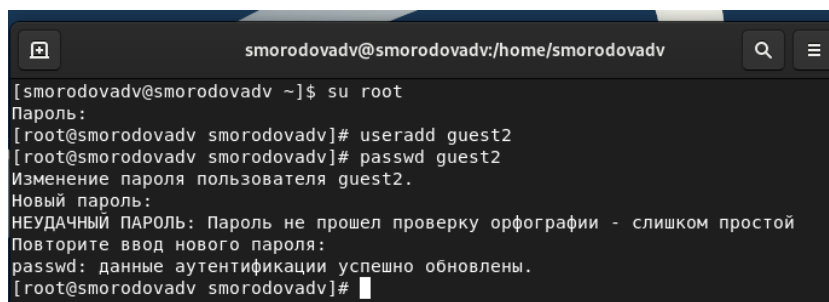
- Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и обычно это группа владельца, хотя для файла можно назначить и другую группу.
- Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла.

Именно с помощью этих наборов полномочий устанавливаются права файлов в linux. Каждый пользователь может получить полный доступ только к файлам, владельцем которых он является или к тем, доступ к которым ему разрешен. Только пользователь Root может работать со всеми файлами независимо от их набора их полномочий. ¹

¹Права доступа к файлам в Linux

3 Выполнение лабораторной работы ¹


1. В установленной операционной системе уже была создана учётная запись пользователя guest (используя учётную запись администратора) и был задан пароль для неё.
2. Аналогичным образом создаем второго пользователя guest2 (рис. 3.1):



```
smorodovadv@smorodovadv:~/home/smorodovadv
[smorodovadv@smorodovadv ~]$ su root
Пароль:
[root@smorodovadv smorodovadv]# useradd guest2
[root@smorodovadv smorodovadv]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не прошел проверку орфографии - слишком простой
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
[root@smorodovadv smorodovadv]#
```

Figure 3.1: Создание пользователя guest2 и задание ему пароля

3. Добавим пользователя guest2 в группу guest при помощи команды gpasswd -a guest2 guest (рис. 3.2):

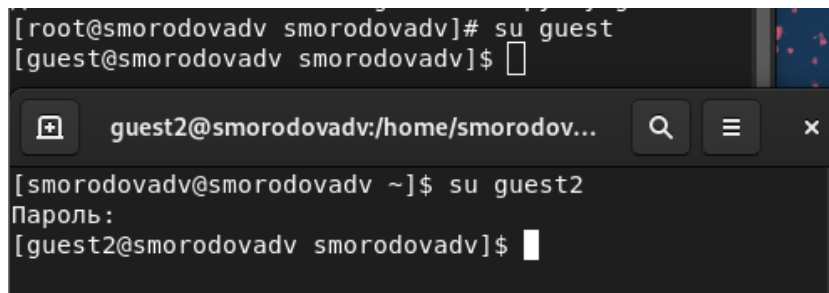


```
[root@smorodovadv smorodovadv]# gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[root@smorodovadv smorodovadv]#
```

Figure 3.2: Добавление пользователя guest2 в группу guest

4. Осуществим вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли (рис. 3.3):

¹Методические материалы к лабораторной работе



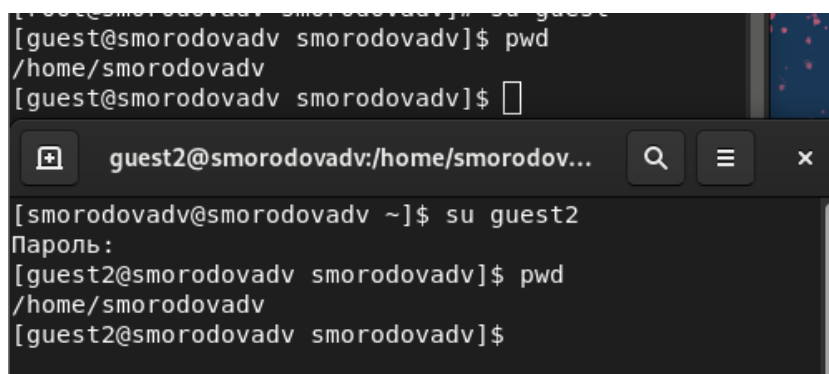
The image shows two terminal windows. The top window is a root shell on a host named 'smorodovadv', where the command 'su guest' is entered, resulting in a shell prompt for the 'guest' user. The bottom window is a regular user shell for 'smorodovadv', where the command 'su guest2' is entered, followed by a password prompt, and then a shell prompt for the 'guest2' user.

```
[root@smorodovadv smorodovadv]# su guest
[guest@smorodovadv smorodovadv]$
```

```
guest2@smorodovadv:/home/smorodov...
[smorodovadv@smorodovadv ~]$ su guest2
Пароль:
[guest2@smorodovadv smorodovadv]$
```

Figure 3.3: Вход в систему от двух пользователей на двух разных консолях

5. Для обоих пользователей командой `pwd` определим директорию, в которой мы находимся (рис. 3.4):



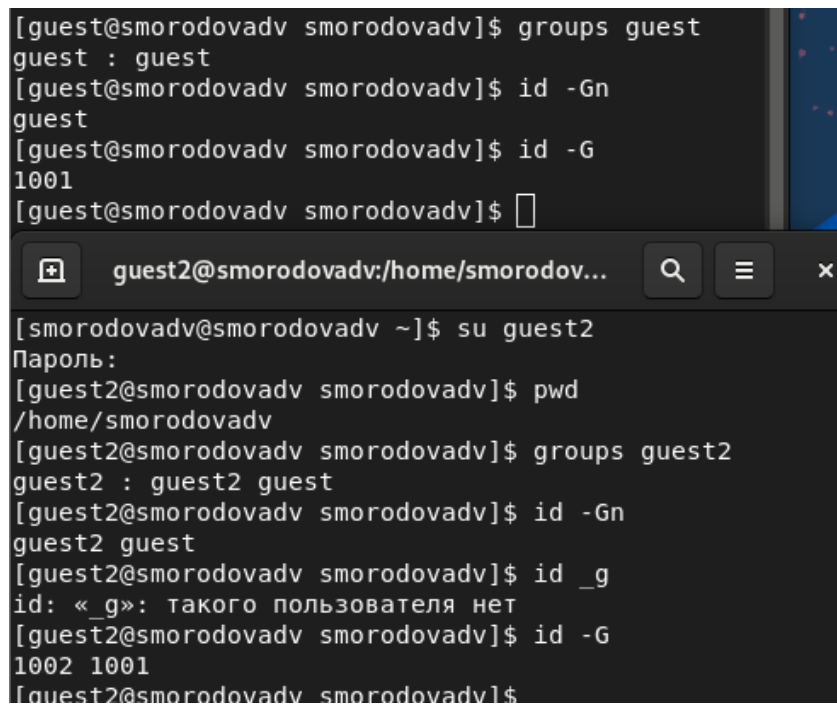
The image shows two terminal windows. In the top window, the 'guest' user runs 'pwd', which outputs '/home/smorodovadv'. In the bottom window, the 'smorodovadv' user switches to 'guest2' and runs 'pwd', which also outputs '/home/smorodovadv'.

```
[root@smorodovadv smorodovadv]# su guest
[guest@smorodovadv smorodovadv]$ pwd
/home/smorodovadv
[guest@smorodovadv smorodovadv]$
```

```
guest2@smorodovadv:/home/smorodov...
[smorodovadv@smorodovadv ~]$ su guest2
Пароль:
[guest2@smorodovadv smorodovadv]$ pwd
/home/smorodovadv
[guest2@smorodovadv smorodovadv]$
```

Figure 3.4: Определение директории, в которой мы находимся

6. Уточним имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определим командами `groups guest` и `groups guest2`, в какие группы входят пользователи `guest` и `guest2`. Сравним вывод команды `groups` с выводом команд `id -Gn` и `id -G`. Данные при этих выводах совпадают (рис. 3.5):



```
[guest@smorodovadv smorodovadv]$ groups guest
guest : guest
[guest@smorodovadv smorodovadv]$ id -Gn
guest
[guest@smorodovadv smorodovadv]$ id -G
1001
[guest@smorodovadv smorodovadv]$
```

guest2@smorodovadv:/home/smorodovadv

```
[smorodovadv@smorodovadv ~]$ su guest2
Пароль:
[guest2@smorodovadv smorodovadv]$ pwd
/home/smorodovadv
[guest2@smorodovadv smorodovadv]$ groups guest2
guest2 : guest2 guest
[guest2@smorodovadv smorodovadv]$ id -Gn
guest2 guest
[guest2@smorodovadv smorodovadv]$ id _g
id: «_g»: такого пользователя нет
[guest2@smorodovadv smorodovadv]$ id -G
1002 1001
[guest2@smorodovadv smorodovadv]$
```

Figure 3.5: Проверка id

7. Посмотрим файл /etc/passwd (рис. 3.6 - 3.7):

```
[guest@smorodovadv smorodovadv]$ cat /etc/group
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:smorodovadv
cdrom:x:11:
mail:x:12:
man:x:15:
dialout:x:18:
floppy:x:19:
games:x:20:
tape:x:33:
video:x:39:
ftp:x:50:
lock:x:54:
audio:x:63:
users:x:100:
nobody:x:65534:
utmp:x:22:
utempter:x:35:
input:x:999:
kvm:x:36:
render:x:998:
systemd-journal:x:190:
systemd-coredump:x:997:
```

Figure 3.6: Файл /etc/passwd

```
smorodovadv:x:1000:
vboxsf:x:976:
guest:x:1001:guest2
guest2:x:1002:
[guest@smorodovadv smorodovadv]$ █
```

Figure 3.7: Файл /etc/passwd

8. От имени пользователя guest2 выполним регистрацию пользователя guest2 в группе guest командой newgrp guest (рис. 3.8):

```
[guest2@smorodovadv smorodovadv]$ newgrp guest
[guest2@smorodovadv smorodovadv]$
```

Figure 3.8: Регистрация пользователя guest2 в группе guest

9. От имени пользователя guest изменим права директории /home/guest, разрешив все действия для пользователей группы при помощи команды `chmod g+rxw /home/guest` (рис. 3.9):

```
[guest@smorodovadv smorodovadv]$ chmod g+rxw /home/guest
[guest@smorodovadv smorodovadv]$
```

Figure 3.9: Изменение прав директории /home/guest

10. Проверим правильность снятия атрибутов 3.10):

```
[guest@smorodovadv ~]$ chmod 000 dir1
[guest@smorodovadv ~]$ ls -l
итого 0
d----- . 2 guest guest 18 сен 14 19:20 dir1
drwxr-xr-x. 2 guest guest 6 сен 14 17:37 Видео
drwxr-xr-x. 2 guest guest 6 сен 14 17:37 Документы
drwxr-xr-x. 2 guest guest 6 сен 14 17:37 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 14 17:37 Изображения
drwxr-xr-x. 2 guest guest 6 сен 14 17:37 Музыка
drwxr-xr-x. 2 guest guest 6 сен 14 17:37 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 14 17:37 'Рабочий стол'
drwxr-xr-x. 2 guest guest 6 сен 14 17:37 Шаблоны
[guest@smorodovadv ~]$
```

Figure 3.10: Проверка правильности снятия атрибутов

11. Заполним таблицу «Установленные права и разрешённые действия для групп», меняя атрибуты у директории `dir1` и файла `file1` от имени пользователя `guest` и делая проверку от пользователя `guest2`, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесем в таблицу знак «+», если не разрешена – знак «-».
12. Получившаяся таблица «Установленные права и разрешённые действия для групп» (рис. 3.11 - 3.12):

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(010)	-	-	-	-	-	-	-	-
d(000)	(020)	-	-	-	-	-	-	-	-
d(000)	(030)	-	-	-	-	-	-	-	-
d(000)	(040)	-	-	-	-	-	-	-	-
d(000)	(050)	-	-	-	-	-	-	-	-
d(000)	(060)	-	-	-	-	-	-	-	-
d(000)	(070)	-	-	-	-	-	-	-	-
d----x---	(010)	(000)	-	-	-	+	-	-	-
d----x---	(010)	(010)	-	-	-	+	-	-	-
d----x---	(010)	(020)	-	-	+	-	-	-	-
d----x---	(010)	(030)	-	-	+	-	-	-	-
d----x---	(010)	(040)	-	-	-	+	-	-	-
d----x---	(010)	(050)	-	-	-	+	-	-	-
d----x---	(010)	(060)	-	-	+	+	-	-	-
d----x---	(010)	(070)	-	-	+	+	-	-	-
d----w----	(020)	(000)	-	-	-	-	-	-	-
d----w----	(020)	(010)	-	-	-	-	-	-	-
d----w----	(020)	(020)	-	-	-	-	-	-	-
d----w----	(020)	(030)	-	-	-	-	-	-	-
d----w----	(020)	(040)	-	-	-	-	-	-	-
d----w----	(020)	(050)	-	-	-	-	-	-	-
d----w----	(020)	(060)	-	-	-	-	-	-	-
d----w----	(020)	(070)	-	-	-	-	-	-	-
d----wx---	(030)	(000)	+	+	-	+	-	+	-
d----wx---	(030)	(010)	+	+	-	+	-	+	-
d----wx---	(030)	(020)	+	+	+	-	-	+	-
d----wx---	(030)	(030)	+	+	+	-	-	+	-
d----wx---	(030)	(040)	+	+	-	+	-	+	-
d----wx---	(030)	(050)	+	+	-	+	-	+	-
d----wx---	(030)	(060)	+	+	+	+	-	+	-
d----wx---	(030)	(070)	+	+	+	+	-	+	-

Figure 3.11: Установленные права и разрешённые действия для групп 1

d---r-----	(040)	(000)	-	-	-	-	+	-	-
d---r-----	(040)	(010)	-	-	-	-	+	-	-
d---r-----	(040)	(020)	-	-	-	-	+	-	-
d---r-----	(040)	(030)	-	-	-	-	+	-	-
d---r-----	(040)	(040)	-	-	-	-	+	-	-
d---r-----	(040)	(050)	-	-	-	-	+	-	-
d---r-----	(040)	(060)	-	-	-	-	+	-	-
d---r-----	(040)	(070)	-	-	-	-	+	-	-
d---r-x---	(050)	(000)	-	-	-	+	+	-	-
d---r-x---	(050)	(010)	-	-	-	+	+	-	-
d---r-x---	(050)	(020)	-	-	+	-	+	-	-
d---r-x---	(050)	(030)	-	-	+	-	+	-	-
d---r-x---	(050)	(040)	-	-	-	+	+	-	-
d---r-x---	(050)	(050)	-	-	-	+	+	-	-
d---r-x---	(050)	(060)	-	-	+	+	+	-	-
d---r-x---	(050)	(070)	-	-	+	+	+	-	-
d---rw----	(060)	(000)	-	-	-	-	+	-	-
d---rw----	(060)	(010)	-	-	-	-	+	-	-
d---rw----	(060)	(020)	-	-	-	-	+	-	-
d---rw----	(060)	(030)	-	-	-	-	+	-	-
d---rw----	(060)	(040)	-	-	-	-	+	-	-
d---rw----	(060)	(050)	-	-	-	-	+	-	-
d---rw----	(060)	(060)	-	-	-	-	+	-	-
d---rw----	(060)	(070)	-	-	-	-	+	-	-
d---rwx---	(070)	(000)	+	+	-	+	+	+	-
d---rwx---	(070)	(010)	+	+	-	+	+	+	-
d---rwx---	(070)	(020)	+	+	+	-	+	+	-
d---rwx---	(070)	(030)	+	+	+	-	+	+	-
d---rwx---	(070)	(040)	+	+	-	+	+	+	-
d---rwx---	(070)	(050)	+	+	-	+	+	+	-
d---rwx---	(070)	(060)	+	+	+	+	+	+	-
d---rwx---	(070)	(070)	+	+	+	+	+	+	-

Figure 3.12: Установленные права и разрешённые действия для групп 2

13. Главное отличие между таблицами в лабораторной работе №2 и этой таблицей в том, что в предыдущей таблице смена атрибутов файла возможна при любых правах директории и файла, а в таблице в лабораторной работе №3 смена атрибутов файла невозможна ни при каких правах.

14. На основании заполненной таблицы определим те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1, заполним таблицу «Минимальные права для совершения операций от имени пользователей входящих в группу» (рис. 3.13):

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(030)	(000)
Удаление файла	d(030)	(000)
Чтение файла	d(010)	(040)
Запись в файл	d(010)	(020)
Переименование файла	d(030)	(000)
Создание поддиректории	d(030)	(000)
Удаление поддиректории	d(030)	(000)

Figure 3.13: Минимальные права для совершения операций от имени пользователей входящих в группу

4 Выводы

В ходе данной лабораторной работы, мы получили практические навыки работы в консоли с атрибутами файлов для групп пользователей.

5 Список литературы

1. Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН”
2. Права доступа к файлам в Linux