

Лабораторная работа №3

Дискреционное разграничение прав в Linux. Два пользователя

Топонен Никита Андреевич

Содержание

Цель работы	5
Задание	6
Теоретическое введение	7
Выполнение лабораторной работы	8
Выводы	20
Список литературы	21

Список иллюстраций

1	Создание пользователя guest2	8
2	Добавление пользователя guest2 в группу guest	8
3	Вход в систему от пользователя guest	9
4	Вход в систему от пользователя guest2	9
5	Нахождение пользователя guest	9
6	Нахождение пользователя guest2	9
7	Имя пользователя guest	9
8	Имя пользователя guest2	10
9	Группа пользователя guest, кто входит в неё и к каким группам принадлежит он сам	10
10	Группа пользователя guest2, кто входит в неё и к каким группам принадлежит он сам	10
11	Группы пользователя guest	10
12	Группы пользователя guest2	11
13	Вывод команды cat /etc/group	11
14	Регистрация пользователя guest2 в группе guest	11
15	Изменение прав на директории пользователя guest	12
16	Таблица 3.1	13
17	Таблица 3.1	14
18	Таблица 3.1	15
19	Таблица 3.1	16
20	Таблица 3.1	17
21	Таблица 3.1	18
22	Те или иные минимально необходимые права для выполнения операций	19

Список таблиц

Цель работы

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

Задание

Выполнить задания из лабораторной работы и проанализировать полученные результаты.

Теоретическое введение

Для выполнения данной лабораторной нет специальной теории. Необходимы общие знания в области компьютерных наук.

Выполнение лабораторной работы

В прошлой лабораторной работе был создан пользователь guest, а также задан пароль для него. Для этого, используя учетную запись администратора, были выполнены команды:

```
useradd guest
```

```
passwd guest
```

Провел аналогичную процедуру создания еще одного пользователя guest2:

```
[guest@natoponen ~]$ su
Пароль:
[root@natoponen guest]# useradd guest2
[root@natoponen guest]# passwd guest2
Изменяется пароль пользователя guest2.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: В пароле должно быть не меньше 7 символов
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
```

Рис. 1: Создание пользователя guest2

Добавил пользователя guest2 в группу guest:

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

Рис. 2: Добавление пользователя guest2 в группу guest

Осуществил вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли:

```
[root@natoponen guest]# su guest
```

Рис. 3: Вход в систему от пользователя guest

```
[guest@natoponen ~]$ su guest2  
Пароль:
```

Рис. 4: Вход в систему от пользователя guest2

Для обоих пользователей командой *pwd* определил директорию, в которой они находятся. Вывод совпадает с приглашением командной строки. Оба пользователя находятся в домашней директории пользователя guest:

```
[guest@natoponen ~]$ pwd  
/home/guest
```

Рис. 5: Нахождение пользователя guest

```
[guest2@natoponen guest]$ pwd  
/home/guest
```

Рис. 6: Нахождение пользователя guest2

Уточнил имя пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам:

```
[guest@natoponen ~]$ whoami\  
> ^C  
[guest@natoponen ~]$ whoami  
guest
```

Рис. 7: Имя пользователя guest

```
[guest2@natoponen guest]$ whoaim
bash: whoaim: команда не найдена...
Аналогичная команда: 'whoami'
[guest2@natoponen guest]$ whoami
guest2
```

Рис. 8: Имя пользователя guest2

```
[guest@natoponen ~]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfi
ned_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 9: Группа пользователя guest, кто входит в неё и к каким группам принадлежит он сам

```
[guest2@natoponen guest]$ id
uid=1002(guest2) gid=1001(guest) группы=1001(guest),1002(guest2) контекст=unconf
ined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 10: Группа пользователя guest2, кто входит в неё и к каким группам принадлежит он сам

Определил командами *groups guest* и *groups guest2*, в какие группы входят пользователи guest и guest2:

```
[guest@natoponen ~]$ groups
guest
[guest@natoponen ~]$ id -Gn
guest
[guest@natoponen ~]$ id -G
1001
```

Рис. 11: Группы пользователя guest

```
[guest2@natoponen guest]$ groups
guest2 guest
[guest2@natoponen guest]$ id -Gn
guest2 guest
[guest2@natoponen guest]$ id -G
1002 1001
```

Рис. 12: Группы пользователя guest2

Первая команда выводит на экран группы пользователя, но без уточнения к какому пользователю относятся группы, т.к. команды работают только для пользователя, через которого открыта консоль. Вторая команда выводит код группы пользователя.

Сравнил полученную информацию с содержимым файла */etc/group*:

```
natoponen:x:1000:natoponen
vboxsf:x:982:
guest:x:1001:guest2
guest2:x:1002:
```

Рис. 13: Вывод команды `cat /etc/group`

Вывод команды совпадает с данными, полученными на предыдущих шагах.

От имени пользователя guest2 выполнил регистрацию пользователя guest2 в группе guest:

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

Рис. 14: Регистрация пользователя guest2 в группе guest

От имени пользователя guest изменил права директории */home/guest*, разрешив все действия для пользователей группы, а затем снял все атрибуты доступа с директории */home/guest/dir1*:

```

[guest@natoponen ~]$ chmod g+rwX /home/guest
[guest@natoponen ~]$ chmod 000 /home/guest/dir1
[guest@natoponen ~]$ ls -l
итого 0
d------. 2 guest guest 6 сен 12 16:38 dir1
drwxr-xr-x. 2 guest guest 6 сен 12 16:28 Видео
drwxr-xr-x. 2 guest guest 6 сен 12 16:28 Документы
drwxr-xr-x. 2 guest guest 6 сен 12 16:28 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 12 16:28 Изображения
drwxr-xr-x. 2 guest guest 6 сен 12 16:28 Музыка
drwxr-xr-x. 2 guest guest 6 сен 12 16:28 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 12 16:28 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 12 16:28 Шаблоны

```

Рис. 15: Изменение прав на директории пользователя guest

Меняя атрибуты у директории *dir1* и файла *file1* от имени пользователя guest и делая проверку от пользователя guest2, заполнил таблицу ниже, определяя опытным путём, какие операции разрешены, а какие нет.

Права директ ории	Пра ва фай ла	Созда ние файла	Удале ние файла	Зап ись в фай л	Чте ние фай ла	Смена директ ории	Просмо тр файлов в директо рии	Переим ено- вание файла	Смена атрибу тов файла
d----- (000)	----- (000)	-	-	-	-	-	-	-	-
d----x-- - (010)	----- (000)	-	-	-	-	+	-	-	-
d----w--- - (020)	----- (000)	-	-	-	-	-	-	-	-
d----wx- -- (030)	----- (000)	+	+	-	-	+	-	+	-
d---r----- (040)	----- (000)	-	-	-	-	-	+	-	-
d---r-x-- - (050)	----- (000)	-	-	-	-	+	+	-	-
d---rw--- - (060)	----- (000)	-	-	-	-	-	+	-	-
d---rwx- -- (070)	----- (000)	+	+	-	-	+	+	+	-
d----- (000)	x--- (010)	-	-	-	-	-	-	-	-
d----x-- - (010)	x--- (010)	-	-	-	-	+	-	-	-
d----w--- - (020)	x--- (010)	-	-	-	-	-	-	-	-
d----wx- --	x---	+	+	-	-	+	-	+	-

Рис. 16: Таблица 3.1

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

Рис. 17: Таблица 3.1

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

Рис. 18: Таблица 3.1

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

Рис. 19: Таблица 3.1

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

Рис. 20: Таблица 3.1

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

Рис. 21: Таблица 3.1

Полученная таблица не совпадает с таблицей из прошлой лабораторной работы, поскольку члены группы не имеют права изменять атрибуты файла. Для остальных операций члену группы нужны такие же права, как у владельца.

На основании заполненной таблицы 3.1 определил те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри

директории dir1 и заполню таблицу:

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

Рис. 22: Те или иные минимально необходимые права для выполнения операций

Выводы

В ходе выполнения данной лабораторной работы я приобрел практические навыки работы в консоли с атрибутами файлов для групп пользователей, а также на практике закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

Список литературы

- Кулябов Д. С., Королькова А. В., Геворкян М. Н Лабораторная работа №3