

Отчёт по лабораторной работе №3

Информационная безопасность

Дискреционное разграничение прав в Linux. Два пользователя

Выполнила: Павлова Полина Алексеевна,
НПИбд-02-21, 1032212967

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	7
3.1	Атрибуты файлов	7
3.2	Проверка прав	9
3.3	Проверка прав	10
3.4	Заполнение таблицы 3.1	10
3.5	Заполнение таблицы 3.2	16
4	Вывод	18
5	Список литературы. Библиография	19

Список иллюстраций

3.1	(рис. 1. 1-4 пункты задания лабораторной)	7
3.2	(рис. 2. 5-7 пункты задания лабораторной)	8
3.3	(рис. 3. 8 пункт задания лабораторной)	8
3.4	(рис. 4. 9 пункт задания лабораторной)	8
3.5	(рис. 5. 10-11 пункты задания лабораторной)	9
3.6	(рис. 6. d(000)	9
3.7	(рис. 7. d(010)	10

1 Цель работы

Получить практические навыки работы в консоли с атрибутами файлов для групп пользователей

2 Теоретическое введение

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [1]

Группы пользователей Linux кроме стандартных root и users, здесь есть еще пару десятков групп. Это группы, созданные программами, для управления доступом этих программ к общим ресурсам. Каждая группа разрешает чтение или запись определенного файла или каталога системы, тем самым регулируя полномочия пользователя, а следовательно, и процесса, запущенного от этого пользователя. Здесь можно считать, что пользователь - это одно и то же что процесс, потому что у процесса все полномочия пользователя, от которого он запущен. [2]

- daemon - от имени этой группы и пользователя daemon запускаются сервисы, которым необходима возможность записи файлов на диск.
- sys - группа открывает доступ к исходникам ядра и файлам - include сохраненным в системе
- sync - позволяет выполнять команду /bin/sync
- games - разрешает играм записывать свои файлы настроек и историю в определенную папку
- man - позволяет добавлять страницы в директорию /var/cache/man
- lp - позволяет использовать устройства параллельных портов
- mail - позволяет записывать данные в почтовые ящики /var/mail/

- `proxy` - используется прокси серверами, нет доступа записи файлов на диск
- `www-data` - с этой группой запускается веб-сервер, она дает доступ на запись `/var/www`, где находятся файлы веб-документов
- `list` - позволяет просматривать сообщения в `/var/mail`
- `nogroup` - используется для процессов, которые не могут создавать файлов на жестком диске, а только читать, обычно применяется вместе с пользователем `nobody`.
- `adm` - позволяет читать логи из директории `/var/log`
- `tty` - все устройства `/dev/vsa` разрешают доступ на чтение и запись пользователям из этой группы
- `disk` - открывает доступ к жестким дискам `/dev/sd*` `/dev/hd*`, можно сказать, что это аналог `root` доступа.
- `dialout` - полный доступ к серийному порту
- `cdrom` - доступ к CD-ROM
- `wheel` - позволяет запускать утилиту `sudo` для повышения привилегий
- `audio` - управление аудиодрайвером
- `src` - полный доступ к исходникам в каталоге `/usr/src/`
- `shadow` - разрешает чтение файла `/etc/shadow`
- `utmp` - разрешает запись в файлы `/var/log/utmp` `/var/log/wtmp`
- `video` - позволяет работать с видеодрайвером
- `plugdev` - позволяет монтировать внешние устройства USB, CD и т д
- `staff` - разрешает запись в папку `/usr/local`

3 Выполнение лабораторной работы

3.1 Атрибуты файлов

1. В установленной операционной системе создайте учётную запись пользователя guest2 (используя учётную запись администратора)

guest1 был создан в предыдущей лабораторной.

2. Задайте пароль для пользователя guest2
3. Добавьте пользователя guest2 в группу guest:

```
[papavloval2@papavloval2 ~]$ sudo -i
[sudo] password for papavloval2:
[root@papavloval2 ~]# useradd guest
useradd: user 'guest' already exists
[root@papavloval2 ~]# passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@papavloval2 ~]# useradd guest2
[root@papavloval2 ~]# passwd guest2
Changing password for user guest2.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@papavloval2 ~]# gpasswd -a guest2 guest
Adding user guest2 to group guest
```

Рис. 3.1: (рис. 1. 1-4 пункты задания лабораторной)

4. Осуществите вход в систему от двух пользователей на двух разных консолях:
guest на первой консоли и guest2 на второй консоли
5. Для обоих пользователей командой pwd определите директорию, в которой вы находитесь. Сравните её с приглашениями командной строки
6. Уточните имя вашего пользователя, его группу, кто входит в неё и к каким группам принадлежит он сам. Определите командами groups guest и groups guest2, в какие группы входят пользователи guest и guest2. Сравните вывод команды groups с выводом команд id -Gn и id -G :

```
[guest@papavlova12 ~]$ pwd
/home/guest
[guest@papavlova12 ~]$ whoami
guest
[guest@papavlova12 ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@papavlova12 ~]$ groups
guest
[guest@papavlova12 ~]$ groups guest
guest : guest
[guest@papavlova12 ~]$ groups guest2
guest2 : guest2 guest
[guest@papavlova12 ~]$ id -Gn
guest
[guest@papavlova12 ~]$ id -G
1001
```

Рис. 3.2: (рис. 2. 5-7 пункты задания лабораторной)

7. Сравните полученную информацию с содержимым файла /etc/group :

```
papavlova12.x.1000.
guest:x:1001:guest2
guest2:x:1002:
[guest@papavlova12 ~]$
```

Рис. 3.3: (рис. 3. 8 пункт задания лабораторной)

8. От имени пользователя guest2 выполните регистрацию пользователя guest2 в группе guest командой newgrp guest :

```
[guest2@papavlova12 ~]$ newgrp guest
[guest2@papavlova12 ~]$
```

Рис. 3.4: (рис. 4. 9 пункт задания лабораторной)

9. От имени пользователя guest измените права директории /home/guest, разрешив все действия для пользователей группы: `chmod g+rx /home/guest`
10. От имени пользователя guest снимите с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1` :

```
[guest@papavlova12 ~]$ chmod g+rx /home/guest
[guest@papavlova12 ~]$ chmod 000 dir1
[guest@papavlova12 ~]$ ls -l
total 0
d----- . 2 guest guest 19 Sep  4 11:40 dir1
```

Рис. 3.5: (рис. 5. 10-11 пункты задания лабораторной)

3.2 Проверка прав

```
[guest2@papavlova12 guest]$ touch dir1/file2
touch: cannot touch 'dir1/file2': Permission denied
[guest2@papavlova12 guest]$ rm dir1/file1
rm: remove write-protected regular file 'dir1/file1'? y
rm: cannot remove 'dir1/file1': Permission denied
[guest2@papavlova12 guest]$ echo "text" > dir1/file1
bash: dir1/file1: Permission denied
[guest2@papavlova12 guest]$ cat dir1/file1
cat: dir1/file1: Permission denied
[guest2@papavlova12 guest]$ cd dir1/
[guest2@papavlova12 dir1]$ ls dir1/
ls: cannot access 'dir1/': No such file or directory
[guest2@papavlova12 dir1]$ cd ../
[guest2@papavlova12 guest]$ ls dir1/
ls: cannot open directory 'dir1/': Permission denied
[guest2@papavlova12 guest]$ mv dir1/file1 dir1/file2
mv: cannot move 'dir1/file1' to 'dir1/file2': Permission denied
[guest2@papavlova12 guest]$ chmod 070 dir1/file1
chmod: changing permissions of 'dir1/file1': Operation not permitted
[guest2@papavlova12 guest]$
```

Рис. 3.6: (рис. 6. d(000))

3.3 Проверка прав

```
[guest2@papavloval2 guest]$ touch dir1/file2
[guest2@papavloval2 guest]$ rm dir1/file2
[guest2@papavloval2 guest]$ echo "text" > dir1/file1
[guest2@papavloval2 guest]$ cat dir1/file1
text
[guest2@papavloval2 guest]$ cd dir1/
[guest2@papavloval2 dir1]$ cd ..?
bash: cd: ..?: No such file or directory
[guest2@papavloval2 dir1]$ cd ../
[guest2@papavloval2 guest]$ ls dir1/
file1
[guest2@papavloval2 guest]$ rm dir1/file2
rm: cannot remove 'dir1/file2': No such file or directory
[guest2@papavloval2 guest]$ mv dir1/file1 dir1/file2
[guest2@papavloval2 guest]$ chmod 111 dir1/file1
chmod: cannot access 'dir1/file1': No such file or directory
[guest2@papavloval2 guest]$ chmod 111 dir1/file2
chmod: changing permissions of 'dir1/file2': Operation not permitted
[guest2@papavloval2 guest]$
```

Рис. 3.7: (рис. 7. d(010))

3.4 Заполнение таблицы 3.1

11. Меняя атрибуты у директории dir1 и файла file1 от имени пользователя guest и делая проверку от пользователя guest2, заполните табл. 3.1, определив опытным путём, какие операции разрешены, а какие нет. Если операция разрешена, занесите в таблицу знак «+», если не разрешена, знак «-». Сравните табл. 2.1 (из лабораторной работы № 2) и табл. 3.1.

		Просмотр							
		Запись				файлов		Смена	
Права директории	Права файла	Создание файла	Удаление файла	Чтение файла	Смена директории	Чтение файла	Запись файла	Переименование файла	Атрибуты файла
d-----	-----	-	-	-	-	-	-	-	-
(000)	(000)								
d-----x---	-----	-	-	-	+	-	-	-	+
(010)	(000)								

Права директории	Права файла	<div> <div>Просмотр</div> <div>Запись</div> <div>Смена</div> <div>Просмотр</div> <div>Смена</div> </div>							
		Создание файла	Удаление файла	Чтение файла	Запись файла	Смена директории	Просмотр файла	Смена файла	Просмотр файла
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-----x---	-----x---	-	-	-	-	-	-	-	-
(000)	(010)								
d-----x---	-----x---	-	-	-	-	+	-	-	+
(010)	(010)								
d----w----	-----x---	-	-	-	-	-	-	-	-
(020)	(010)								
d---wx---	-----x---	+	+	-	-	+	-	+	+
(030)	(010)								
d---r-----	-----x---	-	-	-	-	-	+	-	-
(040)	(010)								
d---r-x---	-----x---	-	-	-	-	+	+	-	+
(050)	(010)								

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

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

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

Права директории	Права файла	Просмотр							
		Запись		Просмотр		Смена		Смена	
		Создание файла	Удаление файла	Чтение файла	Смена файла	Смена директории	Переименование файла	Удаление файла	Удаление директории
d----w----	----rW----	-	-	-	-	-	-	-	-
(020)	(060)								
d----wx---	----rW----	+	+	+	+	+	-	+	+
(030)	(060)								
d---r-----	----rW----	-	-	-	-	-	+	-	-
(040)	(060)								
d---r-x---	----rW----	-	-	+	+	+	+	-	+
(050)	(060)								
d---rW----	----rW----	-	-	-	-	-	+	-	-
(060)	(060)								
d---rwx---	----rW----	+	+	+	+	+	+	+	+
(070)	(060)								
d-----	----rwx---	-	-	-	-	-	-	-	-
(000)	(070)								
d-----x---	----rwx---	-	-	+	+	+	-	-	+
(010)	(070)								
d----w----	----rwx---	-	-	-	-	-	-	-	-
(020)	(070)								
d----wx---	----rwx---	+	+	+	+	+	-	+	+
(030)	(070)								
d---r-----	----rwx---	-	-	-	-	-	+	-	-
(040)	(070)								
d---r-x---	----rwx---	-	-	+	+	+	+	-	+
(050)	(070)								

		Права							
Права директории	Права файла	Создание		Удаление		Чтение		Запись	
		файла	директории	файла	директории	файла	директории	файла	директории
d---rw----	----rwx---	-	-	-	-	-	-	+	-
(060)	(070)								
d---rwx---	----rwx---	+	+	+	+	+	+	+	+
(070)	(070)								

Таблица 3.1 «Установленные права и разрешённые действия для групп»

3.5 Заполнение таблицы 3.2

12. На основании заполненной таблицы определите те или иные минимально необходимые права для выполнения пользователем guest2 операций внутри директории dir1 и заполните табл. 3.2

Операция	Права на директорию	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)

Таблица 3.2 «Минимальные права для совершения операций от имени пользователей входящих в группу»

Сравнивая таблицу 3.1. с таблицей 2.1, можно сказать, что они одинаковы. Единственное различие в том, что в предыдущий раз мы присваивали права владельцу, а в этот раз группе.

4 Вывод

Были получены практические навыки работы в консоли с атрибутами файлов для групп пользователей

5 Список литературы. Библиография

[0] Методические материалы курса

[1] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>

[2] Группы пользователей: <https://losst.pro/gruppy-polzovatelej-linux#%D0%A7%D1%82%D0%B>