

Отчёт по лабораторной работе №3

Информационная безопасность

Дискреционное разграничение прав в Linux. Два пользователя

Выполнила: Коняева Марина Александровна,
НФИбд-01-21, 1032217044

Содержание

Теоретическое введение	4
Цель работы	6
Выполнение лабораторной работы	7
Атрибуты файлов	7
Заполнение таблицы 3.1	9
Заполнение таблицы 3.2	16
Вывод	18
Список литературы. Библиография	19

Список иллюстраций

1	(рис. 1. 1-4 пункты задания лабораторной)	7
2	(рис. 2. 5-7 пункты задания лабораторной)	8
3	(рис. 3. 8 пункт задания лабораторной)	8
4	(рис. 4. 9 пункт задания лабораторной)	8
5	(рис. 5. 10-11 пункты задания лабораторной)	9

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-`

Цель работы

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

Выполнение лабораторной работы

Атрибуты файлов

1. В установленной операционной системе создайте учётную запись пользователя guest2 (используя учётную запись администратора). Задайте пароль для пользователя guest2. Добавьте пользователя guest2 в группу guest:

(guest1 был создан в предыдущей лабораторной)

```
[guest@mkonyaeva ~]$ su
Password:
[root@mkonyaeva guest]# useradd guest2
[root@mkonyaeva guest]# passwd guest2
Changing password for user guest2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@mkonyaeva guest]# gpasswd -a guest2 guest
Adding user guest2 to group guest
[root@mkonyaeva guest]#
```

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

2. Осуществите вход в систему от двух пользователей на двух разных консолях: guest на первой консоли и guest2 на второй консоли. Для обоих пользователей командой pwd определите директорию, в которой вы находитесь. Сравните её с приглашениями командной строки. 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@mkonyaeva:~	guest2@mkonyaeva:/home/guest
File Edit View Search Terminal Help	File Edit View Search Terminal Help
[guest@mkonyaeva ~]\$ pwd	[guest@mkonyaeva ~]\$ su guest2
/home/guest	Password:
[guest@mkonyaeva ~]\$ groups guest	[guest2@mkonyaeva guest]\$ pwd
guest : guest	/home/guest
[guest@mkonyaeva ~]\$ groups	[guest2@mkonyaeva guest]\$ groups guest2
guest	guest2 : guest2 guest
[guest@mkonyaeva ~]\$ id -Gn	[guest2@mkonyaeva guest]\$ groups
guest	guest2 guest
[guest@mkonyaeva ~]\$ id -G	[guest2@mkonyaeva guest]\$ id -Gn
1001	guest2 guest
[guest@mkonyaeva ~]\$	[guest2@mkonyaeva guest]\$ id -G
	1002 1001
	[guest2@mkonyaeva guest]\$

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

- Сравните полученную информацию с содержимым файла `/etc/group` с помощью команды `“cat /etc/group”`:

mkonyaeva:x:1000:	mkonyaeva:x:1000:
vboxsf:x:973:	vboxsf:x:973:
guest:x:1001:guest2	guest:x:1001:guest2
guest2:x:1002:	guest2:x:1002:
[guest@mkonyaeva ~]\$	[guest2@mkonyaeva guest]\$

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

- От имени пользователя `guest2` выполните регистрацию пользователя `guest2` в группе `guest` командой `newgrp guest` :

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

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

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


```
[guest@mkonyaeva ~]$ chmod g+rwX /home/guest
[guest@mkonyaeva ~]$
```

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

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.

		Права							
		Права директории				Права файла			
		См.	Чт.	Зап.	Уда.	См.	Чт.	Зап.	Уда.
		директории	файла	директории	файла	директории	файла	директории	файла
d-----	(000)	-	-	-	-	-	-	-	-
d-----x---	(010)	-	-	-	-	+	-	-	+
d---w----	(020)	-	-	-	-	-	-	-	-

Права директории	Права файла	<div> <div>Про-</div> <div>смотр</div> <div>Сме-</div> <div>фай-</div> <div>Пе-</div> <div>на</div> <div>Сме-</div> <div>лов</div> <div>ре-</div> <div>ат-</div> <div>на</div> <div>в</div> <div>име-</div> <div>ри-</div> <div>бу-</div> <div>тов</div> <div>фай-</div> <div>ла</div> </div>							
		Со-	Уда-	За-	Чте-	Сме-	лов	ре-	ат-
		зда-	ле-	пись	ние	на	ди-	ди-	но-
		ние	ние	в	фай-	рек-	рек-	ва-	ри-
		фай-	фай-	файл	ла	то-	то-	ние	бу-
		ла	ла	файл	ла	рии	рии	файл	тов
		ла	ла	файл	ла	рии	рии	файл	фай-
		ла	ла	файл	ла	рии	рии	файл	ла
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)								

		Про- смотр фай- Сме- лов ре- име- но- ва- ние фай-							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Сме- лов ди- рек- то- рии	ре- име- но- ва- ние файл	на ат- ри- бу- тов фай- ла
Права директории	Права файла								
d---r-x---	-----x---	-	-	-	-	+	+	-	+
(050)	(010)								
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)								

		Про- смотр фай- Пе- на Сме- лов ре- ат- на в име- ри- ди- ди- но- бу- рек- рек- ва- тов то- то- ние фай- рии рии файл ла							
Права директории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Сме- лов ди- рек- то- рии	ре- ва- ние файл	ат- ри- бу- тов фай- ла
d---rwx---	-----w----	+	+	+	-	+	+	+	+
(070)	(020)								
d-----	-----wx---	-	-	-	-	-	-	-	-
(000)	(030)								
d-----x---	-----wx---	-	-	+	-	+	-	-	+
(010)	(030)								
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)								

		Про-							
		смотр				Сме-			
		фай-				лов			
		Пе-				ре-			
		на				ат-			
		Сме-				на			
		в				име-			
		ри-				бу-			
		Со-				Уда-			
		Зда-				За-			
		Чте-				ди-			
		ре-				ре-			
		ва-				но-			
		ри-				бу-			
		тов				фай-			
Права	Права файла	фай-	фай-	в	фай-	то-	то-	ние	фай-
директории		ла	ла	файл	ла	рии	рии	файл	ла
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)								
d---rw----	-----r-----	-	-	-	-	-	+	-	-
(060)	(040)								
d---rwx---	-----r-----	+	+	-	+	+	+	+	+
(070)	(040)								
d-----x---	-----r-x---	-	-	-	-	-	-	-	-
(000)	(050)								
d-----x---	-----r-x---	-	-	-	+	+	-	-	+
(010)	(050)								
d----w----	-----r-x---	-	-	-	-	-	-	-	-
(020)	(050)								

		Про- смотр фай- Пе- на Сме- лов ре- ат- на в име- ри- ди- ди- но- бу- рек- рек- ва- тов то- то- ние фай- рии рии файл ла							
Права директории	Права файла	Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	Сме- на ди- рек- то- рии	Сме- на ди- рек- то- рии	Сме- на ди- рек- то- рии	Сме- на ди- рек- то- рии
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)								
d---w----	----rw----	-	-	-	-	-	-	-	-
(020)	(060)								
d---wx---	----rw----	+	+	+	+	+	-	+	+
(030)	(060)								
d---r-----	----rw----	-	-	-	-	-	+	-	-
(040)	(060)								

		<div> <div>Про-</div> <div>смотр</div> <div>Сме-</div> <div>фай-</div> <div>Пе-</div> <div>на</div> <div>Сме-</div> <div>лов</div> <div>ре-</div> <div>ат-</div> <div>на</div> <div>в</div> <div>име-</div> <div>ри-</div> <div>бу-</div> <div>тов</div> <div>фай-</div> <div>ла</div> </div>							
		Со-	Уда-	За-	Чте-	Сме-	лов	ре-	ат-
		зда-	ле-	пись	ние	ди-	ди-	но-	бу-
		ние	ние	в	фай-	то-	то-	ние	фай-
Права	Права файла	фай-	фай-	файл	ла	рии	рии	файл	ла
директории		ла	ла	файл	ла	рии	рии	файл	ла
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)								
d---rw----	----rwx---	-	-	-	-	-	+	-	-
(060)	(070)								

						Про-			
						смотр	Сме-		
						фай-	Пе-	на	
						Сме-	лов	ре-	ат-
		Со-	Уда-			на	в	име-	ри-
		зда-	ле-	За-	Чте-	ди-	ди-	но-	бу-
		ние	ние	пись	ние	рек-	рек-	ва-	тов
Права		фай-	фай-	в	фай-	то-	то-	ние	фай-
директории	Права файла	ла	ла	файл	ла	рии	рии	файл	ла
d - - - rwx - - -	- - - - rwx - - -	+	+	+	+	+	+	+	+
(070)	(070)								

Таблица 3.1 «Установленные права и разрешённые действия для групп»

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)

Операция	Права на директорию	Права на файл
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.

Вывод

В ходе данной лабораторной работы были получены практические навыки работы в консоли с атрибутами файлов для групп пользователей.

Список литературы. Библиография

[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%BE_%D1