

Отчёт по лабораторной работе №3

Информационная безопасность

Дискреционное разграничение прав в Linux. Два пользователя

Выполнила: Чванова Ангелина Дмитриевна , НПИбд-02-21

Содержание

Цель работы	4
Теоретическое введение	5
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

Цель работы

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

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`

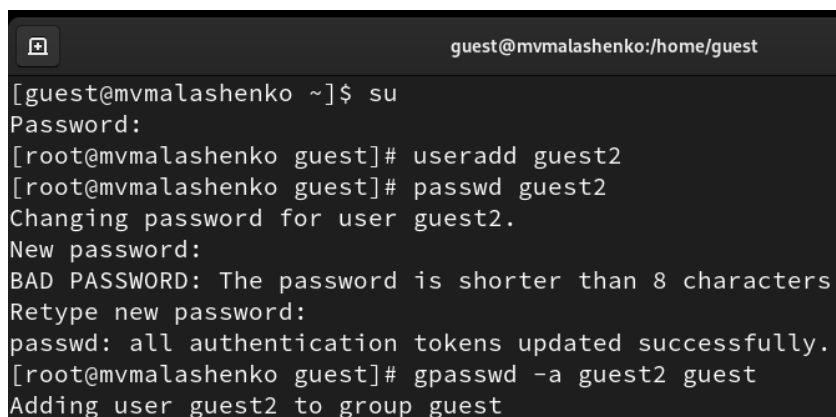
Выполнение лабораторной работы

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:



```
guest@mvmalashenko:/home/guest
[guest@mvmalashenko ~]$ su
Password:
[root@mvmalashenko guest]# useradd guest2
[root@mvmalashenko guest]# 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@mvmalashenko guest]# gpasswd -a guest2 guest
Adding user guest2 to group guest
```

Рис. 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@mvmlashenko ~]$ pwd
/home/guest
[guest@mvmlashenko ~]$ groups guest
guest : guest
[guest@mvmlashenko ~]$ groups
guest
[guest@mvmlashenko ~]$ id -Gn
guest
[guest@mvmlashenko ~]$ id -G
1001
[guest@mvmlashenko ~]$

[guest2@mvmlashenko /home/...]$ su guest2
Password:
[guest2@mvmlashenko guest]$ pwd
/home/guest
[guest2@mvmlashenko guest]$ groups guest2
guest2 : guest2 guest
[guest2@mvmlashenko guest]$ groups
guest2 guest
[guest2@mvmlashenko guest]$ id -Gn
guest2 guest
[guest2@mvmlashenko guest]$ id -G
1002 1001
[guest2@mvmlashenko guest]$

```

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

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

```

guest:x:1001:guest2
guest2:x:1002:
[guest@mvmlashenko ~]$

guest:x:1001:guest2
guest2:x:1002:
[guest2@mvmlashenko guest]$

```

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

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

```

[guest2@mvmlashenko guest]$ newgrp guest

```

Рис. 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+rwX /home/guest`

10. От имени пользователя guest снимите с директории /home/guest/dir1 все атрибуты командой `chmod 000 dir1` :

```
[guest@mvmalashenko ~]$ chmod g+rx /home/guest
[guest@mvmalashenko ~]$ chmod 000 dir1
chmod: cannot access 'dir1': No such file or directory
[guest@mvmalashenko ~]$ chmod 000 dir1
[guest@mvmalashenko ~]$
```

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			
		Чтение	Запись	Исполнение	Скрытие	Чтение	Запись	Исполнение	Скрытие
		директории	директории	директории	директории	файла	файла	файла	файла
Права	Права файла	директории	директории	директории	директории	файла	файла	файла	файла
d-----	-----	-	-	-	-	-	-	-	-
(000)	(000)								

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

		Про- смотр фай- Сме- лов Пе- ре- на Сме- на в име- ри- бу- тов фай-							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	на ди- рек- то- рии	ди- рек- то- рии	но- ва- ние файл	ат- ри- бу- тов фай- ла
Права директории	Права файла								
d----wx---	-----x---	+	+	-	-	+	-	+	+
(030)	(010)								
d---r-----	-----x---	-	-	-	-	-	+	-	-
(040)	(010)								
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)								

		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---r-x---	-----w----	-	-	+	-	+	+	-	+
(050)	(020)								
d---rw----	-----w----	-	-	-	-	-	+	-	-
(060)	(020)								
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)								

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

		Про- смотр фай- Сме- лов ре- име- но- ва- ние файл								Сме- на ат- ри- бу- тов файл
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	Сме- на ди- рек- то- рии
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)									
d----w----	-----rw----	-	-	-	-	-	-	-	-	
(020)	(060)									

		Про- смотр фай- Сме- лов Пе- ре- на Сме- на ри- бу- тов фай-							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	на ди- рек- то- рии	в ди- рек- то- рии	име- но- ва- ние файл	ри- бу- тов фай- ла
Права директории	Права файла								
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 - - - (070)	-	-	-	-	-	-	-	-
d - - - - - x - - - (010)	- - - - rwx - - - (070)	-	-	+	+	+	-	-	+
d - - - - w - - - - (020)	- - - - rwx - - - (070)	-	-	-	-	-	-	-	-
d - - - - wx - - - (030)	- - - - rwx - - - (070)	+	+	+	+	+	-	+	+
d - - - r - - - - - (040)	- - - - rwx - - - (070)	-	-	-	-	-	+	-	-

Права директории	Права файла	<div> <div>Про- смотр фай-</div> <div>Сме- лов ре-</div> <div>на пе- ре-</div> <div>Сме- на в</div> <div>име- но-</div> <div>ва-</div> <div>ри-</div> <div>бу-</div> <div>тов</div> <div>фай-</div> </div>							
		Со- зда- ние фай- ла	Уда- ле- ние фай- ла	За- пись в файл	Чте- ние фай- ла	ди- рек- то- рии	ди- рек- то- рии	файл	ла
d - - - r - x - - - (050)	- - - - rwx - - - (070)	-	-	+	+	+	+	-	+
d - - - rw - - - - (060)	- - - - rwx - - - (070)	-	-	-	-	-	+	-	-
d - - - rwx - - - (070)	- - - - rwx - - - (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)

Операция	Права на директорию	Права на файл
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.

Вывод

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

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%BE_%D1