

Отчет по лабораторной работе №3

Основы информационной безопасности

Дворкина Ева, НКАбд-01-22

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
4.1	Заполнение таблицы 3.1	13
4.2	Заполнение таблицы 3.2	20
5	Выводы	22
6	Список литературы. Библиография	23

Список иллюстраций

4.1	Создание пользователя	9
4.2	Добавление пользователя в группу	9
4.3	Вход в терминал от имени другого пользователя	10
4.4	Текущая директория для guest	10
4.5	Текущая директория для guest2	10
4.6	Информация о пользователе guest2	11
4.7	Информация о пользователе guest	11
4.8	Содержимое файла etc/group	12
4.9	Регистрация пользователя в группе	12
4.10	Изменение прав директории	12
4.11	Изменение прав директории	13
4.12	Пример заполнения таблицы 3.1	13

Список таблиц

1 Цель работы

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

2 Задание

1. Создание пользователя `guest2`, добавление его в группу пользователей `guest`
2. Заполнение таблицы 3.1
3. Заполнение таблицы 3.2 на основе таблицы 3.1.

3 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/vcs` 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`

4 Выполнение лабораторной работы

1. Пользователь guest был создан в лабораторной работе №2, поэтому в этой лабораторной работе его не создаем заново
2. Пароль для пользователя guest тоже был задан в лабораторной работе №2.
3. С правами администратора создаю пользователя guest с помощью команды useradd, далее с помощью команды passwd задаю пароль пользователю (рис. 1).

```
[evdvorkina@evdvorkina ~]$ sudo useradd guest2
[sudo] пароль для evdvorkina:
[evdvorkina@evdvorkina ~]$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: Пароль не указан
Повторите ввод нового пароля:
Извините, но пароли не совпадают.

passwd: Ошибка при операциях с маркером проверки подлинности
[evdvorkina@evdvorkina ~]$
[evdvorkina@evdvorkina ~]$ sudo passwd guest2
Изменение пароля пользователя guest2.
Новый пароль:
Повторите ввод нового пароля:
passwd: данные аутентификации успешно обновлены.
```

Рис. 4.1: Создание пользователя

4. Добавляю пользователя guest2 в группу guest (рис. 2).

```
[evdvorkina@evdvorkina ~]$ sudo gpasswd -a guest2 guest
Добавление пользователя guest2 в группу guest
[evdvorkina@evdvorkina ~]$
```

Рис. 4.2: Добавление пользователя в группу

5. Зашла на двух разных консолях от имени двух разных пользователей с помощью команды `su <имя пользователя>` (рис. 3).

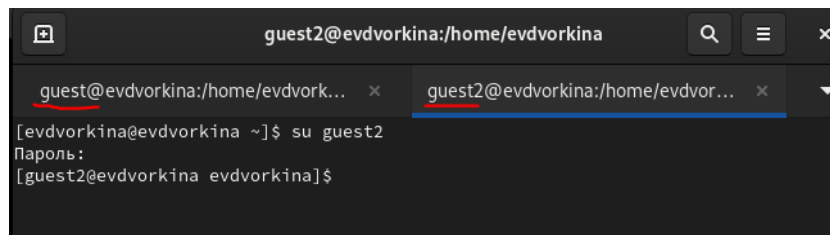


Рис. 4.3: Вход в терминал от имени другого пользователя

6. Проверяю путь директории, в которой я нахожусь с помощью `pwd`.

Проверка для пользователя `guest` (рис. 4).

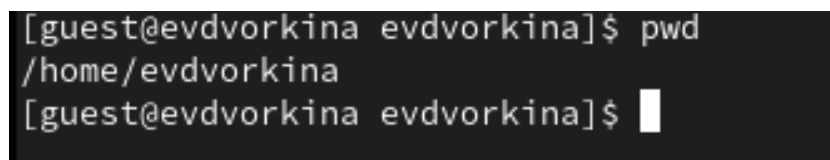


Рис. 4.4: Текущая директория для `guest`

Проверка для пользователя `guest2` (рис. 5).

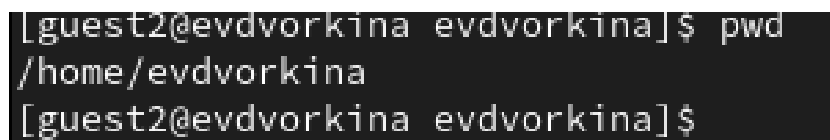


Рис. 4.5: Текущая директория для `guest2`

Стоит отметить, что вход в терминал от имени пользователей был выполнен в домашней директории пользователя `evdvorkina`, которую команда `pwd` вывела. Домашней директорией пользователей она не является. Текущая директория с приглашением командной строки совпадает.

7. Проверяю имя пользователей с помощью команды `whoami`, с помощью команды `id` могу увидеть группы, к которым принадлежит пользователь и коды этих групп (`gid`), команда `groups` просто выведет список групп, в которые входит пользователь.

`id -Gn` - выведет названия групп, которым принадлежит пользователь

`id -G` - выведет только код групп, которым принадлежит пользователь.

Проверка для пользователя `guest2` (рис. 6).

```
[guest2@evdvorkina evdvorkina]$ whoami
guest2
[guest2@evdvorkina evdvorkina]$ id
uid=1002(guest2) gid=1002(guest2) группы=1002(guest2),1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest2@evdvorkina evdvorkina]$ groups guest2
guest2 : guest2 guest
[guest2@evdvorkina evdvorkina]$ groups
guest2 guest
[guest2@evdvorkina evdvorkina]$ id -Gn
guest2 guest
[guest2@evdvorkina evdvorkina]$ id -G
1002 1001
```

Рис. 4.6: Информация о пользователе `guest2`

Проверка для пользователя `guest` (рис. 7).

```
[guest@evdvorkina evdvorkina]$ whoami
guest
[guest@evdvorkina evdvorkina]$ id
uid=1001(guest) gid=1001(guest) группы=1001(guest) контекст=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[guest@evdvorkina evdvorkina]$ groups guest
guest : guest
[guest@evdvorkina evdvorkina]$ groups guest2
guest2 : guest2 guest
[guest@evdvorkina evdvorkina]$ id -Gn
guest
[guest@evdvorkina evdvorkina]$ id -G
1001
[guest@evdvorkina evdvorkina]$ groups
guest
```

Рис. 4.7: Информация о пользователе `guest`

Пользователь `guest2` входит в две группы пользователей: в группу `guest`, потому что я сама его туда добавила, и в группу `guest2`, которая создавалась автоматически при создании пользователя.

8. Вывела интересующее меня содержимое файла `etc/group`, видно, что в группе `guest` два пользователя, а в группе `guest2` один (рис. 8).

```
[guest@evdvorkina evdvorkina]$ cat /etc/group | grep 'guest'
guest:x:1001:guest2
guest2:x:1002:
[guest@evdvorkina evdvorkina]$
```

Рис. 4.8: Содержимое файла `etc/group`

9. От имени пользователя `guest2` регистрирую его в группе `guest` с помощью команды `newgrp` (рис. 9).

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

Рис. 4.9: Регистрация пользователя в группе

10. Добавляю права на чтение, запись и исполнение группе пользователей `guest` (`guest`, `guest2`) на директорию `home/guest` в которой находятся все файлы для последующей работы (рис. 10).

```
[guest@evdvorkina evdvorkina]$ cd
[guest@evdvorkina ~]$ pwd
/home/guest
[guest@evdvorkina ~]$ chmod g+rx /home/guest
```

Рис. 4.10: Изменение прав директории

11. От имени пользователя `guest` снимаю все атрибуты с директории `dir1`, созданной в предыдущей лабораторной работе. Проверяю, что права действительно сняты (рис. 11).

```

/home/guest
[guest@evdvorkina ~]$ chmod g+rxw /home/guest
[guest@evdvorkina ~]$ ls
dir1  test10  Видео      Загрузки    Музыка      'Рабочий стол'
test  test2   Документы  Изображения Общедоступные Шаблоны
[guest@evdvorkina ~]$ chmod 000 dir1
[guest@evdvorkina ~]$ ls
dir1  test10  Видео      Загрузки    Музыка      'Рабочий стол'
test  test2   Документы  Изображения Общедоступные Шаблоны
[guest@evdvorkina ~]$ ls -l
итого 8
d----- 3 guest guest 24 фев 18 21:17 dir1
-rw-r--r-- 1 guest guest 5 фев 18 20:39 test
----- 1 guest guest 5 фев 18 20:27 test10
----- 1 guest guest 0 фев 18 21:05 test2
drwxr-xr-x 2 guest guest 6 фев 18 18:49 Видео
drwxr-xr-x 2 guest guest 6 фев 18 18:49 Документы
drwxr-xr-x 2 guest guest 6 фев 18 18:49 Загрузки

```

Рис. 4.11: Изменение прав директории

4.1 Заполнение таблицы 3.1

Далее проверяю как пользователь guest2 будет взаимодействовать с файлами в этой директории (рис. 12).

```

[guest2@evdvorkina ~]$ cd /home/guest
[guest2@evdvorkina ~]$ ls
dir1  test10  Видео      Загрузки    Музыка      'Рабочий стол'
test  test2   Документы  Изображения Общедоступные Шаблоны
[guest2@evdvorkina ~]$ ls dir1
ls: невозможно открыть каталог 'dir1': Отказано в доступе
[guest2@evdvorkina ~]$ rm dir1/a
rm: невозможно удалить 'dir1/a': Отказано в доступе
[guest2@evdvorkina ~]$ touch dir1/f1
touch: невозможно выполнить touch для 'dir1/f1': Отказано в доступе
[guest2@evdvorkina ~]$ echo 'test' > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest2@evdvorkina ~]$ cat dir1/file1
cat: dir1/file1: Отказано в доступе
[guest2@evdvorkina ~]$ chmod 020 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе

```

Рис. 4.12: Пример заполнения таблицы 3.1

		Права							
		Создание				Просмотр			
		фай-				фай-			
		лов				Смена			
		ат-				ри-			
		бу-				тов			
		Периферия				фай-			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла				ла			
		ла							

Права директории	Права файла	Права							
		Созда- ние фай- ла	Изме- нение фай- ла	Удале- ние фай- ла	Чтение файла	Запис- ь в фай- л	Смена рек- то- рии	Просмотр фай- лов	Смена ат- ри- бу- тов фай- ла
d----w---	-----x--	-	-	-	-	-	-	-	-
(020)	(010)								
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)								

Права директории	Права файла	Права							
		Созда- фай- ла	Модифи- фай- ла	Записи в фай- л фай- ла	Чтение фай- ла	рек- то- рии	рек- то- рии	Просмотр фай- лов	Смена ат- ри- бу- тов фай- ла
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)								
d----w---	-----wx--	-	-	-	-	-	-	-	-
(020)	(030)								
d----wx--	-----wx--	+	+	+	-	+	-	+	+
(030)	(030)								
d---r----	-----wx--	-	-	-	-	-	+	-	-
(040)	(030)								
d---r-x--	-----wx--	-	-	+	-	+	+	-	+
(050)	(030)								

Права директории	Права файла	Права							
		Созда- ние фай- ла	Изме- нение фай- ла	Удале- ние фай- ла	Чтение файла	Запис- ь в фай- л	Смена рек- то- рии	Просмотр фай- лов	Смена ат- ри- бу- тов фай- ла
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)								
d---rw---	----r----	-	-	-	-	-	+	-	-
(060)	(040)								
d---rwx--	----r----	+	+	-	+	+	+	+	+
(070)	(040)								

		Права							
Права директории	Права файла	Права							
		Созда- ние фай- ла	Удале- ние фай- ла	Записи в файл	Чтение файла	Смена рек- то- рии	Просмотр фай- лов	Смена ат- ри- бу- тов	Переименование файла
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							
		Создание фай- ла	Удаление фай- ла	Изменение в файл	Чтение фай- ла	Исполнение рек- то- рии	Просмотр фай- лов	Смена ат- ри- бу- тов	Переименование файл
Права директории	Права файла	ла	ла	файл	ла	рии	рии	файл	ла
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)								

Права директории	Права файла	Права на файл							
		Создание файла	Удаление файла	Запись в файл	Чтение файла	Редактирование файла	Редактирование файла	Перемещение файла	Именование файла
d---r----	----rwx--	-	-	-	-	-	+	-	-
(040)	(070)								
d---r-x--	----rwx--	-	-	+	+	+	+	-	+
(050)	(070)								
d---rw---	----rwx--	-	-	-	-	-	+	-	-
(060)	(070)								
d---rwx--	----rwx--	+	+	+	+	+	+	+	+
(070)	(070)								

Таблица 3.1 «Установленные права и разрешённые действия для групп»

4.2 Заполнение таблицы 3.2

На основе таблицы 3.1 заполняю таблицу 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»

5 Выводы

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

6 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#Что_такое_группы