

Лабораторная работа №3

Дисциплина: Основы информационной безопасности

Коновалова Татьяна Борисовна

Содержание

1	Цель работы	5
2	Теоретические данные	6
3	Задание	8
4	Выполнение лабораторной работы	9
5	Выводы	15
6	Библиография	16

Список иллюстраций

4.1	Создание пользователя и установка пароля	9
4.2	Проверка групп	10
4.3	Команда <code>/etc/passwd</code>	10
4.4	Результат команды <code>/etc/passwd</code>	11
4.5	Регистрация пользователя в группе <code>group</code>	12
4.6	Смена атрибутов	12
4.7	Таблца 3.1 «Установленные права и разрешённые действия» . . .	13
4.8	Таблца 3.1 «Установленные права и разрешённые действия» . . .	14
4.9	Таблица 3.2 «Минимальные права для совершения операций» . .	14

Список таблиц

1 Цель работы

Цель данной лабораторной работы — Получить практические навыки работы в консоли с атрибутами файлов для групп пользователей.

2 Теоретические данные

Рассмотрим три параметра доступа для каждого файла в ОС Linux:

1.Чтение - разрешить доступ к получению содержимого файла, но записывать нельзя. Для каталога позволяет получить список файлов и каталогов, которые в нём располагаются;

2.Запись - разрешить записывать данные в файл или изменять уже имеющиеся. Также можно создавать и менять файлы и каталоги;

3.Выполнение - нельзя выполнить программу, если у неё нет флага выполнения. Этот атрибут устанавливается для всех программ и скриптов, именно с помощью него система понимает, что этот файл нужно запустить как программу.

Атрибуты — это набор основных девяти битов, определяющих какие из пользователей обладают правами на чтение, запись и исполнение. Первые три бита отвечают права доступа владельца, вторые — для группы пользователей, последние — для всех остальных пользователей в системе.

Установка атрибутов производится командой `chmod`. Установка бита чтения (r) позволяет сделать файл доступным для чтения. Наличие бита записи (w) позволяет изменять файл. Установка бита запуска (x) позволяет запускать файл на исполнение.

В ОС Linux, группа — это набор пользователей. Основная цель групп — это определить права на чтение, запись и исполнение сразу для нескольких пользователей, состоящих в группе. Так же пользователи могут быть добавлены в уже существующие группы для получения их прав.

Группы бывают двух видов:

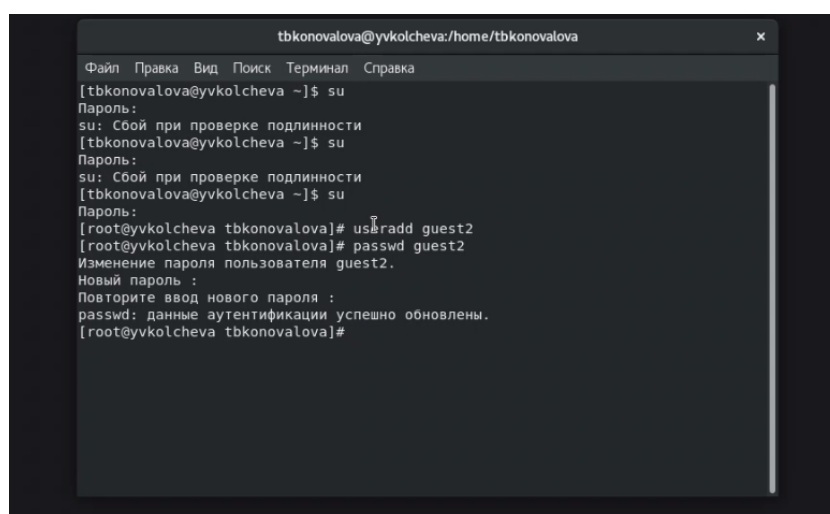
- Первичная группа — это группа, приписанная к файлам, созданным пользователем. Обычно имя первичной группы совпадает с именем пользователя. У каждого пользователя может быть только одна первичная группа.
- Вторичная группа — используется для определения прав для набора пользователей. Пользователь может состоять в нескольких вторичных группах или не состоять ни в одной.

3 Задание

1. Создать нового пользователя в Виртуальной машине, установить для него пароль, чтобы можно было работать с двумя пользователями одновременно. 2. Заполнить таблицу «Установленные права и разрешённые действия» (см. табл. 3.1) 3. На основании заполненной таблицы 3.1 определить те или иные минимально необходимые права для выполнения операций внутри директории. Заполнить таблицу «Минимальные права для совершения операций» 3.2.

4 Выполнение лабораторной работы

1). Создала нового пользователя guest2 командой useradd, затем установила для него пароль с помощью команды passwd guest2 (рис. [4.1]).



```
tbkonovalova@yvkolcheva:/home/tbkonovalova
Файл Правка Вид Поиск Терминал Справка
[tbkonovalova@yvkolcheva ~]$ su
Пароль:
su: Сбой при проверке подлинности
[tbkonovalova@yvkolcheva ~]$ su
Пароль:
su: Сбой при проверке подлинности
[tbkonovalova@yvkolcheva ~]$ su
Пароль:
[root@yvkolcheva tbkonovalova]# useradd guest2
[root@yvkolcheva tbkonovalova]# passwd guest2
Изменение пароля пользователя guest2.
Новый пароль :
Повторите ввод нового пароля :
passwd: данные аутентификации успешно обновлены.
[root@yvkolcheva tbkonovalova]#
```

Рис. 4.1: Создание пользователя и установка пароля

2). Зашла в систему от имени пользователей guest и guest2 на двух терминалах, используя команду su - и только что установленный пароль.

Выполнила команду pwd, которая показывает, что мы находимся в соответствующих домашних каталогах пользователей. Уточнила имя пользователя, используя команду whoami, получила вывод guest и guest2 соответственно. Определила группы для каждого пользователя, в которых состоят пользователи командой groups. Пользователь guest состоит только в группе guest, а пользователь guest2 состоит в двух группах — guest и guest2. Эту же информацию можно узнать с помощью команды id -Gn (рис. [4.2]).

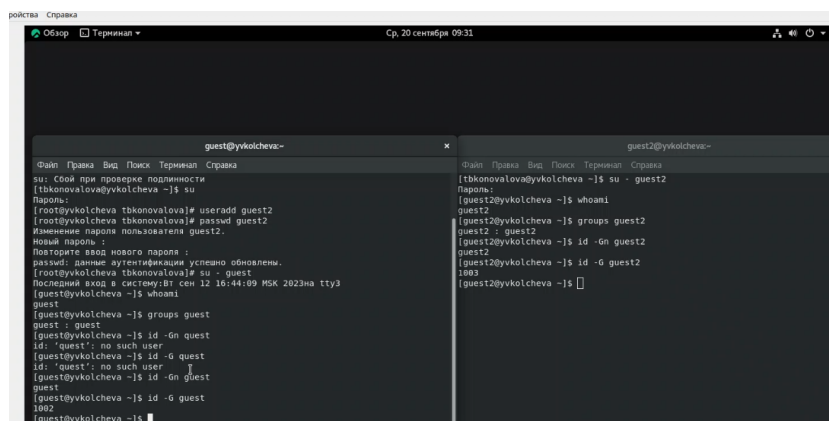


Рис. 4.2: Проверка групп

3). В содержимом файла `/etc/passwd` находим информацию о группах, в которых состоят пользователи, что соответствует данным, полученным с помощью команды `id` и `groups` (рис. [4.3]) и (рис. [4.4]). От имени пользователя `guest2` выполнила регистрацию пользователя в группе командой `newgrp` (рис. [4.5]).

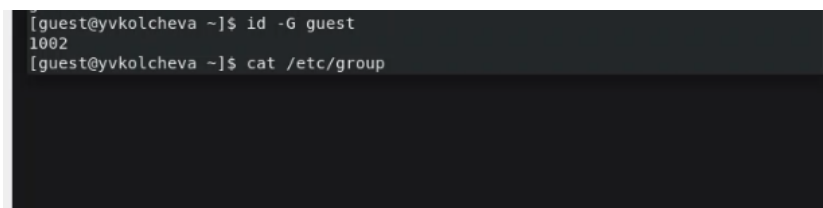


Рис. 4.3: Команда `/etc/passwd`

```
ройства Справка  
Обзор Терминал  
Ср, 20 сентября 0  
guest@yvkolcheva:~  
Файл Правка Вид Поиск Терминал Справка  
pipewire:x:983:  
pulse-access:x:982:  
pulse-rt:x:981:  
pulse:x:171:  
gluster:x:980:  
usbmuxd:x:113:  
rpc:x:32:  
saslauth:x:76:  
avahi:x:70:  
clevis:x:979:  
rpcuser:x:29:  
qemu:x:107:  
flatpak:x:978:  
dnsmasq:x:977:  
colord:x:976:  
libvirt:x:975:  
gdm:x:42:  
gnome-initial-setup:x:974:  
vboxsf:x:973:  
vboxdrmpc:x:972:  
tbkonovalova:x:1001:  
guest:x:1002:  
guest2:x:1003:  
[guest@yvkolcheva ~]$
```

Рис. 4.4: Результат команды /etc/passwd

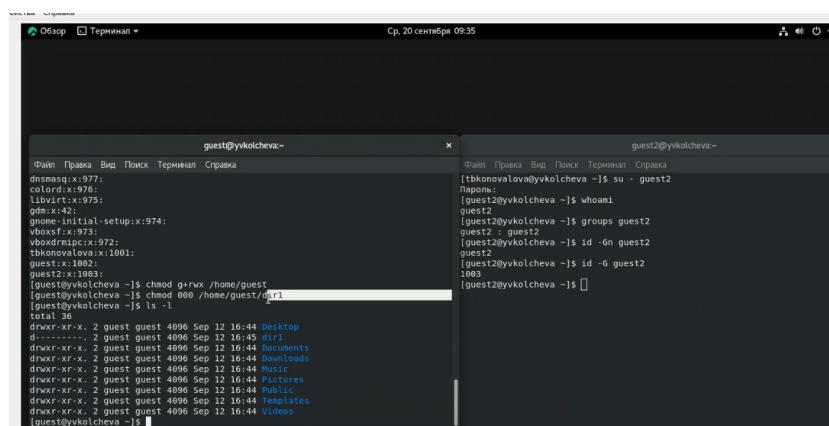


Рис. 4.5: Регистрация пользователя в группе group

4). От имени пользователя guest изменила права на директорию /home/guest, чтобы пользователи в группе получили доступ к файлам в домашнем каталоге. Также меняю директорию dir1 атрибуты с помощью команды chmod 000. Далее проверяем изменения командой ls -l (рис. [4.6]).

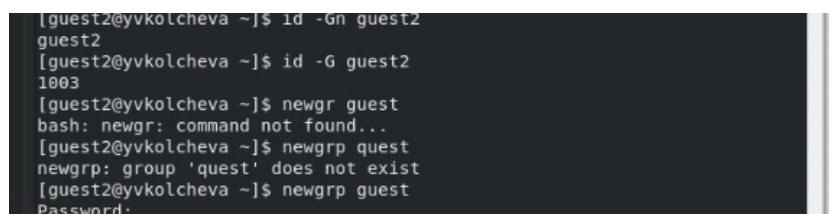


Рис. 4.6: Смена атрибутов

5). Далее решила изучить, как влияют различные комбинации атрибутов файлов и директории на различные действия. Для этого меняла атрибуты файлов от имени пользователя guest командой chmod. А от имени пользователя guest2 пыталась создать файл командой touch, удалить его командой rm, записать в файл командой echo >, прочитать файл командой cat, сменить директорию командой cd, просмотреть директорию командой ls, переименовать файл командой rename и сменить атрибуты командой chattr .

Все приведённые исследования отмечала в таблице (шаблон представлен в описании выполнения лабораторной работы №3). Успех отмечала +, в случае

ошибки доступа записывала -

Все данные я внесла в таблицу 3.1 «Установленные права и разрешённые действия» (рис. [4.7]) и (рис. [4.8]).

Установленные права и разрешённые действия (таб. 2.1)

Права директори и	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директор ии	Просмот р файлов в директор ии	Переиме нование файла	Смена атрибуто в
d (000)	(000)	-	-	-	-	-	-	-	-
d -x (010)	(000)	-	-	-	-	+	-	-	-
d -w- (020)	(000)	-	-	-	-	-	-	-	-
d -wx (030)	(000)	+	+	-	-	+	-	+	-
dr- (040)	(000)	-	-	-	-	-	+	-	-
d r-x (050)	(000)	-	-	-	-	+	+	-	-
d rw- (060)	(000)	-	-	-	-	-	+	-	-
d rwx (070)	(000)	+	+	-	-	+	+	+	-
d (000)	(010)	-	-	-	-	-	-	-	-
d -x (010)	(010)	-	-	-	-	+	-	-	-
d -w- (020)	(010)	-	-	-	-	-	-	-	-
d -wx (030)	(010)	+	+	-	-	+	-	+	-
dr- (040)	(010)	-	-	-	-	-	+	-	-
d r-x (050)	(010)	-	-	-	-	+	+	-	-
d rw- (060)	(010)	-	-	-	-	-	+	-	-
d rwx (070)	(010)	+	+	-	-	+	+	+	-
d (000)	(020)	-	-	-	-	-	-	-	-
d -x (010)	(020)	-	-	+	-	+	-	-	-
d -w- (020)	(020)	-	-	-	-	-	-	-	-
d -wx (030)	(020)	+	+	+	-	+	-	+	-
dr- (040)	(020)	-	-	-	-	-	+	-	-
d r-x (050)	(020)	-	-	+	-	+	+	-	-
d rw- (060)	(020)	-	-	-	-	-	+	-	-
d rwx (070)	(020)	+	+	+	-	+	+	+	-
d (000)	(030)	-	-	-	-	-	-	-	-
d -x (010)	(030)	-	-	+	-	+	-	-	-
d -w- (020)	(030)	-	-	-	-	-	-	-	-
d -wx (030)	(030)	+	+	-	+	+	-	+	-
dr- (040)	(030)	-	-	-	-	-	+	-	-
d r-x (050)	(030)	-	-	+	-	+	+	-	-
d rw- (060)	(030)	-	-	-	-	-	+	-	-
d rwx (070)	(030)	+	+	+	-	+	+	+	-
d (000)	(040)	-	-	-	-	-	-	-	-
d -x (010)	(040)	-	-	-	+	+	-	-	-
d -w- (020)	(040)	-	-	-	-	-	-	-	-
d -wx (030)	(040)	+	+	-	+	+	-	+	-
dr- (040)	(040)	-	-	-	-	-	+	-	-
d r-x (050)	(040)	-	-	-	+	+	+	-	-
d rw- (060)	(040)	-	-	-	-	-	+	-	-
d rwx (070)	(040)	+	+	-	+	+	+	+	-
d (000)	(050)	-	-	-	-	-	-	-	-

Рис. 4.7: Таблца 3.1 «Установленные права и разрешённые действия»

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

Рис. 4.8: Таблица 3.1 «Установленные права и разрешённые действия»

В сравнении с таблицей из Лабораторной работы №2 мы можем наблюдать, что изменилась только возможность изменять атрибуты файлов. Это связано с тем, что во всех комбинациях стоит 0 в начале, что означает отсутствие прав у владельца файла и директории. Остальные же действия доступны как владельцу, так и членам группы, в равной степени при должной конфигурации прав.

6). На основании этой таблицы я заполнила вторую таблицу (3.2) «Минимальные права для совершения операций». В данной таблице указала минимальные требования на права и директорию для выполнения тех или иных действий. Все данные я внесла в таблицу (рис. [4.9]).

Минимальные права для совершения операция (таб. 2.2)

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)	(040)
Запись в файл	d-x (010)	(020)
Переименование файла	d-wx (030)	(000)
Создание поддиректории	d-wx (030)	(000)
Удаление поддиректории	d-wx (030)	(000)

Рис. 4.9: Таблица 3.2 «Минимальные права для совершения операций»

5 Выводы

Приобрела практические навыки работы с атрибутами директорий и файлов в группе пользователей через консоль, выяснила минимальные требования и права для совершения различных действий над файлами и директориями.

6 Библиография

СПИСОК ЛИТЕРАТУРЫ

- 1.Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>
- 2.Теоретические знания, приведённые в Лабораторной работе №3 - https://esystem.rudn.ru/pluginfile.php/2090125/mod_resource/content/4/003-lab_discret_2users.pdf
- 3.Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

- 1.[Электронный ресурс] - доступ: <https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux>
- 2.[Электронный ресурс] - доступ: <https://debianinstall.ru/diskretionnoe-razgranichenie-dostupa-linux/>