

Отчёт по лабораторной работе №2

Дисциплина: Основы информационной безопасности

Полиенко Анастасия Николаевна, НПМбд-01-19

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
4	Выводы	18
	Список литературы	19

Список иллюстраций

3.1	Создание пользователя и установка пароля	7
3.2	Проверка данных пользователя	8
3.3	Проверка атрибутов	8
3.4	Смена атрибутов	9
3.5	Команды над файлами и директориями	10

Список таблиц

3.1	Установленные права и разрешённые действия	10
3.2	Минимальные права для совершения операций	16

1 Цель работы

Получить навыки работы в консоли с правами и атрибутами файлов и директорий, а также проверка необходимых прав для выполнения различных действий для работы с файлами и директориями.

2 Теоретическое введение

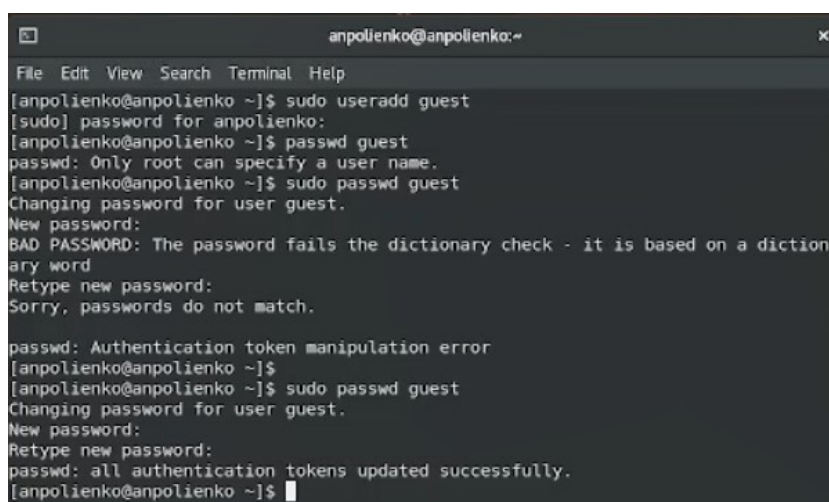
Атрибуты — это набор основных девяти битов, определяющих какие из пользователей обладают правами на чтение, запись и исполнение. Первые три бита отвечают права доступа владельца, вторые — для группы пользователей, последние — для всех остальных пользователей в системе.

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.

Более подробно см. в [1].

3 Выполнение лабораторной работы

Создаём нового пользователя `guest` командой `useradd`, затем устанавливаем для него пароль с помощью команды `passwd guest` (рис. 3.1).

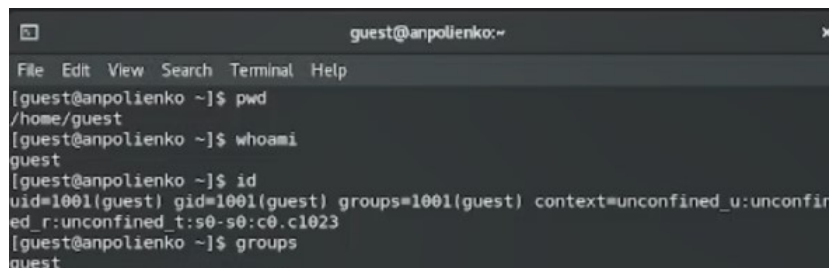


```
anpolienko@anpolienko:~  
File Edit View Search Terminal Help  
[anpolienko@anpolienko ~]$ sudo useradd guest  
[sudo] password for anpolienko:  
[anpolienko@anpolienko ~]$ passwd guest  
passwd: Only root can specify a user name.  
[anpolienko@anpolienko ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary word  
Retype new password:  
Sorry, passwords do not match.  
  
passwd: Authentication token manipulation error  
[anpolienko@anpolienko ~]$  
[anpolienko@anpolienko ~]$ sudo passwd guest  
Changing password for user guest.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[anpolienko@anpolienko ~]$
```

Рис. 3.1: Создание пользователя и установка пароля

Заходим в систему от имени пользователя `guest`, используя только что установленный пароль.

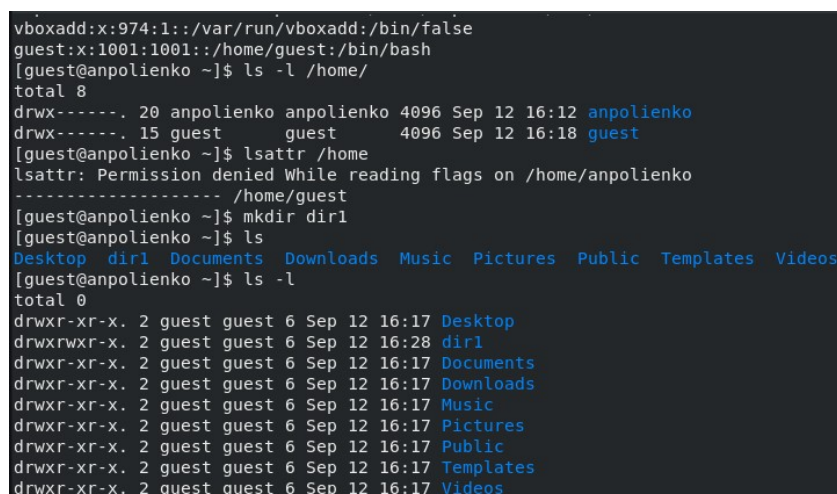
Выполняем команду `rwd`, которая показывает, что мы находимся в домашнем каталоге пользователя `guest`. Уточняем имя пользователя командой `whoami`, ожидаемо получаем вывод `guest`. С помощью команды `id` узнаём, что `uid = 1001`, `gid = 1001` (`guest`). При вводе команды `groups` убеждаемся, что группа состоит из одного пользователя `guest` (рис. 3.2).

A terminal window titled 'guest@anpolienko:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

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

Рис. 3.2: Проверка данных пользователя

В содержимом файла `/etc/passwd` находим информацию о пользователе, что соответствует данным, полученным с помощью команды `id` и `pwd`. Далее определяем содержимое каталога `/home`. С помощью команды `ls -l /home/` видим две домашние директории: `anpolienko` и `guest` с их атрибутами `rwX` в первом бите для каждой. С помощью команды `lsattr /home` можем увидеть расширенные атрибуты только текущего пользователя. Далее создаём новый каталог `dir1` и можем увидеть, что у него больше атрибутов по сравнению со стандартными директориями (рис. 3.3).

A terminal window showing the following commands and output:

```
vboxadd:x:974:1::/var/run/vboxadd:/bin/false
guest:x:1001:1001::/home/guest:/bin/bash
[guest@anpolienko ~]$ ls -l /home/
total 8
drwx----- 20 anpolienko anpolienko 4096 Sep 12 16:12 anpolienko
drwx----- 15 guest guest 4096 Sep 12 16:18 guest
[guest@anpolienko ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/anpolienko
----- /home/guest
[guest@anpolienko ~]$ mkdir dir1
[guest@anpolienko ~]$ ls
Desktop dir1 Documents Downloads Music Pictures Public Templates Videos
[guest@anpolienko ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Desktop
drwxrwxr-x. 2 guest guest 6 Sep 12 16:28 dir1
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Documents
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Music
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Public
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Templates
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Videos
```

Рис. 3.3: Проверка атрибутов

Меняем директорию `dir1` атрибуты с помощью команды `chmod 000`. Далее, при попытке создать файл, видим сообщение об ошибке, т.к. забрали права на всё у всех пользователей. Файл, соответственно, тоже не создаётся (рис. 3.4).


```

[guest@anpolienko ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@anpolienko ~]$ chmod 000 dir1
[guest@anpolienko ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Desktop
d----- . 2 guest guest 6 Sep 12 16:28 dir1
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Documents
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Downloads
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Music
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Pictures
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Public
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Templates
drwxr-xr-x. 2 guest guest 6 Sep 12 16:17 Videos
[guest@anpolienko ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@anpolienko ~]$ ls -l /home/guest/dir1
ls: cannot access '/home/guest/dir1': No such file or directory
[guest@anpolienko ~]$

```

Рис. 3.4: Смена атрибутов

Далее изучим, как влияют различные комбинации атрибутов файлов и директории на различные действия. Для этого будем пытаться 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` (рис. 3.5).

```

guest@anpolienko:~
File Edit View Search Terminal Help
bash: cd: dir1: Permission denied
[guest@anpolienko ~]$ ls dir1
ls: cannot access 'dir1/file1': Permission denied
file1
[guest@anpolienko ~]$ rename file1 file2 ~/dir1/file1
rename: /home/guest/dir1/file1: rename to /home/guest/dir1/file2 failed: Permission denied
[guest@anpolienko ~]$ chattr +A ~/dir1/file1
chattr: Permission denied while trying to stat /home/guest/dir1/file1
[guest@anpolienko ~]$ chmod 700 dir1
[guest@anpolienko ~]$ touch ~/dir1/file2
[guest@anpolienko ~]$ rm ~/dir1/file2
[guest@anpolienko ~]$ echo "test" > ~/dir1/file1
[guest@anpolienko ~]$ cat ~/dir1/file1
test
[guest@anpolienko ~]$ cd dir1
[guest@anpolienko dir1]$ cd
[guest@anpolienko ~]$ ls dir1
file1
[guest@anpolienko ~]$ rename file1 file2 ~/dir1/file1
[guest@anpolienko ~]$ rename file2 file1 ~/dir1/file2
[guest@anpolienko ~]$ chattr +A ~/dir1/file1
[guest@anpolienko ~]$ chattr -A ~/dir1/file1
[guest@anpolienko ~]$

```

Рис. 3.5: Команды над файлами и директориями

В случае успеха будет записывать +, в случае ошибки доступа будем записывать -. Соберём данные в таблицу 3.1.

Таблица 3.1: Установленные права и разрешённые действия

Права	Права	Создание	Удаление	Запись в файл	Чтение файла	Смена директории	Переименование файла	Смена атрибутов файла
d (000)	(000)	-	-	-	-	-	-	-
d -x (100)	(000)	-	-	-	-	+	-	-
d -w- (200)	(000)	-	-	-	-	-	-	-
d -wx (300)	(000)	+	+	-	-	+	-	+

Права дирек- тории	Пра- ва фай- ла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Переиме- нование файла	Сме- на атри- бутов фай- ла
d r- (400)	(000)	-	-	-	-	-	+	-
d r-x (500)	(000)	-	-	-	-	+	+	-
d rw- (600)	(000)	-	-	-	-	-	+	-
d rwx (700)	(000)	+	+	-	-	+	+	+
d (000)	-x (100)	-	-	-	-	-	-	-
d -x (100)	-x (100)	-	-	-	-	+	-	-
d -w- (200)	-x (100)	-	-	-	-	-	-	-
d -wx (300)	-x (100)	+	+	-	-	+	-	+
d r- (400)	-x (100)	-	-	-	-	-	+	-
d r-x (500)	-x (100)	-	-	-	-	+	+	-
d rw- (600)	-x (100)	-	-	-	-	-	+	-

Права дирек- тории	Пра- ва фай- ла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Переиме- нование файла	Сме- на атри- бутов фай- ла
d rwx (700)	-x (100)	+	+	-	-	+	+	+
d (000)	-w- (200)	-	-	-	-	-	-	-
d -x (100)	-w- (200)	-	-	+	-	+	-	-
d -w- (200)	-w- (200)	-	-	-	-	-	-	-
d -wx (300)	-w- (200)	+	+	+	-	+	-	+
d r- (400)	-w- (200)	-	-	-	-	-	+	-
d r-x (500)	-w- (200)	-	-	+	-	+	+	-
d rw- (600)	-w- (200)	-	-	-	-	-	+	-
d rwx (700)	-w- (200)	+	+	+	-	+	+	+
d (000)	-wx (300)	-	-	-	-	-	-	-
d -x (100)	-wx (300)	-	-	+	-	+	-	-

Права дирек- тории	Пра- ва фай- ла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Переиме- нование файла	Сме- на атри- бутов фай- ла
d -w- (200)	-wx (300)	-	-	-	-	-	-	-
d -wx (300)	-wx (300)	+	+	+	-	+	-	+
d r- (400)	-wx (300)	-	-	-	-	-	+	-
d r-x (500)	-wx (300)	-	-	+	-	+	+	-
d rw- (600)	-wx (300)	-	-	-	-	-	+	-
d rwx (700)	-wx (300)	+	+	+	-	+	+	+
d (000)	r- (400)	-	-	-	-	-	-	-
d -x (100)	r- (400)	-	-	-	+	+	-	-
d -w- (200)	r- (400)	-	-	-	-	-	-	-
d -wx (300)	r- (400)	+	+	-	+	+	-	+
d r- (400)	r- (400)	-	-	-	-	-	+	-

Права дирек- тории	Пра- ва фай- ла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Переиме- нование файла	Сме- на атри- бутов фай- ла
d r-x (500)	r- (400)	-	-	-	+	+	+	-
d rw- (600)	r- (400)	-	-	-	-	-	+	-
d rwx (700)	r- (400)	+	+	-	+	+	+	+
d (000)	r-x (500)	-	-	-	-	-	-	-
d -x (100)	r-x (500)	-	-	-	+	+	-	-
d -w- (200)	r-x (500)	-	-	-	-	-	-	-
d -wx (300)	r-x (500)	+	+	-	+	+	-	+
d r- (400)	r-x (500)	-	-	-	-	-	+	-
d r-x (500)	r-x (500)	-	-	-	+	+	+	-
d rw- (600)	r-x (500)	-	-	-	-	-	+	-
d rwx (700)	r-x (500)	+	+	-	+	+	+	+

Права дирек- тории	Пра- ва фай- ла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Переиме- нование файла	Сме- на атри- бутов фай- ла
d (000)	rw- (600)	-	-	-	-	-	-	-
d -x (100)	rw- (600)	-	-	+	+	+	-	-
d -w- (200)	rw- (600)	-	-	-	-	-	-	-
d -wx (300)	rw- (600)	+	+	+	+	+	-	+
d r- (400)	rw- (600)	-	-	-	-	-	+	-
d r-x (500)	rw- (600)	-	-	+	+	+	+	-
d rw- (600)	rw- (600)	-	-	-	-	-	+	-
d rwx (700)	rw- (600)	+	+	+	+	+	+	+
d (000)	rw- (700)	-	-	-	-	-	-	-
d -x (100)	rw- (700)	-	-	+	+	+	-	-
d -w- (200)	rw- (700)	-	-	-	-	-	-	-

Права дирек- тории	Пра- ва фай- ла	Созда- ние файла	Удале- ние файла	За- пись в файл	Чте- ние фай- ла	Смена дирек- тории	Переиме- нование файла	Сме- на атри- бутов фай- ла
d -wx (300)	rwX (700)	+	+	+	+	+	-	+
d r- (400)	rwX (700)	-	-	-	-	-	+	-
d r-x (500)	rwX (700)	-	-	+	+	+	+	-
d rw- (600)	rwX (700)	-	-	-	-	-	+	-
d rwx (700)	rwX (700)	+	+	+	+	+	+	+

На основании этой таблицы создадим другую, в которой опишем минимальные требования на права и директорию для выполнения тех или иных действий. Внесём проанализированные данные в таблицу 3.2.

Таблица 3.2: Минимальные права для совершения операций

Опера- ция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d -wx (300)	— (000)
Удаление файла	d -wx (300)	— (000)

<hr/>		
Опера- ция	Минимальные права на директорию	Минимальные права на файл
<hr/>		
Чтение файла	d -x (100)	r- (400)
Запись в файл	d -x (100)	-w- (200)
Переиме- нование файла	d -wx (300)	— (000)
Создание подди- ректории	d -wx (300)	— (000)
Удаление подди- ректории	d -wx (300)	— (000)
<hr/>		

4 Выводы

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

Список литературы

1. File attributes in Linux [Электронный ресурс]. ITProffi, 2016. URL: <https://itproffi.ru/atributy-failov-v-linux/>.