

Отчет по лабораторной работе №2

Основы информационной безопасности

Малюга Валерия Васильевна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
4.1	Атрибуты файлов	8
4.2	Заполнение таблицы 2.1	14
4.3	Заполнение таблицы 2.2	17
5	Выводы	18
6	Список литературы. Библиография	19

Список иллюстраций

4.1	Добавление пароля для пользователя	8
4.2	Текущая директория	9
4.3	Информация о пользователе	9
4.4	Сравнение информации об имени пользователя	10
4.5	Просмотр файла passwd	11
4.6	Создание поддиректории	12
4.7	Попытка создания файла	13
4.8	Проверка содержимого директории	13
4.9	Изменение прав и проверка возможных действий	14

Список таблиц

1 Цель работы

Получение практических навыков работы в консоли с атрибутами файлов, закрепление теоретических основ дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux

2 Задание

1. Работа с атрибутами файлов
2. Заполнение таблицы “Установленные права и разрешённые действия” (см. табл. 2.1)
3. Заполнение таблицы “Минимальные права для совершения операций” (см. табл. 2.2)

3 Теоретическое введение

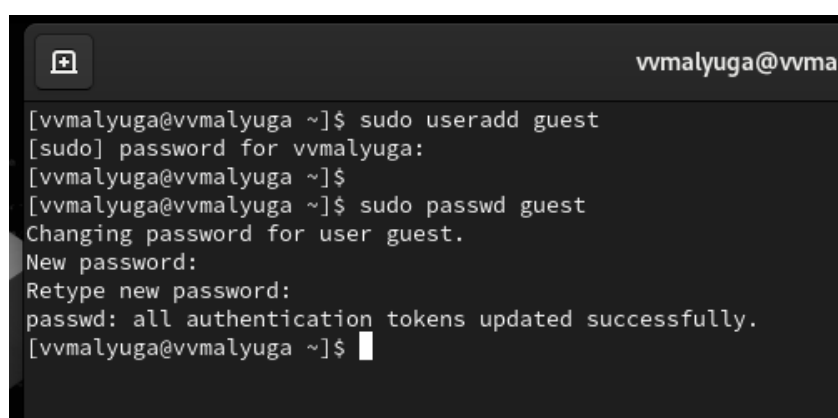
Операционная система — это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем. [1]

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. [2].

4 Выполнение лабораторной работы

4.1 Атрибуты файлов

В операционной системе Rocky создаю нового пользователя guest через учетную запись администратора. Далее задаю пароль для созданной учетной записи (рис. 1).

A screenshot of a terminal window with a dark background. The window title bar shows a window icon and the text 'vvmalyuga@vvmalyuga'. The terminal content shows the following commands and output:

```
[vvmalyuga@vvmalyuga ~]$ sudo useradd guest
[sudo] password for vvmalyuga:
[vvmalyuga@vvmalyuga ~]$
[vvmalyuga@vvmalyuga ~]$ sudo passwd guest
Changing password for user guest.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[vvmalyuga@vvmalyuga ~]$
```

Рис. 4.1: Добавление пароля для пользователя

Сменяю пользователя в системе на только что созданного пользователя guest. Определяю с помощью команды `pwd`, что я нахожусь в директории `/home/guest/`. Эта директория является домашней, ведь в приглашении командой строкой стоит значок `~`, указывающий, что я в домашней директории (рис. 4).

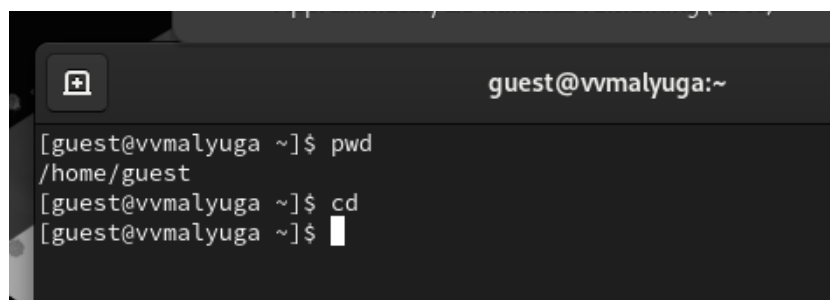
A terminal window with a dark background. The title bar shows a window icon and the text 'guest@vvmalyuga:~'. The terminal content shows a sequence of commands and their outputs: 'pwd' returns '/home/guest', and 'cd' is entered without output. The prompt is '[guest@vvmalyuga ~]\$'.

Рис. 4.2: Текущая директория

Уточняю имя пользователя. В выводе команды `groups` информация только о названии группы, к которой относится пользователь. В выводе команды `id` можно найти больше информации: имя пользователя и имя группы, также коды имени пользователя и группы (рис. 3)


A terminal window with a dark background. The title bar shows a window icon and the text 'guest@vvmalyuga:~'. The terminal content shows a sequence of commands and their outputs: 'whoami' returns 'guest', 'id' returns 'uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023', and 'groups' returns 'guest'. The prompt is '[guest@vvmalyuga ~]\$'.

Рис. 4.3: Информация о пользователе

Имя пользователя в приглашении командной строкой совпадает с именем пользователя, которое выводит команда `whoami` (рис. 4)

```
[guest@vvmalyuga ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/usr/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
sssd:x:997:995:User for sssd:/:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/
geoclue:x:996:994:User for geoclue:/var/lib/geoclue:/sbin/no
rtkit:x:172:172:RealtimeKit:/:/sbin/nologin
pipewire:x:995:992:PipeWire System Daemon:/run/pipewire:/usr
libstoragemgmt:x:990:990:daemon account for libstoragemgmt:/
cockpit-wsinstance:x:989:988:User for cockpit-ws instances:/t
flatpak:x:988:987:User for flatpak system helper:/:/sbin/nolo
colord:x:987:986:User for colord:/var/lib/colord:/sbin/nologt
clevis:x:986:985:Clevis Decryption Framework unprivileged use
setroubleshoot:x:985:984:SELinux troubleshoot server:/var/lib
gdm:x:42:42:./var/lib/gdm:/sbin/nologin
staprunpriv:x:159:159:systemtap unprivileged user:/var/lib/sta
pesign:x:984:983:Group for the pesign signing daemon:/run/pe
gnome-initial-setup:x:983:982:./run/gnome-initial-setup:/sbt
chrony:x:982:981:chrony system user:/var/lib/chrony:/sbin/no
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/u
dnsmasq:x:981:980:Dnsmasq DHCP and DNS server:/var/lib/dnsmas
tcpdump:x:72:72:./:/sbin/nologin
vvmalyuga:x:1000:1000:vvmalyuga:/home/vvmalyuga:/bin/bash
vboxadd:x:980:1:./var/run/vboxadd:/bin/false
guest:x:1001:1001:./home/guest:/bin/bash
[guest@vvmalyuga ~]$
```

Рис. 4.4: Сравнение информации об имени пользователя

Получаю информацию о пользователе с помощью команды

```
cat /etc/passwd | grep guest
```

В выводе получаю коды пользователя и группы, адрес домашней директории (рис. 5).

```

[guest@vvmalyuga ~]$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
[guest@vvmalyuga ~]$ ls -l /home/
total 8
drwx-----. 14 guest      guest      4096 Mar  8 18:39 guest
drwx-----. 18 vvmalyuga vvmalyuga 4096 Mar  8 18:32 vvmalyuga
[guest@vvmalyuga ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/vvmalyuga
----- /home/guest
[guest@vvmalyuga ~]$ mkdir dir1

```

Рис. 4.5: Просмотр файла passwd

Список поддиректорий директории home получилось получить с помощью команды `ls -l`. Права у директории:

vvmalyuga и guest: `drwx---`.

Пыталась проверить расширенные атрибуты директорий. Нет, их увидеть не удалось (рис. 5). Увидеть расширенные атрибуты других пользователей, тоже не удалось, для них даже вывода списка директорий не было.

1Создаю поддиректорию `dir1` для домашней директории. Расширенные атрибуты командой `lsattr` просмотреть у директории не удастся, но атрибуты есть: `drwxr-xr-x`, их удалось просмотреть с помощью команды `ls -l` (рис. 6).

```

[guest@vvmalyuga ~]$ mkdir dir1
[guest@vvmalyuga ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Desktop
drwxr-xr-x. 2 guest guest 6 Mar  8 18:48 dir1
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Documents
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Downloads
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Music
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Pictures
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Public
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Templates
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Videos
[guest@vvmalyuga ~]$
[guest@vvmalyuga ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
----- ./dir1
[guest@vvmalyuga ~]$
```

Рис. 4.6: Создание поддиректории

Снимаю атрибуты командой `chmod 000 dir1`, при проверке с помощью команды `ls -l` видно, что теперь атрибуты действительно сняты (рис. 7).

Попытка создать файл в директории `dir1`. Выдает ошибку: "Permission denied" (рис. 7).

```
----- ./dir1
[guest@vvmalyuga ~]$ chmod 000 dir1
[guest@vvmalyuga ~]$ lsattr
----- ./Desktop
----- ./Downloads
----- ./Templates
----- ./Public
----- ./Documents
----- ./Music
----- ./Pictures
----- ./Videos
lsattr: Permission denied While reading flags on ./dir1
[guest@vvmalyuga ~]$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Desktop
d----- 2 guest guest 6 Mar  8 18:48 dir1
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Documents
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Downloads
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Music
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Pictures
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Public
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Templates
drwxr-xr-x. 2 guest guest 6 Mar  8 18:38 Videos
[guest@vvmalyuga ~]$
```

Рис. 4.7: Попытка создания файла

Вернув права директории и использовав снова команду `ls -l` можно убедиться, что файл не был создан

```
[guest@vvmalyuga ~]$ echo "test" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Permission denied
[guest@vvmalyuga ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
[guest@vvmalyuga ~]$
```

Рис. 4.8: Проверка содержимого директории

Далее выполняются пункты 14 и 15 (рис. 9)

```
[guest@vvmalyuga ~]$ mkdir testdir
touch testdir/testfile
ls -l testdir
total 0
-rw-r--r--. 1 guest guest 0 Mar  8 19:04 testfile
[guest@vvmalyuga ~]$ ^C
[guest@vvmalyuga ~]$ ls -l testdir/testfile
-rw-r--r--. 1 guest guest 0 Mar  8 19:04 testdir/testfile
[guest@vvmalyuga ~]$ ls -l testdir
total 0
-rw-r--r--. 1 guest guest 0 Mar  8 19:04 testfile
[guest@vvmalyuga ~]$ chmod 000 testdir
[guest@vvmalyuga ~]$ ls -l testdir
ls: cannot open directory 'testdir': Permission denied
[guest@vvmalyuga ~]$ ls -l testdir/testfile
ls: cannot access 'testdir/testfile': Permission denied
[guest@vvmalyuga ~]$ sudo ls -l testdir

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for guest:
guest is not in the sudoers file. This incident will be reported.
[guest@vvmalyuga ~]$ rm testdir/testfile
rm: cannot remove 'testdir/testfile': Permission denied
[guest@vvmalyuga ~]$ cat testdir/testfile
cat: testdir/testfile: Permission denied
[guest@vvmalyuga ~]$ mv testdir/testfile testdir/tet
mv: failed to access 'testdir/tet': Permission denied
[guest@vvmalyuga ~]$ ls testdir
ls: cannot open directory 'testdir': Permission denied
[guest@vvmalyuga ~]$ echo "test" > testdir/testfile
bash: testdir/testfile: Permission denied
[guest@vvmalyuga ~]$
```

Рис. 4.9: Изменение прав и проверка возможных действий

4.2 Заполнение таблицы 2.1

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
d(000)	(000)	-	-	-	-	-	-	-	-
d(000)	(100)	-	-	-	-	-	-	-	-
d(000)	(200)	-	-	-	-	-	-	-	-
d(000)	(300)	-	-	-	-	-	-	-	-

d(000)	(400)	-	-	-	-	-	-	-	-
d(000)	(500)	-	-	-	-	-	-	-	-
d(000)	(600)	-	-	-	-	-	-	-	-
d(000)	(700)	-	-	-	-	-	-	-	-
d(100)	(000)	-	-	-	-	+	-	-	+
d(100)	(100)	-	-	-	-	+	-	-	+
d(100)	(200)	-	-	+	-	+	-	-	+
d(100)	(300)	-	-	+	-	+	-	-	+
d(100)	(400)	-	-	-	+	+	-	-	+
d(100)	(500)	-	-	-	+	+	-	-	+
d(100)	(600)	-	-	+	+	+	-	-	+
d(100)	(700)	-	-	+	+	+	-	-	+
d(200)	(000)	-	-	-	-	-	-	-	-
d(200)	(100)	-	-	-	-	-	-	-	-
d(200)	(200)	-	-	-	-	-	-	-	-
d(200)	(300)	-	-	-	-	-	-	-	-
d(200)	(400)	-	-	-	-	-	-	-	-
d(200)	(500)	-	-	-	-	-	-	-	-
d(200)	(600)	-	-	-	-	-	-	-	-
d(200)	(700)	-	-	-	-	-	-	-	-
d(300)	(000)	+	+	-	-	+	-	+	+
d(300)	(100)	+	+	-	-	+	-	+	+
d(300)	(200)	+	+	+	-	+	-	+	+
d(300)	(300)	+	+	+	-	+	-	+	+
d(300)	(400)	+	+	-	+	+	-	+	+
d(300)	(500)	+	+	-	+	+	-	+	+
d(300)	(600)	+	+	+	+	+	-	+	+
d(300)	(700)	+	+	+	+	+	-	+	+

d(400)	(000)	-	-	-	-	-	+	-	-
d(400)	(100)	-	-	-	-	-	+	-	-
d(400)	(200)	-	-	-	-	-	+	-	-
d(400)	(300)	-	-	-	-	-	+	-	-
d(400)	(400)	-	-	-	-	-	+	-	-
d(400)	(500)	-	-	-	-	-	+	-	-
d(400)	(600)	-	-	-	-	-	+	-	-
d(400)	(700)	-	-	-	-	-	+	-	-
d(500)	(000)	-	-	-	-	+	+	-	+
d(500)	(100)	-	-	-	-	+	+	-	+
d(500)	(200)	-	-	+	-	+	+	-	+
d(500)	(300)	-	-	+	-	+	+	-	+
d(500)	(400)	-	-	-	+	+	+	-	+
d(500)	(500)	-	-	-	+	+	+	-	+
d(500)	(600)	-	-	+	+	+	+	-	+
d(500)	(700)	-	-	+	+	+	+	-	+
d(600)	(000)	-	-	-	-	-	+	-	-
d(600)	(100)	-	-	-	-	-	+	-	-
d(600)	(200)	-	-	-	-	-	+	-	-
d(600)	(300)	-	-	-	-	-	+	-	-
d(600)	(400)	-	-	-	-	-	+	-	-
d(600)	(500)	-	-	-	-	-	+	-	-
d(600)	(600)	-	-	-	-	-	+	-	-
d(600)	(700)	-	-	-	-	-	+	-	-
d(700)	(000)	+	+	-	-	+	+	+	+
d(700)	(100)	+	+	-	-	+	+	+	+
d(700)	(200)	+	+	+	-	+	+	+	+
d(700)	(300)	+	+	+	-	+	+	+	+

d(700)	(400)	+	+	-	+	+	+	+	+
d(700)	(500)	+	+	-	+	+	+	+	+
d(700)	(600)	+	+	+	+	+	+	+	+
d(700)	(700)	+	+	+	+	+	+	+	+

Таблица 2.1 «Установленные права и разрешённые действия»

4.3 Заполнение таблицы 2.2

Операция	Минимальные права на директорию	Минимальные права на файл
Создание файла	d(300)	-
Удаление файла	d(300)	-
Чтение файла	d(100)	(400)
Запись в файл	d(100)	(200)
Переименование файла	d(300)	(000)
Создание поддиректории	d(300)	-
Удаление поддиректории	d(300)	-

Таблица 2.2 “Минимальные права для совершения операций”

5 Выводы

Были получены практические навыки работы в консоли с атрибутами файлов, закреплены теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux.

6 Список литературы. Библиография

[1] Операционные системы: <https://blog.skillfactory.ru/glossary/operaczionnaya-sistema/>

[2] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>