

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Ильин Андрей Владимирович

Содержание

1	Цель работы	4
2	Задачи	5
3	Теоретическое введение	6
3.1	Термины	6
3.2	Окружение	6
4	Выполнение лабораторной работы	7
5	Анализ результатов	12
6	Выводы	13
	Список литературы	14

Список иллюстраций

4.1	Пользователь guest	7
4.2	Изучение пользователя	8
4.3	Проверка директории /home и созданной dir1	9
4.4	Права доступа	9
4.5	Эксперименты с правами доступа (1)	10
4.6	Эксперименты с правами доступа (2)	10
4.7	Фрагмент таблицы «Установленные права и разрешённые действия»	10
4.8	Таблицы «Минимальные права для совершения операций» . . .	11

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 Задачи

1. Создать, настроить пользователя guest и изучить информацию о пользователе.
2. Создать и изучить дериктории, провести эксперименты с правами доступа.
3. Заполнить таблицы “Установленные права и разрешённые действия” и “Минимальные права для совершения операций”.

3 Теоретическое введение

3.1 Термины

- Терминал (или «Bash», сокращение от «Bourne-Again shell») — это программа, которая используется для взаимодействия с командной оболочкой. Терминал применяется для выполнения административных задач, например: установку пакетов, действия с файлами и управление пользователями. [1]
- Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными файлами и каталогами. [2]

3.2 Окружение

- Rocky Linux - это корпоративная операционная система с открытым исходным кодом, разработанная таким образом, чтобы быть на 100% совместимой с Red Hat Enterprise Linux. Он находится в стадии интенсивной разработки сообществом. [3]
- Git - это распределенное программное обеспечение для контроля версиями. [4]
- VirtualBox - это кросс-платформенное ПО для виртуализации x86 и AMD64/Intel64 с открытым кодом для корпоративного и домашнего использования. [5]

4 Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создадим учётную запись пользователя guest. Зададим пароль для пользователя guest, после чего выйдем из текущего пользователя. (рис. 4.1)

```
sudo useradd guest
```

```
sudo passwd guest
```

```
logout
```



```
Rocky Linux 9.2 (Blue Onyx)
Kernel 5.14.0-284.11.1.el9_2.x86_64 on an x86_64

[aviljin login: aviljin
Password:
Last login: Sat Sep 16 19:22:05 on tty1
[aviljin@aviljin ~]$ sudo useradd guest

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 aviljin:
[aviljin@aviljin ~]$ sudo passwd guest
Changing password for user guest.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[aviljin@aviljin ~]$ logout
```

Рис. 4.1: Пользователь guest

2. Залогинимся под новым пользователем. Определим директорию, в которой находимся: директория является домашней. Уточним имя пользователя,

используя `whoami`. Уточним имя, группу, а также группы, куда входит пользователь, командой `id`. Вспользуемся командой `groups`. Просмотрим файл `/etc/passwd`. (рис. 4.2)

```
pwd
whoami
id
groups
cat /etc/passwd | grep guest
```



```
aviljin login: guest
Password:
lguest@aviljin ~$ pwd
/home/guest
lguest@aviljin ~$ whoami
guest
lguest@aviljin ~$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfined_r:unconfined_t:s0
-s0:c0.c1023
lguest@aviljin ~$ groups
guest
lguest@aviljin ~$ cat /etc/passwd | grep guest
guest:x:1001:1001::/home/guest:/bin/bash
lguest@aviljin ~$
```

Рис. 4.2: Изучение пользователя

3. Определим существующие в системе директории. Проверим, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории `/home`. Создадим в домашней директории поддиректорию `dir1`, определим командами, какие права доступа и расширенные атрибуты она имеет. (рис. 4.3)

```
ls -l /home/
lsattr /home
mkdir dir1
ls -l
lsattr
```



```

lguest@aviljin ~1$ ls -l /home/
total 0
drwx-----. 2 aviljin aviljin 83 Sep 16 19:31 aviljin
drwx-----. 2 guest  guest  62 Sep 16 19:30 guest
lguest@aviljin ~1$ lsattr /home
lsattr: Permission denied While reading flags on /home/aviljin
----- /home/guest
lguest@aviljin ~1$ pwd
/home/guest
lguest@aviljin ~1$ mkdir dir1
lguest@aviljin ~1$ ls
dir1
lguest@aviljin ~1$ ls -l
total 0
drwxr-xr-x. 2 guest guest 6 Sep 16 19:39 dir1
lguest@aviljin ~1$ lsattr
----- ./dir1
lguest@aviljin ~1$ _

```

Рис. 4.3: Проверка директории /home и созданной dir1

4. Снимем с директории dir1 все атрибуты. Попытаемся создать в директории dir1 файл file1. (рис. 4.4)

```

chmod 000 dir1
ls -l
echo "test" > /home/guest/dir1/file1
ls -l /home/guest/dir1

```

```

lguest@aviljin ~1$ chmod 000 dir1
lguest@aviljin ~1$ ls -l
total 0
d-----. 2 guest guest 6 Sep 16 19:39 dir1
lguest@aviljin ~1$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
lguest@aviljin ~1$ ls -l /home/guest/dir1/
ls: cannot open directory '/home/guest/dir1/': Permission denied

```

Рис. 4.4: Права доступа

5. Заполним таблицу «Установленные права и разрешённые действия» [6]. (рис. 4.5, 4.6, 4.7)

```
lguest@aviljin ~1$ chmod 200 dir1
lguest@aviljin ~1$ ls -l
total 0
d-w-----. 2 guest guest 6 Sep 16 19:39 dir1
lguest@aviljin ~1$ touch dir1/file1
touch: cannot touch 'dir1/file1': Permission denied
lguest@aviljin ~1$ echo "test" > /home/guest/dir1/file1
-bash: /home/guest/dir1/file1: Permission denied
lguest@aviljin ~1$ cd dir1/
-bash: cd: dir1/: Permission denied
lguest@aviljin ~1$ ls dir1/
ls: cannot open directory 'dir1/': Permission denied
```

Рис. 4.5: Эксперименты с правами доступа (1)

```
lguest@aviljin ~1$ chmod 300 dir1
lguest@aviljin ~1$ ls -l
total 0
d-wx-----. 2 guest guest 6 Sep 16 19:39 dir1
lguest@aviljin ~1$ touch dir1/file1
lguest@aviljin ~1$ cd dir1
lguest@aviljin dir1$ chmod 000 file1
lguest@aviljin dir1$ ls -l
ls: cannot open directory './': Permission denied
lguest@aviljin dir1$ echo "test" > file1
-bash: file1: Permission denied
lguest@aviljin dir1$ cat file1
cat: file1: Permission denied
lguest@aviljin dir1$ lsattr
lguest@aviljin dir1$ mv file1 file
lguest@aviljin dir1$ rm file
rm: remove write-protected regular empty file 'file'? y
```

Рис. 4.6: Эксперименты с правами доступа (2)

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переименование файла	Смена атрибутов файла
000	000	-	-	-	-	-	-	-	-
100	000	-	-	-	-	+	-	-	+
200	000	-	-	-	-	-	+	-	-
300	000	+	+	-	-	+	-	+	+
400	000	-	-	-	-	-	+	-	-
500	000	-	-	-	-	+	+	-	+
600	000	-	-	-	-	-	+	-	-
700	000	+	+	-	-	+	+	+	+
000	100	-	-	-	-	-	-	-	-
100	100	-	-	-	-	+	-	-	+
200	100	-	-	-	-	-	-	-	-
300	100	+	+	-	-	+	-	+	+
400	100	-	-	-	-	-	+	-	-
500	100	-	-	-	-	+	+	-	+
600	100	-	-	-	-	-	+	-	-
700	100	+	+	-	-	+	+	+	+
000	200	-	-	-	-	-	-	-	-
100	200	-	-	+	-	+	-	-	+
200	200	-	-	-	-	-	-	-	-
300	200	+	+	+	-	+	-	+	+
400	200	-	-	-	-	-	+	-	-
500	200	-	-	+	-	+	+	-	+
600	200	-	-	-	-	-	+	-	-
700	200	+	+	+	-	+	+	+	+
000	300	-	-	-	-	-	-	-	-
100	300	-	-	+	-	+	-	-	+

Рис. 4.7: Фрагмент таблицы «Установленные права и разрешённые действия»

6. Заполним таблицу «Минимальные права для совершения операций» [6].
(рис. 4.8)

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

Рис. 4.8: Таблицы «Минимальные права для совершения операций»

5 Анализ результатов

Работа выполнена без непредвиденных проблем в соответствии с руководством. Ошибок и сбоев не произошло.

6 Выводы

В рамках лабораторной работы был создан новый пользователь guest. На примере данного пользователя мы разобрали базовые команды, изучили информацию о пользователе. Также подробно разобрали права доступа.

Список литературы

1. Терминал Linux [Электронный ресурс]. URL: [https://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%20\(%D0%B8%D0%BB%D0%B8%20%C2%AB%D0%B8%20%D0%BB%20%D0%BC%D0%B8%20%D0%B8%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8F%D0%BC%D0%B8%7D](https://www.reg.ru/blog/linux-shpargalka-komandy-terminala-dlya-novichkov/#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB%20(%D0%B8%D0%BB%D0%B8%20%C2%AB%D0%B8%20%D0%BB%20%D0%BC%D0%B8%20%D0%B8%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8F%D0%BC%D0%B8%7D).
2. Права доступа [Электронный ресурс]. URL: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>.
3. Документация Rocky Linux [Электронный ресурс]. URL: <https://docs.rockylinux.org/>.
4. Git-Guides [Электронный ресурс]. URL: <https://github.com/git-guides>.
5. VirtualBox [Электронный ресурс]. URL: <https://www.virtualbox.org/>.
6. Полная таблица «Установленные права и разрешённые действия» [Электронный ресурс]. URL: https://github.com/av-ilin/study_2023-2024_infosec.git.