Лабораторная работа №2

Дискреционное разграничение прав в Linux

Ильинский Арсений Александрович

Содержание

Список иллюстраций

Список таблиц

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 (дистрибутив - Rocky) на примерах.

Задание

Выполнить задания из лабораторной работы и проанализировать полученные результаты.

Теоретическое введение

Для выполнения данной лабораторной нет специальной теории.

Выполнение лабораторной работы

Последовательно выполнил все пункты, занося ответы на поставленные вопросы и замечания в отчет:

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создал учётную запись пользователя guest (используя учётную запись администратора с правами root):

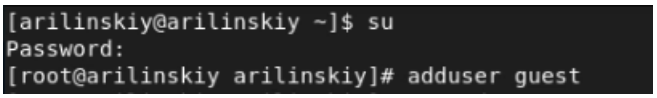

Рис. 1: Создание пользователя guest

2. Задал пароль для пользователя guest (использую учётную запись администратора с правами root):

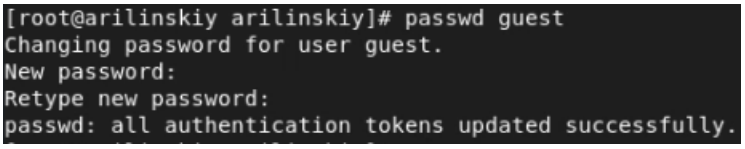

Рис. 2: Установка пароля для guest

3. Вошел в систему от имени пользователя guest:

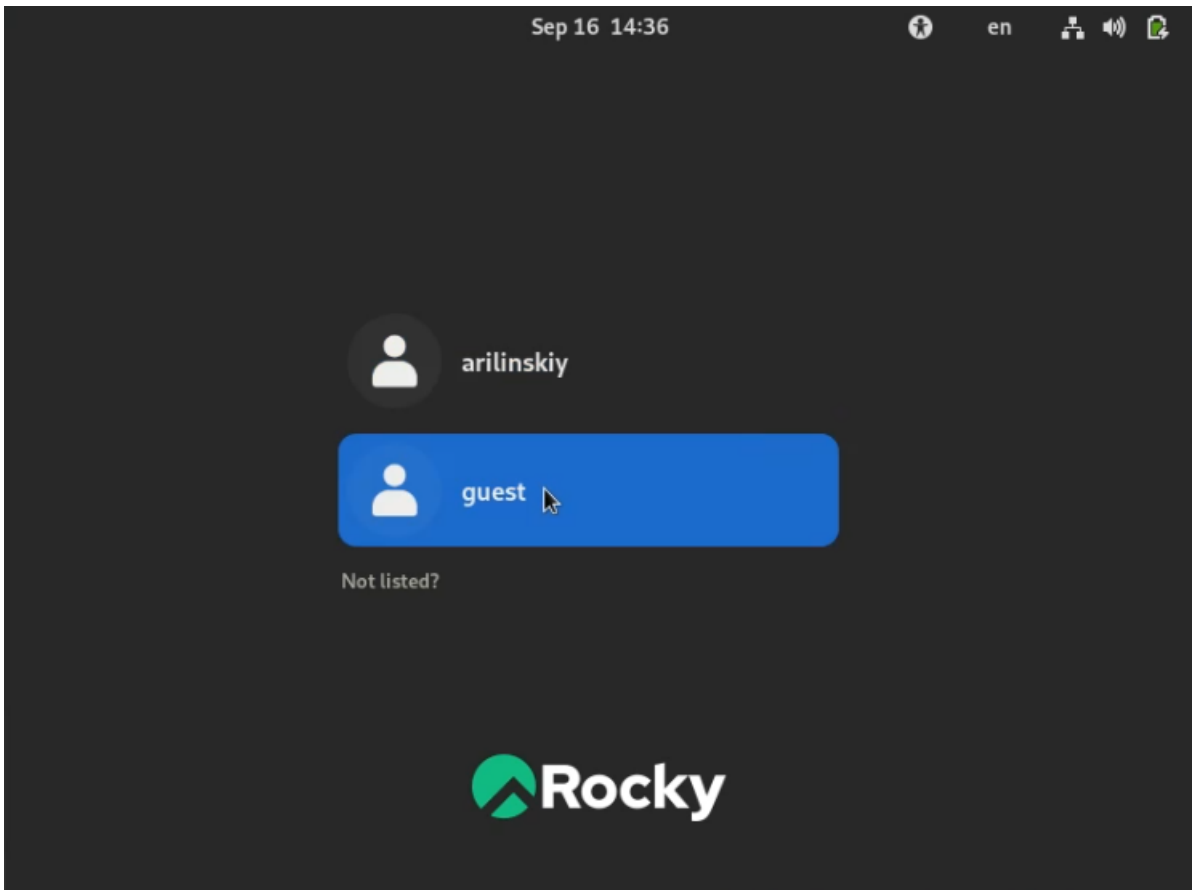

Рис. 3: Вход в систему под guest (1/2)

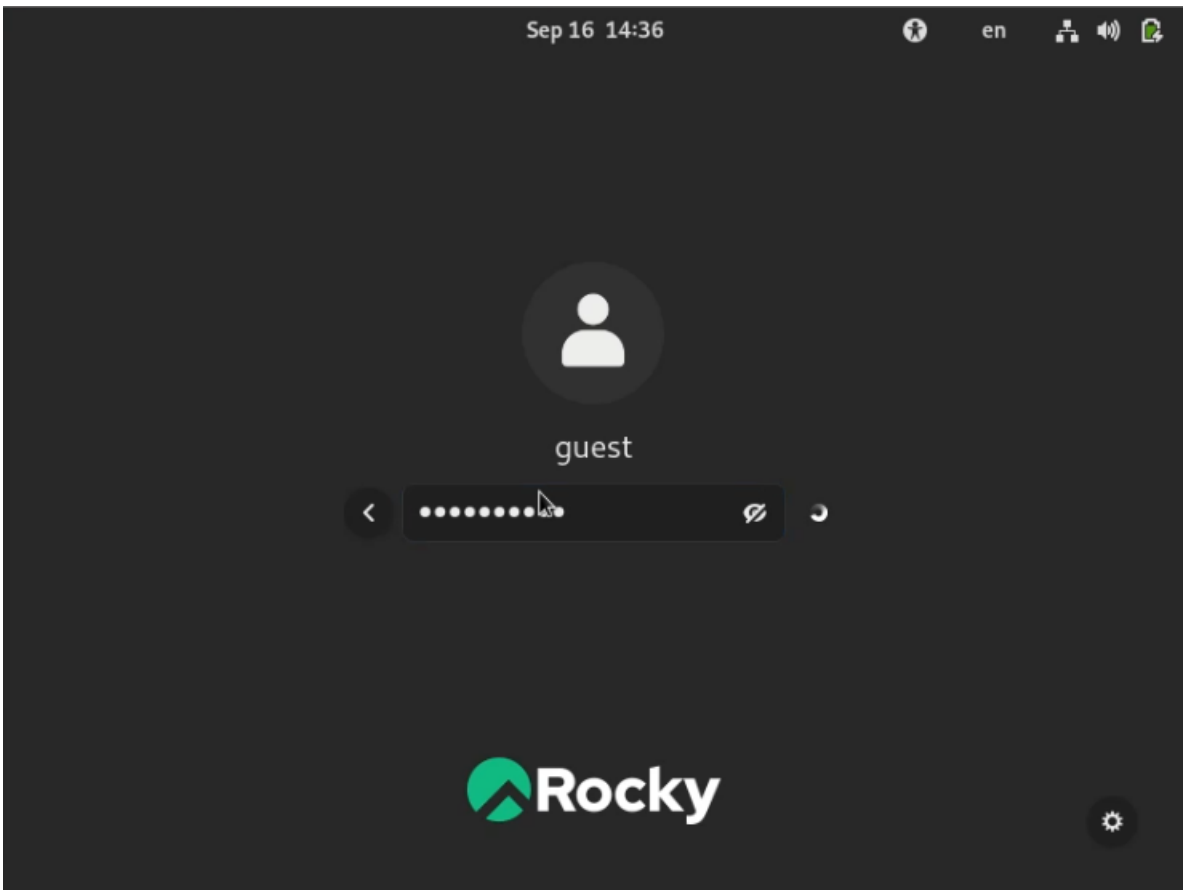

Рис. 4: Вход в систему под guest (2/2)

4. Определил директорию, в которой нахожусь, командой *pwd*. Она является домашней для пользователя guest, что совпадает с приглашением командной строки:

```
[guest@arilinskiy ~]$ pwd
/home/guest
```

Рис. 5: Домашняя директория

5. Уточнил имя пользователя командой whoami:

```
[guest@arilinskiy ~]$ whoami
guest
```

Рис. 6: Определение пользователя

6. Уточнил имя пользователя (1001(guest)), его группу (1001(guest)), а также группы, куда входит пользователь (1001(guest)), командой *id*:

```
[guest@arilinskiy ~]$ id
uid=1001(guest) gid=1001(guest) groups=1001(guest) context=unconfined_u:unconfin
ed_r:unconfined_t:s0-s0:c0.c1023
```

Рис. 7: Имя пользователя, группа, а также группы, куда входит пользователь

а также сравнил с выводом команды *groups*:

```
[guest@arilinskiy ~]$ groups
guest
```

Рис. 8: Группы пользователя

Если сравнивать вывод *id* с выводом *groups*, то очевидно, что команда *id* выводит намного больше информации.

7. Сравнил полученную информацию об имени пользователя с данными, выводимыми в приглашении командной строки:

   Полученная информация об имени пользователя совпадает с данными, выводимыми в приглашении командой строки.

8. Просмотрел файл */etc/passwd* командой *cat /etc/passwd*. Нашел в нём свою учётную запись. Определил uid (1001) пользователя. Определите gid пользователя (1001). Что совпадает с информацией полученной выше:

```
[guest@arilinskiy ~]$ 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
```

Рис. 9: guest в etc/passwd (1/2)

```
dnsmasq:x:977:977:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
arilinskiy:x:1000:1000:arilinskiy:/home/arilinskiy:/bin/bash
guest:x:1001:1001::/home/guest:/bin/bash
```

Рис. 10: guest в etc/passwd (2/2)

9. Определил существующие в системе директории командой *ls -l /home/*:

```
[guest@arilinskiy ~]$ ls -l /home/
total 8
drwx------. 14 arilinskiy arilinskiy 4096 Sep  9 20:52 arilinskiy
drwx------. 14 guest      guest      4096 Sep 16 14:36 guest
```

Рис. 11: Существующие в системе директории

Как видно на рисунке , только пользователь, создавший директорию (*arilinskiy/guest*) имеет права на чтение (r), запись (w) и выполнение (x) файлов в директории. У остальных пользователей никаких прав нет.

10. Проверил, какие расширенные атрибуты установлены на поддиректориях, находящихся в директории /home, командой: *lsattr /home*:

```
[guest@arilinskiy ~]$ lsattr /home
lsattr: Permission denied While reading flags on /home/arilinskiy
---------------------- /home/guest
```

Рис. 12: Расширенные атрибуты

Мне не удалось увидеть расширенные атрибуты как текущей директории, так и директории другого пользователя.

11. Создал в домашней директории поддиректорию dir1 командой *mkdir dir1*:

```
[guest@arilinskiy ~]$ mkdir dir1
```

Рис. 13: Создание поддиректории

Определил командами *ls -l* и *lsattr*, какие права доступа и расширенные атрибуты были выставлены на директорию dir1:

Рис. 14: Права доступа к новому файлу

У всех есть права на чтение (r) и выполнение (x), но только у создателя и группы создателя есть права на запись (w). Расширенные атрибуты просмотреть не удалось.

12. Снял с директории dir1 все атрибуты командой *chmod 000 dir1* и проверил правильность выполнения с помощью команды *ls -l*:

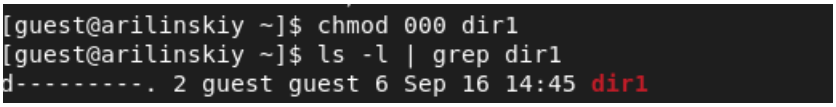

Рис. 15: Изменение атрибутов

13. Попытался создать в директории dir1 файл file1 командой *echo "test" > /home/guest/dir1/file1*:

Рис. 16: Запись в файл без прав (1/2)

Но получил отказ, так как в предыдущем пункте я забрал все права к директории dir1. Соответственно данный файл не был создан.

Попытался проверить это командой *ls -l /home/guest/dir1*, но также получил отказ из-за отсутствия прав:

```
[guest@arilinskiy ~]$ ls -l /home/guest/dir1
ls: cannot open directory '/home/guest/dir1': Permission denied
```

Рис. 17: Запись в файл без прав (2/2)

14. Заполнил таблицу «Установленные права и разрешённые действия»:

Права директории	Права файла	Создание файла	Удаление файла	Запись в файл	Чтение файла	Смена директории	Просмотр файлов в директории	Переимено-вание файла	Смена атрибутов файла
d--------- (000)	--------- (000)	-	-	-	-	-	-	-	-
d--x------ (100)	--------- (000)	-	-	-	-	+	-	-	+
d-w------- (200)	--------- (000)	-	-	-	-	-	-	-	-
d-wx------ (300)	--------- (000)	+	+	-	-	+	-	+	+
dr-------- (400)	--------- (000)	-	-	-	-	-	+	-	-
dr-x------ (500)	--------- (000)	-	-	-	-	+	+	-	+
drw------- (600)	--------- (000)	-	-	-	-	-	+	-	-
drwx------ (700)	--------- (000)	+	+	-	-	+	+	+	+
d--------- (000)	--x------ (100)	-	-	-	-	-	-	-	-
d--x------ (100)	--x------ (100)	-	-	-	-	+	-	-	+

Рис. 18: Установленные права и разрешённые действия (1/6)

(100)	(100)								
d-w------- (200)	--x------ (100)	-	-	-	-	-	-	-	-
d-wx------ (300)	--x------ (100)	+	+	-	-	+	-	+	+
dr-------- (400)	--x------ (100)	-	-	-	-	-	+	-	-
dr-x------ (500)	--x------ (100)	-	-	-	-	+	+	-	+
drw------- (600)	--x------ (100)	-	-	-	-	-	+	-	-
drwx------ (700)	--x------ (100)	+	+	-	-	+	+	+	+
d--------- (000)	-w------- (200)	-	-	-	-	-	-	-	-
d--x------ (100)	-w------- (200)	-	-	+	-	+	-	-	+
d-w------- (200)	-w------- (200)	-	-	-	-	-	-	-	-
d-wx------ (300)	-w------- (200)	+	+	+	-	+	-	+	+
dr-------- (400)	-w------- (200)	-	-	-	-	-	+	-	-

Рис. 19: Установленные права и разрешённые действия (2/6)

dr-x------ (500)	-w------- (200)	-	-	+	-	+	+	-	+
drw------- (600)	-w------- (200)	-	-	-	-	-	+	-	-
drwx------ (700)	-w------- (200)	+	+	+	-	+	+	+	+
d--------- (000)	-wx------ (300)	-	-	-	-	-	-	-	-
d--x------ (100)	-wx------ (300)	-	-	+	-	+	-	-	+
d-w------- (200)	-wx------ (300)	-	-	-	-	-	-	-	-
d-wx------ (300)	-wx------ (300)	+	+	+	-	+	-	+	+
dr-------- (400)	-wx------ (300)	-	-	-	-	-	+	-	-
dr-x------ (500)	-wx------ (300)	-	-	+	-	+	+	-	+
drw------- (600)	-wx------ (300)	-	-	-	-	-	+	-	-
drwx------ (700)	-wx------ (300)	+	+	+	-	+	+	+	+
d---------	r--------	-	-	-	-	-	-	-	-

Рис. 20: Установленные права и разрешённые действия (3/6)

(000)	(400)								
d--x------ (100)	r-------- (400)	-	-	-	+	+	-	-	+
d-w------- (200)	r-------- (400)	-	-	-	-	-	-	-	-
d-wx------ (300)	r-------- (400)	+	+	-	+	+	-	+	+
dr-------- (400)	r-------- (400)	-	-	-	-	-	+	-	-
dr-x------ (500)	r-------- (400)	-	-	-	+	+	+	-	+
drw------- (600)	r-------- (400)	-	-	-	-	-	+	-	-
drwx------ (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)	+	+	-	+	+	-	+	+

Рис. 21: Установленные права и разрешённые действия (4/6)

dr-------- (400)	r-x------ (500)	-	-	-	-	-	+	-	-
dr-x------ (500)	r-x------ (500)	-	-	-	+	+	+	-	+
drw------- (600)	r-x------ (500)	-	-	-	-	-	+	-	-
drwx------ (700)	r-x------ (500)	+	+	-	+	+	+	+	+
d--------- (000)	rw------- (600)	-	-	-	-	-	-	-	-
d--x------ (100)	rw------- (600)	-	-	+	+	+	-	-	+
d-w------- (200)	rw------- (600)	-	-	-	-	-	-	-	-
d-wx------ (300)	rw------- (600)	+	+	+	+	+	-	+	+
dr-------- (400)	rw------- (600)	-	-	-	-	-	+	-	-
dr-x------ (500)	rw------- (600)	-	-	+	+	+	+	-	+
drw------- (600)	rw------- (600)	-	-	-	-	-	+	-	-
drwx------	rw-------	+	+	+	+	+	+	+	+

Рис. 22: Установленные права и разрешённые действия (5/6)

(700)	(600)								
d--------- (000)	rwx------ (700)	-	-	-	-	-	-	-	-
d--x------ (100)	rwx------ (700)	-	-	+	+	+	-	-	+
d-w------- (200)	rwx------ (700)	-	-	-	-	-	-	-	-
d-wx------ (300)	rwx------ (700)	+	+	+	+	+	-	+	+
dr-------- (400)	rwx------ (700)	-	-	-	-	-	+	-	-
dr-x------ (500)	rwx------ (700)	-	-	+	+	+	+	-	+
drw------- (600)	rwx------ (700)	-	-	-	-	-	+	-	-
drwx------ (700)	rwx------ (700)	+	+	+	+	+	+	+	+

Рис. 23: Установленные права и разрешённые действия (6/6)

15. На основании заполненной таблицы определил минимально необходимые права для выполнения операций внутри директории dir1:

Операция	**Минимальные права на директорию**	**Минимальные права на файл**
Создание файла	d-wx------ (300)	--------- (000)
Удаление файла	d-wx------ (300)	--------- (000)
Чтение файла	d--x------ (100)	r-------- (400)
Запись в файл	d--x------ (100)	-w------- (200)
Переименование файла	d-wx------ (300)	--------- (000)
Создание поддиректории	d-wx------ (300)	--------- (000)
Удление поддиректории	d-wx------ (300)	--------- (000)

Рис. 24: Минимально необходимые права для выполнения операций внутри директории

Выводы

Благодаря данной лабораторной работы я приобрел практические навыки работы в консоли с атрибутами файлов, а также на практике закрепил теоретические основы дискреционного разграничения доступа в современных системах с открытым кодом на базе ОС Linux (дистрибутив - Rocky).

Список литературы

- Кулябов Д.С., Королькова А.В., Геворкян М.Н *Лабораторная работа №2*