

Лабораторная работа №2

Дискреционное разграничение прав в Linux. Основные атрибуты

Дугаева Светлана Анатольевна

Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	14

Список таблиц

0.1	Установленные права и разрешенные действия	10
0.2	Минимальные права для совершения операций	13

Список иллюстраций

0.1	Создание учетной записи	6
0.2	Задание пароля	6
0.3	Определение директории	6
0.4	Команда <code>whoami</code>	7
0.5	Команды <code>id</code> и <code>groups</code>	7
0.6	Просмотр файла <code>etc/passwd</code>	7
0.7	Директории	8
0.8	Проверка расширенных атрибутов	8
0.9	Создание поддиректории	8
0.10	Права доступа	8
0.11	Расширенные атрибуты	9
0.12	Снятие всех атрибутов	9
0.13	Попытка создания файла и просмотр содержимого директории	10

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.

Выполнение лабораторной работы

1. В установленной при выполнении предыдущей лабораторной работы операционной системе создала учётную запись пользователя guest(рис. @fig:001)

```
[SDugaeva@localhost ~]$ su
Пароль:
[root@localhost SDugaeva]# useradd guest
```

Рис. 0.1: Создание учетной записи

2. Задала пароль для пользователя guest (рис. @fig:002)

```
[root@localhost SDugaeva]# passwd guest
Смена пароля для пользователя guest.
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: основан на слове из словаря
Повторите ввод нового пароля :
passwd: все токены проверки подлинности успешно обновлены.
```

Рис. 0.2: Задание пароля

3. Вошла в систему от имени пользователя guest.
4. Определила директорию, в которой я нахожусь, командой pwd. Она является домашней (рис. @fig:003)

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

Рис. 0.3: Определение директории

5. Уточнила имя пользователя командой `whoami` (рис. @fig:004)

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

Рис. 0.4: Команда `whoami`

6. Уточнила имя пользователя, его группу, а также группы, куда входит пользователь, командой `id` (рис. @fig:005)

```
[guest@localhost ~]$ id
uid=501(guest) gid=501(guest) группы=501(guest) контекст=unconfined_u:unconfined
_r:unconfined_t:s0-s0:c0.c1023
[guest@localhost ~]$ groups
guest
```

Рис. 0.5: Команды `id` и `groups`

`uid=501`, `gid=501`. Команда `groups` выводит только название группы, в которой состоит данный пользователь, а команда `id` выводит еще и `id` пользователя и группы, а так же данные о группах, в которых он состоит.

7. Полученная информация об имени пользователя совпадает с данными, выводимыми в приглашении командной строки.
8. Посмотрю файл `etc/passwd` командой `cat /etc/passwd | grep guest` (рис. @fig:006)

```
[guest@localhost ~]$ cat /etc/passwd | grep guest
guest:x:501:501:./home/guest:/bin/bash
```

Рис. 0.6: Просмотр файла `etc/passwd`

`uid=501`, `gid=501`, эти значения совпадают с тем, что мы получили в пункте 6.

9. Определяю существующие директории (рис. @fig:007)

```
[guest@localhost ~]$ ls -l /home/
итого 8
drwx-----. 21 guest    guest    4096 0кб  2 13:44 guest
drwx-----. 22 SDugaeva SDugaeva 4096 0кб  2 12:50 SDugaeva
```

Рис. 0.7: Директории

Доступ был получен. У создателя директории есть права на чтение, выполнение и запись файлов в директории. У остальных пользователей (в том числе пользователей групп никаких прав нет.

10. Проверила какие расширенные атрибуты установлены на поддиректориях как текущего так и других пользователей (рис. @fig:008)

```
[guest@localhost ~]$ lsattr /home
-----e- /home/guest
lsattr: Отказано в доступе while reading flags on /home/SDugaeva
```

Рис. 0.8: Проверка расширенных атрибутов

Значит, мы можем использовать extent'ы блоков для хранения файла.

11. Создала в домашней директории поддиректорию dirl (рис. @fig:009)

```
[guest@localhost ~]$ mkdir dirl
```

Рис. 0.9: Создание поддиректории

Определила права доступа (рис. @fig:010)

```
[guest@localhost ~]$ ls -l
итого 36
drwxrwxr-x. 2 guest guest 4096 0кб  2 13:52 dirl
drwxr-xr-x. 2 guest guest 4096 0кб  2 13:44 Видео
drwxr-xr-x. 2 guest guest 4096 0кб  2 13:44 Документы
drwxr-xr-x. 2 guest guest 4096 0кб  2 13:44 Загрузки
drwxr-xr-x. 2 guest guest 4096 0кб  2 13:44 Картинки
drwxr-xr-x. 2 guest guest 4096 0кб  2 13:44 Музыка
drwxr-xr-x. 2 guest guest 4096 0кб  2 13:44 Общедоступные
drwxr-xr-x. 2 guest guest 4096 0кб  2 13:44 Рабочий стол
drwxr-xr-x. 2 guest guest 4096 0кб  2 13:44 Шаблоны
```

Рис. 0.10: Права доступа

У всех пользователей есть права на чтение и выполнение, но только у создателя есть права на запись.

Проверила расширенные атрибуты (рис. @fig:011)

```
[guest@localhost ~]$ lsattr
-----e- ./Загрузки
-----e- ./Рабочий стол
-----e- ./Видео
-----e- ./Картинки
-----e- ./Музыка
-----e- ./Шаблоны
-----e- ./Общедоступные
-----e- ./Документы
-----e- ./dirl
```

Рис. 0.11: Расширенные атрибуты

Аналогично предыдущему пункту.

12. Сняла с директории dirl все атрибуты и проверила правильность выполнения (рис. @fig:012)

```
[guest@localhost ~]$ ls -l
итого 36
d----- . 2 guest guest 4096 0кт 2 13:52 dirl
drwxr-xr-x. 2 guest guest 4096 0кт 2 13:44 Видео
drwxr-xr-x. 2 guest guest 4096 0кт 2 13:44 Документы
drwxr-xr-x. 2 guest guest 4096 0кт 2 13:44 Загрузки
drwxr-xr-x. 2 guest guest 4096 0кт 2 13:44 Картинки
drwxr-xr-x. 2 guest guest 4096 0кт 2 13:44 Музыка
drwxr-xr-x. 2 guest guest 4096 0кт 2 13:44 Общедоступные
drwxr-xr-x. 2 guest guest 4096 0кт 2 13:44 Рабочий стол
drwxr-xr-x. 2 guest guest 4096 0кт 2 13:44 Шаблоны
```

Рис. 0.12: Снятие всех атрибутов

13. Создать файл в директории не удалось. Отказ в доступе был получен потому, что мы сняли все атрибуты с директории dirl. Файл не был создан. Просмотреть содержимое директории также не удалось в связи с той же причиной (рис. @fig:013)

```
[guest@localhost ~]$ echo "test" > /home/guest/dirl/file1
bash: /home/guest/dirl/file1: Отказано в доступе
[guest@localhost ~]$ ls -l /home/guest/dirl
ls: невозможно открыть каталог /home/guest/dirl: Отказано в доступе
```

Рис. 0.13: Попытка создания файла и просмотр содержимого директории

14. Заполнила таблицу “Установленные права и разрешенные действия”. Все данные были определены опытным путем (присутствует в записи выполнения). Если операция разрешена - в таблице стоит “+”, если операция не разрешена - в таблице стоит “-” (таб. 1)

Таблица 0.1: Установленные права и разрешенные действия

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переименование файла	Смена атрибу- тов 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)	-	-	-	+	+	-	-	+

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переимено- вание файла	Смена атрибу- тов файла
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)	-	-	-	-	-	+	-	-

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переимено- вание файла	Смена атрибу- тов файла
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)	+	+	+	+	+	+	+	+

Права дирек- тории	Права фай- ла	Создание фай- ла	Удаление фай- ла	Запись в файл	Чтение фай- ла	Смена дирек- тории	Просмотр файлов в директо- рии	Переимено- вание файла	Смена атрибу- тов файла
d(700)	(700)	+	+	+	+	+	+	+	+

15. На основании заполненной таблицы 1 определила те или иные минимально необходимые права для выполнения операций внутри директории dir1. Заполнила таблицу “Минимальные права для совершения операций” (таб. 2)

Таблица 0.2: Минимальные права для совершения операций

Операция	min права на директорию	min 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)
Удаление поддиректории	(d-wx—)(300)	(— — —)(000)

Выводы

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