

Отчёт по лабораторной работе 3

Соболев Максим Сергеевич

Содержание

1	Дискреционное разграничение прав в Linux. Расширенные атрибуты	4
2	Цель работы	5
3	Задание	6
4	Теоретическое введение	7
5	Выполнение лабораторной работы	8
5.1	Шаг 1	8
5.2	Шаг 2	8
5.3	Шаг 3	8
5.4	Шаг 4	9
5.5	Шаг 5	9
5.6	Шаг 6	9
5.7	Шаг 7	10
5.8	Шаг 8	10
5.9	Шаг 9	10
5.10	Шаг 10	11
	Список литературы	12

Список иллюстраций

5.1	1	8
5.2	2	8
5.3	3	9
5.4	4	9
5.5	5	9
5.6	6	9
5.7	7	10
5.8	8	10
5.9	91	10
5.10	91	11

1 Дискреционное разграничение прав в Linux. Расширенные атрибуты

2 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов

3 Задание

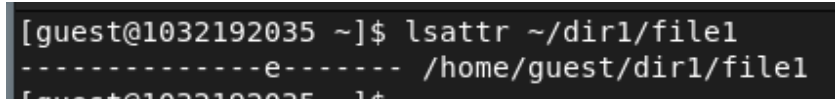
Научиться работать в консоли с с расширенными атрибутами файлов

4 Теоретическое введение

5 Выполнение лабораторной работы

5.1 Шаг 1

От имени пользователя guest определяем расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /home/guest/dir1/file1

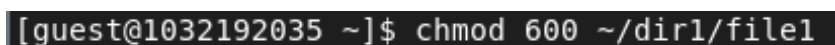


```
[guest@1032192035 ~]$ lsattr ~/dir1/file1
-----e----- /home/guest/dir1/file1
[guest@1032192035 ~]$
```

Рис. 5.1: 1

5.2 Шаг 2

Устанавливаем командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла



```
[guest@1032192035 ~]$ chmod 600 ~/dir1/file1
```

Рис. 5.2: 2

5.3 Шаг 3

Устанавливаем на файл /home/guest/dir1/file1 расширенный атрибут а от имени пользователя guest: chattr +a /home/guest/dir1/file1 В ответ получаем отказ в выполнении операции.


```
[guest@1032192035 ~]$ chattr +a ~/dir1/file1  
chattr: Operation not permitted while setting flags on /home/guest/dir1/file1
```

Рис. 5.3: 3

5.4 Шаг 4

Заходим в другую консоль с правами администратора. Устанавливаем расширенный атрибут `a` на файл `/home/guest/dir1/file1` от имени суперпользователя:
`chattr +a /home/guest/dir1/file1`

```
[root@1032192035 1032192035_pfur.ru]# chattr +a /home/guest/dir1/file1
```

Рис. 5.4: 4

5.5 Шаг 5

От пользователя `guest` проверяем правильность установления атрибута: `lsattr /home/guest/dir1/file1`

```
[guest@1032192035 ~]$ lsattr ~/dir1/file1  
-----a-----e----- /home/guest/dir1/file1
```

Рис. 5.5: 5

5.6 Шаг 6

Выполняем дозапись в файл `file1` слова «test» командой `echo "test" >> /home/guest/dir1/file1`. После этого выполняем чтение файла `file1` командой `cat /home/guest/dir1/file1`. Убеждаемся, что слово `test` было успешно записано в `file1`.

```
[guest@1032192035 ~]$ echo "test" >> ~/dir1/file1  
[guest@1032192035 ~]$ cat ~/dir1/file1  
test
```

Рис. 5.6: 6

5.7 Шаг 7

Пробуем стереть имеющуюся в нём информацию командой `echo "abcd" > /home/guest/dirl/file1`. Пробуем переименовать файл. Получаем отказ в выполнении операции.

```
[guest@1032192035 ~]$ echo "abcd" > ~/dir1/file1
bash: /home/guest/dirl/file1: Operation not permitted
```

Рис. 5.7: 7

5.8 Шаг 8

Пробуем с помощью команды `chmod 000 file1` установить на файл `file1` права, например, запрещающие чтение и запись для владельца файла. Удалось ли вам успешно выполнить указанные команды?

```
[guest@1032192035 ~]$ mv ~/dir1/file1 ~/dir1/file2
mv: cannot move '/home/guest/dirl/file1' to '/home/guest/dirl/file2': Operation
not permitted
```

Рис. 5.8: 8

5.9 Шаг 9

Снимаем расширенный атрибут `a` с файла `/home/guest/dirl/file1` от имени суперпользователя командой `chattr -a /home/guest/dirl/file1`. Повторяем операции, которые нам ранее не удавалось выполнить.

```
[root@1032192035 1032192035_pfur.ru]# chattr -a /home/guest/dirl/file1
```

Рис. 5.9: 91

```
[guest@1032192035 ~]$ echo "abcd" > ~/dir1/file1
[guest@1032192035 ~]$ cat ~/dir1/file1
abcd
[guest@1032192035 ~]$ mv ~/dir1/file1 ~/dir1/file2
[guest@1032192035 ~]$ chmod 000 ~/dir1/file2
```

Рис. 5.10: 91

5.10 Шаг 10

Повторяем аналогичные действия по шагам, заменив атрибут «а» атрибутом «i». Таким образом получаем следующее: файл с атрибутом “а” может быть только дополнен, файл с атрибутом “i” не подлежит никаким изменениям вовсе.

```
[guest@1032192035 ~]$ lsattr ~/dir1/file1
----i-----e----- /home/guest/dir1/file1
[guest@1032192035 ~]$ echo "test" ~/dir1/file1
test /home/guest/dir1/file1
[guest@1032192035 ~]$ echo "test" >> ~/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[guest@1032192035 ~]$ echo "test" > ~/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[guest@1032192035 ~]$ cat ~/dir1/file1
[guest@1032192035 ~]$ chmod 000 ~/dir1/file1
chmod: changing permissions of '/home/guest/dir1/file1': Operation not permitted
[guest@1032192035 ~]$ mv ~/dir1/file1 ~/dir1/file2
mv: cannot move '/home/guest/dir1/file1' to '/home/guest/dir1/file2': Operation not permitted
```

Выводы

В результате выполнения мы повысили навыки использования интерфейса командой строки, познакомились на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имели возможность связать теорию дискреционного разделения доступа с её реализацией на практике в ОС Linux. Составили наглядные таблицы, поясняющие какие операции возможны при тех или иных установленных правах. Опробовали действие на практике расширенных атрибутов «а» и «i».

Список литературы

1. xattr(7) — Linux manual page // Linux man-pages project URL: <https://man7.org/linux/man-pages/man7/xattr.7.html> (дата обращения: 30.09.2022).