

Отчёт по лабораторной работе

Лабораторная работа №_04 / Дискреционное разграничение прав в
Linux. Расширенные атрибуты

Габриэль Тьерри

Содержание

Цель работы	5
Выполнение лабораторной работы	6
Выводы	9

Список таблиц

Список иллюстраций

1	изображение 001	6
2	изображение 002	7
3	изображение 003	7
4	изображение 004	8

Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

Выполнение лабораторной работы

1. От имени пользователя `guest` определите расширенные атрибуты файла `/home/guest/dir1/file1` командой `lsattr /home/guest/dir1/file1`. (изображение 001)
2. Установите командой `chmod 600 file1` на файл `file1` права, разрешающие чтение и запись для владельца файла. (изображение 001)
3. Попробуйте установить на файл `/home/guest/dir1/file1` расширенный атрибут `a` от имени пользователя `guest`: `chattr +a /home/guest/dir1/file1`. (изображение 001)

```
[guest2@tgabriel ~]$ lsattr /home/guest2/dir1/file1
----- /home/guest2/dir1/file1
[guest2@tgabriel ~]$ chmod 600 /home/guest2/dir1/file1
[guest2@tgabriel ~]$ chattr +a /home/guest2/dir1/file1
chattr: Operation not permitted while setting flags on /home/guest2/dir1/file1
```

Рис. 1: изображение 001

4. Зайдите на третью консоль с правами администратора либо повысьте свои права с помощью команды `su`. Попробуйте установить расширенный атрибут `a` на файл `/home/guest/dir1/file1` от имени суперпользователя: `chattr +a /home/guest/dir1/file1`. (изображение 002)
5. От пользователя `guest` проверьте правильность установления атрибута: `lsattr /home/guest/dir1/file1`. (изображение 002)

6. Выполните дозапись в файл file1 слова «test» командой `echo "test" /home/guest/dir1/file1`. (изображение 002) После этого выполните чтение файла file1 командой `cat /home/guest/dir1/file1` Убедитесь, что слово test было успешно записано в file1. (изображение 002)

```
[guest2@tgabriel ~]$ su
Password:
[root@tgabriel guest2]# chattr +a /home/guest2/dir1/file1
[root@tgabriel guest2]# exit
exit
[guest2@tgabriel ~]$ lsattr /home/guest2/dir1/file1
-----a----- /home/guest2/dir1/file1
[guest2@tgabriel ~]$ echo "test" /home/guest2/dir1/file1
test /home/guest2/dir1/file1
[guest2@tgabriel ~]$ cat /home/guest2/dir1/file1
[guest2@tgabriel ~]$ echo "test" >> /home/guest2/dir1/file1
[guest2@tgabriel ~]$ cat /home/guest2/dir1/file1
test
```

Рис. 2: изображение 002

7. Попробуйте удалить файл file1 либо стереть имеющуюся в нём информацию командой `echo "abcd" > /home/guest/dir1/file1` Попробуйте переименовать файл. (изображение 003)
8. Попробуйте 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? (изображение 003)

```
[guest2@tgabriel ~]$ echo "abcd" > /home/guest2/dir1/file1
-bash: /home/guest2/dir1/file1: Operation not permitted
[guest2@tgabriel ~]$ mv /home/guest2/dir1/file1 file10
mv: cannot move '/home/guest2/dir1/file1' to 'file10': Operation not permitted
[guest2@tgabriel ~]$ chmod 000 /home/guest2/dir1/file1
chmod: changing permissions of '/home/guest2/dir1/file1': Operation not permitted
```

Рис. 3: изображение 003

9. Снимите расширенный атрибут a с файла /home/guest/dir1/file1 от имени суперпользователя командой `chattr -a /home/guest/dir1/file1` Повторите операции, которые вам ранее не удавалось выполнить. Ваши наблюдения занесите в отчёт. (изображение 004)

10. . Повторите ваши действия по шагам, заменив атрибут «а» атрибутом «і».

Удалось ли вам дозаписать информацию в файл?

- Нет, не удалось

В результате выполнения работы вы повысили свои навыки использования интерфейса командой строки (CLI), познакомились на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имели возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) 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 «і». (изображение 004)

```
[guest2@tgabriel ~]$ su
MPassword:
[root@tgabriel guest2]# chattr -a /home/guest2/dir1/file1
[root@tgabriel guest2]# exit
exit
[guest2@tgabriel ~]$ chmod 000 /home/guest2/dir1/file1
[guest2@tgabriel ~]$ chattr +I /home/guest2/dir1/file1
Usage: chattr [-pRVf] [--+=aAcCdDeijPsStTuFhX] [-v version] files...
[guest2@tgabriel ~]$ chattr +i /home/guest2/dir1/file1
chattr: Permission denied while reading flags on /home/guest2/dir1/file1
[guest2@tgabriel ~]$ lsattr /home/guest2/dir1/file1
lsattr: Permission denied while reading flags on /home/guest2/dir1/file1
[guest2@tgabriel ~]$ cat /home/guest2/dir1/file1
cat: /home/guest2/dir1/file1: Permission denied
[guest2@tgabriel ~]$ echo "test" >> /home/guest2/dir1/file1
-bash: /home/guest2/dir1/file1: Permission denied
[guest2@tgabriel ~]$
```

Рис. 4: изображение 004

Выводы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.