

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Назарьева Алена НФИбд-03-18

2021, 24 october

inst{1}RUDN University, Moscow, Russian Federation

Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов

Выполнение лабораторной работы

От имени пользователя guest определила расширенные атрибуты файла /home/guest/dir1/file1. Установила командой `chmod 600 file1` на файл `file1` права, разрешающие чтение и запись для владельца файла. Попробовала установить на файл /home/guest/dir1/file1 расширенный атрибут а от имени пользователя guest: В ответ получила отказ от выполнения операции. (рис. -fig. 1)

```
[guest@ainazarieva ~]$ lsattr /home/guest/dirl/file1
..... /home/guest/dirl/file1
[guest@ainazarieva ~]$ chmod 600 file1
[guest@ainazarieva ~]$ chmod 600 /home/guest/dirl/file1
[guest@ainazarieva ~]$ chattr +a /home/guest/dirl/file1
chattr: Операция не позволена while setting flags on /home/guest/dirl/file1
[guest@ainazarieva ~]$
```

Figure 1: пункты 1-3

Повысила свои права с помощью команды `su`. Попробовала установить расширенный атрибут `a` на файл `/home/guest/dir1/file1` от имени суперпользователя: (рис. -fig. 2)

```
[guest@ainazarieva ~]$ su
Пароль:
[root@ainazarieva guest]# chattr +a /home/guest/dir1/file1
[root@ainazarieva guest]# █
```

Figure 2: пункты 4

От пользователя guest проверила правильность
установления атрибута: (рис. -fig. 3)

```
[guest@ainazarieva ~]$ ll /home/guest/dirl/file2  
-rw-----. 1 guest guest 0 окт 24 11:55 /home/guest/dirl/file2
```

Figure 3: пункты 5

Выполнила дозапись в файл file1 слова «test». После этого выполнила чтение файла file1. Убедилась, что слово test было успешно записано в file1. Попробовала удалить файл file1 и стереть имеющуюся в нём информацию. Попробовала переименовать файл. (рис. -fig. 4)

```
[guest@ainazarieva ~]$ touch /home/guest/dirl/file2
[guest@ainazarieva ~]$ echo "abcd" > /home/guest/dirl/file2
[guest@ainazarieva ~]$ cat /home/guest/dirl/file2
abcd
[guest@ainazarieva ~]$ rm /home/guest/dirl/file2
[guest@ainazarieva ~]$ ll /home/guest/dirl
итого 0
----- 1 guest guest 0 окт 24 11:35 file1
[guest@ainazarieva ~]$ mv /home/guest/dirl/file2 /home/guest/dirl/file1
mv: не удалось выполнить stat для «/home/guest/dirl/file2»: Нет такого файла или каталога
[guest@ainazarieva ~]$ mv /home/guest/dirl/file1 /home/guest/dirl/file2
mv: невозможно переместить «/home/guest/dirl/file1» в «/home/guest/dirl/file2»: Операция не позволена
```

Figure 4: пункты 6-7

Попробовала установить на файл file1 права, запрещающие чтение и запись для владельца файла. (рис. -fig. 5)

```
[guest@ainazarieva ~]$ touch /home/guest/dirl/file2
[guest@ainazarieva ~]$ echo "abcd" > /home/guest/dirl/file2
[guest@ainazarieva ~]$ cat /home/guest/dirl/file2
abcd
[guest@ainazarieva ~]$ rm /home/guest/dirl/file2
[guest@ainazarieva ~]$ ll /home/guest/dirl
итого 0
-----. 1 guest guest 0 окт 24 11:35 file1
[guest@ainazarieva ~]$ mv /home/guest/dirl/file2 /home/guest/dirl/file1
mv: не удалось выполнить stat для «/home/guest/dirl/file2»: Нет такого файла или каталога
[guest@ainazarieva ~]$ mv /home/guest/dirl/file1 /home/guest/dirl/file2
mv: невозможно переместить «/home/guest/dirl/file1» в «/home/guest/dirl/file2»: Операция не позволена
```

Figure 5: пункты 8

Сняла расширенный атрибут а с файла /home/guest/dirl/file1 от имени суперпользователя Повторила операции, которые ранее не удавалось выполнить: (рис. -fig. 6)

```
[guest@ainazarieva ~]$ echo "test" > /home/guest/dirl/file1
[guest@ainazarieva ~]$ cat /home/guest/dirl/file1
test
[guest@ainazarieva ~]$ echo "abcd" > /home/guest/dirl/file1
[guest@ainazarieva ~]$ cat /home/guest/dirl/file1
abcd
[guest@ainazarieva ~]$ rm /home/guest/dirl/file1
[guest@ainazarieva ~]$ ls -l /home/guest/dirl
итого 0
[guest@ainazarieva ~]$ touch /home/guest/dirl/file1
[guest@ainazarieva ~]$ ls -l /home/guest/dirl
итого 0
-rw-rw-r--. 1 guest guest 0 окт 24 11:35 file1
[guest@ainazarieva ~]$ chmod 600 /home/guest/dirl/file2
chmod: невозможно получить доступ к «/home/guest/dirl/file2»: Нет такого файла или каталога
[guest@ainazarieva ~]$ chmod 600 /home/guest/dirl/file1
[guest@ainazarieva ~]$ mv /home/guest/dirl/file1 /home/guest/dirl/file2
[guest@ainazarieva ~]$ ls -l /home/guest/dirl
итого 0
-rw-----. 1 guest guest 0 окт 24 11:35 file2
```

Figure 6: пункт 9-600

(рис. -fig. 7)

```
[guest@ainazarieva ~]$ chmod 000 /home/guest/dirl/file2
[guest@ainazarieva ~]$ echo "abcd" > /home/guest/dirl/file2
bash: /home/guest/dirl/file2: Отказано в доступе
[guest@ainazarieva ~]$ mv /home/guest/dirl/file2 /home/guest/dirl/file1
[guest@ainazarieva ~]$ ls -l /home/guest/dirl
итого 0
----- 1 guest guest 0 окт 24 11:35 file1
[guest@ainazarieva ~]$ touch /home/guest/dirl/file2
[guest@ainazarieva ~]$ rm /home/guest/dirl/file2
[guest@ainazarieva ~]$ ls -l /home/guest/dirl
итого 0
----- 1 guest guest 0 окт 24 11:35 file1
[guest@ainazarieva ~]$ █
```

Figure 7: пункт 9-000

Повторила ваши действия по шагам, заменив атрибут «a» атрибутом «i». (рис. -fig. 8)

```
[guest@ainazarieva ~]$ su
Пароль:
[root@ainazarieva guest]# chattr -a /home/guest/dirl/file1
[root@ainazarieva guest]# chattr +i /home/guest/dirl/file1
[root@ainazarieva guest]# █
```

Figure 8: пункт 10

(рис. -fig. 9)

```
[guest@ainazarieva ~]$ ll /home/guest/dirl/file1
----- 1 guest guest 0 окт 24 11:49 /home/guest/dirl/file1
[guest@ainazarieva ~]$ touch /home/guest/dirl/file2
[guest@ainazarieva ~]$ echo "test" /home/guest/dirl/file1
test /home/guest/dirl/file1
[guest@ainazarieva ~]$ echo "test" > /home/guest/dirl/file1
bash: /home/guest/dirl/file1: Отказано в доступе
\[guest@ainazarieva ~]$ rm /home/guest/dirl/file1
rm: удалить защищенный от записи пустой обычный файл «/home/guest/dirl/file1»?
[guest@ainazarieva ~]$
```

Figure 9: пункт 10-000

(рис. -fig. 10)

```

[guest@ainazarieva ~]$ chmod 600 /home/guest/dirl/file1
chmod: изменение прав доступа для «/home/guest/dirl/file1»: Операция не позволена
[guest@ainazarieva ~]$ chmod 600 /home/guest/dirl/file2
[guest@ainazarieva ~]$ ll /home/guest/dirl/file2
-rw-----. 1 guest guest 0 окт 24 11:55 /home/guest/dirl/file2
[guest@ainazarieva ~]$ echo "test" > /home/guest/dirl/file2
[guest@ainazarieva ~]$ cat /home/guest/dirl/file2
test
[guest@ainazarieva ~]$ echo "abcd" > /home/guest/dirl/file2
[guest@ainazarieva ~]$ cat /home/guest/dirl/file2
abcd
[guest@ainazarieva ~]$ mv /home/guest/dirl/file2 /home/guest/dirl/file1
mv: попытаться перезаписать «/home/guest/dirl/file1», несмотря на права доступа 0000 (-
-----)? █

```

Figure 10: пункт 10-600

Мои наблюдения: Если установлен атрибут “a”, файл может быть открыт для записи только в режиме добавления текста. Если установлен атрибут “i”, файл нельзя модифицировать. Это значит нельзя переименовывать, создавать символьные ссылки, исполнять и записывать, снять этот атрибут может только суперпользователь.

Выводы

В результате выполнения работы я повысила свои навыки использования интерфейса командой строки (CLI), познакомилась на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имела возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux. Составила наглядные таблицы, поясняющие какие операции возможны при тех или иных установленных правах. Опробовала действие на практике раёсширенных атрибутов «a» и «i».