# Презентация по выполнению лабораторной работы №4

## Основы информационной безопасности

Паращенко А.Д.

23 сентября 2024

Российский университет дружбы народов, Москва, Россия

# Цель работы

# Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

# Выполнение лабораторной работы

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


**Рис. 1:** 1

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


**Рис. 2:** 2

Пробуем установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest: ***chattr +a /home/guest/dir1/file1*** В ответ получили отказ от выполнения операции


**Рис. 3:** 3

Заходим на вторую консоль и повышаем свои права с помощью команды ***sudo***.

Установливаем расширенный атрибут ***a*** на файл /home/guest/dir1/file1 от имени суперпользователя: ***chattr +a /home/guest/dir1/file1***

```
[adparathenko@adparathenko ~]$ sudo chattr +a /home/quest/dir1/file1
[sudo] password for adparathenko:
[adparathenko@adparathenko ~]$
```

Рис. 4: 4

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

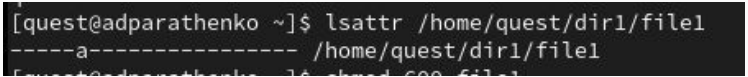


Рис. 5: 5

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*** Убедимся, что слово test было успешно записано в file1.

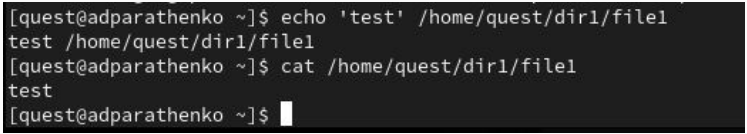


**Рис. 6:** 6

Попробуйте удалить файл file1 либо стереть имеющуюся в нём информацию командой *echo “abcd” > /home/guest/dirl/file1* Пробуем переименовать файл

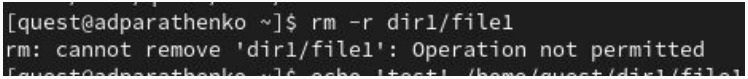


Рис. 7: 7


Рис. 8: 8

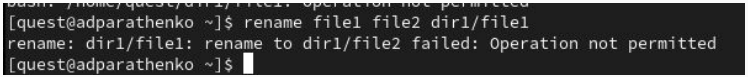


Рис. 9: 9

Пробуем с помощью команды ***chmod 000 file1*** установить на файл file1 права, запрещающие чтение и запись для владельца файла. **Не удалось выполнить указанные команды.**

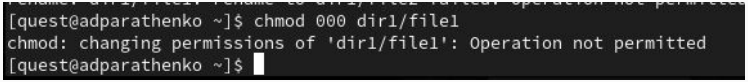


**Рис. 10:** 10

Снимаем расширенный атрибут **a** с файла /home/guest/dirl/file1 от имени суперпользователя командой *sudo chattr -a /home/guest/dir1/file1*


**Рис. 11:** 11

И повторяем операции, которые ранее не удавалось выполнить. **Теперь мы можем выполнить операции.**

Повторяем наши действия по шагам, заменив атрибут «a» атрибутом «i». командой *sudo chattr +i /home/guest/dir1/file1*

```
[adparathenko@adparathenko ~]$ sudo chattr +i /home/quest/dir1/file
[adparathenko@adparathenko ~]$
[quest@adparathenko ~]$ chmod 600 dir1/file
[quest@adparathenko ~]$ lsattr /home/quest/dir1/file
----i---------------- /home/quest/dir1/file
[quest@adparathenko ~]$
```

Рис. 13: 14

```
[quest@adparathenko ~]$ echo 'test' dir1/file
test dir1/file
[quest@adparathenko ~]$ cat /home/quest/dir1/file
cat: /home/quest/dir1/file: Permission denied
[quest@adparathenko ~]$ rm -r dir1/file
rm: cannot remove 'dir1/file': Operation not permitted
[quest@adparathenko ~]$ echo 'abcd' > dir1/file
bash: dir1/file: Operation not permitted
[quest@adparathenko ~]$ rename file file1 dir1/file
rename: dir1/file: rename to dir1/file1 failed: Operation not permitted
[quest@adparathenko ~]$ chmod 000 file
chmod: cannot access 'file': No such file or directory
```

# Вывод

# Вывод

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. Опробовала действие на практике расширенных атрибутов «a» и «i».

::: # Список литературы{.unnumbered} 1) https://esystem.rudn.ru/pluginfile.php/2357151/mod_resource/content/3/004-lab_discret_extattr.pdf