Лабораторная работа № 4

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Казакова Виктория Алексеевна

Содержание

# 1 Цель работы

## 1.1 # Получение практических навыков работы в консоли с расширенными атрибутами файлов.

1. От имени пользователя guest определила расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /home/guest/dir1/file1. (рис. [1](#fig:001))

Figure 1: Определение расширенных атрибутов

Figure 1: Определение расширенных атрибутов

1. Установила командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла. (рис. [2](#fig:002))

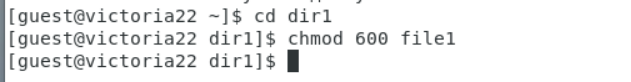


Figure 2: Установка прав

1. Попробовала установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest: chattr +a /home/guest/dir1/file1 В ответ получила отказ от выполнения операции.(рис. [3](#fig:003))

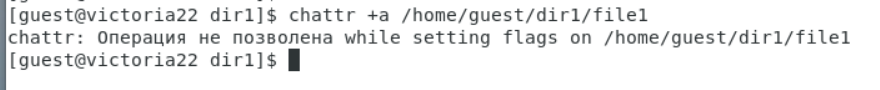


Figure 3: Попытка установки расширенного атрибута

1. Повысила свои права с помощью команды su. Установила расширенный атрибут a на файл /home/guest/dir1/file1 от имени суперпользователя:(рис. [4](#fig:004))

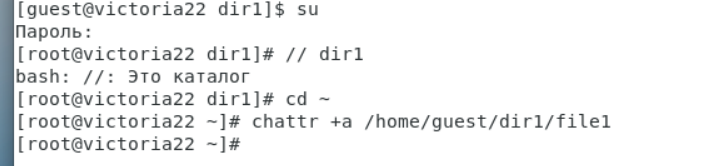


Figure 4: Использование команды su. Установка расширенного атрибута

1. От пользователя guest проверила правильность установления атрибута. (рис. [5](#fig:005))

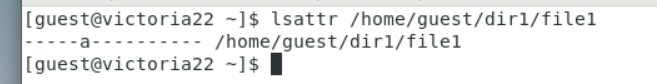


Figure 5: Проверка установленного атрибута

1. Выполнила дозапись в файл file1 слова «test» командой echo “test” /home/guest/dir1/file1 (рис. [6](#fig:006)). После этого выполнила чтение файла file1 командой cat /home/guest/dir1/file1 (рис. [7](#fig:007)). Убедилась, что слово test было успешно записано в file1 (рис. [8](#fig:008)).

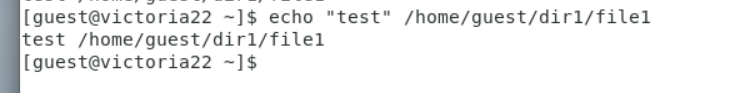


Figure 6: Дозапись файла

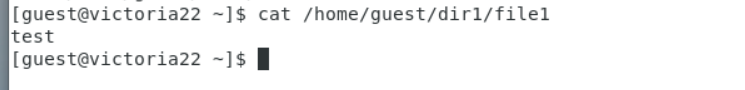


Figure 7: Чтение файла

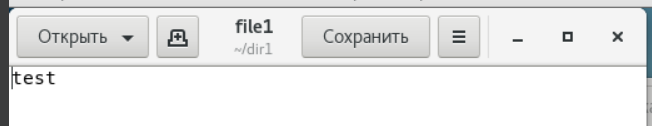


Figure 8: Проверка записи слова test

1. Попробовала удалить файл file1 командой rm (рис. [9](#fig:010)). Попробовала стереть имеющуюся в нём информацию командой echo “abcd” > /home/guest/dirl/file1 (рис. [10](#fig:009)). Попробовала переименовать файл командой mv (рис. [11](#fig:011)).

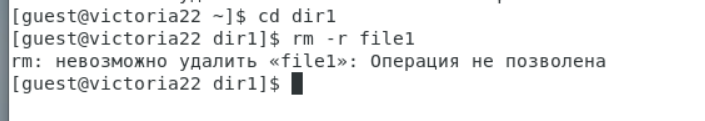


Figure 9: Попытка стереть содержимое файла

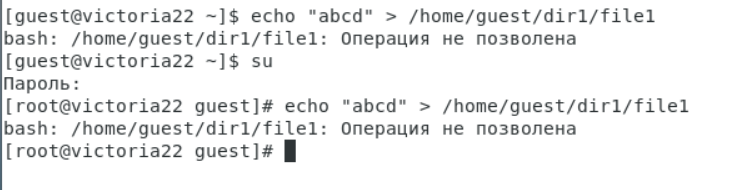


Figure 10: Попытка удаления файла

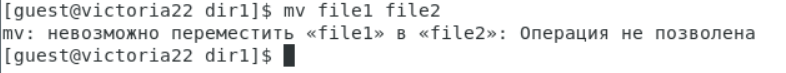


Figure 11: Попытка переименовать файл

1. Попробовала командой chmod 000 file1 установить на файл file1 права, например, запрещающие чтение и запись для владельца файла (рис. [12](#fig:012)). Указанные команды выполнить не удалось.

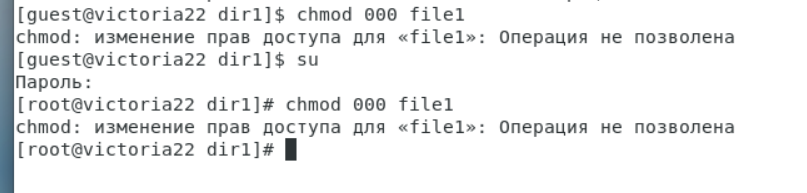


Figure 12: Применение команды chmod

1. Сняла расширенный атрибут a с файла /home/guest/dirl/file1 от имени суперпользователя командой. Повторила операции, которые ранее не удавалось выполнить (рис. [13](#fig:014)). Мои наблюдения: все операции получилось выполнить (кроме переименования) (рис. [14](#fig:013)).



Figure 13: Снятие расширенного атрибуты. Применение операций

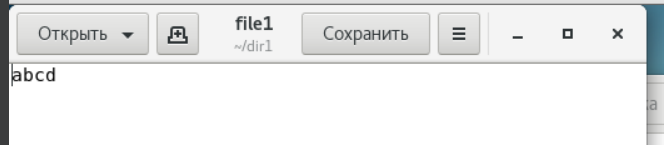


Figure 14: Содержимое файла

1. Повторила действия по шагам, заменив атрибут «a» атрибутом «i» (рис. [15](#fig:015)). Применила операцию дозаписи, преименования и удаления (рис. [16](#fig:016)).

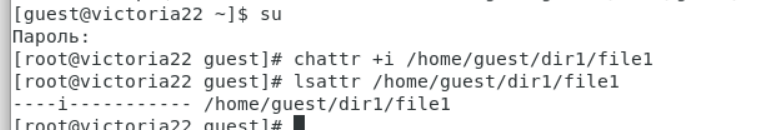


Figure 15: Установка нового расширенного атрибута

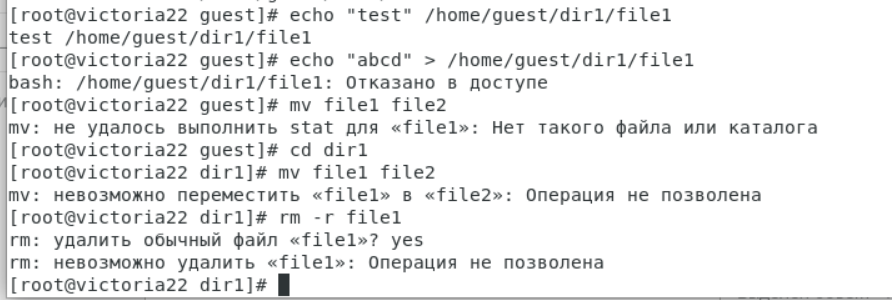


Figure 16: Применение операций

# 2 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. Имели возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux.

# 3 Библиография

1. [Методический материал] [https://esystem.rudn.ru/pluginfile.php/2090275/mod\_resource/content/4/003-lab\_discret\_2users.pdf]
2. [Методический материал] [https://esystem.rudn.ru/pluginfile.php/2090277/mod\_resource/content/3/004-lab\_discret\_extattr.pdf]