Отчет по лабораторной работе №4

Информационная безопасность

Чекалова Лилия Руслановна

Содержание

# 1 Цель работы

* Приобретение практических навыков работы в консоли с расширенными атрибутами файлов.

# 2 Задание

* Установка расширенных атрибутов на файл
* Проверка доступных действий
* Снятие расширенных атрибутов

# 3 Теоретическое введение

Существует несколько видов расширенных атрибутов:

* a: файл с установленным атрибутом «a» можно открыть только в режиме добавления для записи. Только суперпользователь или процесс, обладающий возможностью CAP\_LINUX\_IMMUTABLE, может установить или очистить этот атрибут.
* i: Файл с атрибутом «i» не может быть изменён: его нельзя удалить или переименовать, нельзя создать ссылку на этот файл, большую часть метаданных файла нельзя изменить, и файл нельзя открыть в режиме записи. Только суперпользователь или процесс, обладающий возможностью CAP\_LINUX\_IMMUTABLE, может установить или очистить этот атрибут.
* c: файл с установленным атрибутом «c» автоматически сжимается на диске ядром. При чтении из этого файла возвращаются несжатые данные. Запись в этот файл сжимает данные перед их сохранением на диске.
* и другие.

Более подробно о см. в [1,2].

# 4 Выполнение лабораторной работы

В качестве первого шага лабораторной работы мы осуществили вход от лица пользователя guest и проверили расширенные атрибуты файла file1 с помощью команды lsattr (рис. [1](#fig:001)).

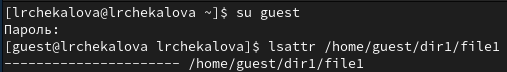


Figure 1: Проверка атрибутов

Далее мы с помощью команды chmod установили права на запись и чтение для владельца файла и попробовали поменять расширенные атрибуты файла командой chattr (рис. [2](#fig:002)). Нам было отказано в изменении атрибута.

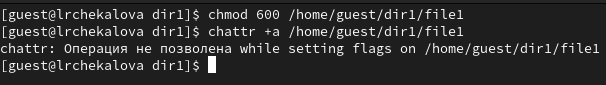


Figure 2: Изменение прав и атрибутов

Установили файлу атрибут «a» от имени суперпользователя и проверили успешность изменения атрибутов с помощью lsattr (рис. [3](#fig:003)).

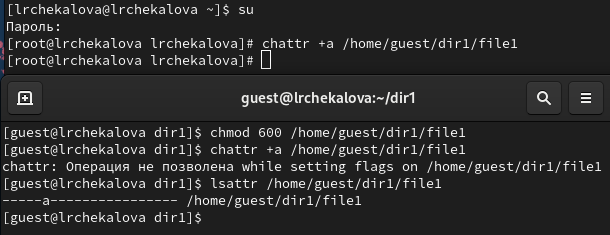


Figure 3: Добавление атрибута a

Выполнили дозапись в файл командой echo и проверили содержимое файла командой cat (рис. [4](#fig:004)).

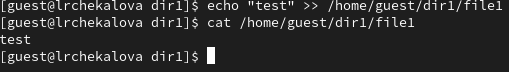


Figure 4: Дозапись в файл

Попробовали удалить файл, заменить находящуюся в нем информацию, поменять права и переименовать файл (рис. [5](#fig:005)). Ни одна из операций не была успешной.

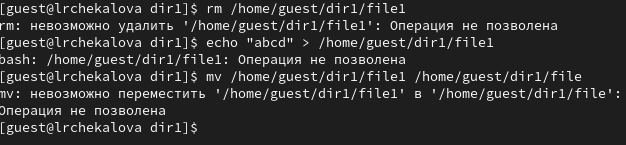


Figure 5: Операции над файлом

Сняли атрибут «a» от лица суперпользователя (рис. [6](#fig:006)).

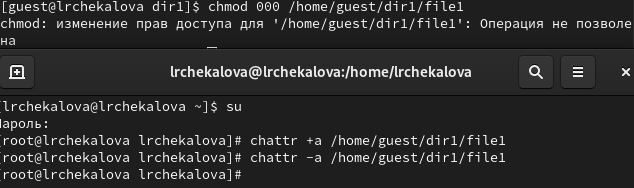


Figure 6: Снятие атрибута «a»

Повторили указанные ранее действия (рис. [7](#fig:007)). На этот раз они выполнились успешно.

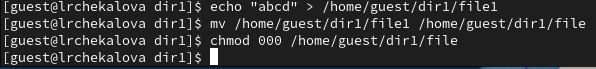


Figure 7: Повтор операций над файлом

Заменили атрибут «a» на атрибут «i» и повторили операции над файлом (рис. [8](#fig:008)). Ни одна из операций, включая дозапись в файл, не была выполнена.

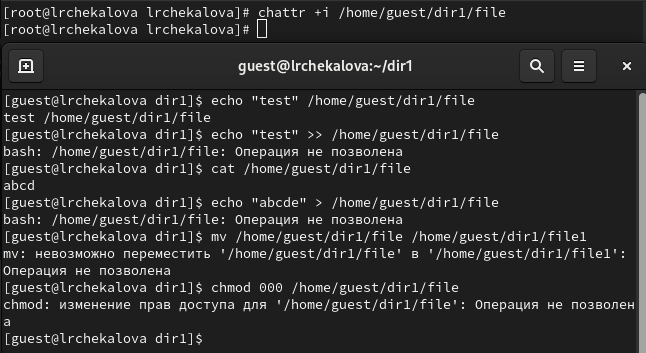


Figure 8: Операции над файлом с атрибутом «i»

Сняли с файла атрибут «i» и повторили действия (рис. [9](#fig:009)). Все операции были завершены успешно.

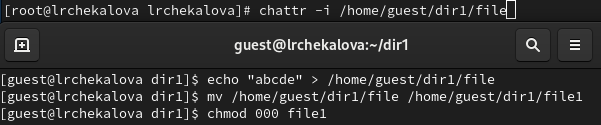


Figure 9: Операции над файлом со снятым атрибутом «i»

# 5 Выводы

В результате лабораторной работы я повысила навыки использования командой строки и узнала, как используются расширенные атрибуты при разграничении доступа. Также я имела возможность связать теорию дискреционного разделения доступа с её реализацией в ОС Linux и опробовала действие на практике расширенных атрибутов «а» и «i».

# Список литературы

1. Дискреционное разграничение прав в Linux. Расширенные атрибуты [Электронный ресурс]. URL: <https://esystem.rudn.ru/mod/resource/view.php?id=1031375>.

2. Атрибуты файлов в файловых системах Linux [Электронный ресурс]. URL: <https://zalinux.ru/?p=6440>.