Отчёт по лабораторной работе №4

Дисциплина: Основы информационной безопасности

Паращенко Антонина Дмитриевна

Содержание

# 1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

# 2 Выполнение лабораторной работы

1. От имени пользователя guest определяем расширенные атрибуты файла /home/guest/dir1/file1 командой ***lsattr /home/guest/dir1/file1*** (рис. 1)

Рис. 1: 1

Рис. 1: 1

1. Установливаем командой ***chmod 600 file1*** на файл file1 права, разрешающие чтение и запись для владельца файла.(рис. 2)

Рис. 2: 2

Рис. 2: 2

1. 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)

Рис. 3: 3

Рис. 3: 3

1. 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*** (рис. 4)

Рис. 4: 4

Рис. 4: 4

1. От пользователя guest проверяем правильность установления атрибута: ***lsattr /home/guest/dir1/file1*** (рис. 5)

Рис. 5: 5

Рис. 5: 5

1. 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)

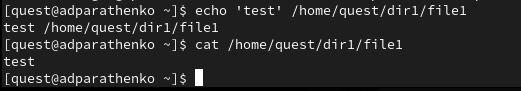


Рис. 6: 6

1. Попробуйте удалить файл file1 либо стереть имеющуюся в нём информацию командой ***echo “abcd” > /home/guest/dirl/file1*** Пробуем переименовать файл(рис. 7), (рис. 8), (рис. 9)

Рис. 7: 7

Рис. 7: 7

Рис. 8: 8

Рис. 8: 8

Рис. 9: 9

Рис. 9: 9

1. 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)

Рис. 10: 10

Рис. 10: 10

1. Снимаем расширенный атрибут **a** с файла /home/guest/dirl/file1 от имени суперпользователя командой ***sudo chattr -a /home/guest/dir1/file1*** (рис. 11)

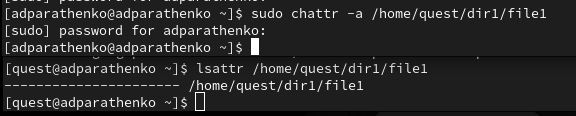


Рис. 11: 11

И повторяем операции, которые ранее не удавалось выполнить. **Теперь мы можем выполнить операции.** (рис. 12)

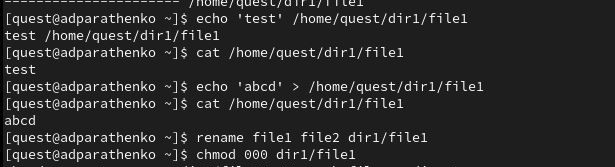


Рис. 12: 12

1. Повторяем наши действия по шагам, заменив атрибут «a» атрибутом «i». командой ***sudo chattr +i /home/guest/dir1/file1*** (рис. 14), (рис. 13)

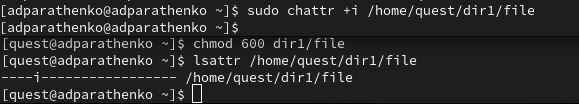


Рис. 13: 14

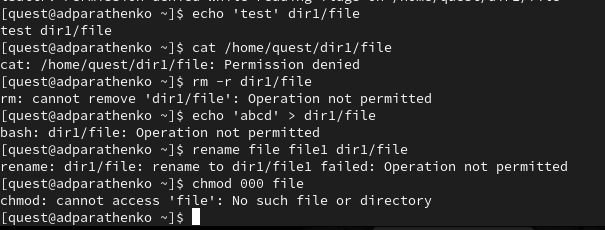


Рис. 14: 13

**В данном случае в файл можно было только записать, а изменить/прочитать, переименовать и изменить его атрибуты - нельзя.**

# 3 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 «а» и «i».

# Список литературы

1. https://esystem.rudn.ru/pluginfile.php/2357151/mod\_resource/content/3/004-lab\_discret\_extattr.pdf ::: {#refs} :::