Лабораторнаяработа № 4

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Усов Александр Александрович НБибд-02-18

Содержание

# 1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов

# 2 Задание

1. Создать файл file1
2. Установить расширенный атрибут a на файл и попробовать применить некоторые команды
3. Снять расширенный атрибут a с файла и попробовать применить команды без него
4. Установить атрибут i на файл и попробовать команды на нем.

# 3 Теоретическое введение

Предположим вы хотите защитить некоторые важные файлы в Linux. При чем они должны быть защищены не только от перезаписи но и от случайного или преднамеренного удаления и перемещения. Предотвратить перезапись или изменение битов доступа к файлов можно с помощью стандартных утилит chmod и chown, но это не идеальное решение, так как у суперпользователя по прежнему остается полный доступ. Но есть еще одно решение. Это команда chattr. Эта утилита позволяет устанавливать и отключать атрибуты файлов, на уровне файловой системы не зависимо от стандартных (чтение, запись, выполнение). Для просмотра текущих аттрибутов можно использовать lsattr. Изначально атрибуты управляемые chattr и lsattr поддерживались только файловыми системами семейства ext (ext2,ext3,ext4). но теперь эта возможность доступна и в других популярных файловых системах таких как XFS, Btrfs, ReiserFS, и т д.

Более подробно см. в [1].

# 4 Выполнение лабораторной работы

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

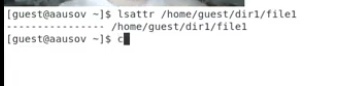


Figure 1: lsattr /home/guest/dir1/file1

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

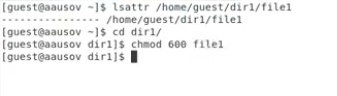


Figure 2: Команда chmod 600 file1

1. Попробовали установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest: chattr +a /home/guest/dir1/file1. (рис. 3).



Figure 3: Расширенный атрибут a от имени пользователя guest

1. Повысили свои права с помощью команды su. Установили расширенный атрибут a на файл /home/guest/dir1/file1 от имени суперпользователя: chattr +a /home/guest/dir1/file1 (рис. 4).

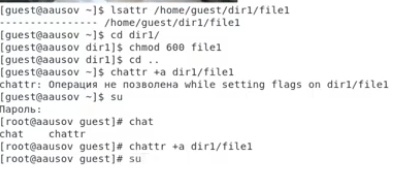


Figure 4: От имени суперпользователя

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

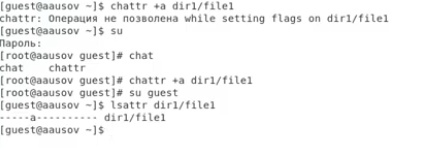


Figure 5: Проверили правильность установления атрибута

1. Выполнили дозапись в файл file1 слова «test» командой: echo “test” /home/guest/dir1/file1. (рис. 6)



Figure 6: Дозапись в файл file1 слова «test»

Далее выполнили чтение файла file1 командой cat /home/guest/dir1/file1. Убедились, что слово test было успешно записано в file1 (рис. 7)

1. Попробовали перезаписать текст в файле file1 командой echo “abcd”>/home/guest/dirl/file1. (рис. 7)

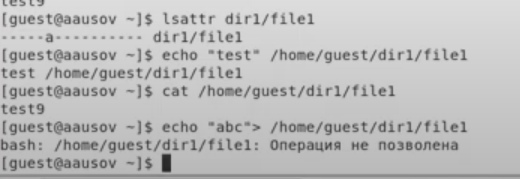


Figure 7: Перезаписать текст в файле file1

Попробовали переименовать файл. Но в каждом случае получили отказ. (рис. 8)

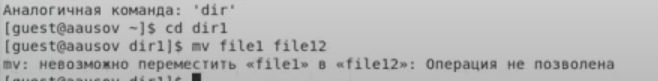


Figure 8: Попробовали переименовать файл.

1. Попробовали с помощью команды chmod 000 file1 установить на файл file1 права, запрещающие чтение и запись для владельца файла. Нам не удалось это сделать. (рис. 9)

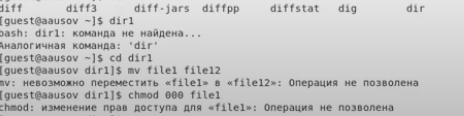


Figure 9: Попробовали с помощью команды chmod 000 file1 установить на файл

1. Сняли расширенный атрибут a с файла /home/guest/dirl/file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1. Повторили операции, которые нам ранее не удавалось выполнить. Ваши наблюдения занесите в отчёт. (рис. 10)

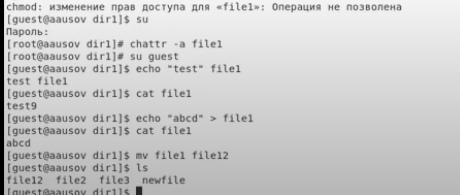


Figure 10: Сняли расширенный атрибут

1. Повторили действия по шагам, заменив атрибут «a» (только добавление к файлу) атрибутом «i» (неизменяемый). (рис. 11)

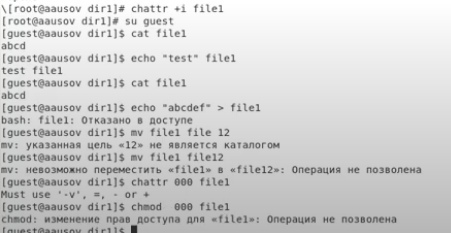


Figure 11: Повторили действия с атрибутом «i»

# 5 Выводы

В результате выполнения работы вы повысили свои навыки использования интерфейса командой строки (CLI), познакомились 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. Опробовали действие на практике расширенных атрибутов «а» и «i».

# Список литературы

1. Команда chattr в linux [Электронный ресурс]. Сайт, 2021. URL: <https://losst.ru/neizmenyaemye-fajly-v-linux>.