Отчет по лабораторной работе №4

Дискреционное разгарничение прав в Linux. Расширенные атрибуты

Бурдина Ксения Павловна

2022 Sep 27th

Содержание

# 1 Цель работы

Целью данной работы является получение практических навыков работы в консоли с расширенными атрибутами файлов.

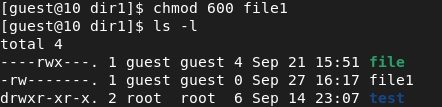
# 2 Ход выполнения лабораторной работы

1. От имени пользователя guest определим расширенные атрибуты файла /home/guest/dir1/file1:

Определение расширенных атрибутов

Определение расширенных атрибутов

1. Установим на файл file1 права, разрешающие чтение и запись для владельца файла:



Установка прав владельца (600)

1. Попробуем установить на файл /home/guest/dir1/file1 расширенный атрибут *a* от имени пользователя guest:

Попытка установки атрибута ‘a’

Попытка установки атрибута ‘a’

В ответ мы получили отказ от выполнения операции, поскольку у нас нет прав на выполнение файла, а соответственно и на изменение его атрибутов.

1. Повысим свои права с помощью команды su и попробуем установить расширенный атрибут *a* на файл /home/guest/dir1/file1 от имени суперпользователя:

Установка атрибута ‘a’ через суперпользователя

Установка атрибута ‘a’ через суперпользователя

1. От пользователя guest проверим правильность установления атрибута:

Проверка установки атрибута ‘a’

Проверка установки атрибута ‘a’

Видим, что наши расширенные атрибуты теперь имеют атрибут *a*.

1. Выполним дозапись в файл file1 слова «test», после чего выполним чтение файла file1:

Дозапись в file1 при +а

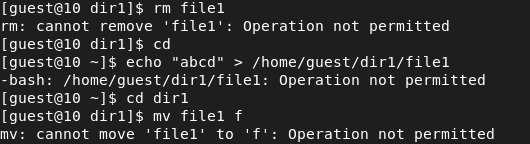
Дозапись в file1 при +а

Чтение file1 при +а

Чтение file1 при +а

Видим, что при выполнении дозаписи вывелась ошибка редактирования, а при проверке мы убедились, что файл остался пустым.

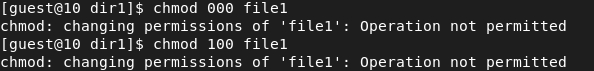
1. Попробуем удалить файл file1 либо стереть имеющуюся в нём информацию, а также переименовать наш файл:



Попытка изменения file1 при +а

Видим, что нам не удалось выполнить ни одного из этих действий.

1. Попробуем установить на файл file1 права, например, запрещающие чтение и запись для владельца файла:



Изменение прав на файл при +а

Нам не удалось успешно выполнить указанные команды.

1. Теперь снимем расширенный атрибут *a* с файла от имени суперпользователя:

Снятие расширенного атрибута ‘a’

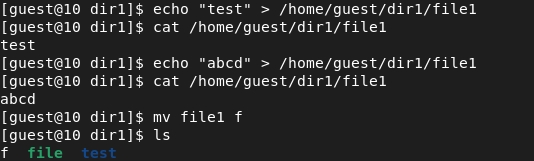
Снятие расширенного атрибута ‘a’

Проверим, что расширенных атрибутов на файл нет:

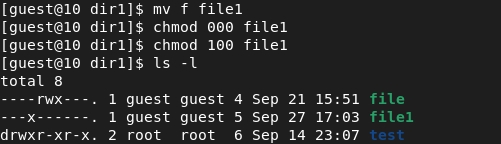
Проверка снятия атрибута ‘a’

Проверка снятия атрибута ‘a’

Повторим операции, которые нам не удавалось ранее [[1]](https://esystem.rudn.ru/pluginfile.php/1651887/mod_resource/content/3/004-lab_discret_extattr.pdf):



Повтор операций после снятия атрибута ‘a’

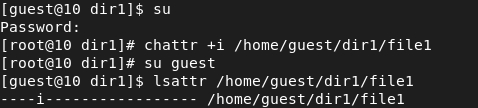


Повтор операций после снятия атрибута ‘a’

Видим, что теперь нам возможны и дозапись в файл, и его просмотр, и переименование файла file1, а также изменение атрибутов файла.

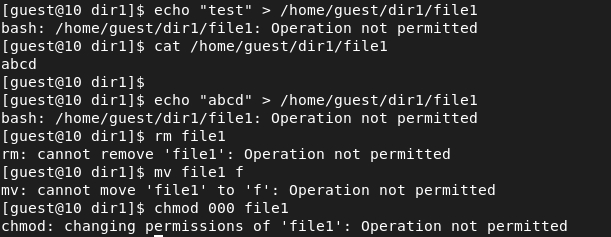
1. Повторим наши действия по шагам, заменив атрибут *a* атрибутом *i*.

Поставим от имени суперпользователя расширенный атрибут *i* и проверим правильность установки атрибута:



Установка атрибута ‘i’

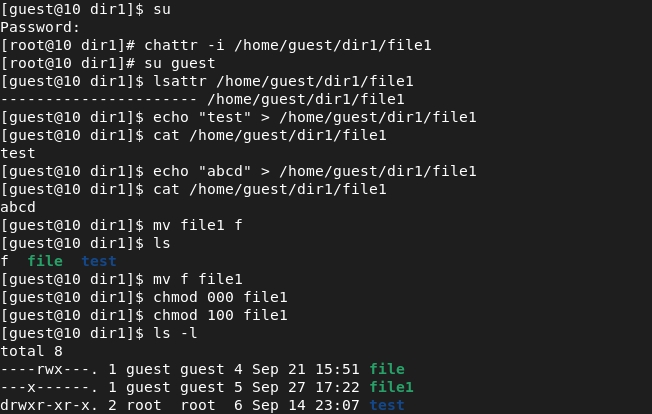
Теперь попробуем выполнить дозапись в файл file1 слова “test”, его прочтение, изменение названия, удаление файла, а также смену атрибутов файла:



Повтор всех операций с атрибутом ‘i’

Видим, что у нас аналогично тому, как было с атрибутом *a*, имеется запрет на выполнение данных действий. Это происходит из-за того, что данные атрибуты запрещают пользователя удалять файл, изменять его содержимое, а также переименовывать [[2]](https://translated.turbopages.org/proxy_u/en-ru.ru.04fe409b-6333f962-77c5da5e-74722d776562/https/www.computerhope.com/unix/chattr.htm).

Соответственно, для продолжения работы с файлом нам необходимо снять данный атрибут и проверить, что нам действительно снова доступны все действия с файлом file1:



Снятие атрибута ‘i’ и повтор действий с файлом

Видим, что у нас снова есть возможность выполнять все действия, описанные в лабораторной работе.

# 3 Выводы

В ходе работы мы 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 *a* и *i*.

# 4 Список литературы

1. Методические материалы курса [[1]](https://esystem.rudn.ru/pluginfile.php/1651887/mod_resource/content/3/004-lab_discret_extattr.pdf)
2. Электронный источник “Команды Linux chattr и lsattr” [[2]](https://translated.turbopages.org/proxy_u/en-ru.ru.04fe409b-6333f962-77c5da5e-74722d776562/https/www.computerhope.com/unix/chattr.htm)