Отчет по лабораторной работе №4

Основы информационной безопасности

Чувакина Мария Владимировна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов

2 Теоретическое введение

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [1]

Расширенные атрибуты файлов Linux представляют собой пары имя:значение, которые постоянно связаны с файлами и каталогами, подобно тому как строки окружения связаны с процессом. Атрибут может быть определён или не определён. Если он определён, то его значение может быть или пустым, или не пустым. [2]

Расширенные атрибуты дополняют обычные атрибуты, которые связаны со всеми inode в файловой системе (т. е., данные stat(2)). Часто они используются для предоставления дополнительных возможностей файловой системы, например, дополнительные возможности безопасности, такие как списки контроля доступа (ACL), могут быть реализованы через расширенные атрибуты. [3]

Установить атрибуты:

- chattr filename

Значения:

- chattr +a # только добавление. Удаление и переименование запрещено;
- chattr +A # не фиксировать данные об обращении к файлу
- chattr +c # сжатый файл

- chattr +d # неархивируемый файл
- chattr +i # неизменяемый файл
- chattr +S # синхронное обновление
- chattr +s # безопасное удаление, (после удаления место на диске переписывается нулями)
- chattr +u # неудаляемый файл
- chattr -R # рекурсия

Просмотреть атрибуты:

- lsattr filename

Опции:

- lsattr -R # рекурсия
- lsattr -a # вывести все файлы (включая скрытые)
- lsattr -d # не выводить содержимое директории

3 Выполнение лабораторной работы

1. От имени пользователя guest, созданного в прошлых лабораторных работах, определяю расширенные атрибуты файла `/home/guest/dir1/file1` (рис. 1).

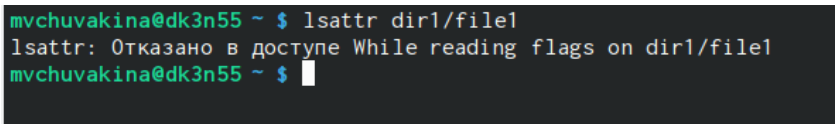

Рис. 3.1: Определение атрибутов

2. Изменяю права доступа для файла home/guest/dir1/file1 с помощью chmod 600 (рис. 2).

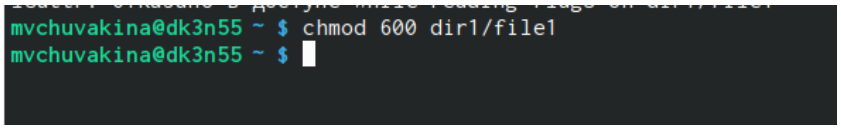

Рис. 3.2: Изменение прав доступа

3. Пробую установить на файл /home/guest/dir1/file1(рис. 3).

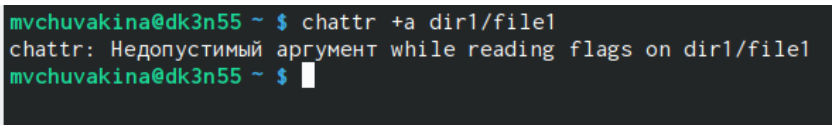

Рис. 3.3: Попытка установки рассширенных атрибутов

4. Устанавливаю расширенные права уже от имени суперпользователя(рис. 4).

```
mvchuvakina@dk3n55 ~ $ sudo chattr +a /home/guest/dir1/file1

Мы полагаем, что ваш системный администратор изложил вам основы
безопасности. Как правило, всё сводится к трём следующим правилам:

    №1) Уважайте частную жизнь других.
    №2) Думайте, прежде чем что-то вводить.
    №3) С большой властью приходит большая ответственность.

По соображениям безопасности пароль, который вы введёте, не будет виден.

Пароль:
```

Рис. 3.4: Установка расширенных атрибутов

5. От пользователя guest проверяю правильность установки атрибута (рис. 5).

```
mvchuvakina@dk3n55 ~ $ lsattr dir1/file1
lsattr: Недопустимый аргумент While reading flags on dir1/file1
mvchuvakina@dk3n55 ~ $
```

Рис. 3.5: Проверка атрибутов

6. Выполняю **дозапись** в файл с помощью `echo 'test' >> dir1/file1`, далее выполняю чтение файла, убеждаюсь, что дозапись была выполнена (рис. 6).

```
mvchuvakina@dk3n55 ~ $ echo "test" >> dir1/file1
mvchuvakina@dk3n55 ~ $ cat dir1/file1
test
test
mvchuvakina@dk3n55 ~ $
```

Рис. 3.6: Дозапись в файл

7. Пробую удалить файл. (рис. 7).

```
mvchuvakina@dk3n55 ~ $ rm dir1/file1
mvchuvakina@dk3n55 ~ $
```

Рис. 3.7: Попытка удалить файл

То же самое получаю при попытке переименовать файл(рис. 8).

```
mvchuvakina@dk3n55 ~ $ mv dir1/file1 dir1/aaa
mv: не удалось выполнить stat для 'dir1/file1': Нет такого файла или каталога
mvchuvakina@dk3n55 ~ $
```

Рис. 3.8: Попытка переименовать файл

8. Получаю отказ от выполнения при попытке установить другие права доступа (рис. 9).

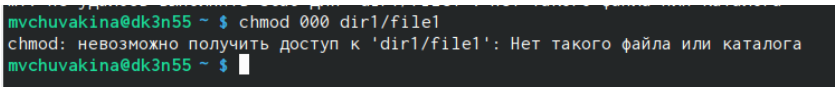

Рис. 3.9: Попытка изменить права доступа

9. Снимаю расширенные атрибуты с файла (рис. 10).

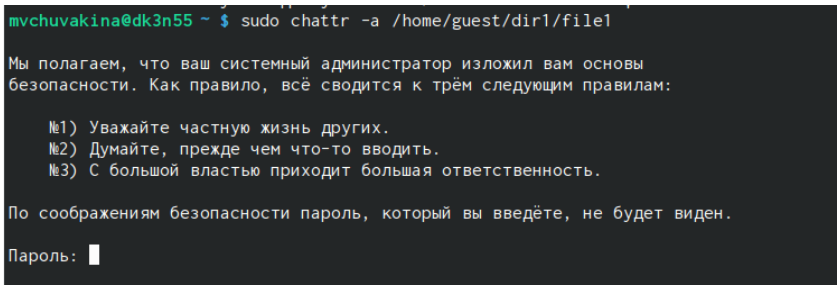

Рис. 3.10: Снятие расширенных атрибутов

Проверяю ранее не удавшиеся действия: чтение, переименование, изменение прав доступа. (рис. 11).

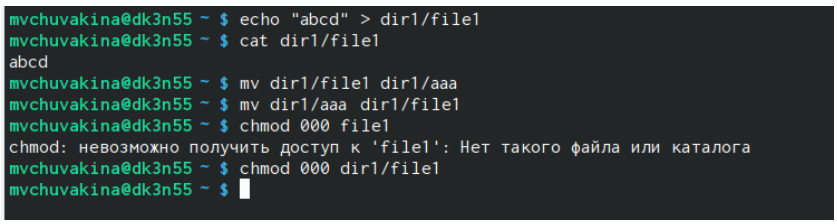

Рис. 3.11: Проверка выполнения действий

10. Пытаюсь добавить расширенный атрибут i от имени пользователя guest (рис. 12).

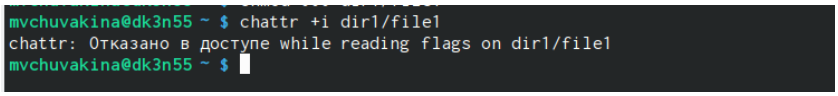

Рис. 3.12: Попытка добавить расширенный атрибут

Добавляю расширенный атрибут i от имени суперпользователя (рис. 13).

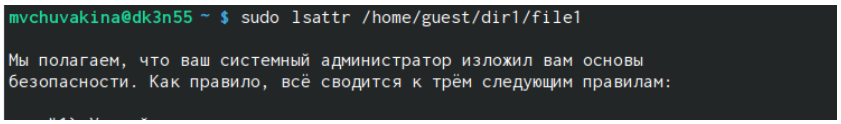

Рис. 3.13: Добавление расширенного атрибута

Пытаюсь записать в файл, дозаписать, переименовать или удалить (рис. 14).

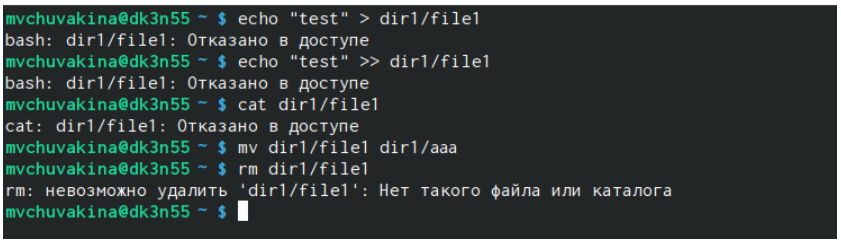

Рис. 3.14: Проверка выполнения действий

4 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 «a» и «i»

:::