

Отчет по лабораторной работе №4

Основы информационной безопасности

Бабенко Константин, НКАбд-01-23

Содержание

Цель работы	1
Теоретическое введение	1
Выполнение лабораторной работы	2
Выводы	5
Список литературы. Библиография	6

Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов

Теоретическое введение

Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенными 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:

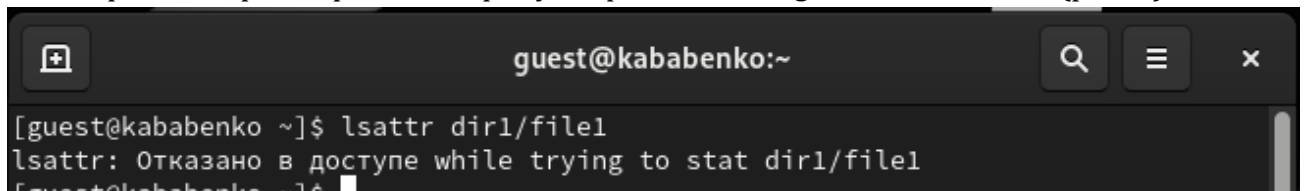
- `lsattr filename`

Опции:

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

Выполнение лабораторной работы

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



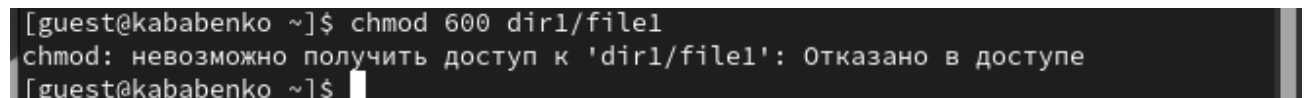
```

guest@kababenko:~
[guest@kababenko ~]$ lsattr dir1/file1
lsattr: Отказано в доступе while trying to stat dir1/file1
[guest@kababenko ~]$

```

Определение атрибутов

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



```

[guest@kababenko ~]$ chmod 600 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest@kababenko ~]$

```

Изменение прав доступа

3. Пробую установить на файл `/home/guest/dir1/file1` расширенный атрибут `a` от имени пользователя `guest`, в ответ получаю отказ от выполнения операции (рис. 3).

```
[guest@kababenko ~]$ chattr +a dir1/file1
chattr: Отказано в доступе while trying to stat dir1/file1
[guest@kababenko ~]$
```

Попытка установки расширенных атрибутов

4. Устанавливаю расширенные права уже от имени суперпользователя, теперь нет отказа от выполнения операции (рис. 4).

```
[guest@kababenko ~]$ 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 что-то вводить.
    №3) С большой властью приходит большая ответственность.

[sudo] пароль для guest:
Попробуйте ещё раз.
[sudo] пароль для guest:
Попробуйте ещё раз.
[sudo] пароль для guest:
sudo: 3 incorrect password attempts
[guest@kababenko ~]$
```

Установка расширенных атрибутов

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

```
[guest@kababenko ~]$ lsattr dir1/file1
lsattr: Отказано в доступе while trying to stat dir1/file1
[guest@kababenko ~]$
```

Проверка атрибутов

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

```
[guest@kababenko ~]$ echo "test" >> dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@kababenko ~]$
```

Дозапись в файл

7. Пробую удалить файл, получаю отказ от выполнения действия. (рис. 7).

```
[guest@kababenko ~]$ rm dir1/file1
rm: невозможно удалить 'dir1/file1': Отказано в доступе
[guest@kababenko ~]$
```

Попытка удалить файл

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

```
[guest@kababenko ~]$ mv dir1/file1 dir1/aa
mv: не удалось получить доступ к 'dir1/aa': Отказано в доступе
[guest@kababenko ~]$
```

Попытка переименовать файл

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

```
[guest@kababenko ~]$ chmod 000 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest@kababenko ~]$
```

Попытка изменить права доступа

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

```
[guest@kababenko ~]$ chmod 000 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest@kababenko ~]$
```

Снятие расширенных атрибутов

Проверяю ранее не удавшиеся действия: чтение, переименование, изменение прав доступа. Теперь все из этого выполняется (рис. 11).

```
[guest@kababenko ~]$ echo "test" >> dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@kababenko ~]$ rm dir1/file1
rm: невозможно удалить 'dir1/file1': Отказано в доступе
[guest@kababenko ~]$ mv dir1/file1 dir1/aa
mv: не удалось получить доступ к 'dir1/aa': Отказано в доступе
[guest@kababenko ~]$ chmod 000 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest@kababenko ~]$ echo "abcd" > dir1/file1
bash: dir1/file1: Отказано в доступе
[guest@kababenko ~]$ cat dir1/file1
cat: dir1/file1: Отказано в доступе
[guest@kababenko ~]$ mv dir1/file1 dir1/aa
mv: не удалось получить доступ к 'dir1/aa': Отказано в доступе
[guest@kababenko ~]$ chmod 000 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Отказано в доступе
[guest@kababenko ~]$
```

Проверка выполнения действий

10. Пытаюсь добавить расширенный атрибут `i` от имени пользователя `guest`, как и раньше, получаю отказ (рис. 12).

```
[guest@kababenko ~]$ chatter +i dir1/file1
chattr: Отказано в доступе while trying to stat dir1/file1
[guest@kababenko ~]$
```

Попытка добавить расширенный атрибут

Добавляю расширенный атрибут `i` от имени суперпользователя, теперь все выполнено верно (рис. 13).

```
[guest@kababenko ~]$ sudo chatter +i /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 что-то вводить.
№3) С большой властью приходит большая ответственность.

[sudo] пароль для guest:
guest is not in the sudoers file. This incident will be reported.
[guest@kababenko ~]$ sudo lsattr /home/guest/dir1/file1
[sudo] пароль для guest:
Попробуйте ещё раз.
[sudo] пароль для guest:
guest is not in the sudoers file. This incident will be reported.
[guest@kababenko ~]$ K2o0c0т6я
bash: K2o0c0т6я: команда не найдена...
[guest@kababenko ~]$
```

Добавление расширенного атрибута

Пытаюсь записать в файл, дозаписать, переименовать или удалить, ничего из этого сделать нельзя (рис. 14).

```
[guest@kababenko ~]$ sudo chatter +i /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 что-то вводить.
№3) С большой властью приходит большая ответственность.

[sudo] пароль для guest:
guest is not in the sudoers file. This incident will be reported.
[guest@kababenko ~]$ sudo lsattr /home/guest/dir1/file1
[sudo] пароль для guest:
Попробуйте ещё раз.
[sudo] пароль для guest:
guest is not in the sudoers file. This incident will be reported.
[guest@kababenko ~]$ K2o0c0т6я
bash: K2o0c0т6я: команда не найдена...
[guest@kababenko ~]$
```

Проверка выполнения действий

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»

Список литературы. Библиография

[0] Методические материалы курса

[1] Права доступа: <https://codechick.io/tutorials/unix-linux/unix-linux-permissions>

[2] Расширенные атрибуты: <https://ru.manpages.org/xattr/7>

[3] Операции с расширенными атрибутами: <https://p-n-z-8-8.livejournal.com/64493.html>