

Отчет по лабораторной работе №4

Основы информационной безопасности

Швецов Михаил, НКАбд-01-23

Содержание

1	Цель работы	1
2	Теоретическое введение.....	1
3	Выполнение лабораторной работы	2
4	Выводы	4
5	Список литературы. Библиография.....	5

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 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 определен или не определен. Если он определен, 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).

```
[guest@mrshvecov ~]$ sudo lsattr dir1/file1
[sudo] пароль для guest:
[guest@mrshvecov ~]$ chmod 600 dir1/file1
```

Определение атрибутов

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

```
[guest@mrshvecov ~]$ sudo lsattr dir1/file1
[sudo] пароль для guest:
[guest@mrshvecov ~]$ chmod 600 dir1/file1
```

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@mrshvecov ~]$ chattr +a dir1/file1
chattr: Операция не позволена while setting flags on dir1/file1
[guest@mrshvecov ~]$
```

Попытка установки расширенных атрибутов

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

```
[mrshvecov@mrshvecov ~]$ sudo chattr +a /home/guest/dir1/file1
[sudo] пароль для mrshvecov:
[mrshvecov@mrshvecov ~]$ su guest
```

Установка расширенных атрибутов

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

```
[guest@mrshvecov mrshvecov]$ lsattr dir1/file1
lsattr: Отказано в доступе while trying to stat dir1/file1
[guest@mrshvecov mrshvecov]$ cd ~
[guest@mrshvecov ~]$ lsattr dir1/file1
dir1/file1/..: Отказано в доступе
dir1/file1/...: Отказано в доступе
[guest@mrshvecov ~]$ sudo lsattr dir1/file1
[guest@mrshvecov ~]$
```

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@mrshvecov ~]$ echo "test" >> dir1/file1
bash: dir1/file1: Это каталог
[guest@mrshvecov ~]$ cat dir1/file1
cat: dir1/file1: Это каталог
```

Дозапись в файл

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

```
[guest@mrshvecov ~]$ rm dir1/file1
rm: невозможно удалить 'dir1/file1': Это каталог
[guest@mrshvecov ~]$
```

Попытка удалить файл

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

```
[guest@mrshvecov ~]$ mv dir1/file1
mv: невозможно удалить 'dir1/file1': Это каталог
[guest@mrshvecov ~]$
```

Попытка переименовать файл

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

```
[guest@mrshvecov ~]$ mv dir1/file1 dir1/aaa
mv: невозможно переместить 'dir1/file1' в 'dir1/aaa': Операция не позволена
```

Попытка изменить права доступа

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

```
[guest@mrshvecov ~]$ chmod 000 dir1/file1
chmod: изменение прав доступа для 'dir1/file1': Операция не позволена
[guest@mrshvecov ~]$ su mrshvecov
Пароль:
[mrshvecov@mrshvecov guest]$ sudo chattr -a dir1/file1
[mrshvecov@mrshvecov guest]$ sudo lsattr dir1/file1
[mrshvecov@mrshvecov guest]$ su guest
Пароль:
[guest@mrshvecov ~]$ echo "abcd" > dir1/file1
bash: dir1/file1: Это каталог
[guest@mrshvecov ~]$
```

Снятие расширенных атрибутов

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

```
[guest@mrshvecov ~]$ chmod 000 dir1/file1
chmod: изменение прав доступа для 'dir1/file1': Операция не позволена
[guest@mrshvecov ~]$ su mrshvecov
Пароль:
[mrshvecov@mrshvecov guest]$ sudo chattr -a dir1/file1
[mrshvecov@mrshvecov guest]$ sudo lsattr dir1/file1
[mrshvecov@mrshvecov guest]$ su guest
Пароль:
[guest@mrshvecov ~]$ echo "abcd" > dir1/file1
bash: dir1/file1: Это каталог
[guest@mrshvecov ~]$
```

Проверка выполнения действий

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

```
[guest@mrshvecov ~]$ mv dir1/aaa dir1/file1
[guest@mrshvecov ~]$ chmod 000 dir1/file1
[guest@mrshvecov ~]$ chattr +i dir1/file1
chattr: Отказано в доступе while reading flags on dir1/file1
```

Попытка добавить расширенный атрибут

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

```
[guest@mrshvecov ~]$ mv dir1/aaa dir1/file1
[guest@mrshvecov ~]$ chmod 000 dir1/file1
[guest@mrshvecov ~]$ chattr +i dir1/file1
chattr: Отказано в доступе while reading flags on dir1/file1
```

Добавление расширенного атрибута

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

```
[guest@mrshvecov ~]$ mv dir1/file1 dir1/aaa
[guest@mrshvecov ~]$ mv dir1/aaa dir1/file1
[guest@mrshvecov ~]$ chmod 000 dir1/file1
[guest@mrshvecov ~]$ chattr +i dir1/file1
chattr: Отказано в доступе while reading flags on dir1/file1
[guest@mrshvecov ~]$ su mrshvecov
Пароль:
[mrshvecov@mrshvecov guest]$ sudo chattr +i dir1/file1
[mrshvecov@mrshvecov guest]$ sudo lsattr dir1/file1
```

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 «а» и «i»

5 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>