

Отчет по лабораторной работе №4

Основы информационной безопасности

Ничипорова Елена Дмитриевна

Содержание

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

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 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

Выполнение лабораторной работы

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

```
mkdir: cannot create directory 'dir1/file1': Permission denied
[guest@localhost ~]$ lsattr dir1/file1
```

Определение атрибутов

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

```
[guest@localhost ~]$ 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@localhost ~]$ chattr +a dir1/file1
```

Попытка установки расширенных атрибутов

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

```
[guest@localhost ~]$ su root
Password:
[root@localhost guest]# sudo chattr +a /home/guest/dir1/file1
```

Установка расширенных атрибутов

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

```
chattr: no such file or directory while trying to stat
[root@localhost guest]# lsattr dir1/file1
```

Проверка атрибутов

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

```
[root@localhost guest]# echo "test" >> dir1/file1
[root@localhost guest]# cat dir1/file1
test
[root@localhost guest]#
```

Дозапись в файл

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

```
[guest@localhost ~]$ rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@localhost ~]$ _
```

Попытка удалить файл

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

```
[guest@localhost ~]$ mv dir1/file1 dir1/aaa
mv: failed to access 'dir1/aaa': Permission denied
[guest@localhost ~]$ _
```

Попытка переименовать файл

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

```
[guest@localhost ~]$ chmod 000 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@localhost ~]$
```

Попытка изменить права доступа

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

```
[guest@localhost ~]# su root
Password:
[root@localhost guest]# sudo chattr -a /home/guest/dir1/file1
[root@localhost guest]# sudo lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[root@localhost guest]#
```

Снятие расширенных атрибутов

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

```
[guest@localhost ~]# chmod 000 file1
chmod: cannot access 'file1': No such file or directory
[guest@localhost ~]# chmod 000 dir1/file1
chmod: cannot access 'dir1/file1': Permission denied
[guest@localhost ~]# _
```

Проверка выполнения действий

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

```
[guest@localhost ~]# chattr +i dir1/file1
chattr: Permission denied while trying to stat dir1/file1
[guest@localhost ~]#
```

Попытка добавить расширенный атрибут

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

```
[guest@localhost ~]# su root
Password:
[root@localhost guest]# sudo chattr +i /home/guest/dir1/file1
[root@localhost guest]# sudo lsattr /home/guest/dir1/file1
----i----- /home/guest/dir1/file1
[root@localhost guest]#
```

Добавление расширенного атрибута

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

```
[root@localhost guest]# su guest
[guest@localhost ~]# echo "test" > dir1/file1
bash: dir1/file1: Permission denied
[guest@localhost ~]# echo "test" >> dir1/file1
bash: dir1/file1: Permission denied
[guest@localhost ~]# cat dir1/file1
cat: dir1/file1: Permission denied
[guest@localhost ~]# mv dir1/file1 dir1/aaa
mv: failed to access 'dir1/aaa': Permission denied
[guest@localhost ~]# rm dir1/file1
rm: cannot remove 'dir1/file1': Permission denied
[guest@localhost ~]# _
```

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>