

Лабораторная работа №4

Дисциплина: Информационная безопасность

Боровикова Карина Владимировна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	10
5	Выводы	14
	Список литературы	15

Список иллюстраций

4.1	Определяем расширенные атрибуты файла /home/guest/dir1/file1, меняем права доступа на файл, добавляем атрибут “а”, проверяем добавление, записываем данные в файл, проверяем содержимое, пробуем перезаписать содержимое файла	10
4.2	Получаем права администратора, добавляем атрибут “а”, переходим в директорию /home/guest/dir1/file1, проверяем содержимое, проверяем атрибуты файла file1, убираем атрибут “а”, добавляем атрибут “i”, проверяем содержимое, проверяем атрибуты файла file1, убираем атрибут “i”	11
4.3	Устанавливаем права запрещающие чтение и запись для владельца файла, проверяем содержимое файла, пытаемся перезаписать файл, проверяем содержимое, повторяем действия для случая с другим атрибутом	12
4.4	Создаем файл, так как мы его удаляли, пытаемся перезаписать информацию в файл, проверяем содержимое, видим, что файл пуст, пробуем поменять права доступа, пробуем удалить файл	13

Список таблиц

3.1	Расширенные атрибуты	7
-----	--------------------------------	---

1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

2 Задание

- Произвести работу в консоли с атрибутами файлов для пользователей суперпользователя и гостя;
- Опытным путем проверить работу атрибутов “a” и “i”.

3 Теоретическое введение

В Linux атрибуты файла - это свойства метаданных, которые описывают поведение файла. Например, атрибут может указывать, сжат ли файл, или указывать, можно ли удалить файл. Помимо прав доступа каждый из файлов стандартной файловой системы Linux имеет набор атрибутов, регламентирующих особенности работы с ним. Атрибуты поддерживаются такими файловыми системами Linux, как Ext4, Btrfs и XFS. Команда `lsattr` позволяет вызывать соответствующую утилиту для их вывода.

Базовый синтаксис команды выглядит следующим образом:

```
lsattr [параметры] файлы
```

Наиболее важными параметрами являются параметр `-R`, позволяющий рекурсивно выводить атрибуты файлов в дереве директорий, параметр `-a`, позволяющий выводить информацию и об атрибутах скрытых файлов и параметр `-d`, позволяющий выводить информацию об атрибутах директорий вместо обработки их содержимого. В том случае, если утилите не передаются имена файлов, она выводит информацию об атрибутах файлов из текущей директории.

Наиболее важные атрибуты приведены в таблице ниже 3.1:

Таблица 3.1: Расширенные атрибуты

Атрибут	Значение
A	Запрещает обновлять метку времени доступа к файлу

Атрибут	Значение
a	Автоматически устанавливает режим дополнения при открытии файла для записи
C	Запрещает использовать механизм копирования при записи (Copy-on-Write) при модификации содержимого файла
D	При применении к директории активирует режим синхронной записи изменений содержащихся в ней файлов
d	Запрещает утилите dump создавать резервную копию файла
E	Указывает на ошибку сжатия содержимого файла ядром ОС (не может быть установлен пользователем)
e	Указывает на использование экстендов для ссылок на соответствующие файлу дисковые блоки (не может быть установлен пользователем)
h	Указывает на то, что размер файла исчисляется в количестве блоков ФС, а не ее секторов, то есть, размер файла превышал или превышает в данный момент 2 ТБ (не может быть установлен пользователем)
I	Указывает на то, что содержимое директории было проиндексировано утилитой htree
i	Запрещает всем пользователям, в том числе супрепользователю, модифицировать файл, а именно, записывать в него данные, удалять переименовывать или создавать ссылки на него

Атрибут	Значение
j	Принудительно активирует режим журналирования ФС при записи данных в файл
s	Активирует механизм надежного удаления, автоматически записывающий нулевые блоки на диск после удаления файла пользователем
S	Активирует режим синхронной записи изменений содержимого файла на диск
T	При применении к директории указывает на то, что ее поддиректории не связаны и могут размещаться в отдельных группах блоков
t	Запрещает оптимизации использования блоков файла
u	Запрещает удаление содержимого файла при его удалении из ФС с целью получения возможности его последующего восстановления
X	Указывает на возможность прямого доступа к содержимому сжатого ядром ОС файла (не может быть установлен пользователем)
Z	Указывает на неактуальность сжатого ядром ОС файла (не может быть установлен пользователем)

4 Выполнение лабораторной работы

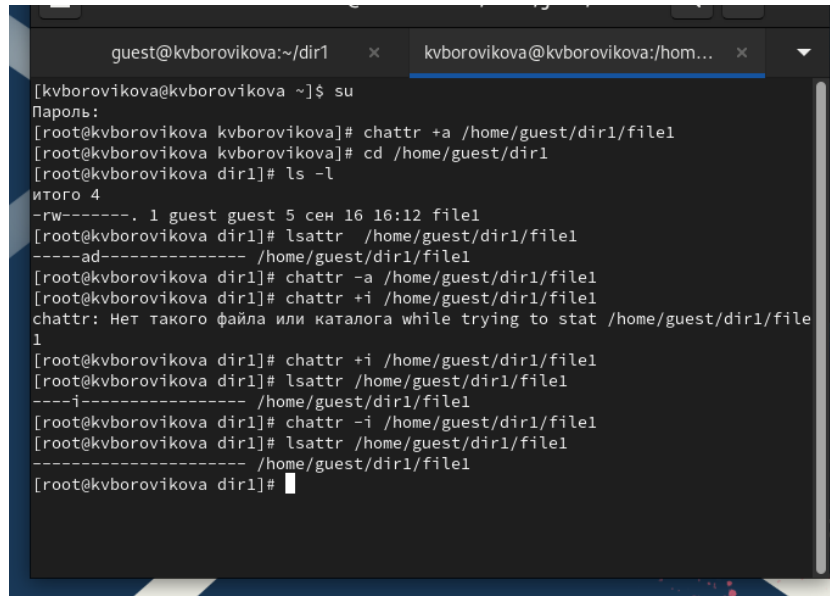
1. От имени пользователя guest определим расширенные атрибуты файла /home/guest/dir1/file1 командой `lsattr /home/guest/dir1/file1`. (рис. 4.1)

```
[guest@kvborovikova dir1]$ lsattr /home/guest/dir1/file1
-----d----- /home/guest/dir1/file1
[guest@kvborovikova dir1]$ chmod 600 file1
[guest@kvborovikova dir1]$ ls
file1
[guest@kvborovikova dir1]$ ls -l
итого 4
-rw-----. 1 guest guest 5 сен 16 16:12 file1
[guest@kvborovikova dir1]$ chattr +a /home/guest/dir1/file1
chattr: Операция не позволена while setting flags on /home/guest/dir1/file1
[guest@kvborovikova dir1]$ lsattr /home/guest/dir1/file1
-----ad----- /home/guest/dir1/file1
[guest@kvborovikova dir1]$ echo "test" /home/guest/dir1/file1
test /home/guest/dir1/file1
[guest@kvborovikova dir1]$ cat /home/guest/dir1/file1
test
[guest@kvborovikova dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Операция не позволена
```

Рис. 4.1: Определяем расширенные атрибуты файла /home/guest/dir1/file1, меняем права доступа на файл, добавляем атрибут “а”, проверяем добавление, записываем данные в файл, проверяем содержимое, пробуем перезаписать содержимое файла

2. Установим командой `chmod 600 file1` на файл file1 права, разрешающие чтение и запись для владельца файла (рис. 4.1).
3. Попробуем установить на файл /home/guest/dir1/file1 расширенный атрибут а от имени пользователя guest: `chattr +a /home/guest/dir1/file1` В ответ мы получаем отказ от выполнения операции.(рис. 4.1)

4. Заходим на другую консоль с правами администратора. Установим расширенный атрибут `a` на файл `/home/guest/dir1/file1` от имени суперпользователя: `chattr +a /home/guest/dir1/file1` (рис. 4.2).

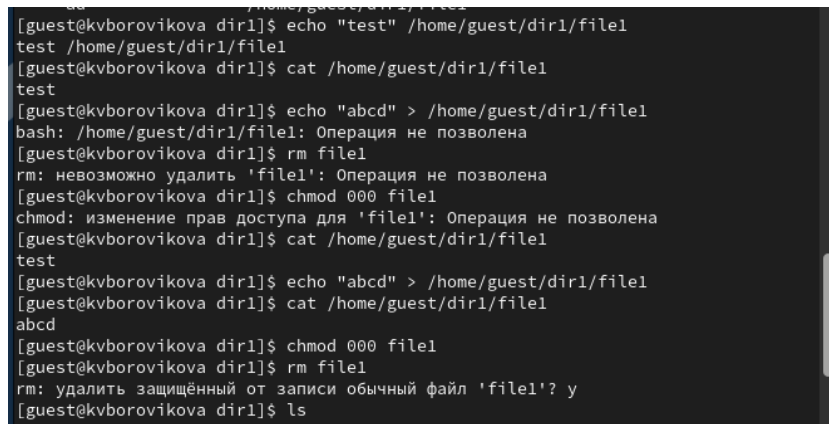


```
guest@kvborovikova:~/dir1 x kvborovikova@kvborovikova:/hom... x
[kvborovikova@kvborovikova ~]$ su
Пароль:
[root@kvborovikova kvborovikova]# chattr +a /home/guest/dir1/file1
[root@kvborovikova kvborovikova]# cd /home/guest/dir1
[root@kvborovikova dir1]# ls -l
итого 4
-rw-----. 1 guest guest 5 сен 16 16:12 file1
[root@kvborovikova dir1]# lsattr /home/guest/dir1/file1
-----ad----- /home/guest/dir1/file1
[root@kvborovikova dir1]# chattr -a /home/guest/dir1/file1
[root@kvborovikova dir1]# chattr +i /home/guest/dir1/file1
chattr: Нет такого файла или каталога while trying to stat /home/guest/dir1/file
1
[root@kvborovikova dir1]# chattr +i /home/guest/dir1/file1
[root@kvborovikova dir1]# lsattr /home/guest/dir1/file1
----i----- /home/guest/dir1/file1
[root@kvborovikova dir1]# chattr -i /home/guest/dir1/file1
[root@kvborovikova dir1]# lsattr /home/guest/dir1/file1
-----ad----- /home/guest/dir1/file1
[root@kvborovikova dir1]#
```

Рис. 4.2: Получаем права администратора, добавляем атрибут “a”, переходим в директорию `/home/guest/dir1/file1`, проверяем содержимое, проверяем атрибуты файла `file1`, убираем атрибут “a”, добавляем атрибут “i”, проверяем содержимое, проверяем атрибуты файла `file1`, убираем атрибут “i”

5. От пользователя `guest` проверим правильность установления атрибута: `lsattr /home/guest/dir1/file1` (рис. 4.1).
6. Выполним дозапись в файл `file1` слова «test» командой `echo "test" /home/guest/dir1/file1` После этого выполним чтение файла `file1` командой `cat /home/guest/dir1/file1` Убедимся, что слово `test` было успешно записано в `file1` (рис. 4.1).
7. Попробуем удалить файл `file1` либо стереть имеющуюся в нём информацию командой `echo "abcd" > /home/guest/dir1/file1` Не удалось. Попробуем переименовать файл командой `mv file1 file2`. Так же не удалось (рис. 4.1).

8. Попробуем с помощью команды `chmod 000 file1` установить на файл `file1` права, например, запрещающие чтение и запись для владельца файла. Указанные выше команды выполнить не удалось, так как атрибут `a` нам в этом противостоит (рис. 4.3).



```
[guest@kvborovikova dir1]$ echo "test" /home/guest/dir1/file1
test /home/guest/dir1/file1
[guest@kvborovikova dir1]$ cat /home/guest/dir1/file1
test
[guest@kvborovikova dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Операция не позволена
[guest@kvborovikova dir1]$ rm file1
rm: невозможно удалить 'file1': Операция не позволена
[guest@kvborovikova dir1]$ chmod 000 file1
chmod: изменение прав доступа для 'file1': Операция не позволена
[guest@kvborovikova dir1]$ cat /home/guest/dir1/file1
test
[guest@kvborovikova dir1]$ echo "abcd" > /home/guest/dir1/file1
[guest@kvborovikova dir1]$ cat /home/guest/dir1/file1
abcd
[guest@kvborovikova dir1]$ chmod 000 file1
[guest@kvborovikova dir1]$ rm file1
rm: удалить защищенный от записи обычный файл 'file1'? y
[guest@kvborovikova dir1]$ ls
```

Рис. 4.3: Устанавливаем права запрещающие чтение и запись для владельца файла, проверяем содержимое файла, пытаемся перезаписать файл, проверяем содержимое, повторяем действия для случая с другим атрибутом

9. Снимем расширенный атрибут `a` с файла `/home/guest/dir1/file1` от имени суперпользователя командой `chattr -a /home/guest/dir1/file1`. Повторим операции, которые нам ранее не удавалось выполнить. Видим, что выполнить команды удалось (рис. 4.2-4.3).
10. Повторим наши действия по шагам, заменив атрибут «`a`» атрибутом «`i`» (рис. 4.4). Выполнить действия не удалось, так как нам мешает атрибут `i` (рис. 4.4).

```
guest@kvborovikova: /home/guest/dir1$ touch file1
[guest@kvborovikova dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Операция не позволена
[guest@kvborovikova dir1]$ cat /home/guest/dir1/file1
[guest@kvborovikova dir1]$ chmod 000 file1
chmod: изменение прав доступа для 'file1': Операция не позволена
[guest@kvborovikova dir1]$ rm file1
rm: невозможно удалить 'file1': Операция не позволена
[guest@kvborovikova dir1]$
```

Рис. 4.4: Создаем файл, так как мы его удаляли, пытаемся перезаписать информацию в файл, проверяем содержимое, видим, что файл пуст, пробуем поменять права доступа, пробуем удалить файл

5 Выводы

В результате выполнения 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 «а» и «і».

Список литературы