

Лабораторная работа № 4

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Абакумов Егор Александрович

Содержание

Цель работы	5
Задание	6
Теоретическое описание	7
Ход работы	9
Выводы	15
Список литературы	16

List of Figures

0.1	Права на файл и попытка изменения атрибутов	9
0.2	Изменение расширенных атрибутов файла	10
0.3	Попытка записи в файл с атрибутом “a”	10
0.4	Тестирование файла с атрибутом “a”	11
0.5	Дозаписывание файла с атрибутом “a”	11
0.6	Удаление атрибута “a”	12
0.7	Тестирование файла без атрибута “a”	12
0.8	Добавление атрибута “i”	12
0.9	Тестирование файла с атрибутом “i”	13
0.10	Дозаписывание файла с атрибутом “i”	13
0.11	Удаление атрибута “i”	13
0.12	Тестирование файла без атрибута “i”	14

List of Tables

Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

Задание

Провести практические занятия по взаимодействию с расширенными атрибутами файлов в ОС Linux.

Теоретическое описание

В операционной системе Linux есть много отличных функций безопасности, но она из самых важных - это система прав доступа к файлам. Linux, как последователь идеологии ядра Linux в отличие от Windows, изначально проектировался как многопользовательская система, поэтому права доступа к файлам в linux продуманы очень хорошо.

У каждого файла имеется определённый набор свойств в файловой системе. Например, это права доступа, владелец, имя, метки времени. В Linux каждый файл имеет довольно много свойств, например, права доступа устанавливаются трижды (для владельца, группы и всех прочих), метки времени также бывают трёх разных видов (время создание, доступа и изменения) [1].

Кроме того файлам и директориям могут быть установлены расширенные атрибуты доступа. Файловые атрибуты могут использовать администраторы и пользователи для защиты файлов от случайных удалений и изменений, а также их применяют злоумышленники, делая невозможным удаление вредоносного файла.

Для работы с этими атрибутами обычно используются утилиты `chattr` и `lsattr`, входящие в пакет `e2fsprogs` и предустановленные во всех современных дистрибутивах. Базовый синтаксис `chattr` выглядит следующим образом:

```
chattr options [operator][attributes] files
```

Вот некоторые доступные атрибуты:

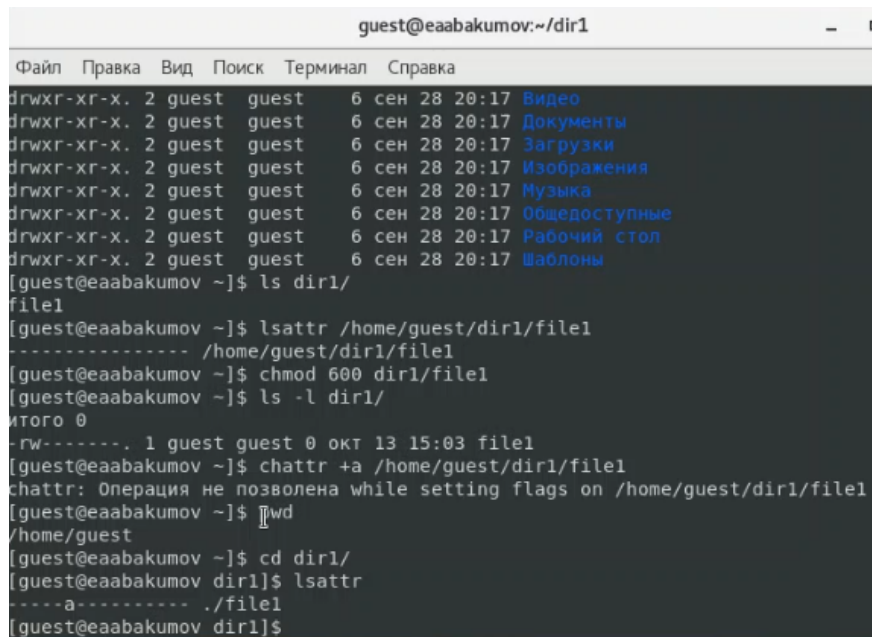
а - файл может быть открыт только в режиме добавления; А - не обновлять время перезаписи; с - автоматически сжимать при записи на диск; С - отключить копирование при записи; D - работает только для папки, когда установлен, все

изменения синхронно записываются на диск сразу же; e - использовать extent'ы блоков для хранения файла; i - сделать неизменяемым; j - все данные перед записью в файл будут записаны в журнал; s - безопасное удаление с последующей перезаписью нулями; S - синхронное обновление, изменения файлов с этим атрибутом будут сразу же записаны на диск; t - файлы с этим атрибутом не будут храниться в отдельных блоках; u - содержимое файлов с этим атрибутом не будет удалено при удалении самого файла и потом может быть восстановлено.

Тем не менее, не стоит забывать, что вы не можете использовать `chattr` как меру безопасности так как атрибуты легко изменить. Один из способов решения этой проблемы - ограничить доступ к самой утилите `chattr`[2].

Ход работы

1. Из-под пользователя guest проверяем расширенные атрибуты файла file1 командой lsattr, далее ставим права 600 на файл и пытаемся добавить атрибут “a” к файлу. Не получается, тогда делаем это из-под суперпользователя, проверяем (иллюстр. 0.1, 0.2).



```
guest@eaabakumov:~/dir1
Файл  Правка  Вид  Поиск  Терминал  Справка
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Видео
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Документы
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Загрузки
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Изображения
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Музыка
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Общедоступные
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Рабочий стол
drwxr-xr-x. 2 guest guest 6 сен 28 20:17 Шаблоны
[guest@eaabakumov ~]$ ls dir1/
file1
[guest@eaabakumov ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@eaabakumov ~]$ chmod 600 dir1/file1
[guest@eaabakumov ~]$ ls -l dir1/
итого 0
-rw-----. 1 guest guest 0 окт 13 15:03 file1
[guest@eaabakumov ~]$ chattr +a /home/guest/dir1/file1
chattr: Операция не позволена while setting flags on /home/guest/dir1/file1
[guest@eaabakumov ~]$ llwd
/home/guest
[guest@eaabakumov ~]$ cd dir1/
[guest@eaabakumov dir1]$ lsattr
-----a----- ./file1
[guest@eaabakumov dir1]$
```

Figure 0.1: Права на файл и попытка изменения атрибутов

```
root@eaabakumov:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@eaabakumov ~]$ su -  
Пароль:  
Последний вход в систему: Ср окт 13 15:02:59 MSK 2021 на pts/0  
[root@eaabakumov ~]# whoami  
root  
[root@eaabakumov ~]# chattr +a /home/guest/dirl/file1  
[root@eaabakumov ~]# lsattr /home/guest/dirl/file1  
----+----- /home/guest/dirl/file1  
[root@eaabakumov ~]#
```

Figure 0.2: Изменение расширенных атрибутов файла

2. Теперь командой `echo` пытаемся записать в файл текст, что у нас не выходит, не хватает прав (иллюстр. 0.3). Попытка перезаписать файл, удалить его или переименовать так же не приносит успеха - нет прав. Как и на изменение прав к файлу (иллюстр. 0.4). Однако дозаписывание в файл получается (иллюстр. 0.5)

```
[guest@eaabakumov dirl]$ echo "test" > /home/guest/dirl/file1  
bash: /home/guest/dirl/file1: Операция не позволена  
[guest@eaabakumov dirl]$ cat file1  
[guest@eaabakumov dirl]$ echo "test" > file1  
bash: file1: Операция не позволена
```

Figure 0.3: Попытка записи в файл с атрибутом “а”

```
guest@eaabakumov:~/dir1
Файл Правка Вид Поиск Терминал Справка
[guest@eaabakumov dir1]$ cat file2
test
[guest@eaabakumov dir1]$ cat file1
[guest@eaabakumov dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Нет такого файла или каталога
[guest@eaabakumov dir1]$ ls
file1 file2
[guest@eaabakumov dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Операция не позволена
[guest@eaabakumov dir1]$ rm file1
rm: невозможно удалить «file1»: Операция не позволена
[guest@eaabakumov dir1]$ mv file1 hello_123
mv: невозможно переместить «file1» в «hello_123»: Операция не позволена
[guest@eaabakumov dir1]$ chmod 000 file1
chmod: изменение прав доступа для «file1»: Операция не позволена
[guest@eaabakumov dir1]$ ls -l
итого 4
-rw-----. 1 guest guest 0 окт 13 15:03 file1
-rw-rw-r--. 1 guest guest 5 окт 13 15:21 file2
[guest@eaabakumov dir1]$ rm file2
[guest@eaabakumov dir1]$ ls -l
итого 0
-rw-----. 1 guest guest 0 окт 13 15:03 file1
[guest@eaabakumov dir1]$
```

Figure 0.4: Тестирование файла с атрибутом “а”

```
[guest@eaabakumov dir1]$ echo "test" >> file1
[guest@eaabakumov dir1]$ cat file1
test
[guest@eaabakumov dir1]$ lsattr
-----a----- ./file1
[guest@eaabakumov dir1]$ S
```

Figure 0.5: Дозаписывание файла с атрибутом “а”

3. Теперь снимаем атрибут “а” и пытаемся повторить все прошлые действия (иллюстр. 0.6, 0.7). В этот раз у нас получается произвести все изменения штатно.

```
root@eaabakumov:~  
Файл Правка Вид Поиск Терминал Справка  
[guest@eaabakumov ~]$ su -  
Пароль:  
Последний вход в систему: Ср окт 13 15:02:59 MSK 2021 на pts/0  
[root@eaabakumov ~]# whoami  
root  
[root@eaabakumov ~]# chattr +a /home/guest/dir1/file1  
[root@eaabakumov ~]# lsattr /home/guest/dir1/file1  
-----a----- /home/guest/dir1/file1  
[root@eaabakumov ~]# chattr -a /home/guest/dir1/file1  
[root@eaabakumov ~]#
```

Figure 0.6: Удаление атрибута “a”

```
[guest@eaabakumov dir1]$ lsattr  
-----a----- ./file1  
[guest@eaabakumov dir1]$ cat file1  
[guest@eaabakumov dir1]$ echo "test" > file1  
[guest@eaabakumov dir1]$ cat file1  
test  
[guest@eaabakumov dir1]$ echo "abcd" > /home/guest/dir1/file1  
[guest@eaabakumov dir1]$ cat file1  
abcd  
[guest@eaabakumov dir1]$ mv file1 hello_123  
[guest@eaabakumov dir1]$ ls  
hello_123  
[guest@eaabakumov dir1]$ cat hello_123  
abcd  
[guest@eaabakumov dir1]$ rm hello_123  
[guest@eaabakumov dir1]$ ls  
[guest@eaabakumov dir1]$ ls -a  
.
```

Figure 0.7: Тестирование файла без атрибута “a”

4. Попробуем то же самое для атрибута “i”. В этот раз у нас так же не вышло сделать ни одного действия, даже дозаписывания (иллюстр. 0.8, 0.9, 0.10)

```
[root@eaabakumov ~]# chattr +i /home/guest/dir1/file1  
[root@eaabakumov ~]#
```

Figure 0.8: Добавление атрибута “i”

```

[guest@eaabakumov dir1]$ lsattr
----i----- ./file1
[guest@eaabakumov dir1]$ cat file1
[guest@eaabakumov dir1]$ echo "test" > file1
bash: file1: Отказано в доступе
[guest@eaabakumov dir1]$ cat file1
[guest@eaabakumov dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Отказано в доступе
[guest@eaabakumov dir1]$ mv file1 hello_123
mv: невозможно переместить «file1» в «hello_123»: Операция не позволена
[guest@eaabakumov dir1]$ rm file1
rm: удалить защищенный от записи пустой обычный файл «file1»? y
rm: невозможно удалить «file1»: Операция не позволена
[guest@eaabakumov dir1]$ chmod 000 file1
chmod: изменение прав доступа для «file1»: Операция не позволена
[guest@eaabakumov dir1]$ ls -l
итого 0
-rw-----. 1 guest guest 0 окт 13 15:25 file1
[guest@eaabakumov dir1]$ lsattr

```

Figure 0.9: Тестирование файла с атрибутом “i”

```

[guest@eaabakumov dir1]$ lsattr
----i----- ./file1
[guest@eaabakumov dir1]$ echo "test_2_str" >> file1
bash: file1: Отказано в доступе
[guest@eaabakumov dir1]$ cat file1
test
[guest@eaabakumov dir1]$ █

```

Figure 0.10: Дозаписывание файла с атрибутом “i”

5. Теперь уберем атрибут “i” и попробуем все действия еще раз. На этот раз без проблем, штатно (иллюстр. 0.11, 0.12).

```

[root@eaabakumov ~]# chatter +i /home/guest/dir1/file1
[root@eaabakumov ~]# chatter -i /home/guest/dir1/file1
[root@eaabakumov ~]#

```

Figure 0.11: Удаление атрибута “i”

```

[guest@eaabakumov dir1]$ lsattr
----- ./file1
[guest@eaabakumov dir1]$ echo "test" > file1
[guest@eaabakumov dir1]$ cat file1
test
[guest@eaabakumov dir1]$ echo "abcd" > /home/guest/dir1/file1
[guest@eaabakumov dir1]$ cat file1
abcd
[guest@eaabakumov dir1]$ mv file1 hello_123
[guest@eaabakumov dir1]$ ls
hello_123
[guest@eaabakumov dir1]$ ls -l
итого 4
-rw-----. 1 guest guest 5 окт 13 15:29 hello_123
[guest@eaabakumov dir1]$ chmod 000 hello_123
[guest@eaabakumov dir1]$ ls -l
итого 4
-----. 1 guest guest 5 окт 13 15:29 hello_123
[guest@eaabakumov dir1]$ rm hello_123
rm: удалить защищенный от записи обычный файл «hello_123»? y
[guest@eaabakumov dir1]$ ls
[guest@eaabakumov dir1]$

```

Figure 0.12: Тестирование файла без атрибута “i”

Выводы

В ходе работы мы успешно получили практические навыки работы в консоли с расширенными атрибутами файлов.

Список литературы

1. Атрибуты файлов в Linux. // zalinux.ru. 2021. URL: <https://zalinux.ru/?p=6440> (дата обращения 13.10.2021).
2. КОМАНДА CHATTR В LINUX. // Losst. 2020. URL: <https://losst.ru/neizmenyaemye-fajly-v-linux> (дата обращения 13.10.2021).
3. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-математических и естественных наук. М.: РУДН, 2015. 64 с..