

Лабораторная работа № 4

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Усов Александр Александрович НБибд-02-18

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	13
	Список литературы	14

Список иллюстраций

4.1	lsattr /home/guest/dir1/file1	8
4.2	Команда chmod 600 file1	8
4.3	Расширенный атрибут а от имени пользователя guest	9
4.4	От имени суперпользователя	9
4.5	Проверили правильность установления атрибута	9
4.6	Дозапись в файл file1 слова «test»	10
4.7	Перезаписать текст в файле file1	10
4.8	Попробовали переименовать файл.	10
4.9	Попробовали с помощью команды chmod 000 file1 установить на файл	11
4.10	Сняли расширенный атрибут	11
4.11	Повторили действия с атрибутом «i»	12

Список таблиц

1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов

2 Задание

1. Создать файл file1
2. Установить расширенный атрибут a на файл и попробовать применить некоторые команды
3. Снять расширенный атрибут a с файла и попробовать применить команды без него
4. Установить атрибут i на файл и попробовать команды на нем.

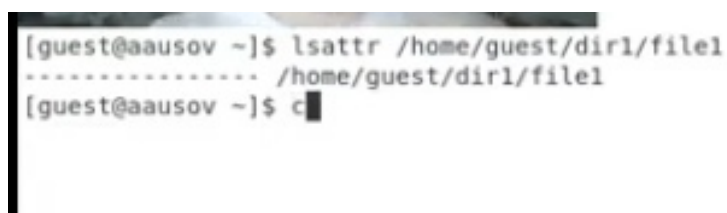
3 Теоретическое введение

Предположим вы хотите защитить некоторые важные файлы в Linux. При чем они должны быть защищены не только от перезаписи но и от случайного или преднамеренного удаления и перемещения. Предотвратить перезапись или изменение битов доступа к файлам можно с помощью стандартных утилит `chmod` и `chown`, но это не идеальное решение, так как у суперпользователя по прежнему остается полный доступ. Но есть еще одно решение. Это команда `chattr`. Эта утилита позволяет устанавливать и отключать атрибуты файлов, на уровне файловой системы не зависимо от стандартных (чтение, запись, выполнение). Для просмотра текущих атрибутов можно использовать `lsattr`. Изначально атрибуты управляемые `chattr` и `lsattr` поддерживались только файловыми системами семейства `ext` (`ext2`, `ext3`, `ext4`). но теперь эта возможность доступна и в других популярных файловых системах таких как `XFS`, `Btrfs`, `ReiserFS`, и т д.

Более подробно см. в [1].

4 Выполнение лабораторной работы

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



```
[guest@aausov ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@aausov ~]$ c
```

Рис. 4.1: lsattr /home/guest/dir1/file1

2. Установили командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла. (рис. 4.2).



```
[guest@aausov ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@aausov ~]$ cd dir1/
[guest@aausov dir1]$ chmod 600 file1
[guest@aausov dir1]$
```

Рис. 4.2: Команда chmod 600 file1

3. Попробовали установить на файл /home/guest/dir1/file1 расширенный атрибут а от имени пользователя guest: chattr +a /home/guest/dir1/file1. (рис. 4.3).


```
[guest@aausov ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@aausov ~]$ cd dir1/
[guest@aausov dir1]$ chmod 600 file1
[guest@aausov dir1]$ cd ..
[guest@aausov ~]$ chatter +a dir1/file1
chattr: Операция не позволена while setting flags on dir1/file1
[guest@aausov ~]$
```

Рис. 4.3: Расширенный атрибут а от имени пользователя guest

4. Повысили свои права с помощью команды su. Установили расширенный атрибут а на файл /home/guest/dir1/file1 от имени суперпользователя: chatter +a /home/guest/dir1/file1 (рис. 4.4).

```
[guest@aausov ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@aausov ~]$ cd dir1/
[guest@aausov dir1]$ chmod 600 file1
[guest@aausov dir1]$ cd ..
[guest@aausov ~]$ chatter +a dir1/file1
chattr: Операция не позволена while setting flags on dir1/file1
[guest@aausov ~]$ su
Пароль:
[root@aausov guest]# chat
chat    chatter
[root@aausov guest]# chatter +a dir1/file1
[root@aausov guest]# su
```

Рис. 4.4: От имени суперпользователя

5. От пользователя guest проверили правильность установления атрибута: lsattr /home/guest/dir1/file1 (рис. 4.5)

```
[guest@aausov ~]$ chatter +a dir1/file1
chattr: Операция не позволена while setting flags on dir1/file1
[guest@aausov ~]$ su
Пароль:
[root@aausov guest]# chat
chat    chatter
[root@aausov guest]# chatter +a dir1/file1
[root@aausov guest]# su guest
[guest@aausov ~]$ lsattr dir1/file1
-----a----- dir1/file1
[guest@aausov ~]$
```

Рис. 4.5: Проверили правильность установления атрибута

6. Выполнили дозапись в файл file1 слова «test» командой: echo “test” /home/guest/dir1/file1. (рис. 4.6)

```
[guest@aausov ~]$ su
Пароль:
[root@aausov guest]# chat
chat  chattr
[root@aausov guest]# chattr +a dir1/file1
[root@aausov guest]# su guest
[guest@aausov ~]$ lsattr dir1/file1
-----a----- dir1/file1
[guest@aausov ~]$ echo "test" dir1/file1
test dir1/file1
[guest@aausov ~]$
```

Рис. 4.6: Дозапись в файл file1 слова «test»

Далее выполнили чтение файла file1 командой cat /home/guest/dir1/file1. Убедились, что слово test было успешно записано в file1 (рис. 4.7)

7. Попробовали перезаписать текст в файле file1 командой echo “abcd”>/home/guest/dir1/file1 (рис. 4.7)

```
test9
[guest@aausov ~]$ lsattr dir1/file1
-----a----- dir1/file1
[guest@aausov ~]$ echo "test" /home/guest/dir1/file1
test /home/guest/dir1/file1
[guest@aausov ~]$ cat /home/guest/dir1/file1
test9
[guest@aausov ~]$ echo "abc"> /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Операция не позволена
[guest@aausov ~]$
```

Рис. 4.7: Перезаписать текст в файле file1

Попробовали переименовать файл. Но в каждом случае получили отказ. (рис. 4.8)

```
Аналогичная команда: 'dir'
[guest@aausov ~]$ cd dir1
[guest@aausov dir1]$ mv file1 file12
mv: невозможно переместить «file1» в «file12»: Операция не позволена
[guest@aausov dir1]$
```

Рис. 4.8: Попробовали переименовать файл.

8. Попробовали с помощью команды `chmod 000 file1` установить на файл `file1` права, запрещающие чтение и запись для владельца файла. Нам не удалось это сделать. (рис. 4.9)

```
diff      diff3      diff-jars diffpp      diffstat dig      dir
[guest@aausov ~]$ dir1
bash: dir1: команда не найдена...
Аналогичная команда: 'dir'
[guest@aausov ~]$ cd dir1
[guest@aausov dir1]$ mv file1 file12
mv: невозможно переместить «file1» в «file12»: Операция не позволена
[guest@aausov dir1]$ chmod 000 file1
chmod: изменение прав доступа для «file1»: Операция не позволена
```

Рис. 4.9: Попробовали с помощью команды `chmod 000 file1` установить на файл

9. Сняли расширенный атрибут `a` с файла `/home/guest/dir1/file1` от имени суперпользователя командой `chattr -a /home/guest/dir1/file1`. Повторили операции, которые нам ранее не удавалось выполнить. Ваши наблюдения занесите в отчёт. (рис. 4.10)

```
chmod: изменение прав доступа для «file1»: Операция не позволена
[guest@aausov dir1]$ su
Пароль:
[root@aausov dir1]# chattr -a file1
[root@aausov dir1]# su guest
[guest@aausov dir1]$ echo "test" file1
test file1
[guest@aausov dir1]$ cat file1
test9
[guest@aausov dir1]$ echo "abcd" > file1
[guest@aausov dir1]$ cat file1
abcd
[guest@aausov dir1]$ mv file1 file12
[guest@aausov dir1]$ ls
file12 file2 file3 newfile
[guest@aausov dir1]$
```

Рис. 4.10: Сняли расширенный атрибут

10. Повторили действия по шагам, заменив атрибут «`a`» (только добавление к файлу) атрибутом «`i`» (неизменяемый). (рис. 4.11)

```

\root@aausov dir1]# chattr +i file1
[root@aausov dir1]# su guest
[guest@aausov dir1]$ cat file1
abcd
[guest@aausov dir1]$ echo "test" file1
test file1
[guest@aausov dir1]$ cat file1
abcd
[guest@aausov dir1]$ echo "abcdef" > file1
bash: file1: Отказано в доступе
[guest@aausov dir1]$ mv file1 file 12
mv: указанная цель «12» не является каталогом
[guest@aausov dir1]$ mv file1 file12
mv: невозможно переместить «file1» в «file12»: Операция не позволена
[guest@aausov dir1]$ chattr 000 file1
Must use '-v', '=', '-' or '+'
[guest@aausov dir1]$ chmod 000 file1
chmod: изменение прав доступа для «file1»: Операция не позволена
[guest@aausov dir1]$

```

Рис. 4.11: Повторили действия с атрибутом «i»

5 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 «і».

Список литературы

1. Команда `chattr` в `linux` [Электронный ресурс]. Сайт, 2021. URL: <https://loss.t.ru/neizmenyaemye-fajly-v-linux>.