

Лабораторная работа №4

Основы информационной безопасности

Тойчубекова Асель Нурлановна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	11
6	Список литературы	12

Список иллюстраций

4.1	Установка прав доступа к файлу file1	8
4.2	Установка расширенного атрибута а на file1	8
4.3	Проверка разрешенных действий с атрибутом а	9
4.4	Попытка сменить права доступа к file1	9
4.5	Проверка действий без атрибута а	10
4.6	Изменение атрибута файла на i	10
4.7	Проверка разрешенных действий с атрибутом i	10

Список таблиц

1 Цель работы

Целью данной лабораторной работы является получение практических навыков работы в консоли с расширенными атрибутами файлов.

2 Задание

Выполнить все пункты в порядке выполнения лабораторной работы.

3 Теоретическое введение

В операционных системах на основе Linux и Unix расширенные атрибуты (extended attributes, xattr) представляют собой механизм, который позволяет добавлять метаданные к файлам и каталогам. Они дополняют стандартные права доступа (чтение, запись, исполнение), предоставляя дополнительные уровни защиты и управления файлами. Расширенные атрибуты полезны для обеспечения безопасности, защиты от случайного удаления или изменения, а также для системных и прикладных задач.

Одним из наиболее известных примеров использования расширенных атрибутов является флаг `immutable (i)`, который делает файл неизменяемым: его нельзя модифицировать, удалить или переименовать, даже если у пользователя есть права на запись. Другой важный атрибут — `append-only (a)`, который разрешает только добавление данных в файл, но запрещает их удаление или перезапись. Эти атрибуты полезны, например, в журналах системных логов или критически важных конфигурационных файлах.

Работа с расширенными атрибутами осуществляется с помощью команд `lsattr` (для просмотра атрибутов) и `chattr` (для их изменения). Например, команда `chattr +i file` делает файл неизменяемым, а `chattr -i file` снимает это ограничение (требуется `root`-права). Благодаря этим возможностям расширенные атрибуты широко применяются в системном администрировании, обеспечивая дополнительную защиту файлов от нежелательных изменений.

4 Выполнение лабораторной работы

От имени пользователя `guest` определим расширенные атрибуты файла `/home/guest/dir1/file1` командой `lsattr /home/guest/dir1/file1`. Далее установим на `file1` права, разрешающие чтение и запись для владельца файла. Затем попробуем установить на файл расширенный атрибут `a`. Мы видим, что нам отказано от выполнении операции. (рис. 4.1).

```
[guest@antoyjchubekova ~]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@antoyjchubekova ~]$ su
Password:
[root@antoyjchubekova guest]# chmod 600 dir1/file1
[root@antoyjchubekova guest]# exit
exit
[guest@antoyjchubekova ~]$ chattr +a /home/guest/dir1/file1
chattr: Permission denied while reading flags on /home/guest/dir1/file1
[guest@antoyjchubekova ~]$
```

Рис. 4.1: Установка прав доступа к файлу `file1`

Попробуем установить расширенный атрибут `a` на файл `/home/guest/dir1/file1` от имени суперпользователя. Затем правильность установки атрибута командой `lsattr`. Мы видим, что все было успешно установлено. (рис. 4.2).

```
guest@antoyjchubekova:~ x guest@antoyjchubekova:/home/gu... x
[guest@antoyjchubekova ~]$ su
Password:
[root@antoyjchubekova guest]# chattr +a /home/guest/dir1/file1
[root@antoyjchubekova guest]# lsattr /home/guest/dir1/file1
-----a----- /home/guest/dir1/file1
```

Рис. 4.2: Установка расширенного атрибута `a` на `file1`

Выполним запись в файл `file1` слова «test» командой `echo "test" > /home/guest/dir1/file1`. Затем проверим, выполнив чтение файла, командой `cat /home/guest/dir1/file1`.

Мы видим, что слово `test` было успешно записано в файл. Далее попробуем стереть имеющуюся в нем информацию и перезаписать ее командой `echo "abcd" > /home/guest/dir1/file1`. Мы видим, что нам было отказано в доступе, так как атрибут `i` позволяет только добавлять информацию, а не изменять ее. Также если мы попытаемся переименовать файл нам будет отказано в доступе. (рис. 4.3).

```
[root@antoyjchubekova guest]# echo "test" /home/guest/dir1/file1
test /home/guest/dir1/file1
[root@antoyjchubekova guest]# cat dir1/file1
test
[root@antoyjchubekova guest]# echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[root@antoyjchubekova guest]# mv dir1/file1 dir1/file3
mv: cannot move 'dir1/file1' to 'dir1/file3': Operation not permitted
[root@antoyjchubekova guest]#
```

Рис. 4.3: Проверка разрешенных действий с атрибутом `a`

Попробуем с помощью команды `chmod 000 file1` установить на файл `file1` права, например, запрещающие чтение и запись для владельца файла. Мы видим, что нам отказано в доступе. (рис. 4.4).

```
[root@antoyjchubekova guest]# chmod 000 dir1/file1
chmod: changing permissions of 'dir1/file1': Operation not permitted
[root@antoyjchubekova guest]#
```

Рис. 4.4: Попытка сменить права доступа к `file1`

Снимем расширенный атрибут `a` с файла `/home/guest/dir1/file1` от имени суперпользователя командой `chattr -a /home/guest/dir1/file1`. Теперь попробуем снова переписать информацию в `file1` и командой `cat` видим, что все успешно перезаписалось. Также при попытке перезаписать файл у нас все получилось. (рис. 4.5).

```

[root@antoyjchubekova guest]# chattr -a /home/guest/dirl/file1
[root@antoyjchubekova guest]# echo "abcd" > /home/guest/dirl/file1
bash: /home/guest/dirl/file1: No such file or directory
[root@antoyjchubekova guest]# echo "abcd" > /home/guest/dirl/file1
[root@antoyjchubekova guest]# cat dirl/file1
abcd
[root@antoyjchubekova guest]# mv dirl/file1 dirl/file3
[root@antoyjchubekova guest]# ls
Desktop  Documents  file2  Music      Public      Videos
dirl     Downloads  file3  Pictures  Templates
[root@antoyjchubekova guest]# ls dirl
file3
[root@antoyjchubekova guest]#

```

Рис. 4.5: Проверка действий без атрибута а

Повторим наши действия по шагам, заменив атрибут «а» атрибутом «і». (рис. 4.6).

```

[root@antoyjchubekova guest]# chattr +i /home/guest/dirl/file1
[root@antoyjchubekova guest]# lsattr /home/guest/dirl/file1
----i----- /home/guest/dirl/file1
[root@antoyjchubekova guest]#

```

Рис. 4.6: Изменение атрибута файла на і

Попробуем записать текст в файл. Мы видим, что нам отказано в доступе. С помощью команды cat мы видим, что информация не перезаписана. Попробуем перезаписать информацию в файле. Мы видим, что нам также отказано в доступе. Затем если мы попробуем удалить или переименовать файл нам также отказано в доступе. Изменить права доступа у нас также не получается. (рис. 4.7).

```

[root@antoyjchubekova guest]# lsattr /home/guest/dirl/file1
----i----- /home/guest/dirl/file1
[root@antoyjchubekova guest]# echo "test" > /home/guest/dirl/file1
bash: /home/guest/dirl/file1: Operation not permitted
[root@antoyjchubekova guest]# cat /home/guest/dirl/file1
abcd
[root@antoyjchubekova guest]# echo "abcd" > /home/guest/dirl/file1
bash: /home/guest/dirl/file1: No such file or directory
[root@antoyjchubekova guest]# echo "abcd" > /home/guest/dirl/file1
bash: /home/guest/dirl/file1: Operation not permitted
[root@antoyjchubekova guest]# rm dirl/file1
rm: remove regular file 'dirl/file1'?
[root@antoyjchubekova guest]# rm dirl/file1
rm: remove regular file 'dirl/file1'? y
rm: cannot remove 'dirl/file1': Operation not permitted
[root@antoyjchubekova guest]# mv dirl/file1 dirl/file3
mv: cannot move 'dirl/file1' to 'dirl/file3': Operation not permitted
[root@antoyjchubekova guest]# chmod 000 file1
chmod: cannot access 'file1': No such file or directory
[root@antoyjchubekova guest]# chmod 000 dirl/file1
chmod: changing permissions of 'dirl/file1': Operation not permitted
[root@antoyjchubekova guest]#

```

Рис. 4.7: Проверка разрешенных действий с атрибутом і

5 Выводы

В ходе выполнения лабораторной работы №4 я получила практические навыки работы в консоли с расширенными атрибутами файлов.

6 Список литературы

- https://esystem.rudn.ru/pluginfile.php/2580982/mod_resource/content/3/004-lab_discret_extattr.pdf