

Основы информационной безопасности

**Лабораторная работа № 4 | Дискреционное разграничение прав в
Linux. Расширенные атрибуты**

Мугари Абдеррахим - НКАбд-03-22

Содержание

1	Цель работы	5
2	Выполнение лабораторной работы	6
2.1	выводы по результатам выполнения заданий:	10
3	Выводы, согласованные с целью работы:	11

Список иллюстраций

2.1	определение расширенных атрибутов и предоставление файлу прав на чтение и запись	6
2.2	попытка присвоить файлу расширенный атрибут без прав супер-пользователя	7
2.3	добавление расширенного атрибута в файл	7
2.4	добавление информации в файл с расширенным атрибутом а . . .	7
2.5	попытка выполнить некоторые операции с файлом с расширенным атрибутом	8
2.6	удаление расширенного атрибута из файла и повторное выполнение команды, которые не были разрешены	8
2.7	удаление расширенного атрибута из файла и повторное выполнение команды, которые не были разрешены	9
2.8	добавление атрибута i и повторение предыдущих команд	9
2.9	добавление атрибута i и повторение предыдущих команд	10

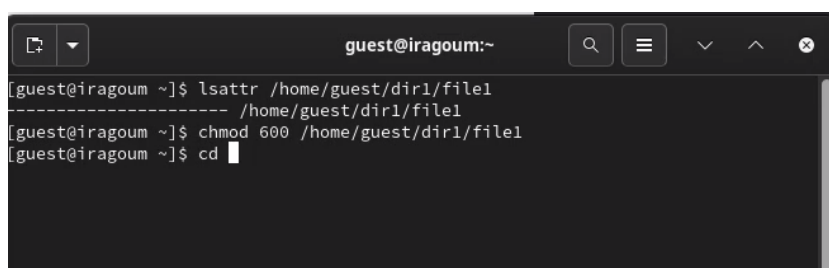
Список таблиц

1 Цель работы

- Получение практических навыков работы в консоли с расширенными атрибутами файлов

2 Выполнение лабораторной работы

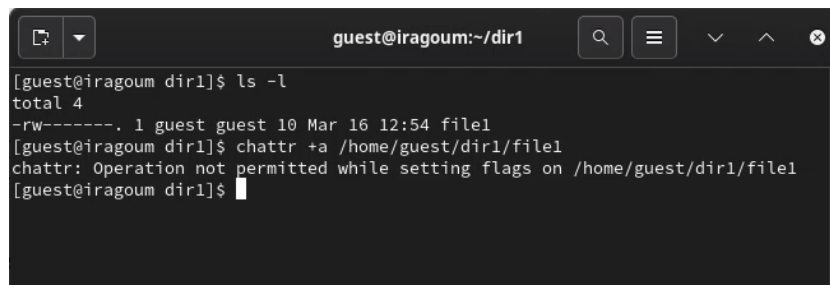
1. От имени гостевого пользователя мы определили расширенные атрибуты файла `/home/guest/dir1/file1` с помощью команды `lsattr /home/guest/dir1/file1`, а затем с помощью команды `chmod 600 file1` мы устанавливаем права на чтение и запись для владельца файла в файле `file1` (рис. 2.1).



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

Рис. 2.1: определение расширенных атрибутов и предоставление файлу прав на чтение и запись

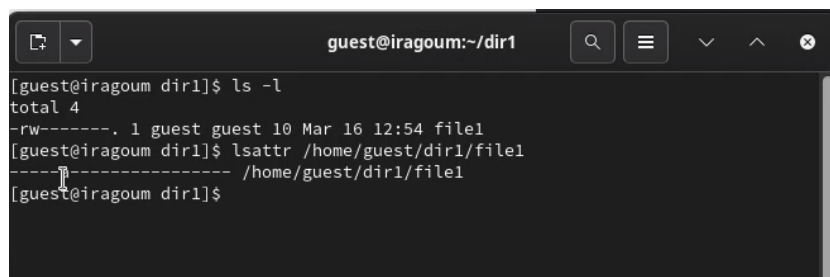
2. после этого мы пытаемся установить расширенный атрибут `a` от имени пользователя `guest` в файл `/home/guest/dir1/file1`, используя команду `chattr +a /home/guest/dir1/file1`, но операция была прервана, поскольку она должна выполняться с суперпользователем привилегии (рис. 2.2).



```
guest@iragoum:~/dir1
[guest@iragoum dir1]$ ls -l
total 4
-rw-----. 1 guest guest 10 Mar 16 12:54 file1
[guest@iragoum dir1]$ chattr +a /home/guest/dir1/file1
chattr: Operation not permitted while setting flags on /home/guest/dir1/file1
[guest@iragoum dir1]$
```

Рис. 2.2: попытка присвоить файлу расширенный атрибут без прав суперпользователя

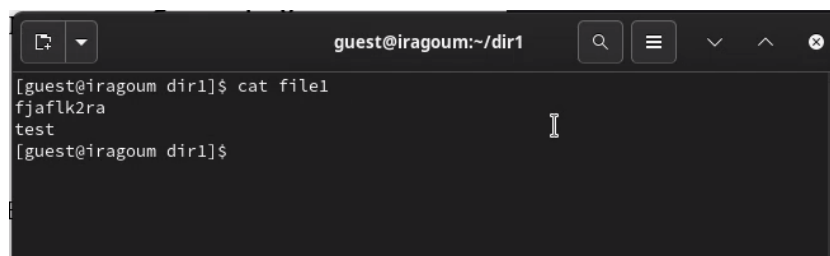
3. после этого с помощью команды **su** мы получили доступ к суперпользователю и добавили расширенный атрибут, и мы проверили это с помощью команды **lsattr /home/guest/dir1/file1** (рис. 2.3).



```
guest@iragoum:~/dir1
[guest@iragoum dir1]$ ls -l
total 4
-rw-----. 1 guest guest 10 Mar 16 12:54 file1
[guest@iragoum dir1]$ lsattr /home/guest/dir1/file1
-----+----- /home/guest/dir1/file1
[guest@iragoum dir1]$
```

Рис. 2.3: добавление расширенного атрибута в файл

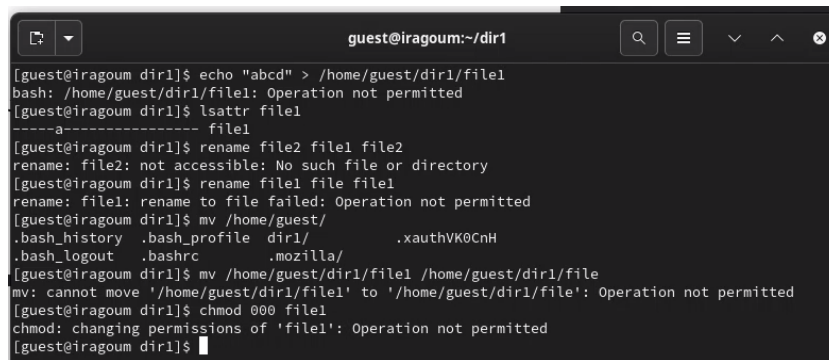
4. после этого мы добавили слово “test” в файл file1 с помощью команды **echo “test” » /home/guest/dir1/file1**, а затем мы проверили, было ли добавлено слово, прочитав файл с помощью команды **cat file1** (рис. 2.4).



```
guest@iragoum:~/dir1
[guest@iragoum dir1]$ cat file1
fjafk2ra
test
[guest@iragoum dir1]$
```

Рис. 2.4: добавление информации в файл с расширенным атрибутом а

5. на этом шаге мы попытались стереть содержащуюся в нем информацию с помощью команды **echo "abcd" > /home/guest/dir/file1**, что было запрещено из-за расширенного атрибута, затем мы попытались переименовать файл и даже удалить его права, но все это было запрещено, все благодаря расширенному атрибуту **a** (рис. 2.5).



```
guest@iragoum:~/dir1
[guest@iragoum dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[guest@iragoum dir1]$ lsattr file1
-----a----- file1
[guest@iragoum dir1]$ rename file2 file1 file2
rename: file2: not accessible: No such file or directory
[guest@iragoum dir1]$ rename file1 file file1
rename: file1: rename to file failed: Operation not permitted
[guest@iragoum dir1]$ mv /home/guest/
.bash_history .bash_profile dir1/ .xauthVK0CnH
.bash_logout .bashrc .mozilla/
[guest@iragoum dir1]$ mv /home/guest/dir1/file1 /home/guest/dir1/file
mv: cannot move '/home/guest/dir1/file1' to '/home/guest/dir1/file': Operation not permitted
[guest@iragoum dir1]$ chmod 000 file1
chmod: changing permissions of 'file1': Operation not permitted
[guest@iragoum dir1]$
```

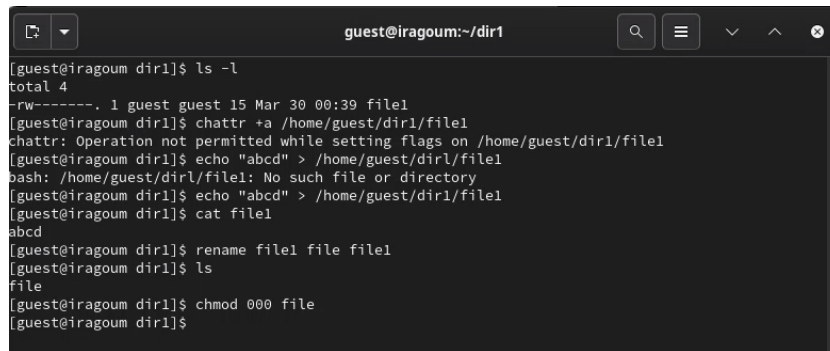
Рис. 2.5: попытка выполнить некоторые операции с файлом с расширенным атрибутом

6. затем мы удалили расширенный атрибут **a** из файла **/home/guest/dir/file1** от имени суперпользователя командой **chattr -a /home/guest/dir1/file1** и после повторения операций, которые были отклонены, все они были выполнены (рис. 2.6) (рис. 2.6) (рис. 2.7).



```
guest@iragoum:~/dir1
[guest@iragoum dir1]$ su
Password:
[root@iragoum dir1]# chattr -a /home/
guest/ guest2/ iragoum/
[root@iragoum dir1]# chattr -a file1
[root@iragoum dir1]# exit
exit
[guest@iragoum dir1]$
```

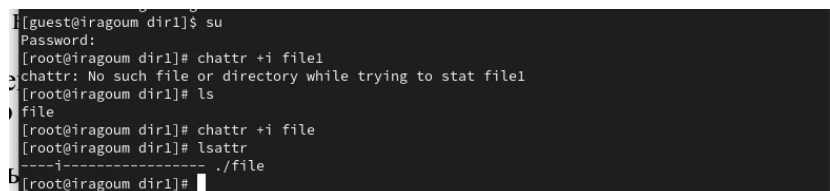
Рис. 2.6: удаление расширенного атрибута из файла и повторное выполнение команд, которые не были разрешены

A terminal window titled 'guest@iragoum:~/dir1' showing a series of commands and their outputs. The user lists the file 'file1', attempts to set the 'a' attribute with 'chattr +a', which fails with a permission error. They then echo 'abcd' into 'file1', verify its content with 'cat', rename it to 'file', and finally set permissions to '000' with 'chmod 000 file'.

```
guest@iragoum:~/dir1
[guest@iragoum dir1]$ ls -l
total 4
-rw-----. 1 guest guest 15 Mar 30 00:39 file1
[guest@iragoum dir1]$ chattr +a /home/guest/dir1/file1
chattr: Operation not permitted while setting flags on /home/guest/dir1/file1
[guest@iragoum dir1]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: No such file or directory
[guest@iragoum dir1]$ echo "abcd" > /home/guest/dir1/file1
[guest@iragoum dir1]$ cat file1
abcd
[guest@iragoum dir1]$ rename file1 file file1
[guest@iragoum dir1]$ ls
file
[guest@iragoum dir1]$ chmod 000 file
[guest@iragoum dir1]$
```

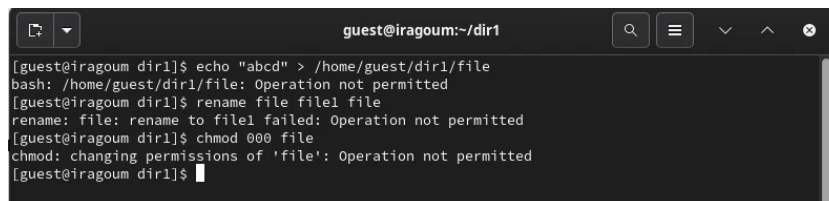
Рис. 2.7: удаление расширенного атрибута из файла и повторное выполнение команды, которые не были разрешены

7. и, наконец, мы повторили шаги, заменив атрибут “a” атрибутом “i”. и переделал операцию в файле, и в этом случае все они были запрещены, потому что i (неизменяемый): Когда атрибут i установлен для файла, он делает файл неизменяемым, что означает, что его содержимое нельзя изменить, удалить, переименовать или связать с ним. Даже суперпользователь (root) не может изменить или удалить файл, пока не будет удален атрибут i. Этот атрибут обычно используется для критически важных системных файлов для предотвращения случайных или несанкционированных изменений (рис. 2.8).

A terminal window showing the user switching to root with 'su', then attempting to set the 'i' attribute with 'chattr +i file1'. This also fails with a permission error. The user then lists the file and attempts to set the 'i' attribute on 'file' (which is 'file1' renamed), which also fails.

```
[guest@iragoum dir1]$ su
Password:
[root@iragoum dir1]# chattr +i file1
chattr: No such file or directory while trying to stat file1
[root@iragoum dir1]# ls
file
[root@iragoum dir1]# chattr +i file
[root@iragoum dir1]# lsattr
-----i----- ./file
[root@iragoum dir1]#
```

Рис. 2.8: добавление атрибута i и повторение предыдущих команд

A terminal window titled 'guest@iragoum:~/dir1' with a search bar and window controls. The terminal shows the following commands and output:

```
[guest@iragoum dir1]$ echo "abcd" > /home/guest/dir1/file
bash: /home/guest/dir1/file: Operation not permitted
[guest@iragoum dir1]$ rename file file1 file
rename: file: rename to file1 failed: Operation not permitted
[guest@iragoum dir1]$ chmod 000 file
chmod: changing permissions of 'file': Operation not permitted
[guest@iragoum dir1]$
```

Рис. 2.9: добавление атрибута i и повторение предыдущих команд

2.1 выводы по результатам выполнения заданий:

- К концу лабораторной работы мы приобрели практические навыки работы в консоли с атрибутами файлов для различных групп пользователей, понимая, как:
 1. Ограничивать доступ к файлам с помощью установки расширенных атрибутов.
 2. Работать с различными уровнями привилегий пользователей, включая суперпользователя.
 3. Проверять установку атрибутов и их воздействие на файлы.
 4. Использовать атрибуты а и i для защиты файлов от изменений и удаления.
 5. Проводить тесты, чтобы убедиться в правильной установке атрибутов и их воздействии на файлы.

3 Выводы, согласованные с целью работы:

- К концу лабораторной работы мы приобрели практические навыки работы в консоли с атрибутами файлов для различных групп пользователей