

Отчёт по лабораторной работе №4

Основы информационной безопасности

Машков Илья Евгеньевич

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
3.1	Работа с расширенными атрибутами файлов	7
4	Выводы	11
	Список литературы	12

Список иллюстраций

3.1	Проверка расширенных атрибутов.	7
3.2	Изменение прав у файла.	7
3.3	Попытка установки расширенных атрибутов от имени обычного пользователя.	7
3.4	Добавление расширенного атрибута от имени суперпользователя.	8
3.5	Проверка атрибутов у файла.	8
3.6	Дозапись и чтение.	8
3.7	Удаление.	8
3.8	Переименование файла.	9
3.9	Изменение прав у файла при установленном атрибуте.	9
3.10	Удаление расширенного атрибута.	9
3.11	Повторный прогон вышеперечисленных операций.	9
3.12	Попытка установки атрибута i на тот же файл.	9
3.13	Попытка установки атрибута i на тот же файл от имени суперпользователя.	10
3.14	Ещё один прогон команд, но при атрибуте i.	10

Список таблиц

1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

2 Задание

1. Работа с расширенными атрибутами файлов.

3 Выполнение лабораторной работы

3.1 Работа с расширенными атрибутами файлов

1. Для начала от имени пользователя, созданного в прошлой лабе, просматриваю какие расширенные атрибуты имеются у файла `dir1/file1` (спойлер: их нет) (рис. 3.1).

```
[guest@localhost ~]$ lsattr dir1/file1
----- dir1/file1
```

Рис. 3.1: Проверка расширенных атрибутов.

2. Изменяю права доступа у этого файла на `600` (рис. 3.2).

```
[guest@localhost ~]$ chmod 600 dir1/file1
[guest@localhost ~]$
```

Рис. 3.2: Изменение прав у файла.

3. Теперь пробую от имени моего пользователя выдать расширенный атрибут а данному файлу, но получаю отказ (рис. 3.3).

```
[guest@localhost ~]$ chattr +a dir1/file1
chattr: Отказано в доступе while reading flags on dir1/file1
```

Рис. 3.3: Попытка установки расширенных атрибутов от имени обычного пользователя.

4. Делаю то же самое, но от имени суперпользователя, и в этот раз всё получилось (рис. 3.4).

```
[iemashkov@localhost guest]$ sudo chattr +a /home/guest/dir1/file1  
[sudo] пароль для iemashkov:  
[iemashkov@localhost guest]$
```

Рис. 3.4: Добавление расширенного атрибута от имени суперпользователя.

5. Теперь проверяю то, что атрибут был выдан, от имени guest (рис. 3.5).

```
[guest@localhost ~]$ lsattr dir1/file1  
-----a----- dir1/file1  
[guest@localhost ~]$
```

Рис. 3.5: Проверка атрибутов у файла.

6. Пробую произвести дозапись и чтение данного файла и не получаю отказа (рис. 3.6).

```
[guest@localhost ~]$ echo "test" >> dir1/file1  
[guest@localhost ~]$ cat dir1/file1  
test  
test  
[guest@localhost ~]$
```

Рис. 3.6: Дозапись и чтение.

7. Но при удалении я получаю отказ (рис. 3.7).

```
[guest@localhost ~]$ rm dir1/file1  
rm: невозможно удалить 'dir1/file1': Операция не позволена  
[guest@localhost ~]$
```

Рис. 3.7: Удаление.

8. Отказ получаю и при переименовании файла (рис. 3.8).


```
[guest@localhost ~]$ mv dir1/file1 dir1/abcdf
mv: невозможно переместить 'dir1/file1' в 'dir1/abcdf': Операция не позволена
[guest@localhost ~]$
```

Рис. 3.8: Переименование файла.

9. Такой же результат и при изменении прав у файла (рис. 3.9).

```
[guest@localhost ~]$ chmod 000 dir1/file1
chmod: изменение прав доступа для 'dir1/file1': Операция не позволена
[guest@localhost ~]$
```

Рис. 3.9: Изменение прав у файла при установленном атрибуте.

10. Теперь от имени суперпользователя снимаю этот атрибут (рис. 3.10).

```
[iemashkov@localhost guest]$ sudo chattr -a /home/guest/dir1/file1
[sudo] пароль для iemashkov:
[iemashkov@localhost guest]$ sudo lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[iemashkov@localhost guest]$
```

Рис. 3.10: Удаление расширенного атрибута.

И снова делаю прогон всё тех же операций, но в этот раз отказа не получаю (кроме того, где я немного поторопился) (рис. 3.11).

```
[guest@localhost ~]$ echo "adkdakd" > dir1/file1
[guest@localhost ~]$ cat dir1/file1
adkdakd
[guest@localhost ~]$ mv dir1/file1 dir1/abcdf
[guest@localhost ~]$ chmod 000 dir1/file1
chmod: невозможно получить доступ к 'dir1/file1': Нет такого файла или каталога
[guest@localhost ~]$ mv dir1/abcdf dir1/file1
[guest@localhost ~]$ chmod 000 dir1/file1
[guest@localhost ~]$
```

Рис. 3.11: Повторный прогон вышеперечисленных операций.

11. Теперь добавляю атрибут *i* на тот же файл от обычного пользователя, но, ожидаемо, получаю отказ (рис. 3.12).

```
[guest@localhost ~]$ chattr +i dir1/file1
chattr: Отказано в доступе while reading flags on dir1/file1
[guest@localhost ~]$
```

Рис. 3.12: Попытка установки атрибута *i* на тот же файл.

Т.к. от имени обычного пользователя ничего не вышло, я ставлю этот атрибут от имени суперпользователя (рис. 3.13).

```
[iemashkov@localhost guest]$ sudo chattr +i /home/guest/dirl/file1
[iemashkov@localhost guest]$ sudo lsattr /home/guest/dirl/file1
----i----- /home/guest/dirl/file1
[iemashkov@localhost guest]$
```

Рис. 3.13: Попытка установки атрибута *i* на тот же файл от имени суперпользователя.

12. Делаю ещё один прогон таких операций как: дозапись, перезапись, чтение, переименование, удаление и изменение прав – но ничего не выходит (рис. 3.14).

```
[guest@localhost ~]$ echo "test" > dirl/file1
bash: dirl/file1: Операция не позволена
[guest@localhost ~]$ echo "test" >> dirl/file1
bash: dirl/file1: Операция не позволена
[guest@localhost ~]$ cat dirl/file1
cat: dirl/file1: Отказано в доступе
[guest@localhost ~]$ mv dirl/file1 dirl/abcdf
mv: невозможно переместить 'dirl/file1' в 'dirl/abcdf': Операция не позволена
[guest@localhost ~]$ rm dirl/file1
rm: невозможно удалить 'dirl/file1': Операция не позволена
[guest@localhost ~]$
```

Рис. 3.14: Ещё один прогон команд, но при атрибуте *i*.

4 Выводы

В результате выполнения работы я повысил свои навыки использования интерфейса командой строки (CLI), познакомился на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имел возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux. Опробовал действие на практике расширенных атрибутов «a» и «i»

Список литературы

Основы информационной безопасности

Права доступа

Расширенные атрибуты

Операции с расширенными атрибутами