

Отчёт по лабораторной работе №4

Дисциплина: Основы информационной безопасности

Маметкадыров Ынтымак, НПМбд-02-20

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	6
Выводы	9
Список литературы	10

List of Figures

0.1	Проверка расширенных атрибутов	6
0.2	Установка расширенного атрибута а	7
0.3	Проверка действий при наличии атрибута а	7
0.4	Проверка действий при отсутствии атрибута а	8
0.5	Проверка действий при наличии атрибута і	8

Цель работы

Получить навыки работы в консоли с расширенными атрибутами файлов.

Теоретическое введение

Атрибуты — это набор основных девяти битов, определяющих какие из пользователей обладают правами на чтение, запись и исполнение. Первые три бита отвечают права доступа владельца, вторые — для группы пользователей, последние — для всех остальных пользователей в системе.

Установка атрибутов производится командой `chmod`. Установка бита чтения (`r`) позволяет сделать файл доступным для чтения. Наличие бита записи (`w`) позволяет изменять файл. Установка бита запуска (`x`) позволяет запускать файл на исполнение.

Более подробно см. в `[@gnu-doc:bash]`.

Расширенные атрибуты — это система дополнительной информации, которая может быть добавлена к файлу или директории в файловой системе.

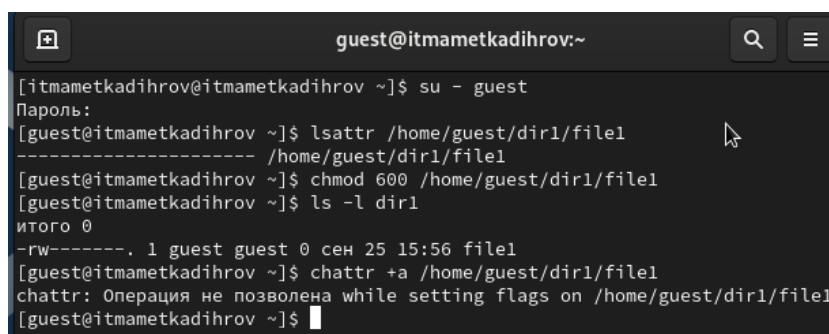
Некоторые примеры расширенных атрибутов:

- `a` — файл можно открыть только в режиме добавления.
- `A` — при доступе к файлу его запись `atime` не изменяется.
- `s` — файл автоматически сжимается.
- `e` — файл использует экстенды.
- `E` — файл, каталог или символьная ссылка зашифрованы файловой системой.
- `F` — поиски путей в директории выполняются без учёта регистра.
- `i` — файл не может быть изменён.
- `m` — файл не сжимается.

Более подробно см. в `[@gnu-doc-1:bash]`

Выполнение лабораторной работы

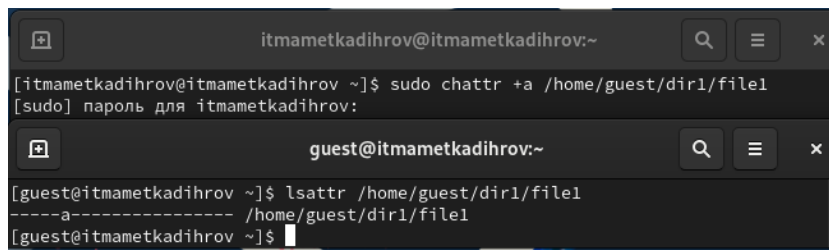
От имени пользователя guest посмотрим расширенные атрибуты файла file1 с помощью команды `lsattr`. Далее изменим права на этот файл с помощью команды `chmod 600 file1`, сделав его доступным только для чтения и записи. После этого при попытке добавить расширенный атрибут с помощью команды `chattr` мы получаем сообщение об ошибке (рис. [-@fig:001]).



```
guest@itmametskadihrov:~  
[itmametskadihrov@itmametskadihrov ~]$ su - guest  
Пароль:  
[guest@itmametskadihrov ~]$ lsattr /home/guest/dir1/file1  
----- /home/guest/dir1/file1  
[guest@itmametskadihrov ~]$ chmod 600 /home/guest/dir1/file1  
[guest@itmametskadihrov ~]$ ls -l dir1  
итого 0  
-rw-----. 1 guest guest 0 сен 25 15:56 file1  
[guest@itmametskadihrov ~]$ chattr +a /home/guest/dir1/file1  
chattr: Операция не позволена while setting flags on /home/guest/dir1/file1  
[guest@itmametskadihrov ~]$
```

Figure 0.1: Проверка расширенных атрибутов

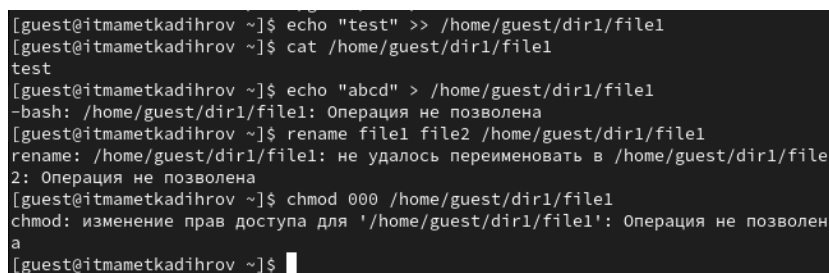
От имени администратора в другой консоли добавляем файлу file1 атрибут `a` командой `chattr +a`. Убеждаемся в корректном установлении атрибута с помощью команды `lsattr` (рис. [-@fig:002]).



```
itmametkadihrov@itmametkadihrov:~  
[itmametkadihrov@itmametkadihrov ~]$ sudo chatter +a /home/guest/dir1/file1  
[sudo] пароль для itmametkadihrov:  
  
guest@itmametkadihrov:~  
[guest@itmametkadihrov ~]$ lsattr /home/guest/dir1/file1  
-----a----- /home/guest/dir1/file1  
[guest@itmametkadihrov ~]$
```

Figure 0.2: Установка расширенного атрибута а

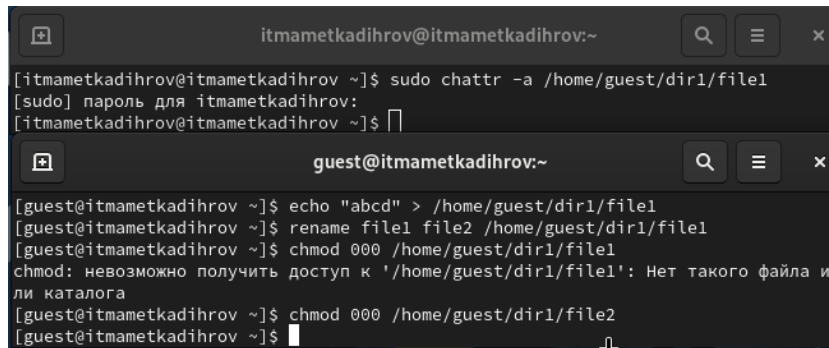
Дозаписываем в конец файла новую информацию с помощью команды `echo` » и проверяем, что это действительно произошло, командой `cat`. Далее пытаемся стереть информацию в файле с помощью команды `echo >`, на что получаем ошибку. Также не удаётся переименовать файл и изменить его атрибуты командой `chmod` из-за той же ошибки в правах доступа (рис. [-@fig:003]).



```
[guest@itmametkadihrov ~]$ echo "test" >> /home/guest/dir1/file1  
[guest@itmametkadihrov ~]$ cat /home/guest/dir1/file1  
test  
[guest@itmametkadihrov ~]$ echo "abcd" > /home/guest/dir1/file1  
-bash: /home/guest/dir1/file1: Операция не позволена  
[guest@itmametkadihrov ~]$ rename file1 file2 /home/guest/dir1/file1  
rename: /home/guest/dir1/file1: не удалось переименовать в /home/guest/dir1/file  
2: Операция не позволена  
[guest@itmametkadihrov ~]$ chmod 000 /home/guest/dir1/file1  
chmod: изменение прав доступа для '/home/guest/dir1/file1': Операция не позволен  
a  
[guest@itmametkadihrov ~]$
```

Figure 0.3: Проверка действий при наличии атрибута а

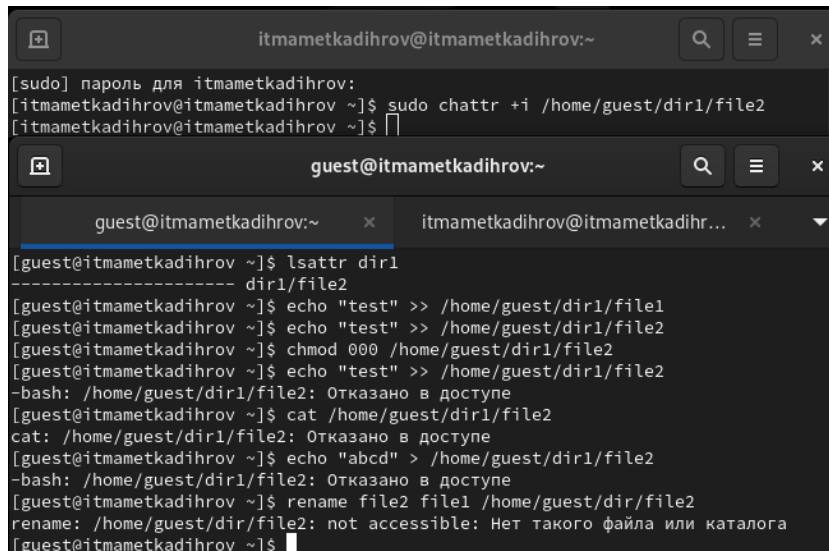
Снимаем расширенный атрибут `a` командой `chattr -a` от лица администратора. При повторе ранее описанных действий теперь не произошло ошибок и они все выполнились (рис. [-@fig:004]).



```
itmametkadihrov@itmametkadihrov:~  
[itmametkadihrov@itmametkadihrov ~]$ sudo chattr -a /home/guest/dir1/file1  
[sudo] пароль для itmametkadihrov:  
[itmametkadihrov@itmametkadihrov ~]$  
guest@itmametkadihrov:~  
[guest@itmametkadihrov ~]$ echo "abcd" > /home/guest/dir1/file1  
[guest@itmametkadihrov ~]$ rename file1 file2 /home/guest/dir1/file1  
[guest@itmametkadihrov ~]$ chmod 000 /home/guest/dir1/file1  
chmod: невозможно получить доступ к '/home/guest/dir1/file1': Нет такого файла и  
ли каталога  
[guest@itmametkadihrov ~]$ chmod 000 /home/guest/dir1/file2  
[guest@itmametkadihrov ~]$
```

Figure 0.4: Проверка действий при отсутствии атрибута a

От имени администратора добавим файлу расширенный атрибут i и повторим ранее описанные действия. По итогу получаем, что в этом случае файл можно только читать, но нельзя никак изменить. (рис. [-@fig:005]).



```
itmametkadihrov@itmametkadihrov:~  
[sudo] пароль для itmametkadihrov:  
[itmametkadihrov@itmametkadihrov ~]$ sudo chattr +i /home/guest/dir1/file2  
[itmametkadihrov@itmametkadihrov ~]$  
guest@itmametkadihrov:~  
guest@itmametkadihrov:~ x itmametkadihrov@itmametkadihr... x  
[guest@itmametkadihrov ~]$ lsattr dir1  
----- dir1/file2  
[guest@itmametkadihrov ~]$ echo "test" >> /home/guest/dir1/file1  
[guest@itmametkadihrov ~]$ echo "test" >> /home/guest/dir1/file2  
[guest@itmametkadihrov ~]$ chmod 000 /home/guest/dir1/file2  
[guest@itmametkadihrov ~]$ echo "test" >> /home/guest/dir1/file2  
-bash: /home/guest/dir1/file2: Отказано в доступе  
[guest@itmametkadihrov ~]$ cat /home/guest/dir1/file2  
cat: /home/guest/dir1/file2: Отказано в доступе  
[guest@itmametkadihrov ~]$ echo "abcd" > /home/guest/dir1/file2  
-bash: /home/guest/dir1/file2: Отказано в доступе  
[guest@itmametkadihrov ~]$ rename file2 file1 /home/guest/dir/file2  
rename: /home/guest/dir/file2: not accessible: Нет такого файла или каталога  
[guest@itmametkadihrov ~]$
```

Figure 0.5: Проверка действий при наличии атрибута i

Выводы

Приобрели практические навыки работы с расширенными атрибутами файлов через консоль, опробовали на практике действия с файлами с установленными на них расширенными атрибутами а и і.

Список литературы

- Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: <http://bugtraq.ru/library/books/attack1/index.html>
- Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: <http://bugtraq.ru/library/books/attack/index.html>
- Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.
- Введение в информационную безопасность. Типы уязвимостей. (Д.Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Вводная лекция. Сетевая безопасность. Стек протоколов TCP/IP. (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Межсетевые экраны. (В. Иванов, МГУ)
- Практические аспекты сетевой безопасности. Сетевая безопасность. Системы обнаружения и фильтрации компьютерных атак (IDS/IPS). (Д. Гамаюнов, МГУ)
- Практические аспекты сетевой безопасности. Контроль нормального поведения приложений. Security Enhanced Linux (SELinux) (В. Сахаров, МГУ)