

Лабораторная работа №4

Дисциплина: Основы информационной безопасности

Коновалова Татьяна Борисовна

Содержание

1	Цель работы	5
2	Теоретические данные	6
3	Задание	8
4	Выполнение лабораторной работы	9
5	Выводы	12
6	Библиография	13

Список иллюстраций

4.1	Проверка расширенных атрибутов	9
4.2	Установка расширенного атрибута а	9
4.3	Проверка корректности установки атрибута +а	10
4.4	Проверка действий при наличии атрибута а	10
4.5	Проверка действий при отсутствии атрибута а	11
4.6	Установка атрибута і	11
4.7	Проверка действий при наличии атрибута і	11

Список таблиц

1 Цель работы

Цель данной лабораторной работы — Получить навыки работы в консоли с расширенными атрибутами файлов.

2 Теоретические данные

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.

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.
- `c` — 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.

Установка атрибутов производится командой `chmod`. Установка бита чтения (`r`) позволяет сделать файл доступным для чтения. Наличие бита записи (`w`) поз-

воляет изменять файл. Установка бита запуска (x) позволяет запускать файл на исполнение.

В ОС Linux, группа — это набор пользователей. Основная цель групп — это определить права на чтение, запись и исполнение сразу для нескольких пользователей, состоящих в группе. Так же пользователи могут быть добавлены в уже существующие группы для получения их прав.

Группы бывают двух видов:

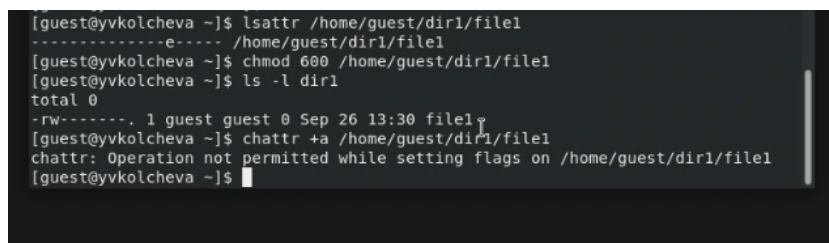
- Первичная группа — это группа, приписанная к файлам, созданным пользователем. Обычно имя первичной группы совпадает с именем пользователя. У каждого пользователя может быть только одна первичная группа.
- Вторичная группа — используется для определения прав для набора пользователей. Пользователь может состоять в нескольких вторичных группах или не состоять ни в одной.

3 Задание

1.Определить расширенные атрибуты файла в Виртуальной машине. 2.Установка расширенного атрибута “а” на файл 3.Снять расширенные атрибуты “а” с файла

4 Выполнение лабораторной работы

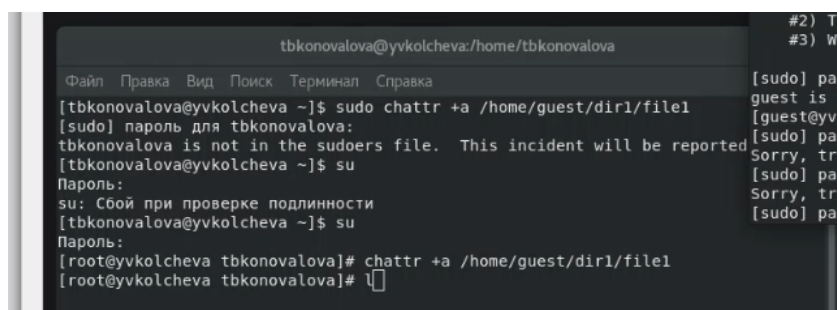
1). От имени пользователя guest просмотрела расширенные атрибуты файла file1 с помощью команды lsattr. После этого изменила права на этот файл с помощью команды chmod 600 file1, сделав его доступным только для чтения и записи. Далее при попытке добавить расширенный атрибут с помощью команды chattr я получила сообщение об ошибке (рис. [4.1]).



```
[guest@yvvkolcheva ~]$ lsattr /home/guest/dir1/file1
-----e----- /home/guest/dir1/file1
[guest@yvvkolcheva ~]$ chmod 600 /home/guest/dir1/file1
[guest@yvvkolcheva ~]$ ls -l dir1
total 0
-rw-----. 1 guest guest 0 Sep 26 13:30 file1
[guest@yvvkolcheva ~]$ chattr +a /home/guest/dir1/file1
chattr: Operation not permitted while setting flags on /home/guest/dir1/file1
[guest@yvvkolcheva ~]$
```

Рис. 4.1: Проверка расширенных атрибутов

2). От имени администратора в другой консоли добавила файлу file1 атрибут а командой chattr +a. Также убедилась в корректном установлении атрибута с помощью команды lsattr (рис. [4.2]) и (рис. [4.3]).



```
tbkonovalova@yvvkolcheva:/home/tbkonovalova
Файл Правка Вид Поиск Терминал Справка
[tbkonovalova@yvvkolcheva ~]$ sudo chattr +a /home/guest/dir1/file1
[sudo] пароль для tbkonovalova:
tbkonovalova is not in the sudoers file. This incident will be reported.
[tbkonovalova@yvvkolcheva ~]$ su
Пароль:
su: Сбой при проверке подлинности
[tbkonovalova@yvvkolcheva ~]$ su
Пароль:
[root@yvvkolcheva tbkonovalova]# chattr +a /home/guest/dir1/file1
[root@yvvkolcheva tbkonovalova]#
```

Рис. 4.2: Установка расширенного атрибута а

```
ted [guest@yvkolcheva ~]$ lsattr /home/guest/dirl/file1
-----a-----e----- /home/guest/dirl/file1
[guest@yvkolcheva ~]$ echo "test" /home/guest/dirl/file1
test /home/guest/dirl/file1
[guest@yvkolcheva ~]$
```

Рис. 4.3: Проверка корректности установки атрибута +a

3). Дозаписала в конец файла новую информацию с помощью команды `echo` » и проверила, что это действительно произошло, используя команду `cat`. После этого попыталась стереть информацию в файле с помощью команды `echo >`, на что получила ошибку. Мне также не удалось переименовать файл и изменить его атрибуты командой `chmod` из-за той же ошибки в правах доступа (рис. [4.4]).

```
[guest@yvkolcheva ~]$ echo "test" /home/guest/dirl/file1
test /home/guest/dirl/file1
[guest@yvkolcheva ~]$ cat /home/guest/dirl/file1
[guest@yvkolcheva ~]$ echo "abcd" /home/guest/dirl/file1
abcd /home/guest/dirl/file1
[guest@yvkolcheva ~]$ cat /home/guest/dirl/file1
[guest@yvkolcheva ~]$ echo "test" >> /home/guest/dirl/file1
[guest@yvkolcheva ~]$ echo "abcd" >> /home/guest/dirl/file1
[guest@yvkolcheva ~]$ cat /home/guest/dirl/file1
test
abcd
[guest@yvkolcheva ~]$ echo "abcd" > /home/guest/dirl/file1
bash: /home/guest/dirl/file1: Operation not permitted
[guest@yvkolcheva ~]$ rename file1 file2 /home/guest/dirl/file1
rename: /home/guest/dirl/file1: rename to /home/guest/dirl/file2 failed: Operati
on not permitted
[guest@yvkolcheva ~]$ chmod 000 /home/guest/dirl/file1
chmod: changing permissions of '/home/guest/dirl/file1': Operation not permitted
[guest@yvkolcheva ~]$
```

Рис. 4.4: Проверка действий при наличии атрибута a

4). Сняла расширенный атрибут “a” командой `chattr -a` от лица администрато-
ра. При повторе ранее описанных действий теперь не произошло ошибок и они
все выполнились (рис. [4.5]).

```

[tkonovalova@yvkolcheva ~]$ sudo chattr +a /home/guest/dir1/file1
[sudo] пароль для tkonovalova:
tkonovalova is not in the sudoers file. This incident will be reported.
[tkonovalova@yvkolcheva ~]$ su
Пароль:
su: Сбой при проверке подлинности
[tkonovalova@yvkolcheva ~]$ su
Пароль:
[root@yvkolcheva tkonovalova]# chattr +a /home/guest/dir1/file1
[root@yvkolcheva tkonovalova]# chattr -a /home/guest/dir1/file1
[root@yvkolcheva tkonovalova]#

[guest@yvkolcheva ~]$ echo "abcd" > /home/guest/dir1/file1
[guest@yvkolcheva ~]$ rename file1 file2 /home/guest/dir1/file1
[guest@yvkolcheva ~]$ rename file2 file1 /home/guest/dir1/file1
[guest@yvkolcheva ~]$ chmod 000 /home/guest/dir1/file1
[guest@yvkolcheva ~]$ chmod 000 /home/guest/dir1/file1
[guest@yvkolcheva ~]$

```

Рис. 4.5: Проверка действий при отсутствии атрибута а

5). От имени администратора добавила файлу расширенный атрибут *i* и повторила действия, описанные ранее. В итоге получила, что в этом случае файл можно только читать, но его нельзя никак изменить (рис. [4.6]).

```

[root@yvkolcheva tkonovalova]# chattr +i /home/guest/dir1/file1
[root@yvkolcheva tkonovalova]#

```

Рис. 4.6: Установка атрибута *i*

```

[guest@yvkolcheva ~]$ lsattr /home/guest/dir1/file1
---i-----e----- /home/guest/dir1/file1
[guest@yvkolcheva ~]$ echo "12345" /home/guest/dir1/file1
12345 /home/guest/dir1/file1
[guest@yvkolcheva ~]$ echo "12345" >> /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[guest@yvkolcheva ~]$ cat /home/guest/dir1/file1
abcd
[guest@yvkolcheva ~]$ echo "abcd" > /home/guest/dir1/file1
bash: /home/guest/dir1/file1: Operation not permitted
[guest@yvkolcheva ~]$ rename file1 file2 /home/guest/dir1/file1
rename: /home/guest/dir1/file1: rename to /home/guest/dir1/file2 failed: Operation not permitted
[guest@yvkolcheva ~]$ chmod 000 /home/guest/dir1/file1
chmod: changing permissions of '/home/guest/dir1/file1': Operation not permitted
[guest@yvkolcheva ~]$

```

Рис. 4.7: Проверка действий при наличии атрибута *i*

5 Выводы

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

6 Библиография

СПИСОК ЛИТЕРАТУРЫ

- 1.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>
- 2.Теоретические знания, приведённые в Лабораторной работе №4 - https://esystem.rudn.ru/pluginfile.php/2090127/mod_resource/content/3/004-lab_discret_extattr.pdf
- 3.Запечников С. В. и др. Информационная безопасность открытых систем. Том 1. — М.: Горячая линия -Телеком, 2006.

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

- 1.[Электронный ресурс] - доступ: <https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux>
- 2.[Электронный ресурс] - доступ: <https://debianinstall.ru/diskretnoe-razgranichenie-dostupa-linux/>