

Отчет по лабораторной работе №4

по дисциплине: Информационная безопасность

Ван И

Содержание

| | | |
|----------|---------------------------------------|-----------|
| 1 | Цели работы | 4 |
| 2 | Задание | 5 |
| 3 | Теоретическое введение | 6 |
| 4 | Выполнение лабораторной работы | 7 |
| 5 | Выводы | 11 |
| 6 | Список литературы | 12 |

Список иллюстраций

| | | |
|------|---|----|
| 4.1 | Расширенные атрибуты файла /home/guest/dir1/file1 | 7 |
| 4.2 | Попытка установки атрибута а на файл /home/guest/dir1/file1 от имени пользователя guest | 7 |
| 4.3 | Установка атрибута а на файл /home/guest/dir1/file1 | 8 |
| 4.4 | Атрибуты на файл /home/guest/dir1/file1 | 8 |
| 4.5 | Запись и чтение файла /home/guest/dir1/file1 | 8 |
| 4.6 | Попытка удаления информации и переименования файла /home/guest/dir1/file1 | 8 |
| 4.7 | Попытка установления прав на файл /home/guest/dir1/file1 | 9 |
| 4.8 | Снятие атрибута а с файла /home/guest/dir1/file1 | 9 |
| 4.9 | Повторение операций после снятия атрибута а | 9 |
| 4.10 | Повторение операций после установки атрибута i | 10 |

1 Цели работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

2 Задание

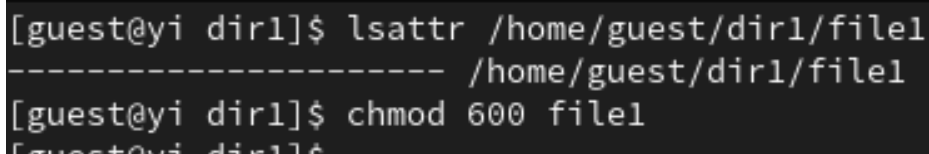
1. Исследовать доступность команд при установленном расширенном атрибуте а.
2. Исследовать доступность команд при установленном расширенном атрибуте і.

3 Теоретическое введение

- Операционная система — это комплекс программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем [1].
- Права доступа определяют, какие действия конкретный пользователь может или не может совершать с определенным файлами и каталогами. С помощью разрешений можно создать надежную среду — такую, в которой никто не может поменять содержимое ваших документов или повредить системные файлы. [2].

4 Выполнение лабораторной работы

1. От имени пользователя guest определим расширенные атрибуты файла /home/guest/dir1/file1. Установим на файл file1 права, разрешающие чтение и запись для владельца файла (4.1).



```
[guest@yi dir1]$ lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[guest@yi dir1]$ chmod 600 file1
[guest@yi dir1]$
```

Рис. 4.1: Расширенные атрибуты файла /home/guest/dir1/file1

2. Попробуем установить на файл /home/guest/dir1/file1 расширенный атрибут а от имени пользователя guest (4.2).



```
[guest@yi dir1]$ chattr +a /home/guest/dir1/file1
chattr: Операция не позволена while setting flags on /home/guest/dir1/file1
[guest@yi dir1]$
```

Рис. 4.2: Попытка установки атрибута а на файл /home/guest/dir1/file1 от имени пользователя guest

3. Откроем еще одну консоль с правами администратора. Установим на файл /home/guest/dir1/file1 расширенный атрибут а (4.3).

```
[guest@yi dir1]$ su
Пароль:
[root@yi dir1]# lsattr /home/guest/dir1/file1
----- /home/guest/dir1/file1
[root@yi dir1]# chattr +a /home/guest/dir1/file1
```

Рис. 4.3: Установка атрибута а на файл /home/guest/dir1/file1

5. От пользователя guest проверим правильность установления атрибута (4.4).

```
[root@yi dir1]# lsattr /home/guest/dir1/file1
----a----- /home/guest/dir1/file1
[root@yi dir1]#
```

Рис. 4.4: Атрибуты на файл /home/guest/dir1/file1

6. Выполним дозапись в файл file1 слова «test» и выполним чтение файла file1 (4.5).

```
[root@yi dir1]# echo "test" >> file1
[root@yi dir1]# cat file1
hello
test
[root@yi dir1]#
```

Рис. 4.5: Запись и чтение файла /home/guest/dir1/file1

7. Попробуем стереть имеющуюся в файле информацию и переименовать его(4.6).

```
[root@yi dir1]# echo "abcd" > file1
bash: file1: Операция не позволена
[root@yi dir1]# rename file2 file1 /home/guest/dir1/file1
[root@yi dir1]# ls
file1
[root@yi dir1]# rename file1 file2 /home/guest/dir1/file1
rename: /home/guest/dir1/file1: не удалось переименовать в /home/guest/dir1/file
2: Операция не позволена
```

Рис. 4.6: Попытка удаления информации и переименования файла /home/guest/dir1/file1

8. Попробуем установить на файл file1 права, запрещающие чтение и запись для владельца файла. Этому сделать не удалось(4.7).

```
[root@yi dir1]# chmod 000 file1
chmod: изменение прав доступа для 'file1': Операция не позволена
[root@yi dir1]#
```

Рис. 4.7: Попытка устанавления прав на файл /home/guest/dir1/file1

9. Снимем расширенный атрибут а с файла /home/guest/dir1/file1 от имени суперпользователя (4.8).

```
[root@yi dir1]# chatter -a file1
[root@yi dir1]# lsattr file1
----- file1
```

Рис. 4.8: Снятие атрибута а с файла /home/guest/dir1/file1

10. Повторим операции, которые нам ранее не удавалось выполнить. Теперь все операции выполняются (4.9).

```
[root@yi dir1]# echo "abcd" > file1
[root@yi dir1]# cat file1
abcd
[root@yi dir1]# rename file1 file2 /home/guest/dir1/file1
[root@yi dir1]# ls
file2
[root@yi dir1]# rename file2 file1 /home/guest/dir1/file2
[root@yi dir1]# chmod 000 file1
```

Рис. 4.9: Повторение операций после снятия атрибута а

11. Повторим действия по шагам, заменив атрибут «а» атрибутом «і» (4.10).

```
[root@yi dir1]# chattr +i file1
[root@yi dir1]# lsattr file1
----i----- file1
[root@yi dir1]# echo "abcd" > file1
bash: file1: Операция не позволена
[root@yi dir1]# rename file1 file2 /home/guest/dir1/file1
rename: /home/guest/dir1/file1: не удалось переименовать в /home/guest/dir1/file
2: Операция не позволена
[root@yi dir1]# chmod 000 file1
chmod: изменение прав доступа для 'file1': Операция не позволена
[root@yi dir1]#
```

Рис. 4.10: Повторение операций после установки атрибута i

5 Выводы

В ходе лабораторной работы нам удалось получить практические навыки работы в консоли с расширенными атрибутами файлов. «а» и «і».

6 Список литературы

1. Операционные системы [Электронный ресурс]. URL: <https://softline.tm/solutions/programmnoe-obespechenie/operating-system>.
2. Права доступа [Электронный ресурс]. URL: <https://w.wiki/7UBB>.