

Презентация №4
по Лабораторной работе №4

Рытов Алексей

Цель работы

Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

Выполнение лабораторной работы

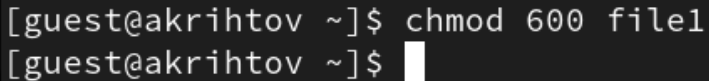
Выполнение лабораторной работы

1. От имени пользователя guest определили расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /home/guest/dir1/file1 (рис. 1).

```
[guest@akrihtov ~]$ lsattr /home/guest/file1
----- /home/guest/file1
[guest@akrihtov ~]$ S
```

Рис. 1: Расширенные атрибуты файла file1

2. Установили командой `chmod 600 file1` на файл `file1` права, разрешающие чтение и запись для владельца файла. (рис. 2).

A screenshot of a terminal window with a dark background and light gray text. The prompt is [guest@akrihtov ~]\$ and the command chmod 600 file1 has been entered. The cursor is at the end of the command line.

```
[guest@akrihtov ~]$ chmod 600 file1  
[guest@akrihtov ~]$
```

Рис. 2: Команда `chmod 600`

3. Попробовали установить на файл /home/guest/dir1/file1 расширенный атрибут а от имени пользователя guest: `chattr +a /home/guest/dir1/file1` (рис. 3).

```
[guest@akrihtov ~]$ chattr +a /home/guest/file1
chattr: Operation not permitted while setting flags on /home/guest/file1
[guest@akrihtov ~]$
```

Рис. 3: Расширенный атрибут а

4. Попробовали установить расширенный атрибут а на файл /home/guest/dir1/file1 от имени суперпользователя (рис. 4).

```
[guest@akrihtov ~]$ sudo chattr +a /home/guest/file1  
[guest@akrihtov ~]$
```

Рис. 4: Установка расширенного атрибута а на файл

5. От пользователя guest проверьте правильность установления атрибута (рис. 5).

```
[guest@akrihtov ~]$ lsattr /home/guest/file1  
-----a----- /home/guest/file1  
[guest@akrihtov ~]$
```

Рис. 5: Результат проверки

6. Выполнили дозапись в файл file1 слова «test» (рис. 6).

```
[guest@akrihtov dir]$ sudo echo "test" > /home/guest/dir/file1  
[guest@akrihtov dir]$ cat /home/guest/dir/file1  
test  
[guest@akrihtov dir]$
```

Рис. 6: Дозапись в файл

7. Попробовали удалить файл file1 либо стереть имеющуюся в нём информацию командой (рис. 7).

```
[guest@akrihtov dir]$ echo "abcd" > /home/guest/dir/file1  
bash: /home/guest/dir/file1: Operation not permitted  
[guest@akrihtov dir]$
```

Рис. 7: Удаление файла

8. Попробуйте с помощью команды установить на файл file1 права, например, запрещающие чтение и запись для владельца файла (рис. 8).

```
[guest@akrihtov dir]$ chmod 000 file1  
chmod: changing permissions of 'file1': Operation not permitted  
[guest@akrihtov dir]$
```

Рис. 8: Установка прав

9. Сняли расширенный атрибут `a` с файла `/home/guest/dirl/file1` от имени суперпользователя (рис. 9).

```
[guest@akrihtov dir]$ sudo chattr -a /home/guest/dir/file1  
[guest@akrihtov dir]$ echo "abcd" > /home/guest/dir/file1  
[guest@akrihtov dir]$ chmod 000 file1  
[guest@akrihtov dir]$
```

Рис. 9: Снятие атрибута

10. Повторили наши действия по шагам, заменив атрибут «a» атрибутом «i» (рис. 10).

```
[guest@akrihtov dir]$ sudo chattr -i /home/guest/dir/file1
[guest@akrihtov dir]$ echo "abcd" > /home/guest/dir/file1
bash: /home/guest/dir/file1: Permission denied
[guest@akrihtov dir]$ chmod 000 file1
[guest@akrihtov dir]$
```

Рис. 10: Действия с атрибутом i

Выводы

Выводы

В результате выполнения работы вы повысили свои навыки использования интерфейса командой строки (CLI), познакомились на примерах с тем, как используются основные и расширенные атрибуты при разграничении доступа. Имели возможность связать теорию дискреционного разделения доступа (дискреционная политика безопасности) с её реализацией на практике в ОС Linux.