Отчет по лабораторной работе №4

Основы информационной безопасности

Назармамадов Умед Джамшедович

Содержание

[Цель работы 1](#_Toc209035955)

[Теоретическое введение 2](#_Toc209035956)

[Выполнение лабораторной работы 3](#_Toc209035957)

[Выводы 6](#_Toc209035958)

[Список литературы 6](#_Toc209035959)

Список иллюстраций

[Создание файла 3](#_Toc209035960)

[Создание файла 3](#_Toc209035961)

[Просмотр 3](#_Toc209035962)

[Права 3](#_Toc209035963)

[Атриюут 4](#_Toc209035964)

[Поставление 4](#_Toc209035965)

[Проверить 4](#_Toc209035966)

[Проверить 4](#_Toc209035967)

[Убедиться 5](#_Toc209035968)

[поменять права 5](#_Toc209035969)

[Снять 5](#_Toc209035970)

[Повторить опыт 5](#_Toc209035971)

[Повторить опыт 6](#_Toc209035972)

[Повторить опыт 6](#_Toc209035973)

[Повторить опыт 6](#_Toc209035974)

Список таблиц

**Элементы списка иллюстраций не найдены.**

# Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов

# Теоретическое введение

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. [1]

Расширенные атрибуты файлов Linux представляют собой пары имя:значение, которые постоянно связаны с файлами и каталогами, подобно тому как строки окружения связаны с процессом. Атрибут может быть определён или не определён. Если он определён, то его значение может быть или пустым, или не пустым. [2]

Расширенные атрибуты дополняют обычные атрибуты, которые связаны со всеми inode в файловой системе (т. е., данные stat(2)). Часто они используются для предоставления дополнительных возможностей файловой системы, например, дополнительные возможности безопасности, такие как списки контроля доступа (ACL), могут быть реализованы через расширенные атрибуты. [3]

Установить атрибуты:

chattr filename Значения:

chattr +a # только добавление. Удаление и переименование запрещено;

chattr +A # не фиксировать данные об обращении к файлу

chattr +c # сжатый файл

chattr +d # неархивируемый файл

chattr +i # неизменяемый файл

chattr +S # синхронное обновление

chattr +s # безопасное удаление, (после удаления место на диске переписывается нулями)

chattr +u # неудаляемый файл

chattr -R # рекурсия

Просмотреть атрибуты:

lsattr filename Опции:

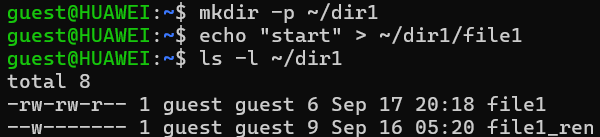
lsattr -R # рекурсия

lsattr -a # вывести все файлы (включая скрытые)

lsattr -d # не выводить содержимое директории

# Выполнение лабораторной работы

Создал в начале тестовый файл (рис. [-@fig:001]).



|  |
| --- |
| Создание файла |

Создание файла



|  |
| --- |
| Создание файла |

Создание файла

Посмотрим расширенные атрибуты file1 (рис. [-@fig:003]).

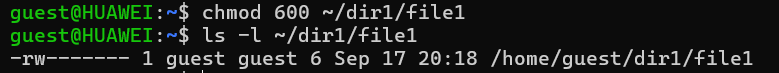
Изображение выглядит как текст, Шрифт, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

|  |
| --- |
| Просмотр |

Просмотр

Выставляю обычные права (600) (рис. [-@fig:004]).



|  |
| --- |
| Права |

Права

Попытка поставить append-only атрибут a «как user» (рис. [-@fig:005]).



|  |
| --- |
| Атриюут |

Атриюут

Поставить a от администратора (рис. [-@fig:006]).

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

|  |
| --- |
| Поставление |

Поставление

Проверить, что a применился (рис. [-@fig:007]).

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

|  |
| --- |
| Проверить |

Проверить

Проверить дозапись и чтение (рис. [-@fig:008]).

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

|  |
| --- |
| Проверить |

Проверить

Убедиться, что нельзя удалять/перезаписывать/переименовывать (рис. [-@fig:009]).

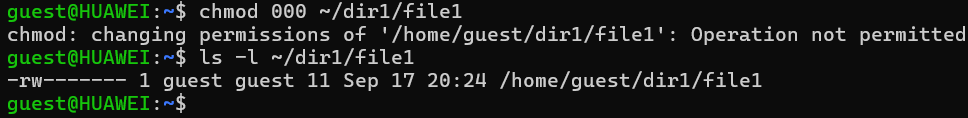
Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

|  |
| --- |
| Убедиться |

Убедиться

Попробовать поменять права при +a (рис. [-@fig:010]).



|  |
| --- |
| поменять права |

поменять права

Снять a и повторить «запрещённые» действия (рис. [-@fig:011]).

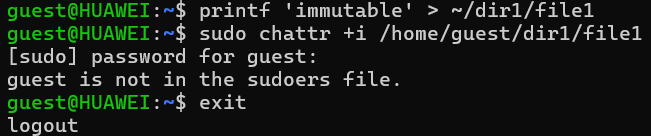
Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

|  |
| --- |
| Снять |

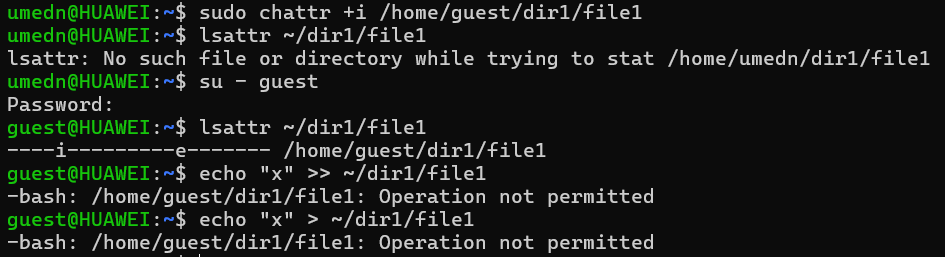
Снять

Повторить опыт, но с атрибутом i (immutable) (рис. [-@fig:012]).



|  |
| --- |
| Повторить опыт |

Повторить опыт



|  |
| --- |
| Повторить опыт |

Повторить опыт

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

|  |
| --- |
| Повторить опыт |
|  |

Повторить опыт

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

|  |
| --- |
| Повторить опыт |

Повторить опыт

# Выводы

Во время выполнения работы были развиты навыки работы через интерфейс командной строки (CLI), на практике рассмотрено применение базовых и дополнительных атрибутов доступа. Теоретические основы дискреционной модели безопасности были сопоставлены с их практической реализацией в Linux. Также была проверена работа расширенных атрибутов «a» и «i», позволяющих ограничивать изменение и удаление файлов.

# Список литературы

[0] Методические материалы курса

[1] Права доступа: https://codechick.io/tutorials/unix-linux/unix-linux-permissions

[2] Расширенные атрибуты: https://ru.manpages.org/xattr/7

[3] Операции с расширенными атрибутами: https://p-n-z-8-8.livejournal.com/64493.html