Лабораторная работа №4

Дисциплина: Информационная безопасность

Манаева Варвара Евгеньевна

Содержание

# 1 Техническое оснащение:

* Персональный компьютер с операционной системой Windows 10;
* Планшет для записи видеосопровождения и голосовых комментариев;
* Microsoft Teams, использующийся для записи скринкаста лабораторной работы;
* Приложение Pycharm для редактирования файлов формата *md*;
* *pandoc* для конвертации файлов отчётов и презентаций.

# 2 Цели и задачи работы

## 2.1 Цель

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

## 2.2 Задачи

* Совершим ряд операций с файлом, которому выдали расширенный атрибут a;
* Совершим ряд операций с файлом, которому выдали расширенный атрибут i;
* Сравним возможность выполнения различных операций с разными атрибутами.

# 3 Теоретическое введение [1]

Расширенные атрибуты файловых объектов — поддерживаемая некоторыми файловыми системами возможность ассоциировать с файловыми объектами произвольные метаданные. В отличие от обычных атрибутов файловых объектов (таких, как владелец, права доступа, время создания и пр.), содержание расширенных атрибутов не специфицируется в файловой системе и может принимать любые значение. С точки зрения реализации расширенные атрибуты представляют собой пары ключ:значение, ассоциированные с файловыми объектами. Типичными применениями расширенных атрибутов является хранение таких данных, как автор документа, контрольные суммы, источник документа, информация для контроля доступа.

Каждый расширенный атрибут имеет имя вида namespace.attrname, при этом пространства имен namespace определяют назначение атрибута. Пространство, имен systen используется системными (ядерными) компонентами, например, для списков контроля доступа POSIX ACL.

Пространство имен security используется системными компонентами безопасности, в частности для хранения привилегий исполняемых программ (capabilities), и меток модуля принудительного контроля доступа SELinux.

Пространства имен trusted и user предназначены для атрибутов внеядерных компонент программ, выполняющихся привилегированным и обычными пользователями соответственно.

Table 1: Информация о некоторых расширенных атрибутах

| Атрибуты | Информация об атрибуте |
| --- | --- |
| a | Файл с установленным атрибутом a можно открыть только в режиме добавления для записи.Только суперпользователь или процесс, обладающий возможностью CAP\_LINUX\_IMMUTABLE, может установить или очистить этот атрибут. |
| i | Файл с атрибутом «i» не может быть изменён: его нельзя удалить или переименовать, нельзя создать ссылку на этот файл, большую часть метаданных файла нельзя изменить, и файл нельзя открыть в режиме записи.Только суперпользователь или процесс, обладающий возможностью CAP\_LINUX\_IMMUTABLE, может установить или очистить этот атрибут. |

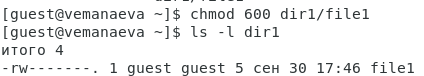
# 4 Выполнение лабораторной работы [2]

1. От имени пользователя guest определим расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /home/guest/dir1/file1

Определение атрибутов

Определение атрибутов

1. Установим командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла.



Установка прав на чтение и запись файла

1. Попробуем установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest командой chattr +a /home/guest/dir1/file1

Попытка установить расширенный атрибут на файл

Попытка установить расширенный атрибут на файл

1. Зайдём на третью консоль с правами администратора и попробуем установить расширенный атрибут a на файл /home/guest/dir1/file1 командой chattr +a /home/guest/dir1/file1

Установка расширенного атрибута на файл

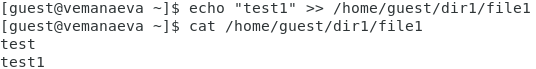
Установка расширенного атрибута на файл

1. От пользователя guest проверьте правильность установления атрибута командой lsattr /home/guest/dir1/file1

Проверка правильности установки атрибута

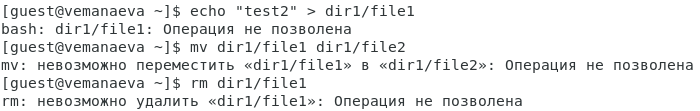
Проверка правильности установки атрибута

1. Выполним дозапись в файл file1 слова «test» командой echo "test" >> /home/guest/dir1/file1, после чего выполним чтение файла file1 командой cat /home/guest/dir1/file1



Дозапись в файл

1. Попробуем удалить файл file1, стереть имеющуюся в нём информацию командой echo "abcd" > /home/guest/dirl/file1 и переименовать файл



Попытки переименования, стирания информации и удаления файла

1. Попробуйте с помощью команды chmod 000 file1 установить на файл file1 права, например, запрещающие чтение и запись для владельца файла.

Попытка смены атрибутов файла

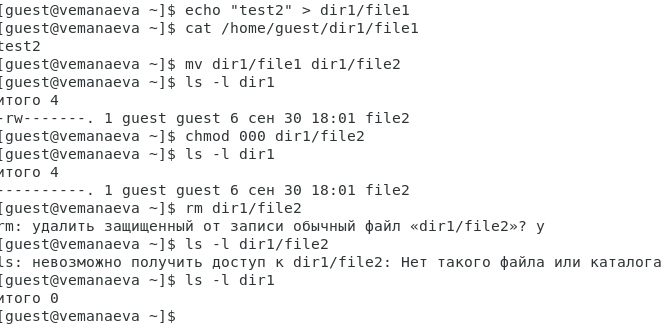
Попытка смены атрибутов файла

Указания команды выполнить не удалось.

1. Снимем расширенный атрибут a с файла /home/guest/dirl/file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1 и повторим неполучившиеся действия

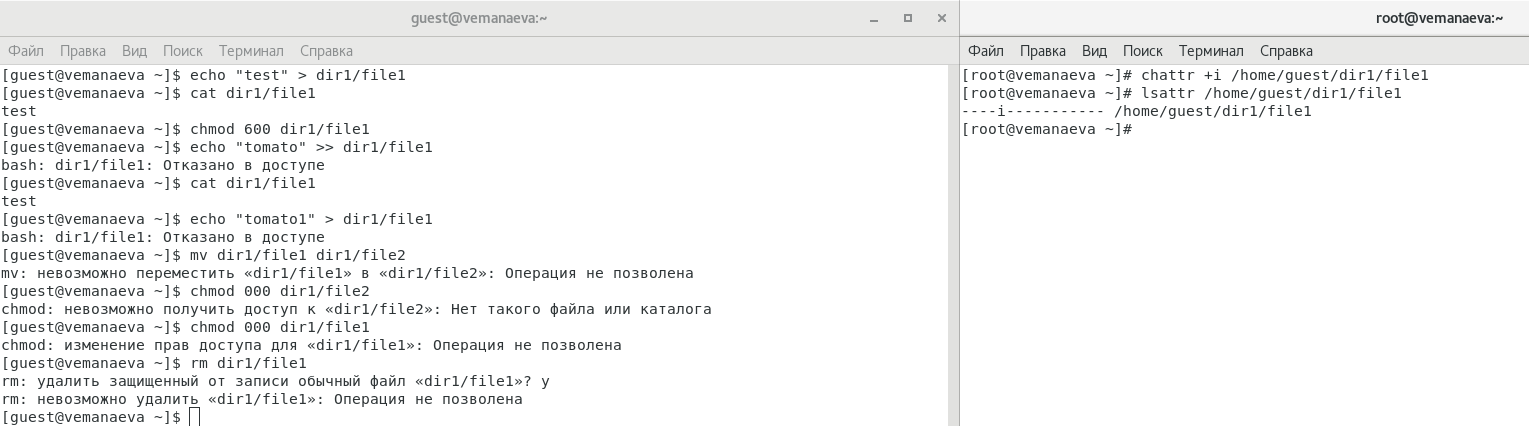
Снятие расширенного атрибута

Снятие расширенного атрибута

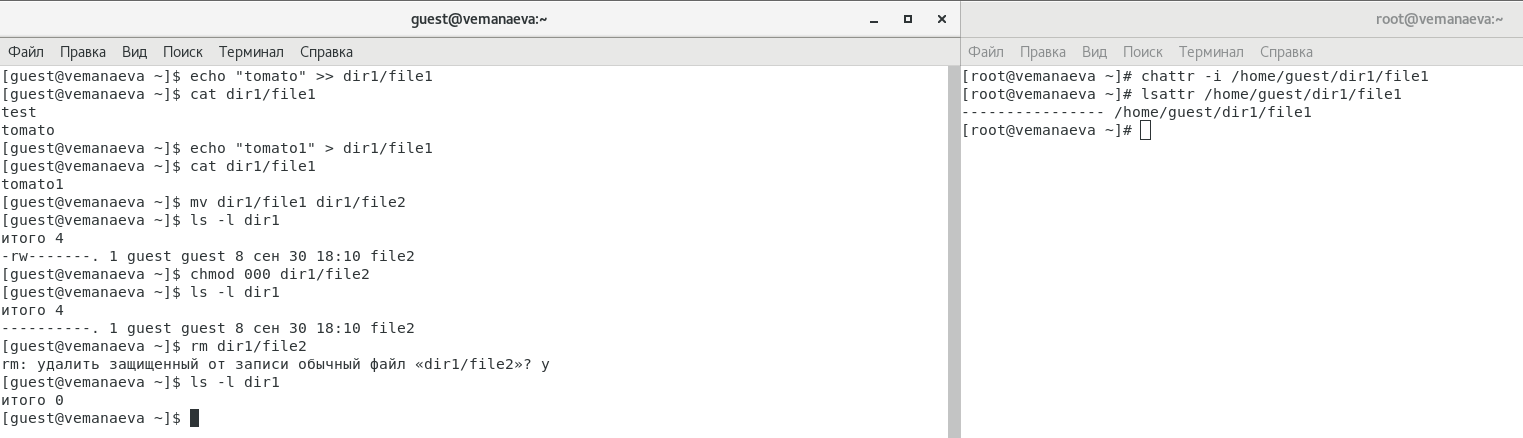


Повторение команд после снятия расширенного атрибута

1. Повтором аналогичные шаги с атрибутом i и заполним таблицу на основании произведённых действий



Повторение команд с расширенным атрибутом i



Повторение команд без расширенного атрибута i

Table 2: Возможность выполнения ряда операций с файлом при наличии расширенных атрибутов

| Операция | С атрибутом “a” | Без атрибута “a” | С атрибутом “i” | Без атрибута “i” |
| --- | --- | --- | --- | --- |
| Запись в файл | + | + | - | + |
| Чтение файла | + | + | + | + |
| Удаление файла | - | + | - | + |
| Удаление информации в файле | - | + | - | + |
| Переименование файла | - | + | - | + |
| Смена атрибутов файла | - | + | - | + |

# 5 Выводы по проделанной работе

## 5.1 Вывод

В результате выполнения работы мы повысили свои навыки использования интерфейса командой строки, 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. Составили наглядные таблицы, поясняющие какие операции возможны при тех или иных установленных правах. Опробовали действие на практике расширенных атрибутов «а» и «i».

Были записаны скринкасты выполнения и защиты лабораторной работы.

Ссылки на скринкасты:

* [Выполнение, Youtube](https://youtu.be/4THXw94p6FY)
* [Выполнение, Rutube](https://rutube.ru/video/ab099f3ab125a2d9fccccd2b84d3aa4e)
* [Защита презентации, Youtube](https://youtu.be/xFmnCHeRNFU)
* [Защита презентации, Rutube](https://rutube.ru/video/cf8502ffd59b97c9b726fa7d069c5593)

# 6 Список литературы

1. Колисниченко Д. Linux. От новичка к профессионалу. В подлиннике. 8-е изд. 2022. 688 с.

2. Лабораторная работа № 4. Дискреционное разграничение прав в Linux. Два пользователя [Электронный ресурс]. Российский Университет Дружбы Народов имени Патрису Лумумбы, 2023. URL: <https://esystem.rudn.ru/mod/resource/view.php?id=1031375>.