Отчёт по лабораторной работе №4

Основы информационной безопасности

Надежда Александровна Рогожина

Содержание

# 1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

# 2 Задание

1. От имени пользователя guest определите расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /home/guest/dir1/file1
2. Установите командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла.
3. Попробуйте установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest: chattr +a /home/guest/dir1/file1. В ответ вы должны получить отказ от выполнения операции.
4. Зайдите на третью консоль с правами администратора либо повысьте свои права с помощью команды su. Попробуйте установить расширенный атрибут a на файл /home/guest/dir1/file1 от имени суперпользователя: chattr +a /home/guest/dir1/file1.
5. От пользователя guest проверьте правильность установления атрибута: lsattr /home/guest/dir1/file1
6. Выполните дозапись в файл file1 слова «test» командой echo "test" /home/guest/dir1/file1 После этого выполните чтение файла file1 командой cat /home/guest/dir1/file1 Убедитесь, что слово test было успешно записано в file1.
7. Попробуйте удалить файл file1 либо стереть имеющуюся в нём информацию командой echo "abcd" > /home/guest/dirl/file1 Попробуйте переименовать файл.
8. Попробуйте с помощью команды chmod 000 file1 установить на файл file1 права, например, запрещающие чтение и запись для владельца файла. Удалось ли вам успешно выполнить указан- ные команды?
9. Снимите расширенный атрибут a с файла /home/guest/dirl/file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1 Повторите операции, которые вам ранее не удавалось выполнить. Ваши наблюдения занесите в отчёт.
10. Повторите ваши действия по шагам, заменив атрибут «a» атрибутом «i». Удалось ли вам дозаписать информацию в файл? Ваши наблюдения занесите в отчёт.

# 3 Теоретическое введение

Команда lsattr выводит атрибуты файла:

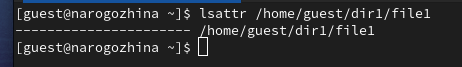
В табл. [[1](#tbl:std-dir)] приведено краткое описание стандартных атрибутов Unix.

Table 1: Описание некоторых атрибутов файлов

| Атрибут | Значение |
| --- | --- |
| A | Запрещает обновлять метку времени доступа к файлу |
| a | Автоматически устанавливает режим дополнения при открытии файла для записи |
| C | Запрещает использовать механизм копирования при записи (Copy-on-Write) при модификации содержимого файла |
| D | При применении к директории активирует режим синхронной записи изменений содержащихся в ней файлов |
| d | Запрещает утилите dump создавать резервную копию файла |
| E | Указывает на ошибку сжатия содержимого файла ядром ОС (не может быть установлен пользователем) |
| e | Указывает на использование экстентов для ссылок на соответствующие файлу дисковые блоки (не может быть установлен пользователем) |
| h | Указывает на то, что размер файла исчисляется в количестве блоков ФС, а не ее секторов, то есть, размер файла превышал или превышает в данный момент 2 ТБ (не может быть установлен пользователем) |
| I | Указывает на то, что содержимое директории было проиндексировано утилитой htree |
| i | Запрещает всем пользователям, в том числе супрепользователю, модифицировать файл, а именно, записывать в него данные, удалять переименовывать или создавать ссылки на него |
| j | Принудительно активирует режим журналирования ФС при записи данных в файл |
| s | Активирует механизм надежного удаления, автоматически записывающий нулевые блоки на диск после удаления файла пользователем |
| S | Активирует режим синхронной записи изменений содержимого файла на диск |
| T | При применении к директории указывает на то, что ее поддиректории не связаны и могут размещаться в отдельных группах блоков |
| t | Запрещает оптимизации использования блоков файла |
| u | Запрещает удаление содержимого файла при его удалении из ФС с целью получения возможности его последующего восстановления |
| X | Указывает на возможность прямого доступа к содержимому сжатого ядром ОС файла (не может быть установлен пользователем) |
| Z | Указывает на неактуальность сжатого ядром ОС файла (не может быть установлен пользователем) |

# 4 Выполнение лабораторной работы

1. От имени пользователя guest определите расширенные атрибуты файла /home/guest/dir1/file1 командой lsattr /home/guest/dir1/file1 (рис. [??]).



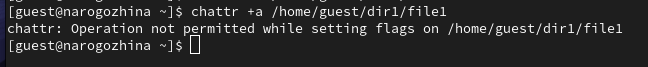
Определение атрибутов файла

1. Установите командой chmod 600 file1 на файл file1 права, разрешающие чтение и запись для владельца файла (рис. [??]).

Смена доступа к файлу

Смена доступа к файлу

1. Попробуйте установить на файл /home/guest/dir1/file1 расширенный атрибут a от имени пользователя guest: chattr +a /home/guest/dir1/file1. В ответ вы должны получить отказ от выполнения операции (рис. [??]).



Попытка смены атрибутов

1. Зайдите на третью консоль с правами администратора либо повысьте свои права с помощью команды su. Попробуйте установить расширенный атрибут a на файл /home/guest/dir1/file1 от имени суперпользователя: chattr +a /home/guest/dir1/file1 (рис. [??]).

Смена атрибутов

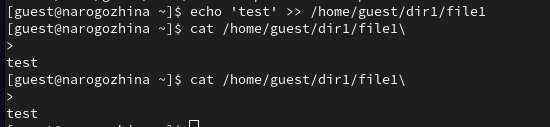
Смена атрибутов

1. От пользователя guest проверьте правильность установления атрибута: lsattr /home/guest/dir1/file1 (рис. [??]).

Проверка

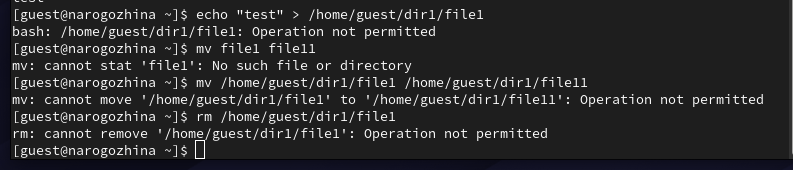
Проверка

1. Выполните дозапись в файл file1 слова «test» командой echo "test" /home/guest/dir1/file1 После этого выполните чтение файла file1 командой cat /home/guest/dir1/file1 Убедитесь, что слово test было успешно записано в file1. (рис. [??]).



Дозапись в файл и вывод

1. Попробуйте удалить файл file1 либо стереть имеющуюся в нём информацию командой echo "abcd" > /home/guest/dirl/file1 Попробуйте переименовать файл (рис. [??]).



Попытка переименовать файл и переименования

1. Попробуйте с помощью команды chmod 000 file1 установить на файл file1 права, например, запрещающие чтение и запись для владельца файла. Удалось ли вам успешно выполнить указан- ные команды? (рис. [??]).

Попытка смены атрибутов

Попытка смены атрибутов

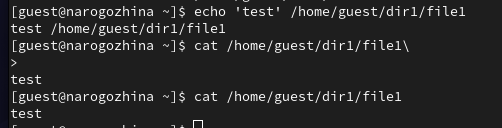
1. Снимите расширенный атрибут a с файла /home/guest/dirl/file1 от имени суперпользователя командой chattr -a /home/guest/dir1/file1 Повторите операции, которые вам ранее не удавалось выполнить. Ваши наблюдения занесите в отчёт. (рис. [??], рис. [??], рис. [??], рис. [??], рис. [??])

Смена атрибутов от имени root

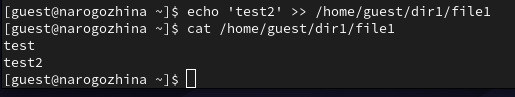
Смена атрибутов от имени root

Проверка

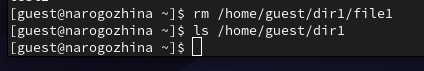
Проверка



Проверка echo

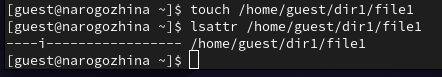


Проверка echo



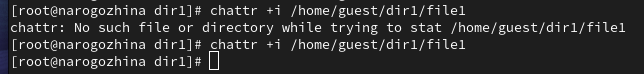
Проверка удаления файла

После удаления, создадим файл заново (рис. [??]):

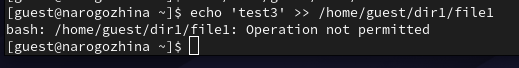


Проверка

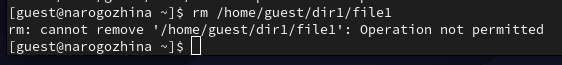
1. Повторите ваши действия по шагам, заменив атрибут «a» атрибутом «i». Удалось ли вам дозаписать информацию в файл? Ваши наблюдения занесите в отчёт (рис. [??], рис. [??], рис. [??], рис. [??])



Проверка



Проверка



Проверка

Проверка

Проверка

# 5 Выводы

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

# Список литературы