Лабораторная работа № 4

Дискреционное разграничение прав в Linux. Расширенные атрибуты

Абу Сувейлим Мухаммед Мунифович

Содержание

# 1 Цель работы

Получение практических навыков работы в консоли с расширенными атрибутами файлов.

# 2 Задание

Использовать интерфейс командой строки (CLI) при выполнении лабораторной работы

# 3 Теоретическое введение

В метаданных каждого объекта (в inode файла/директории) содержится список разрешений на доступ к нему для разных категорий субъектов [1].

Атрибуты Minimal ACL поддерживают три базовых класса субъектов доступа к файлу (класс All объединяет все три класса):

User access (u) – доступ для владельца файла; Group access (g) – доступ для группы, владеющей файлом; Other access (o) – доступ для остальных пользователей (кроме пользователя root). All access (a) – доступ для всех субъектов доступа (u, g, o). Для каждого из этих классов определены три типа разрешений:

На чтение содержимого файла (read) – символ «r». На запись внутри файла или изменения его содержимого (write) – символ «w». На исполнение файла (если это бинарный исполняемый файл или файл сценария интерпретатора (execute)) – символ «x» [2].

# 4 Выполнение лабораторной работы

От имени пользователя guest хотели определить расширенные атрибуты файла /home/guest/dir1/f1 командой (рис. 1):

Команда lsattr

Рис. 1: Команда lsattr

но получили отказ.

Установили командой chmod 600 f1 на файл f1 права, разрешающие чтение и запись для владельца файла (рис. 2):

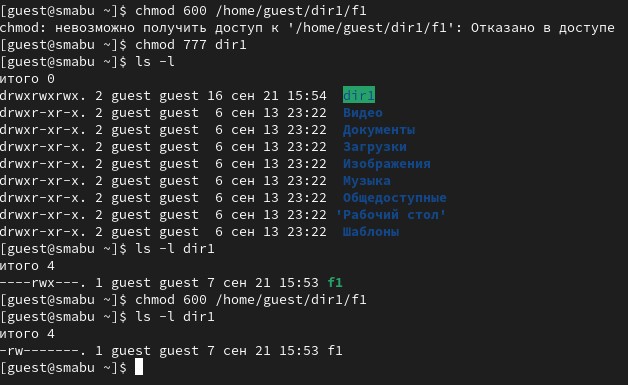


Рис. 2: Команда chmod

Попробавли установить на файл /home/guest/dir1/f1 расширенный атрибут a от имени пользователя guest (рис. 3):

Команда chattr +a

Рис. 3: Команда chattr +a

В ответ мы получили отказ от выполнения операции.

Повысили свои права с помощью команды su. Попробавли установить расширенный атрибут a на файл /home/guest/dir1/f1 от имени суперпользователя (рис. 4):

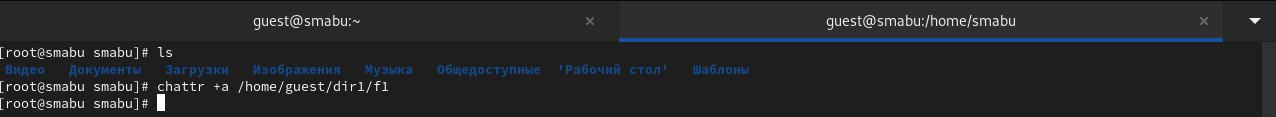


Рис. 4: Команда chattr +a через root

От пользователя guest проверbkb правильность установления атрибута (рис. 5):

Команда lsattr f1 на guest

Рис. 5: Команда lsattr f1 на guest

Выполним дозапись в файл f1 слова «test» командой (рис. 6):

Команда echo > f1 на guest

Рис. 6: Команда echo > f1 на guest

После этого выполним чтение файла file1 командой (рис. 7):

Команда cat f1 на guest

Рис. 7: Команда cat f1 на guest

Переименовать файл f1 невозможно (рис. 8):

Команда mv f1 f11

Рис. 8: Команда mv f1 f11

После снятии расширенный атрибут a с файла /home/guest/dirl/f1 от имени суппользователя командой (рис. 9):

Команда chattr -a

Рис. 9: Команда chattr -a

Все команды, которые мы не смогли выполнить выполнялись (рис. 10, 11):

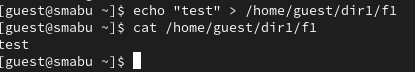


Рис. 10: Команда echo



Рис. 11: Команда mv

Повторим наши действия по шагам, заменив атрибут «a» атрибутом «i» (рис. 12):

Команда chattr +i

Рис. 12: Команда chattr +i

Получили отказ (рис. 13):

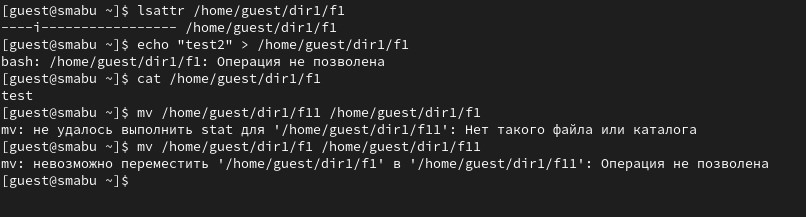


Рис. 13: Команды echo и mv

# 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

1. [// skillbox.ru](https://skillbox.ru/media/code/kali-linux-obzor-distributiva-dlya-budushchikh-khakerov/).

2. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.