Лабораторная работа №5

Дискреционное разграничение прав в Linux. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Валиева Найля Разимовна

Содержание

# Цель работы

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов. [1]

# Задание

1. Подготовить лабораторный стенд
2. Рассмотреть компиляцию программ
3. Создать программы
4. Исследовать Sticky-бит

# Выполнение лабораторной работы

1. Предварительно установила компилятор gcc с помощью команды (рис - @fig:001).



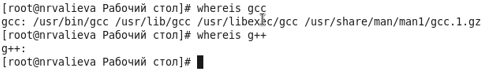
Установка компилятора gcc

Отключила систему защиты SELinux с помощью команды . После этого команда вывела (рис @fig:002).

Отключение системы запретов

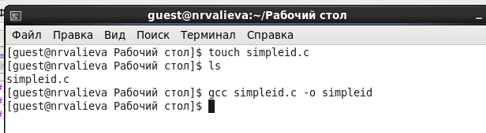
Отключение системы запретов

1. Изучила компиляцию программ. Компилятор языка С называется gcc. Компилятор языка С++ называется g++ и запускается с параметрами почти так же, как gcc. Проверила это с поомщью команд и (рис @fig:003).

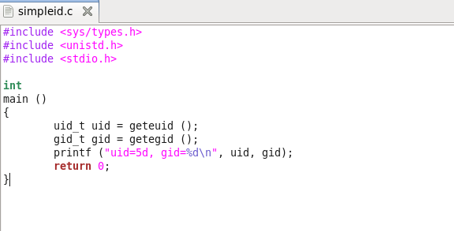


Проверка названий компиляторов

1. Вошла в в систему от имени пользователя и создала программу (рис @fig:004 и рис @fig:005).



Создание программы simpleid.c (часть 1)



Создание программы simpleid.c (часть 2)

Скомпилировала программу и убедилась, что файл программы создан с помощью команды (рис @fig:006)

Компиляция программы

Компиляция программы

Выполнила программу (рис @fig:007)

Выполнение созданной программы

Выполнение созданной программы

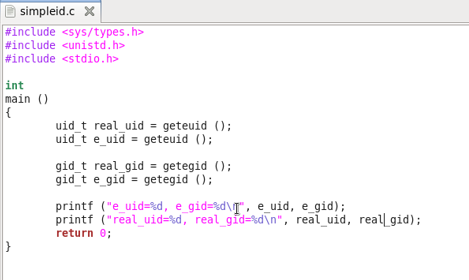
Выполнила системную программу (рис @fig:008)

Выполнение системной программы 

Выполнение системной программы

Вывод обоих команд совпадает.

Усложнила программу, добавив вывод действительных идентификаторов (рис @fig:009)



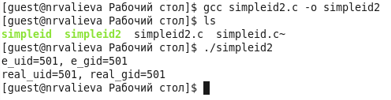
Усложнение программы

Получившуюся программу назвала (рис @fig:010)

Переименование программы

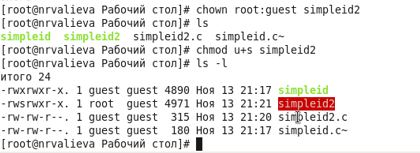
Переименование программы

Скомпилировала и запустила (рис @fig:011)



Компиляция и запуск файла

От имени суперпользователя выполнила следующие команды (рис @fig:012)



Смена владельца и атрибутов от имени суперпользователя

Использовала для временного повышения своих прав (рис @fig:013)

Использование оператора 

Использование оператора

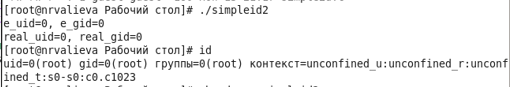
Команда используется для получения прав суперпользователя.

Выполнила проверку правильности установки новых атрибутов и смены владельца файла (рис @fig:014)

Проверка правильности установления атрибутов

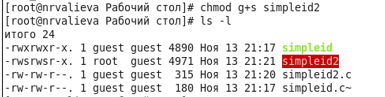
Проверка правильности установления атрибутов

Запустила и (рис @fig:015)



Проверка id пользователя и группы

Проделала то же самое относительно SetGID-бита (рис @fig:016)

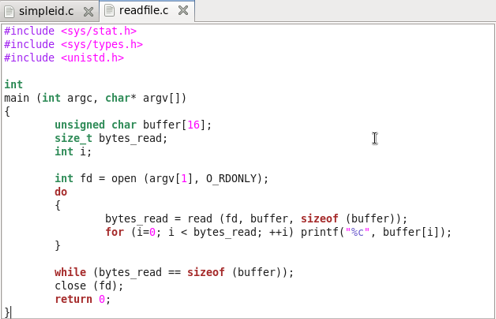


Повторение операций относительно SetGID-бита

Создала программу (рис @fig:017 и рис @fig:018)

Создание программы  (часть 1)

Создание программы (часть 1)



Создание программы (часть 2)

Откомпилировала созданную программу (рис @fig:019)



Компиляция программы

Сменила владельца у файла и изменила права так, чтобы только суперпользователь мог прочитать его, а не мог (рис @fig:020)

Смена владельца и изменение прав файла

Смена владельца и изменение прав файла

Проверила, что пользователь не может прочитать файл (рис @fig:021)

Попытка прочесть файл

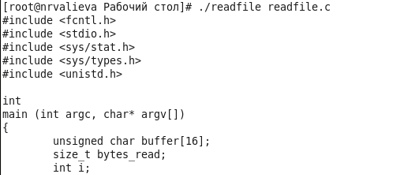
Попытка прочесть файл

Сменила у программы владельца и установила SetUID-бит (рис @fig:022)

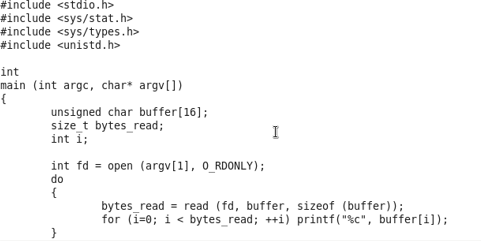
Смена владельца и установка SetUID-бита

Смена владельца и установка SetUID-бита

Проверила, может ли программа прочитать файл . Да, может. (рис @fig:023 и рис @fig:024)

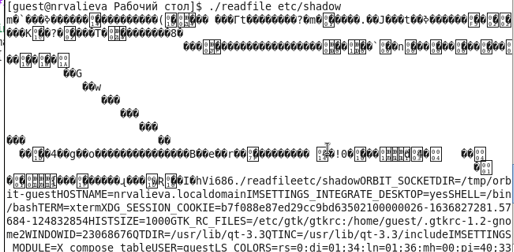


Проверка чтения файла (часть 1)



Проверка чтения файла (часть 2)

Проверила, может ли программа прочитать файл . Да, может. (рис @fig:025)



Проверка чтения файла

1. Исследовала Sticky-бит  
   Выяснила, что атрибут Sticky установлен на директорию , для чего выполнила команду (рис @fig:026)

Проверка нахождения атрибута Sticky на директории 

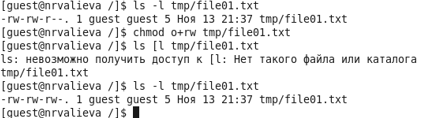
Проверка нахождения атрибута Sticky на директории

От имени пользователя создала файл в директории со словом (рис @fig:027):

Создание файла и внесение записи в него

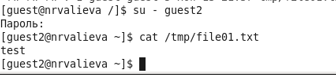
Создание файла и внесение записи в него

Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей “все остальные” (рис @fig:028):



Просмотр атрибутов файла и установление прав на чтение и запись для категории “все остальные”

От имени пользователя (не являющегося владельцем) прочитала файл (рис @fig:029):



Чтение файла от имени пользователя

От имени пользователя дозаписала в файл слово (рис @fig:030):

Дозапись слова в файл от имени пользователя 

Дозапись слова в файл от имени пользователя

Проверила содержимое файла (рис @fig:031):

Проверка содежимого в файле от имени пользователя 

Проверка содежимого в файле от имени пользователя

От имени пользователя записала в файл слово , стерев при этом всю имеющуюся в файле информацию (рис @fig:032):

Перезапись информации в файл от имени пользователя 

Перезапись информации в файл от имени пользователя

Проверила содержимое файла (рис @fig:033):

Проверка содежимого в файле от имени пользователя 

Проверка содежимого в файле от имени пользователя

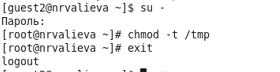
От имени пользователя попробовала удалить файл (рис @fig:034):

Попытка удаления файла от имени пользователя 

Попытка удаления файла от имени пользователя

Мне не удалось удалить файл.

Повысила свои права до суперпользователя и выполнила после этого команду, снимающую атрибут (Sticky-бит) с директории (рис @fig:035):



Повышение прав до суперпользователя. Снятие атрибута

Покинула режим суперпользователя командой (рис @fig:036):

Выход из режима суперпользователя

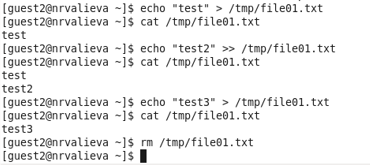
Выход из режима суперпользователя

От имени пользователя проверила, что атрибута у директории нет (рис @fig:037):

Проверка отсутствия атрибута 

Проверка отсутствия атрибута

Повторила предыдущие шаги (рис @fig:038):



Повтор предыдущих шагов

Как видно из рисунка, удалось выполнить все команды, которые были рассмотрены выше, включая удаление.

Повысила свои права до суперпользователя и вернула атрибут на директорию (рис @fig:039):

Переход в режим суперпользователя и возврат атрибута 

Переход в режим суперпользователя и возврат атрибута

# Выводы

Изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов