Лабораторная работа №5

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

Роман Владимирович Иванов

Содержание

# Цель работы

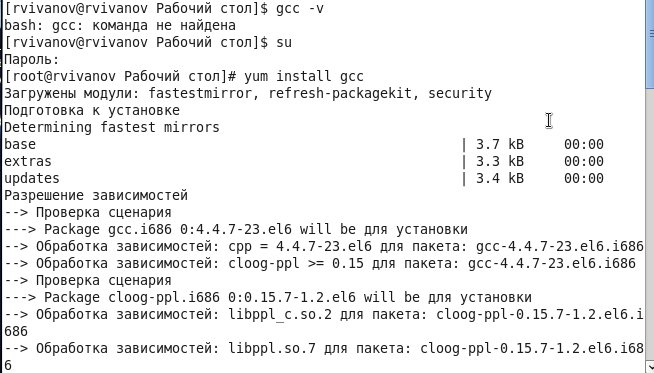
Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов. [1]

# Задание

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

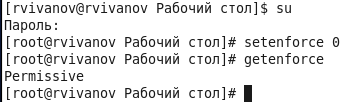
# Выполнение лабораторной работы

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



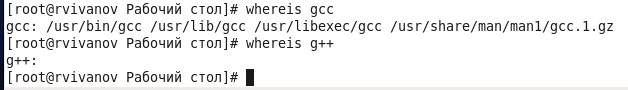
Установка компилятора gcc

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



Отключение системы запретов

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

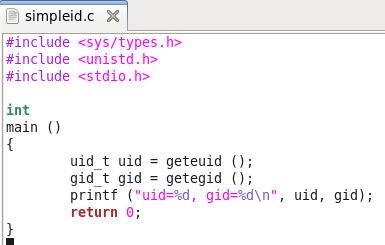


Проверка названий компиляторов

1. Вошел в в систему от имени пользователя и создал программу (рис -@fig:004 и рис -@fig:005).

Создание программы simpleid.c (часть 1)

Создание программы simpleid.c (часть 1)



Создание программы simpleid.c (часть 2)

Скомпилировал программу и убедился, что файл программы создан с помощью команды (рис -@fig:006)

Компиляция программы

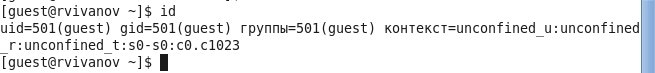
Компиляция программы

Выполнил программу (рис -@fig:007)

Выполнение созданной программы

Выполнение созданной программы

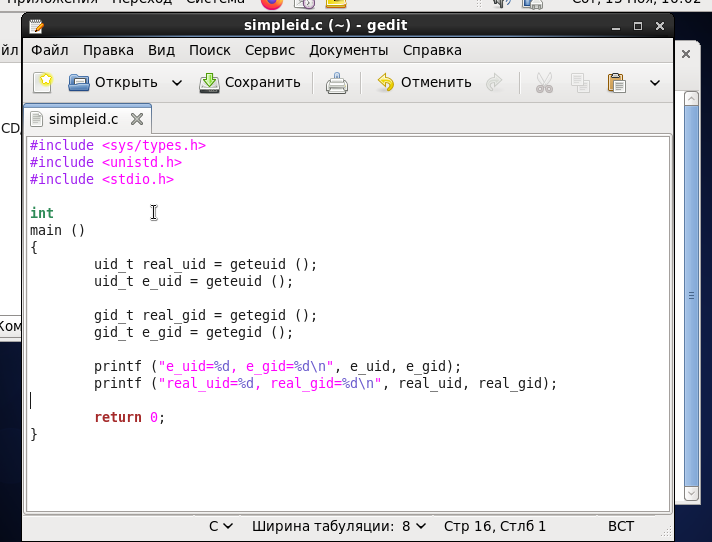
Выполнил системную программу (рис -@fig:008)



Выполнение системной программы

Вывод обоих способ совпадает.

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



Усложнение программы

Получившуюся программу назвал (рис -@fig:010)

Переименование программы

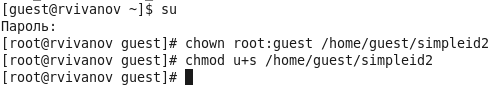
Переименование программы

Скомпилировал и запустил (рис -@fig:011)



Компиляция и запуск файла

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



Смена владельца и атрибутов от имени суперпользователя

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

Использование оператора 

Использование оператора

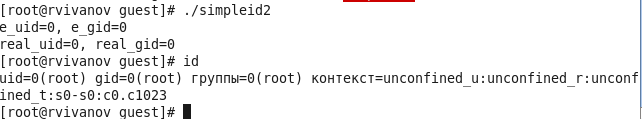
Команда используется для получения прав суперпользователя.

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

Проверка правильности установления атрибутов

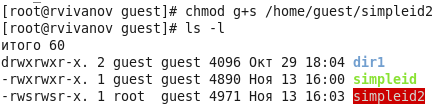
Проверка правильности установления атрибутов

Запустил и (рис -@fig:015)



Проверка id пользователя и группы

Проделал тоже самое относительно SetGID-бита (рис -@fig:016)

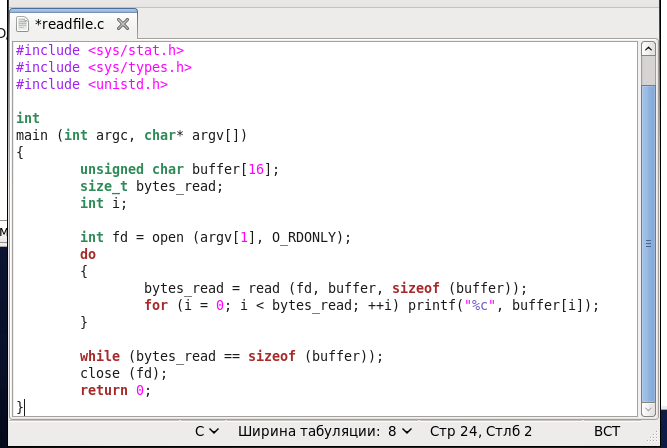


Повторение операций относительно SetGID-бита

Создал программу (рис -@fig:017 и рис -@fig:018)

Создание программы  (часть 1)

Создание программы (часть 1)



Создание программы (часть 2)

Откомпилировал созданную программу (рис -@fig:019)

Компиляция программы

Компиляция программы

Сменил владельца у файла и изменил 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

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

Попытка прочесть файл

Попытка прочесть файл

Сменил у программы владельца и утсановил SetUID-бит (рис -@fig:022)

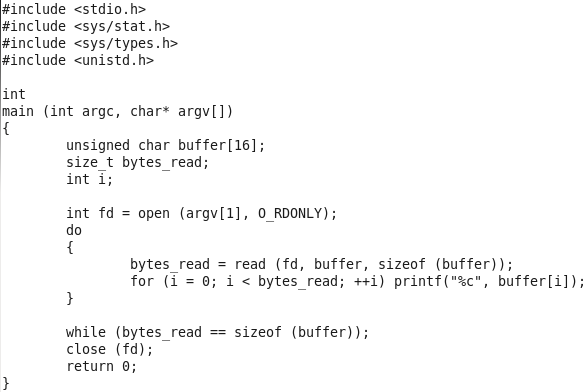
Смена владельца и установка SetUID-бита

Смена владельца и установка SetUID-бита

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

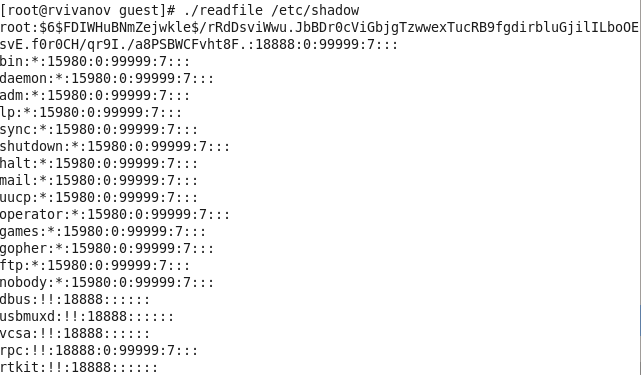
Проверка чтения файла (часть 1)

Проверка чтения файла (часть 1)



Проверка чтения файла (часть 2)

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



Проверка чтения файла

1. Исследовал Sticky-бит  
   Выяснил, что атрибут Sticky установлен на директорию , для чего выполнил команду (рис -@fig:026)

Проверка нахождения атрибута Sticky на директории 

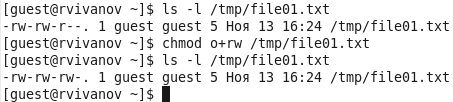
Проверка нахождения атрибута Sticky на директории

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

Создание файла и внесение записи в него

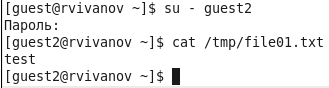
Создание файла и внесение записи в него

Просмотрел атрибуты у только что созданного файла и разрешил 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) прочитал файл (рис -@fig:029):



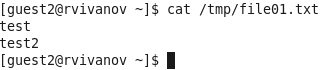
Чтение файла от имени пользователя

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

Дозапись слова в файл от имени пользователя 

Дозапись слова в файл от имени пользователя

Проверил содержимое файла (рис -@fig:031):



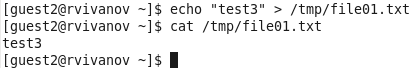
Проверка содежимого в файле от имени пользователя

От имени пользователя записал 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

Проверил содержимое файла (рис -@fig:033):



Проверка содежимого в файле от имени пользователя

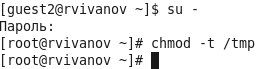
От имени пользователя попробовал удалить файл (рис -@fig:034):

Попытка удаления файла от имени пользователя 

Попытка удаления файла от имени пользователя

Мне не удалось удалить файл.

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



Повышение прав до суперпользователя. Снятие атрибута

Покинул режим суперпользователя командой (рис -@fig:036):

Выход из режима суперпользователя

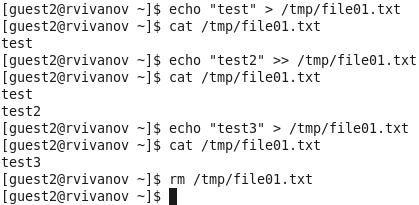
Выход из режима суперпользователя

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

Проверка отсутствия атрибута 

Проверка отсутствия атрибута

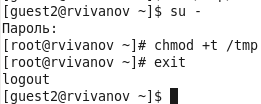
Повторил предыдущие шаги (рис -@fig:038):



Повтор предыдущих шагов

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

Повысил свои права до суперпользователя и вернул атрибут на директорию (рис -@fig:039):



Переход в режим суперпользователя и возврат атрибута

# Выводы

Изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел 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