Отчёт по лабораторной работе 5

Основы информационной безопасности

Нджову Нелиа

Содержание

# 1 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.

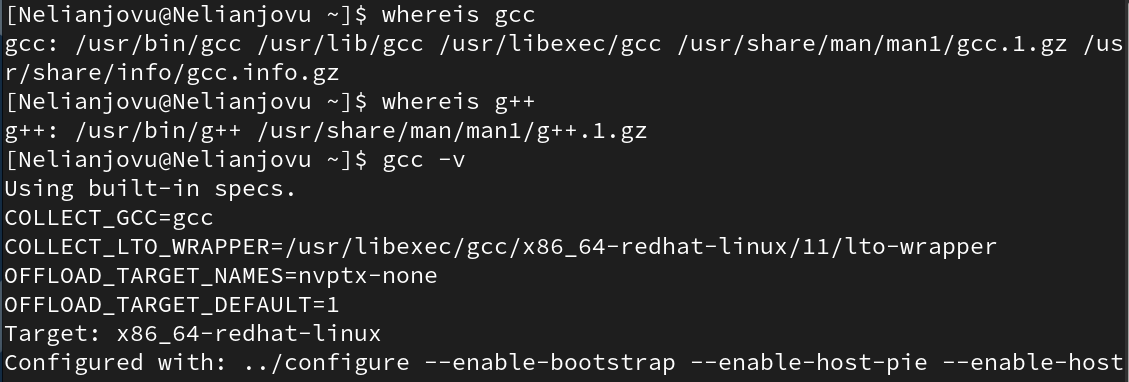
# 2 Задание

1. Создание программы
2. Исследование Sticky-бита

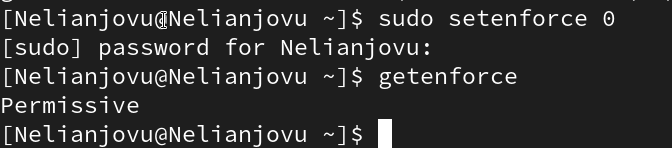
# 3 Выполнение лабораторной работы

**1. Создание программы**

Для этой лабораторной работы, вам необходимо проверить установлен ли компилятор(gcc), используя команду gcc -v. Также осуществляется отключение системы запретом с помощью setenforce 0(рис.1 и рис.2)

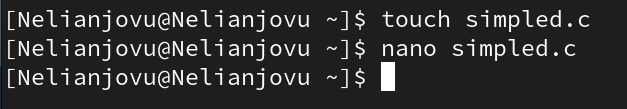


Подготовка к лабораторной работе

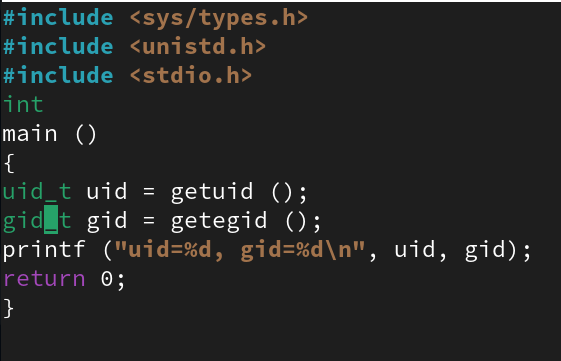


Подготовка к лабораторной работе

Я не мог использовать своего guest пользователя, потому что получила сообщение ошибке когда попробавала установить файл. Из за этого, я использовала суперпользователя, я создала файл simpled.c и записала в него код(рис.3 и рис.4)

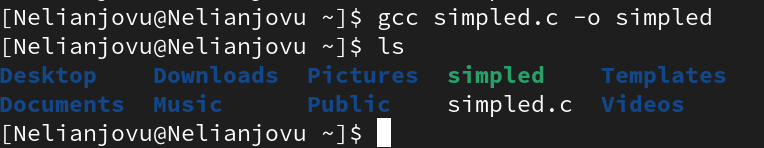


Создание файла



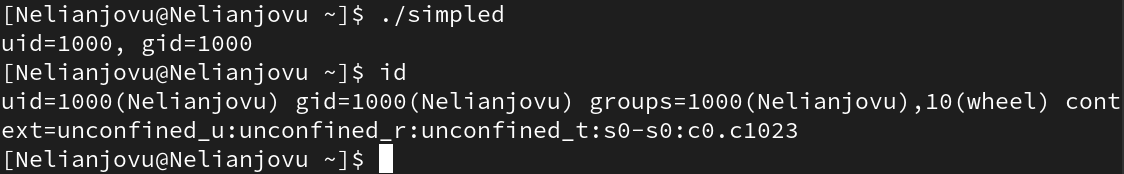
Содержимое файла

Я скомпилировала файл, проверила что он скомпилирован(рис.5)



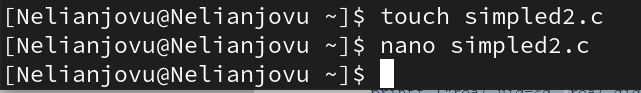
Компиляция файла

Я запустила исполняемый файл. Номера пользователя и группы указаны в выходных данных файла, они отличаются от выходных данных команды id тем, что в выходных данных для исполняемого файла отображается меньше информации, чем в команде id(рис.6)

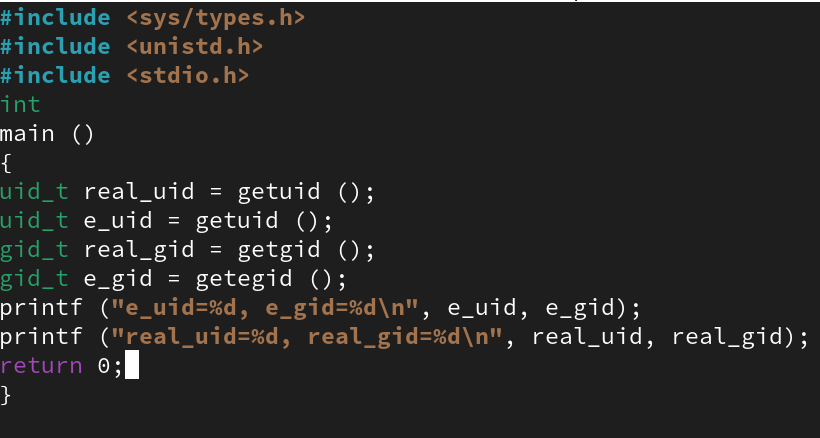


Сравнение команд

Я создала, записывала в файл в simpled2.с(рис.7 и рис.8)

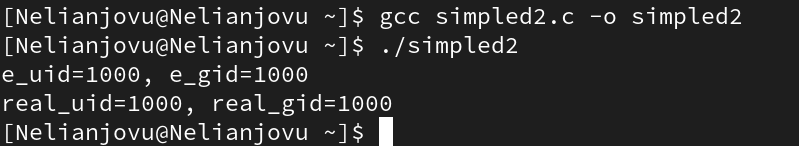


Создание файла



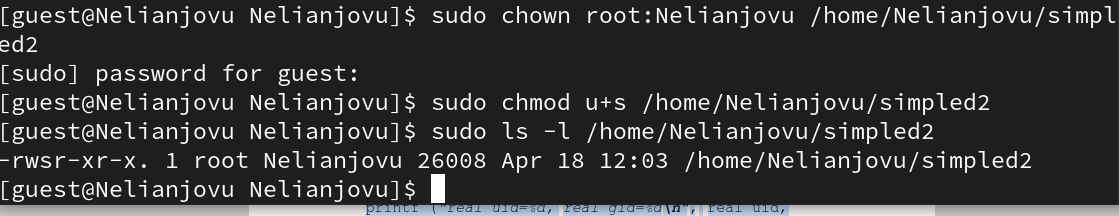
Содержимое файла

Я компилировала файл и запустила программы(рис.9)



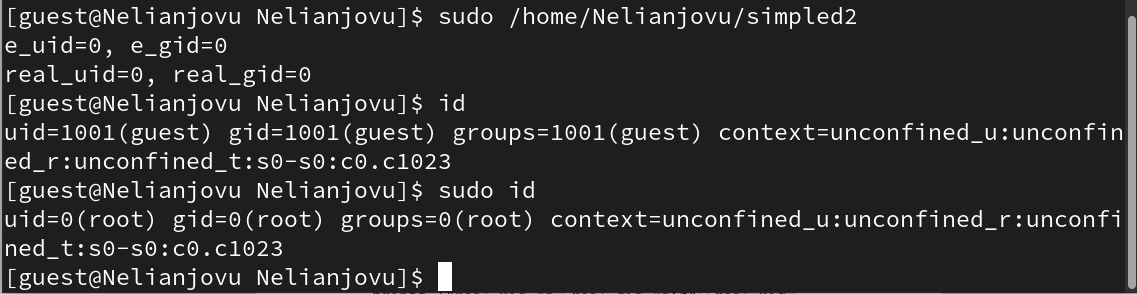
Компиляция файла

Я использовала chown, чтобы сменить владельца файла на суперпользователя, и chmod, чтобы изменить права доступа(рис.10)



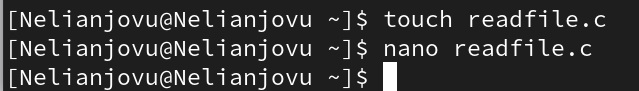
Смена владельца файла и прав доступа к файлу

Я сравнила выходные данные программы и команды id, в очередной раз получила больше информации, используя команды id, чем наша программа(рис.11)

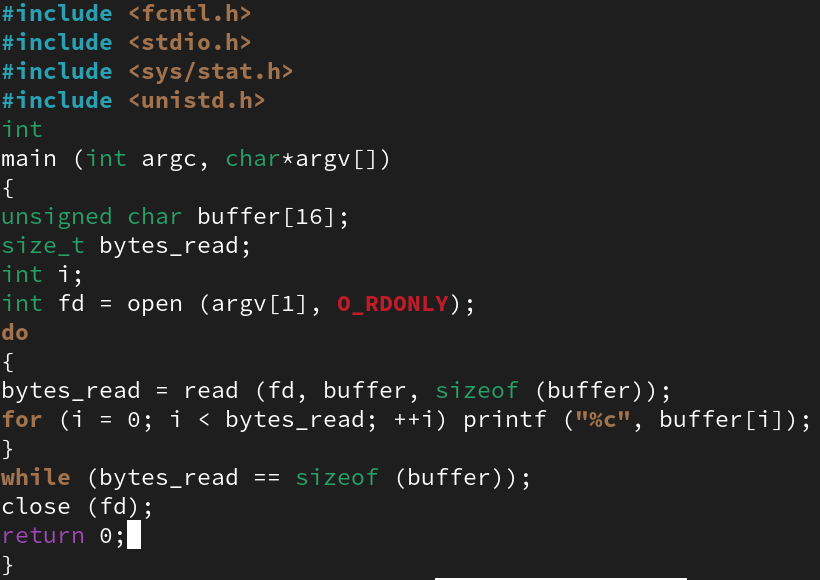


Запуск файла

Я создала, записывала в файл в readfile.с(рис.12 и рис.13)

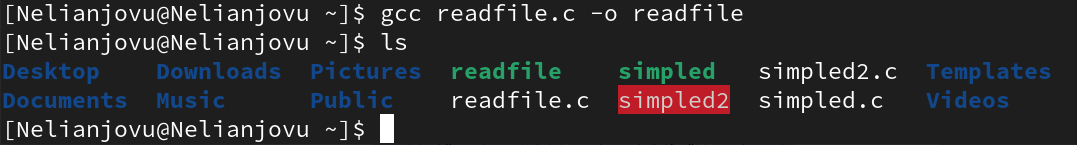


Создание файла



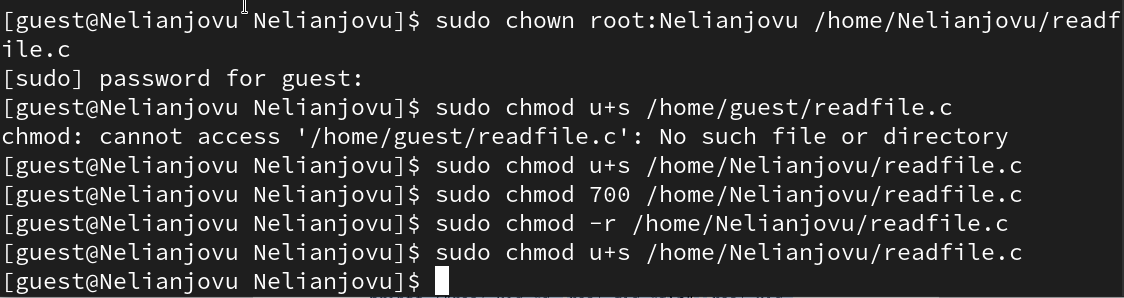
Содержимое файла

Я компилировала файл(рис.14)



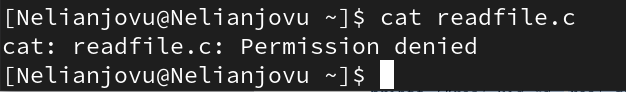
Компиляция файла

И снова, от имени пользователя guest, я меняла владельца файла для чтения. Затем я меняла права доступа, чтобы пользователи Nelianjovu не мог прочитать содержимое файла(рис.15)



Смена владельца файла и прав доступа к файлу

Я попыталась прочитать содержимое файла readfile.с у пользователя Nelianjovu. Я не могу прочитать файл(рис.16)



Попытка прочесть содержимое файла

При попытке прочитать тот же файл с помощью программы readfile выдается сообщение “размытая информация”(рис.17)



Попытка прочесть содержимое файла программой

При попытке прочитать содержимое файла shadow с помощью программы readfile выдается тоже сообщение “размытая информация”(рис.18)



Попытка прочесть содержимое файла программой

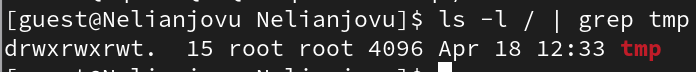
При попытке прочитать содержимое файла shadow с помощью программы readfile от имени пользователя guest получилось(рис.19)



Чтение файла от имени пользователя guest

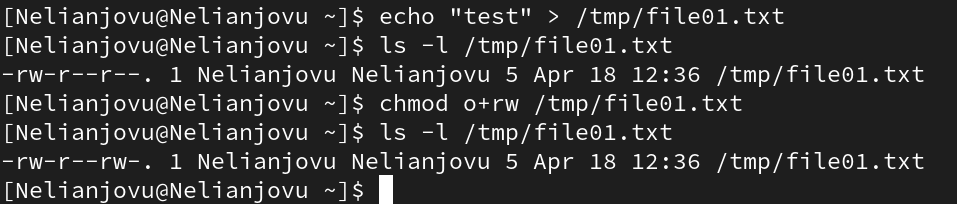
**2. Исследование Sticky-бита**

Я проверила папку tmp на наличие атрибута Sticky, потому что в выходных данных есть буква t, значит, атрибут установлен(рис.20)



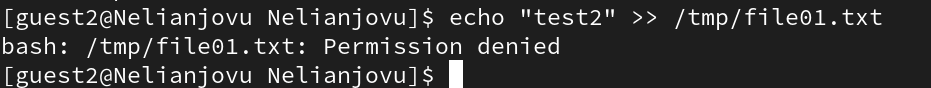
Проверка атрибутов директории tmp

От имени пользователя Nelianjovu создала файл с текстом, добавляла права на чтение и запись для других пользователей(рис.21)



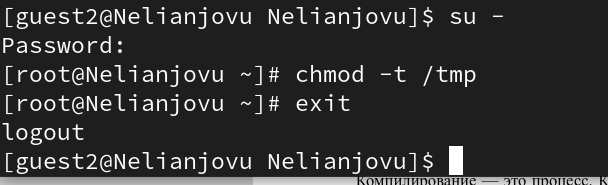
Создание файла, изменение прав доступа

Вхожу в систему от имени пользователя guest2, от его имени перезаписать информацию в файле file 01.txt не могу(рис.22)



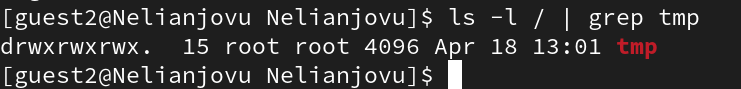
Попытка запись файла

От имени суперпользователя снимала с директории атрибут Sticky(рис.23)



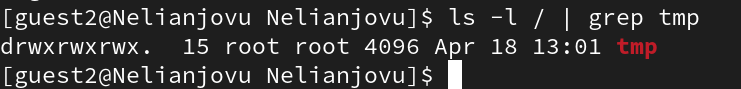
Смена атрибутов файла

Я проверила, что атрибут действительно снят(рис.24)



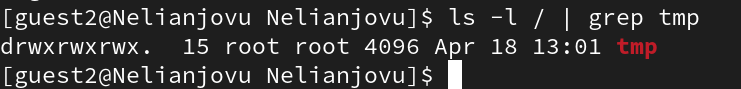
Проверка атрибутов директории

Далее я повторила предыдущие действия. Согласно результатам, запись в файл и повторная запись в файл оставались невозможными без Sticky-бита(рис.25)



Повтор предыдущих действий

Затем я вернула каталог tmp с атрибутом t от имени суперпользователя(рис.26)



Изменение атрибутов

# 4 Выводы

Выполнив эту работу, я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов и получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрила работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.