Лабораторная работа №5.

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Силкина Мария Александровна

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.

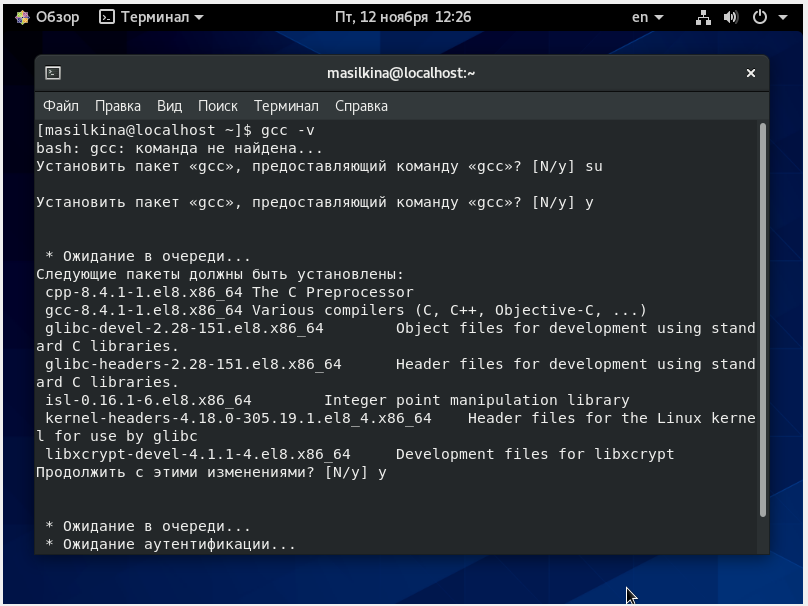
# Задачи

1. Выполнить лабораторную работу согласно заданному порядку.
2. Ознакомится с применением SetUID- и Sticky-битов, изучение их влияния.

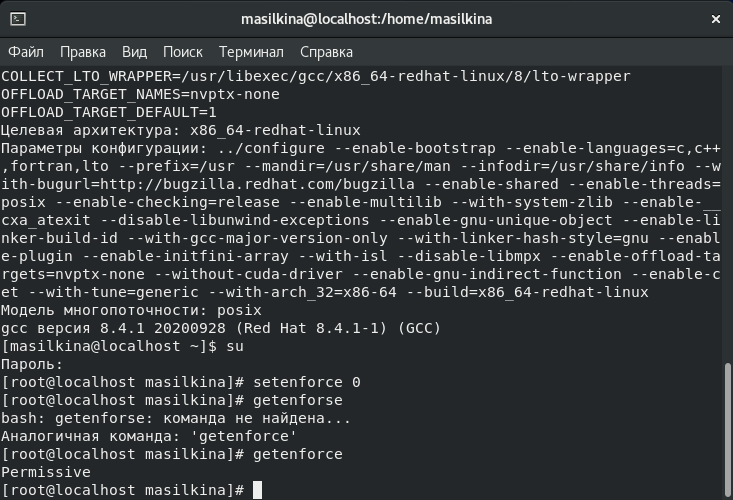
# Выполнение лабораторной работы

## Подготовка лабораторного стенда

Первый шаг заключался в установке компилятора gcc для дальнейшего выполнения лабораторной работы, а также отключении системы запретов (рис 1. @fig:001) (рис 2. @fig:002).



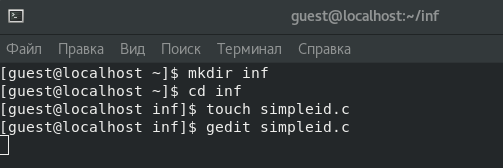
Установка компилятора



Отключение системы запретов

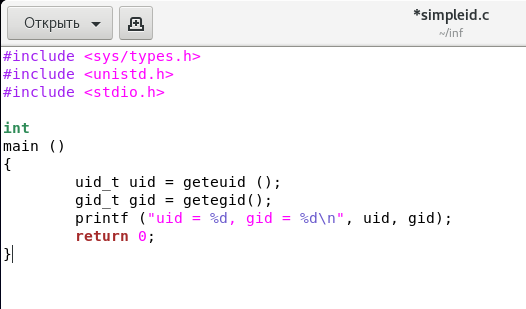
## Создание программ

Я зашла в систему от имени пользователя guest, создала файл simpleid.c (рис 3. @fig:003)



Создание файла и его редактирование

Записала в файл simpleid.c требуемый код (рис 4. @fig:004)



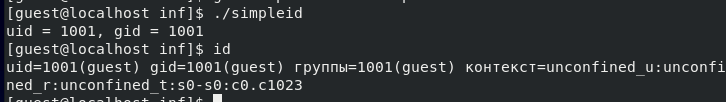
Код программы

Скомпилировала файл simpleid.c (рис 5. @fig:005)

Компиляция

Компиляция

Запустила программу simpleid и системную программу id для сравнения полученных результатов, выведенна информация была идентичной (рис 6. @fig:006)



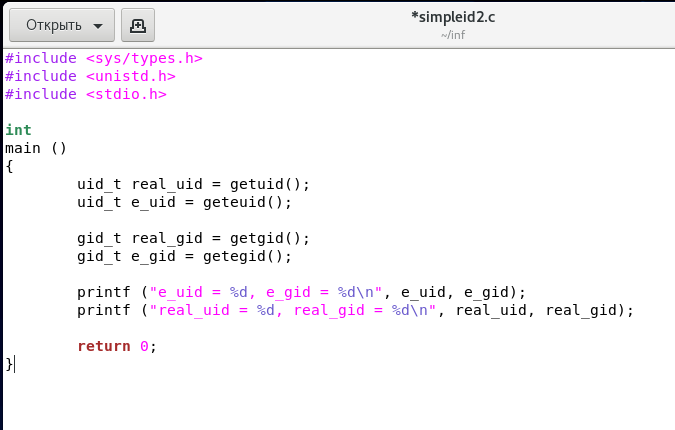
Сравнение вывода программ

Далее я создала второй файл программы simpleid2.c (рис 7. @fig:007)

Создание и редактирование файла

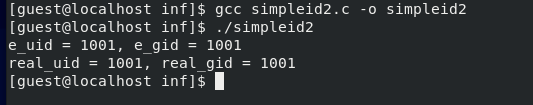
Создание и редактирование файла

Записала в нее код из инструкции к лабораторной работе, он сложнее нежели прошлый, так как в него добавился вывод действительных идентификаторов (рис 8. @fig:008)



Код программы

Скомпилировала и запустила данный файл. Вывод оказался аналогичен выводу предыдущей программы (рис 9. @fig:009)



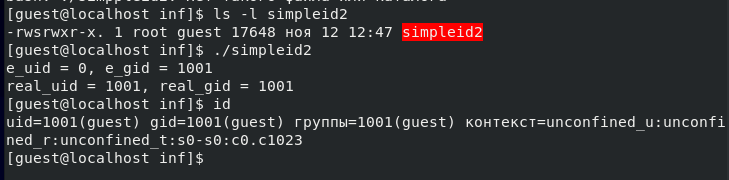
Компиляция и вывод

От имени суперпользователя выполнила команды: для изенения владельца программы и права, с которыми пользователь может выполнить файл только с разрешением владельца (рис 10. @fig:010)

Выполнение команд

Выполнение команд

Запустила simpleid2 и системную программу id для сравнения полученных результатов, выведенная информация отличалась в одном пункте. Проделала тоже самое относительно SetGID-бита (рис 11. @fig:011)

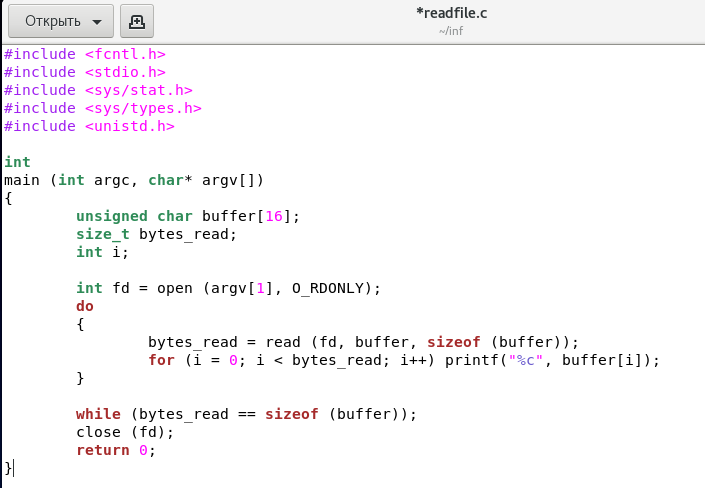


Сравнение вывода программ

Создала новый файл readfile.c и ззаписала в него код из инструкции, скомпилировала ее (рис 12. @fig:012) (рис 13. @fig:013)

Создание файла

Создание файла



Код программы

Сменила владельца файла и изменила права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог и сделала проверку (рис 14. @fig:014) (рис 15. @fig:015) (рис 16. @fig:016)

Смен владельца

Смен владельца

Изменение прав

Изменение прав

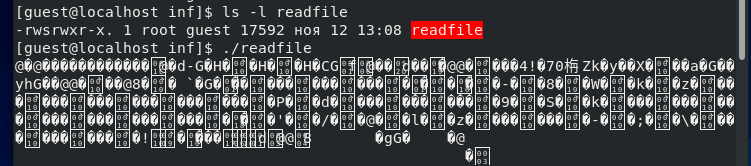
Проверка

Проверка

Установила SetUID-бит и проверила (рис 17. @fig:017) (рис 18. @fig:018)

Установка SetUID-бита

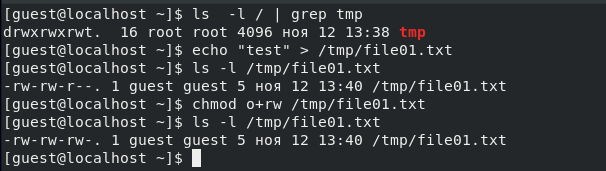
Установка SetUID-бита



Проверка

## Исследование Sticky-бита

Для начала я выяснила установлен ли атрибут Sticky на директории /tmp. Атрибут установлен и обозначается “t”. От имени пользователя guest я создала файл, в который записала слово “test”, посмотрела атрибуты у файла, установила права для разрешения чтения и записи для категории пользователей “others” и проверила, что они верны (рис 19. @fig:019)



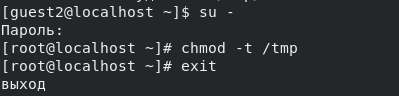
Проверка наличия атрибута, создание файла, установка прав на него

Далее я зашла под пользователем guest2 и попыталась отредактировать дважды данный файл, заменив в нем слово. Данное действие было выполнено успешно. Мне также удавалось проверять содержимое файла, однако удалить файл не получилось (рис 20. @fig:020)



Выполнение действий

Следующим действием я сняла атрибут Sticky на директории /tmp от имени суперпользователя. (рис 21. @fig:021)



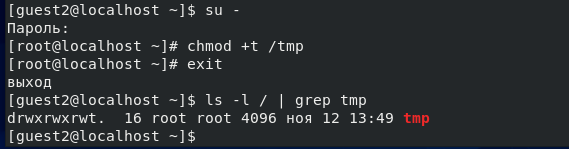
Удаление атрибута

Дальше я попыталась повторить все ранее проделанные действия от пользователя guest2 и мне удалось перезаписать файл, прочитать и удалить (рис 22. @fig:022)



Выполнение действий без атрибута Sticky

Повысила права до суперпользователя и вернула атрибут t на директорию (рис 23. @fig:023)



Возвращение атрибута t

# Выводы

При выполнении данной лабораторной работы я получила практические навыки работы в консоли с дополнительными атрибутами файлов. Я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрела работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Библиография

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.