Отчёт по лабораторной работе

Лабораторная работа 5

Дзугаева Лилия Владславовна

Table of Contents

# 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.

# Выполнение лабораторной работы

1. Вошёл в систему от имени пользователя guest. (рис. 1):

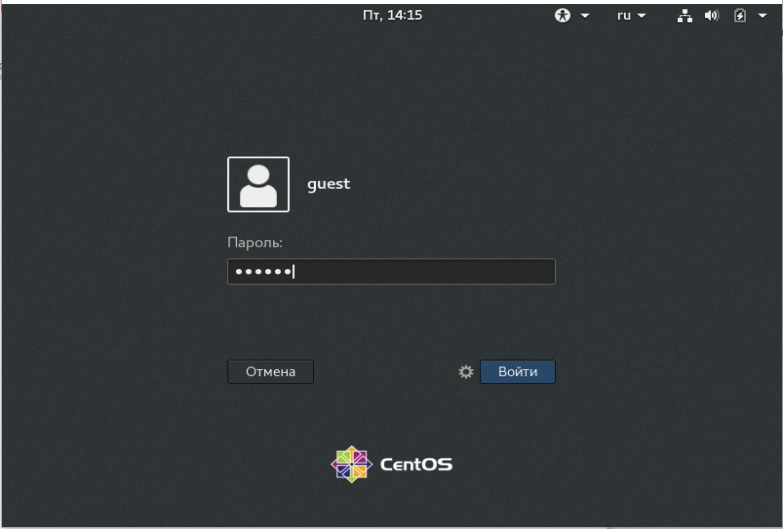


рис. 1. Вход в систему

1. Создал программу simpleid.c (рис. 2)

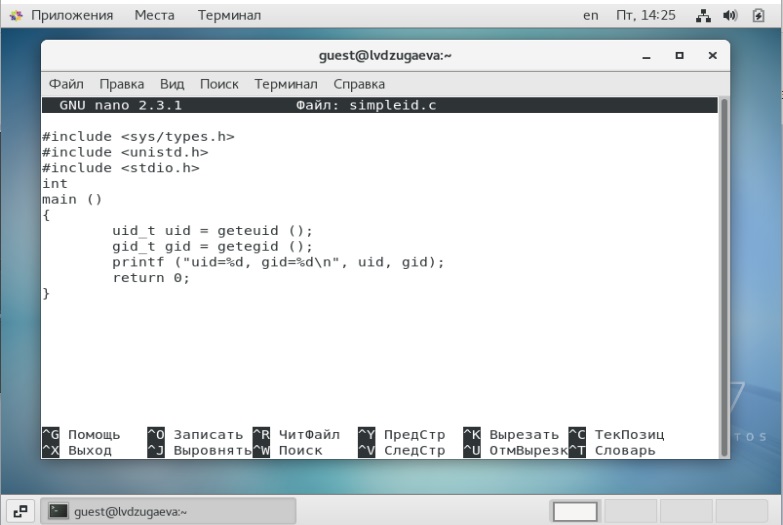


рис. 2. Создание программы

1. Скомпилировал программу и убедился, что файл программы создан: *gcc simpleid.c -o simpleid* (рис. 3).

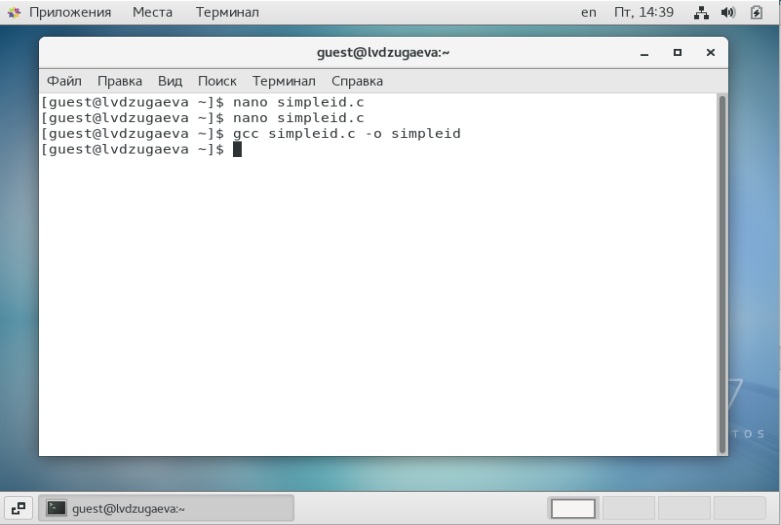


рис. 3. Компиляция программы

1. Выполнил программу simpleid: *./simpleid* (рис. 4)

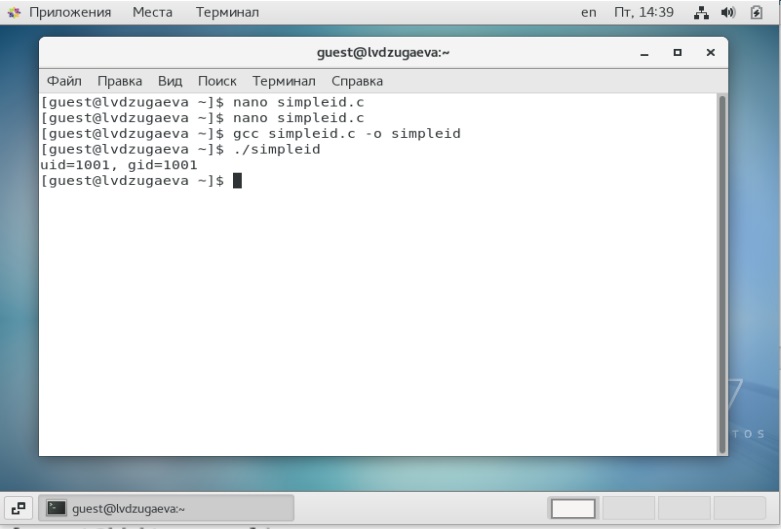


рис. 4. Выполнение программы

1. Выполнил системную программу id и сравнил полученный результат с данными предыдущего пункта задания: программа работает верно, результаты совпадают. (рис. 5)

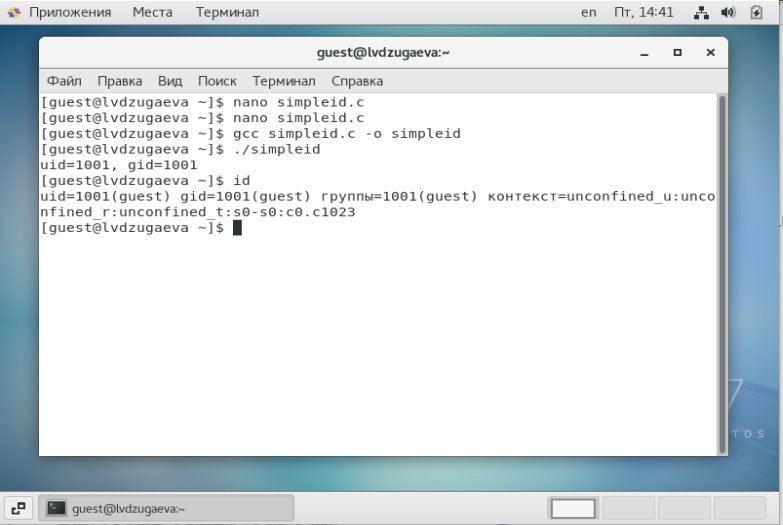


рис. 5. Верность выполнения программы

1. Усложнил программу, добавив вывод действительных идентификаторов: (рис. 6)

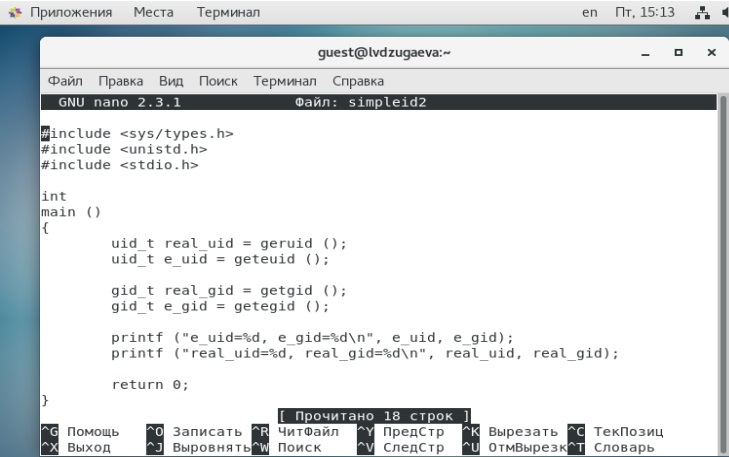


рис. 6. Усложнение программы

Получившуюся программу назвал *simpleid2.c*.

1. Скомпилировал и запустил simpleid2.c. (рис. 7)

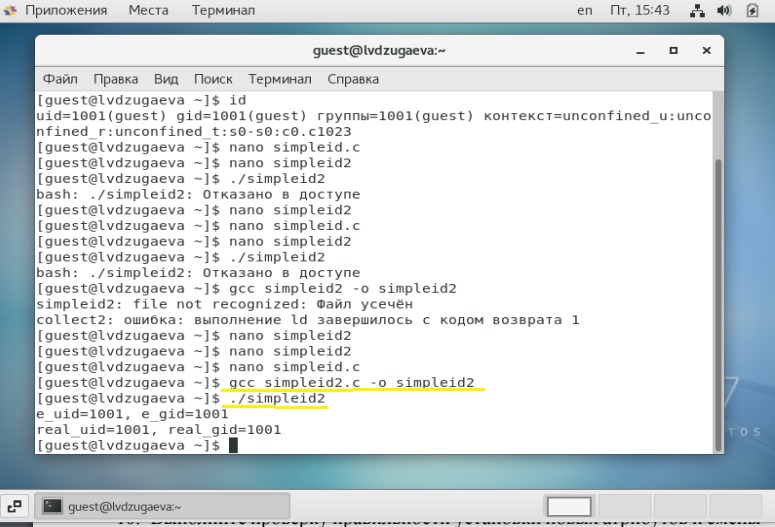


рис. 7. Компиляция второй программы

1. От имени суперпользователя выполнил команды: *chown root:guest /home/guest/simpleid2* и *chmod u+s /home/guest/simpleid2* (рис. 8)

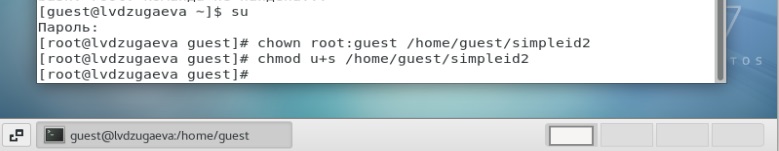


рис. 8. Выполнение команд

1. Временно повысил свои права с помощью команды su (рис. 9)

рис. 9. Повышение прав

рис. 9. Повышение прав

1. Выполнил проверку правильности установки новых атрибутов и смены владельца файла simpleid2: *ls –l simpleid2* (рис. 10)

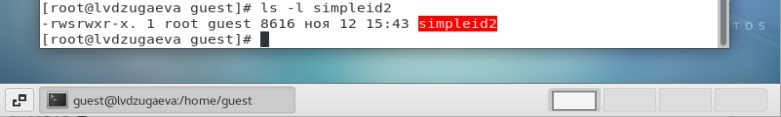


рис. 10. Проверка шагов

1. Запустил simpleid2 и id: (рис. 11)

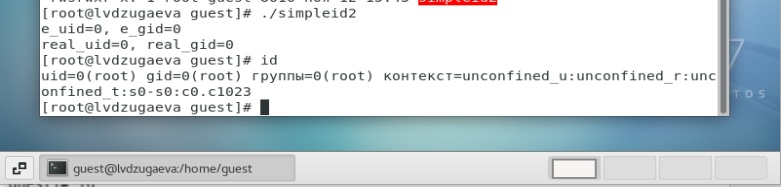


рис. 11. Запуск программы

Результаты совпадают.

1. Проделал тоже самое относительно SetGID-бита. (рис. 12)

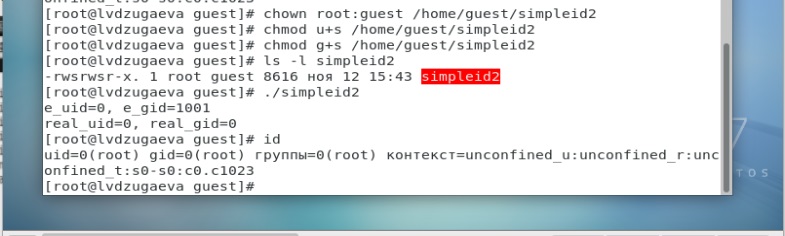


рис. 12. Повтор предыдущих шагов

1. Создал программу readfile.c (рис. 13)

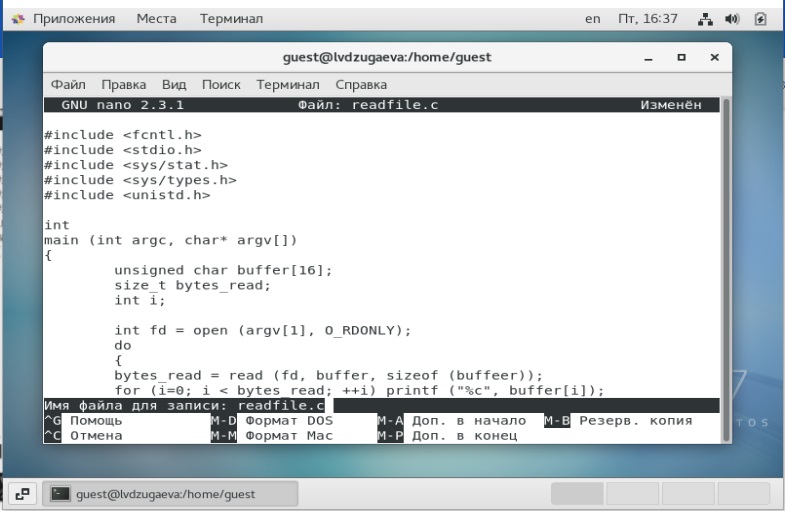


рис. 13. Создание третьей программы

1. Откомпилировал её. (рис. 14)

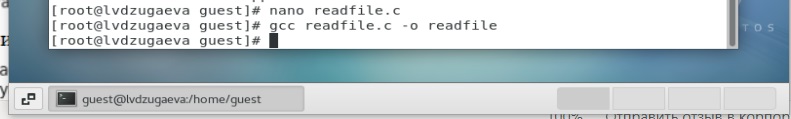


рис. 14. Компиляция программы

1. Сменил владельца у файла readfile.c и изменил права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог. (рис. 15)

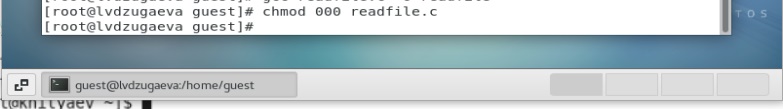


рис. 15. Смена владельца

**Исследование Sticky-бита**

1. Выяснил, установлен ли атрибут Sticky на директории /tmp, для чего выполнил команду *ls -l / | grep tmp*. (рис. 1)

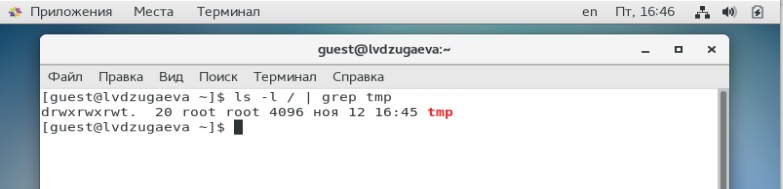


рис. 1. Проверка атрибута

1. От имени пользователя guest создал файл file01.txt в директории /tmp со словом test: *echo “test” > /tmp/file01.txt*. (рис. 2)

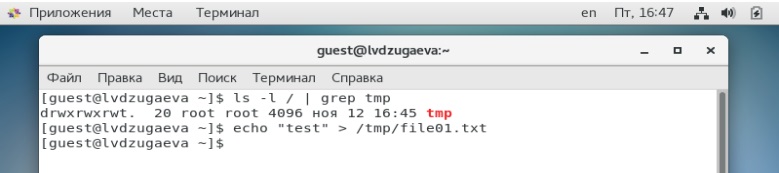


рис. 2. Создание файла

1. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные». Первоначально все группы имели право на чтение, а запись могли осуществлять все, кроме «остальных пользователей». (рис. 3)

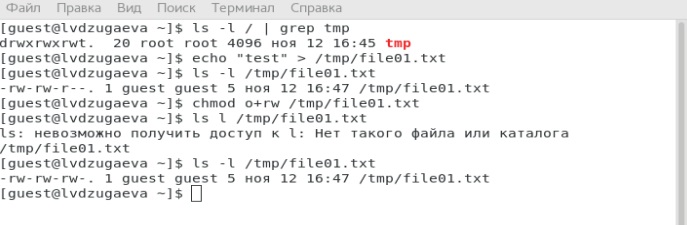


рис. 3. Просмотр атрибутов

1. От пользователя guest2 (не являющегося владельцем) попробовал прочитать файл /tmp/file01.txt. (рис. 4)

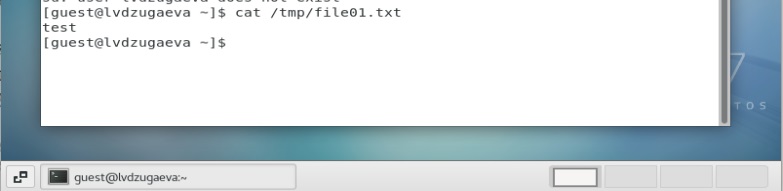


рис. 4. Чтение файла

1. От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test2, стерев при этом всю имеющуюся в файле информацию с помощью команды *echo “test2” > /tmp/file01.txt*. (рис. 5)



рис. 5. Дозапись в файл

1. Проверил содержимое файла командой *cat /tmp/file01.txt* (рис. 6)

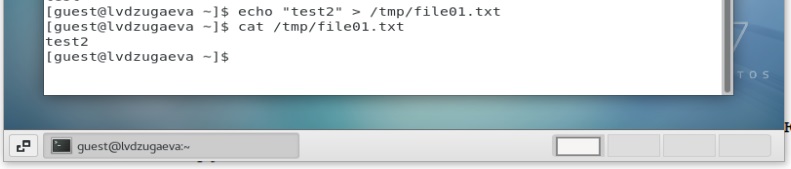


рис. 6. Проверка содержимого

1. От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test3 командой *echo “test3” > /tmp/file01.txt*. (рис. 7)

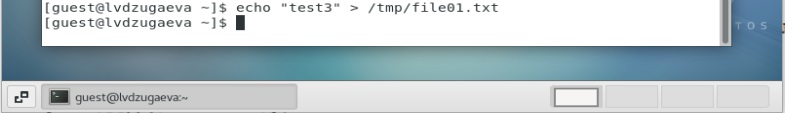


рис. 7. Дозапись в файл

1. Проверил содержимое файла командой *cat /tmp/file01.txt*. (рис. 8)

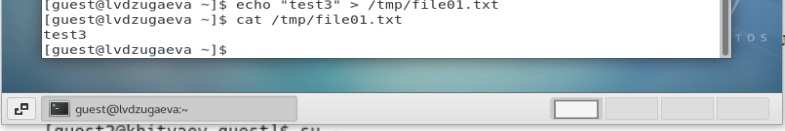


рис. 8. Проверка содержимого

1. От пользователя guest2 попробовал удалить файл /tmp/file01.txt c помощью команды *rm /tmp/file0l.txt*. (рис. 9)

рис. 9. Удаление файла

рис. 9. Удаление файла

1. Повысил свои права до суперпользователя командой su - и выполнил после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: (рис. 10)

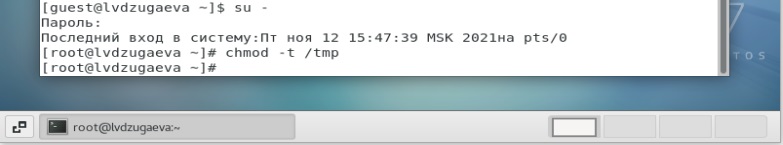


рис. 10. Выполнение команды

1. Покинул режим суперпользователя командой exit. (рис. 11)

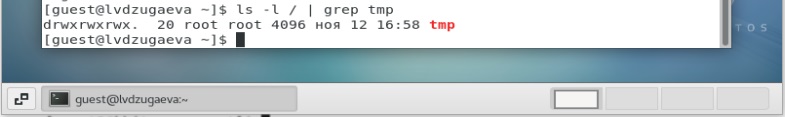


рис. 11. Смена режима

1. Повысил свои права до суперпользователя c помощью команды su - и вернул атрибут t на директорию /tmp. (рис. 12)



рис. 12. Повышение прав

# Выводы

Благодаря данной лабораторной работе, я 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{.unnumbered}