**Лабораторная работа №5: отчет.**

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

Евдокимов Максим Михайлович. Группа - НФИбд-01-20.

**Содержание**

[**Цель работы** **5**](#_Toc10152)

[**Задание** **6**](#_Toc10153)

[**Теория** **7**](#_Toc10154)

[Подготовка лабораторного стенда 7](#_Toc10155)

[Компилирование программ 7](#_Toc10156)

[**Выполнение лабораторной работы** **8**](#_Toc10157)

[Пункт 1.0 8](#_Toc10158)

[Пункт 1.1 8](#_Toc10159)

[Пункт 1.2 9](#_Toc10160)

[Пункт 1.3 9](#_Toc10161)

[Пункт 1.4 9](#_Toc10162)

[Пункт 1.5 10](#_Toc10163)

[Пункт 1.6 10](#_Toc10164)

[Пункт 1.7 11](#_Toc10165)

[Пункт 1.8 11](#_Toc10166)

[Пункт 1.9 11](#_Toc10167)

[Пункт 1.10 12](#_Toc10168)

[Пункт 1.11 13](#_Toc10169)

[Пункт 1.12 13](#_Toc10170)

[Пункт 1.13 13](#_Toc10171)

[Пункт 1.14 14](#_Toc10172)

[Пункт 1.15 14](#_Toc10173)

[Пункт 1.16 15](#_Toc10174)

[Пункт 1.17 15](#_Toc10175)

[Пункт 1.18 15](#_Toc10176)

[Пункт 1.19 16](#_Toc10177)

[**Исследование Sticky-бита** **17**](#_Toc10178)

[Пункт 2.1 17](#_Toc10179)

[Пункт 2.2 17](#_Toc10180)

[Пункт 2.3 17](#_Toc10181)

[Пункт 2.4 18](#_Toc10182)

[Пункт 2.5 18](#_Toc10183)

[Пункт 2.6 18](#_Toc10184)

[Пункт 2.7 19](#_Toc10185)

[Пункт 2.8 19](#_Toc10186)

[Пункт 2.9 19](#_Toc10187)

[Пункт 2.10 20](#_Toc10188)

[Пункт 2.11 20](#_Toc10189)

[Пункт 2.12 20](#_Toc10190)

[Пункт 2.13 21](#_Toc10191)

[Пункт 2.14 21](#_Toc10192)

[Пункт 2.15 22](#_Toc10193)

[**Выводы** **23**](#_Toc10194)

[**Список литературы** **24**](#_Toc10195)

**Список иллюстраций**

1. Подготовка . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
2. Вход в систему . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
3. Код simpleid . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
4. Компиляция и проверка . . . . . . . . . . . . . . . . . . . . . . . 9
5. Запуск программы simpleid . . . . . . . . . . . . . . . . . . . . . 10
6. Проверка через id . . . . . . . . . . . . . . . . . . . . . . . . . . 10
7. Код simpleid2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10
8. Компиляция и запуск . . . . . . . . . . . . . . . . . . . . . . . . 11
9. Изменяем UID файла . . . . . . . . . . . . . . . . . . . . . . . . . 11
10. Расмотрим файлы . . . . . . . . . . . . . . . . . . . . . . . . . . 12
11. Проверка программы simpleid2 . . . . . . . . . . . . . . . . . . . 12
12. Запуск программы simpleid2 . . . . . . . . . . . . . . . . . . . . 13
13. Меняем GID файла . . . . . . . . . . . . . . . . . . . . . . . . . . 13
14. Код readfile.c . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14
15. Компиляция readfile.c . . . . . . . . . . . . . . . . . . . . . . . . 14
16. Изменение владельца readfile . . . . . . . . . . . . . . . . . . . . 14
17. Проверка readfile.c . . . . . . . . . . . . . . . . . . . . . . . . . . 15
18. Смена пользователя readfile . . . . . . . . . . . . . . . . . . . . . 15
19. Провека 1 работы программы readfile . . . . . . . . . . . . . . . . 16
20. Провека 2 работы программы readfile . . . . . . . . . . . . . . . . 16
21. Смотрим атрибуты директории /tmp . . . . . . . . . . . . . . . . 17
22. Создание файла file01.txt . . . . . . . . . . . . . . . . . . . . . . 17
23. Изменение прав доступа . . . . . . . . . . . . . . . . . . . . . . 18
24. Проверяем содержимое файла . . . . . . . . . . . . . . . . . . . 18
25. Изменяем содержание файла . . . . . . . . . . . . . . . . . . . . 18
26. Проверяем содержимое файла . . . . . . . . . . . . . . . . . . . 19
27. Изменяем содержание файла . . . . . . . . . . . . . . . . . . . . 19
28. Проверяем содержимое файла . . . . . . . . . . . . . . . . . . . 19
29. Продуем удалить файл . . . . . . . . . . . . . . . . . . . . . . . . 20
30. меняем атрибут Sticky-бита . . . . . . . . . . . . . . . . . . . . . 20
31. Выход из суперпользователя . . . . . . . . . . . . . . . . . . . . 20
32. Проверка атрибутов . . . . . . . . . . . . . . . . . . . . . . . . . 21
33. Повтор шагов . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 21
34. удаление файла . . . . . . . . . . . . . . . . . . . . . . . . . . . 22
35. Возвращаем все изменения . . . . . . . . . . . . . . . . . . . . . 22

# 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.

# Задание

1. Изучить основы и особенности компилирование программ на Linux, работа с gcc, понятие объектный файл и другие.
2. Изучение механизмов изменения идентификаторов SetUID, SetGID и Stickyбитов.
3. Исследование Sticky-бита и рассмотрение его принципов работы в случае двух пользователей.

# Теория

## Подготовка лабораторного стенда

Командой “gcc -v” проверяем наличие gcc и если нет то используем команду

“yum install gcc”. Также чтобы менять атрибуты в системе уберём встроенную защиту от их изменений - SELinux, при помощи команды “setenforce 0”. И проверив что она работает командой “getenforce”, которая должна вывести: Permissive.

## Компилирование программ

Компиляторы, доступные в Linux-системах, являются частью коллекции GNU-компиляторов, известной как GCC (GNU Compiller Collection, подробнее см. http://gcc.gnu.org). В неё входят компиляторы языков С, С++, Java, Objective-C, Fortran и Chill. Будем использовать лишь первые два.

Так из наличие можно проверить двумя командами: “whereis gcc” и “whereis g++”. Также в ходе работы будет создаваться - объектные файлы, которые невозможно запускать и использовать, поэтому после компиляции для получения готовой программы объектные файлы необходимо скомпоновать (автоудалить). Поэтому в ходе работы мы будем использовать команду “gcc файл.c -o файл” (где файл это имя файла кода с расширением .c), она не остовляет объектных файлов и даёт готовый к запуску файл.

# Выполнение лабораторной работы

## Пункт 1.0

Выполняем подготовку перед тем как начать работать, проверив наличие необходимых программ и их местоположение.

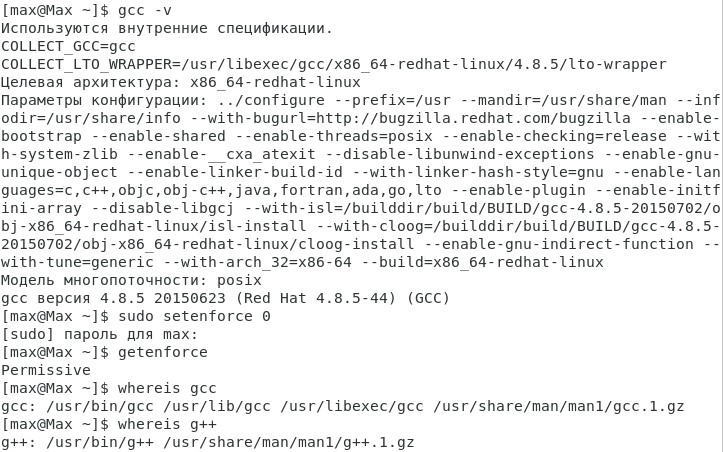


Рис. 1: Подготовка

## Пункт 1.1

Войдим в систему от имени пользователя guest.



Рис. 2: Вход в систему

## Пункт 1.2

Создаём программу simpleid.c и вводим указанный код.

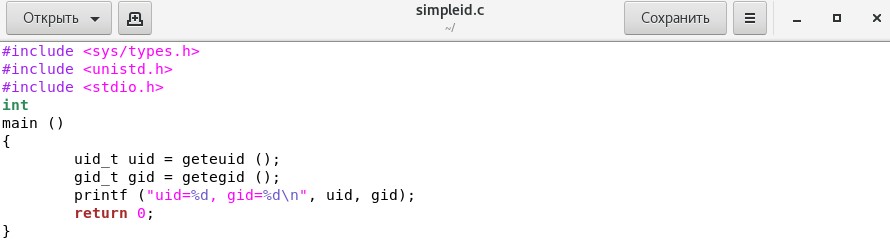


Рис. 3: Код simpleid

## Пункт 1.3

Скомплилируем программу командой “gcc simpleid.c -o simpleid” и убедимся, что файл программы создан просмотрев папку.

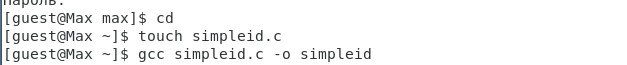


Рис. 4: Компиляция и проверка

## Пункт 1.4

Выполните программу simpleid командой “./simpleid”.



Рис. 5: Запуск программы simpleid

## Пункт 1.5

Выполним системную программу “id” и сравним полученный вами результат с данными предыдущего пункта задания.

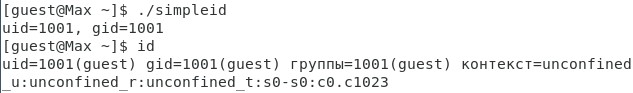


Рис. 6: Проверка через id

## Пункт 1.6

Усложняем программу, добавив вывод действительных идентификаторов. Для этого создадим новый файл командой “touch simpleid2.с”.

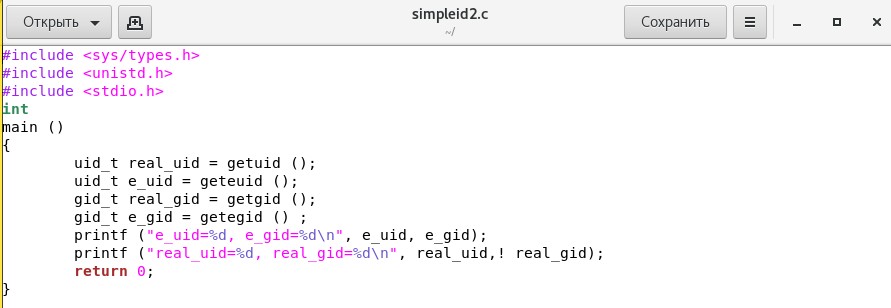


Рис. 7: Код simpleid2

## Пункт 1.7

Скомпилируйте и запустите simpleid2.c командами “gcc simpleid2.c -o simpleid2” и “./simpleid2”.

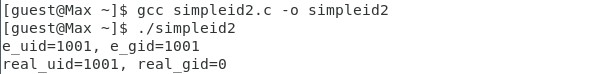


Рис. 8: Компиляция и запуск

## Пункт 1.8

От имени суперпользователя выполним команды “sudo chown root:guest /home/guest/simpleid2” и “sudo chmod u+s /home/guest/simpleid2”.



Рис. 9: Изменяем UID файла

## Пункт 1.9

Используя sudo или повысив временно свои права с помощью su. Поясним, что делают эти команды.

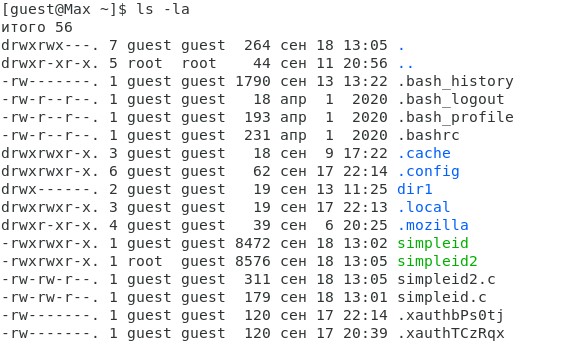


Рис. 10: Расмотрим файлы

## Пункт 1.10

Выполним проверку правильности установки новых атрибутов и смены владельца файла simpleid2 командой “ls -l simpleid2”.

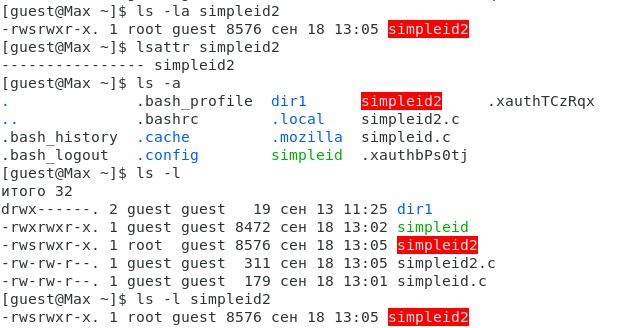


Рис. 11: Проверка программы simpleid2

## Пункт 1.11

Запустим simpleid2 и id командами “./simpleid2” и “id”. Сравним результаты.

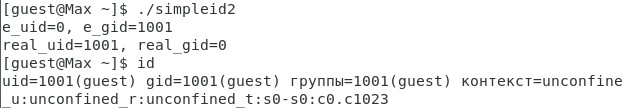


Рис. 12: Запуск программы simpleid2

## Пункт 1.12

Проделаем тоже самое относительно SetGID-бита командой “sudo chmod g+s /home/guest/simpleid2”.



Рис. 13: Меняем GID файла

## Пункт 1.13

Создаём программу readfile.c.

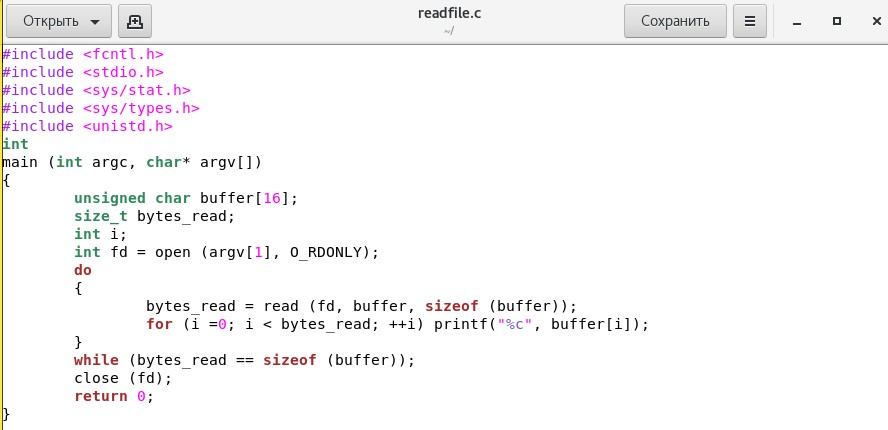


Рис. 14: Код readfile.c

## Пункт 1.14

Откомпилируем код выше ранее используемыми командами.



Рис. 15: Компиляция readfile.c

## Пункт 1.15

Сменим владельца у файла readfile.c (или любого другого текстового файла в системе) и изменим права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог. (выполнено не в полной мере)



Рис. 16: Изменение владельца readfile

## Пункт 1.16

Проверим, что пользователь guest не может прочитать файл readfile.c.

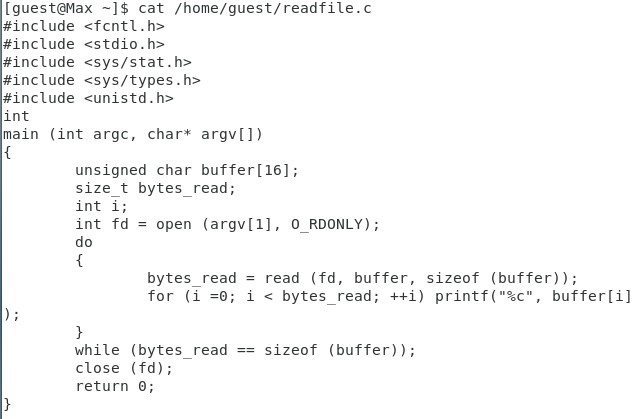


Рис. 17: Проверка readfile.c

## Пункт 1.17

Сменим у программы readfile владельца и установите SetU’D-бит.



Рис. 18: Смена пользователя readfile

## Пункт 1.18

Проверим, может ли программа readfile прочитать файл readfile.c?

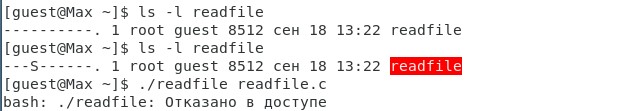


Рис. 19: Провека 1 работы программы readfile

## Пункт 1.19

Проверим, может ли программа readfile прочитать файл /etc/shadow? Отразим полученный результат и ваши объяснения в отчёте

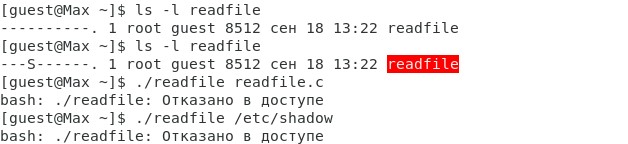


Рис. 20: Провека 2 работы программы readfile

# Исследование Sticky-бита

## Пункт 2.1

Выясняем, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду “ls -l / | grep tmp”.



Рис. 1: Смотрим атрибуты директории /tmp

## Пункт 2.2

От имени пользователя guest создим файл file01.txt в директории /tmp со словом test командой “echo”test” > /tmp/file01.txt”.



Рис. 2: Создание файла file01.txt

## Пункт 2.3

Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные» команды “ls -l /tmp/file01.txt”, “chmod o+rw /tmp/file01.txt” и “ls -l /tmp/file01.txt”.

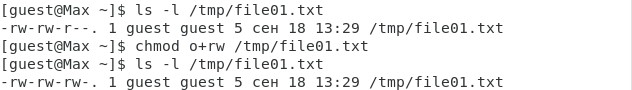


Рис. 3: Изменение прав доступа

## Пункт 2.4

От пользователя guest2 (не являющегося владельцем) попробуем прочитать файл командой “cat /tmp/file01.txt”.



Рис. 4: Проверяем содержимое файла

## Пункт 2.5

От пользователя guest2 дозаписываем в файл /tmp/file01.txt слово test2 командой “echo”test2” > /tmp/file01.txt”. Что проходит успешно.



Рис. 5: Изменяем содержание файла

## Пункт 2.6

Проверим содержимое файла командой “cat /tmp/file01.txt”.



Рис. 6: Проверяем содержимое файла

## Пункт 2.7

От пользователя guest2 попробуйте записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой “echo”test3” >

/tmp/file01.txt”.

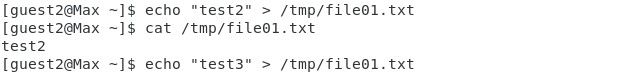


Рис. 7: Изменяем содержание файла

## Пункт 2.8

Проверим содержимое файла командой “cat /tmp/file01.txt”.



Рис. 8: Проверяем содержимое файла

## Пункт 2.9

От пользователя guest2 попробуем удалить файл /tmp/file01.txt командой “rm

/tmp/fileOl.txt”.



Рис. 9: Продуем удалить файл

## Пункт 2.10

Повысим свои права до суперпользователя командой “su -” и выполните после этого команду, снимающую атрибут t (Sticky-бит) “chmod -t /tmp”.

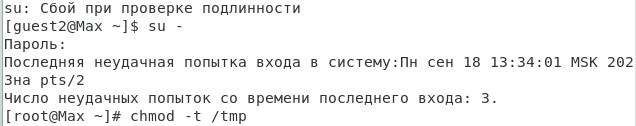


Рис. 10: меняем атрибут Sticky-бита

## Пункт 2.11

Покиньте режим суперпользователя командой “exit”.

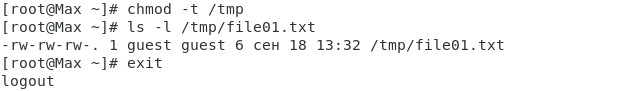


Рис. 11: Выход из суперпользователя

## Пункт 2.12

От пользователя guest2 проверим, что атрибута t у директории /tmp нет: “ls -l / | grep tmp”.



Рис. 12: Проверка атрибутов

## Пункт 2.13

Повторив предыдущие шаги, можем заметить что мы теперь можем взаимодействовать с файлом как раньше и способны его удалить.

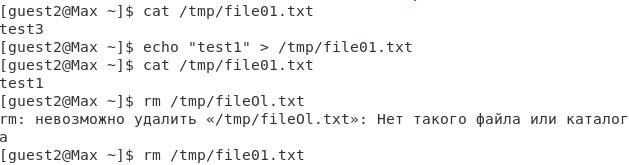


Рис. 13: Повтор шагов

## Пункт 2.14

Удалось удалить файл от имени пользователя, не являющегося его владельцем.

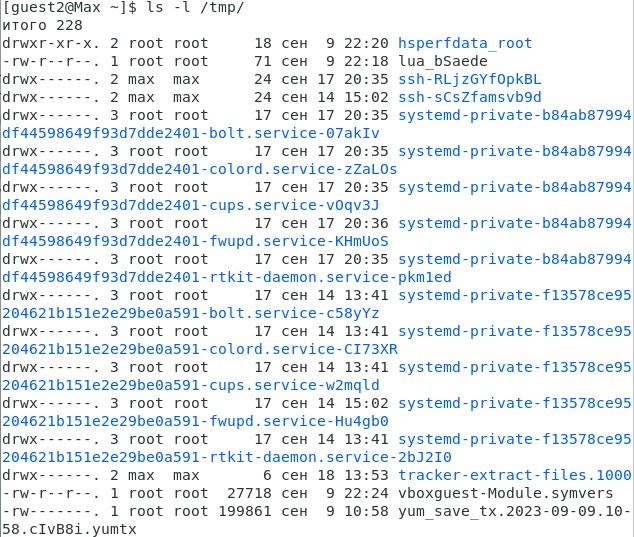


Рис. 14: удаление файла

## Пункт 2.15

Повысим свои права до суперпользователя и вернём атрибут t на директорию выполнив цепочку команд “su -”,“chmod +t /tmp” и “exit”.



Рис. 15: Возвращаем все изменения

# Выводы

Изучены механизмы изменения идентификаторов UID, GID и Sticky-битов. Получены практическе навыки работы в консоли с дополнительными атрибутами. Рассмотрены работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Список литературы

1. [Основные команды для работы с Linux](https://eternalhost.net/blog/sozdanie-saytov/osnovnye-komandy-linux)
2. [Основы управления пользоателем и командой su](https://losst.pro/komanda-su-v-linux)
3. [Файл лабораторной работы](https://esystem.rudn.ru/pluginfile.php/2090279/mod_resource/content/2/005-lab_discret_sticky.pdf)
4. [Linux всё о правах доступа к файлам](https://itdid.ru/file_permissions.html)
5. [Работа с дополнительными атрибутами](https://help.ubuntu.ru/wiki/стандартные_права_unix)