Отчёт по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Тимур Дмитриевич Калинин

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 Выполнение лабораторной работы

## 2.1 Создание программы

1. Войдите в систему от имени пользователя guest
2. Создайте программу simpleid.c ([Рис. 1](#fig:001)).

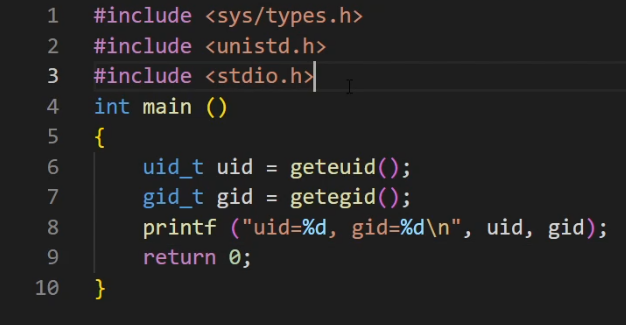


Figure 1: Код simpleid.c

1. Скомплилируйте программу и убедитесь, что файл программы создан ([Рис. 2](#fig:002))
2. Выполните программу simpleid ([Рис. 2](#fig:002)).

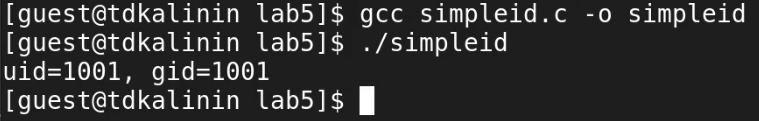


Figure 2: Компиляция и выполнение

1. Выполните системную программу id и сравните полученный вами результат с данными предыдущего пункта задания ([Рис. 3](#fig:003)).

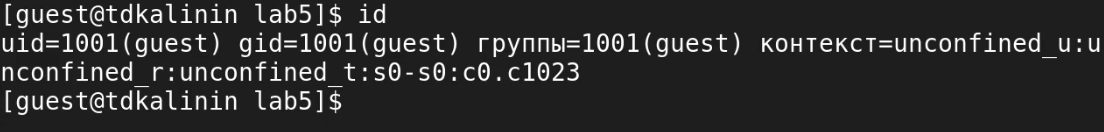


Figure 3: Выполнение id

1. Усложните программу, добавив вывод действительных идентификаторов ([Рис. 4](#fig:004)).

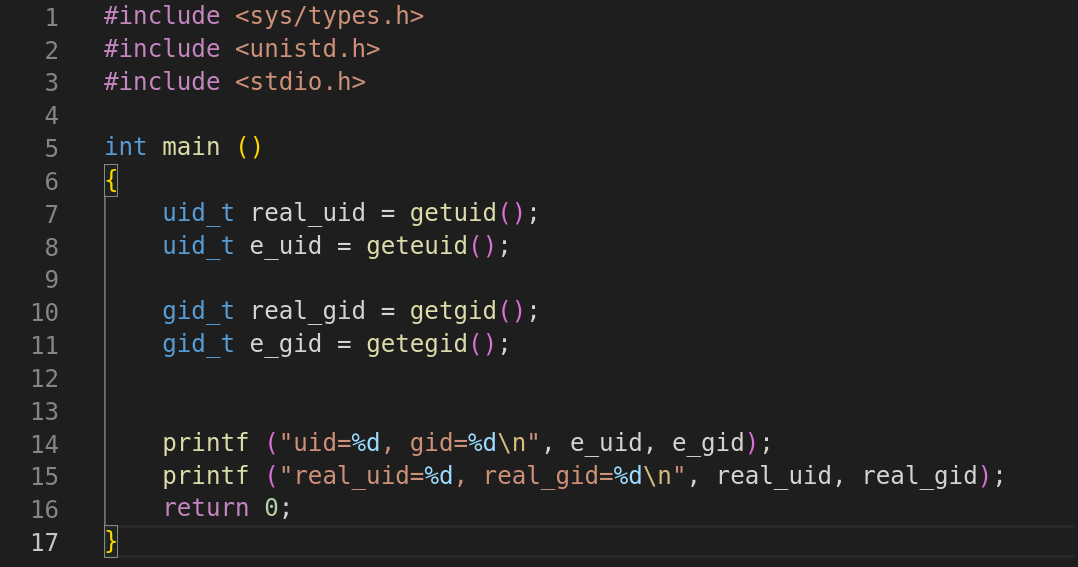


Figure 4: Код simpleid2.c

1. Скомпилируйте и запустите simpleid2.c ([Рис. 5](#fig:005)).

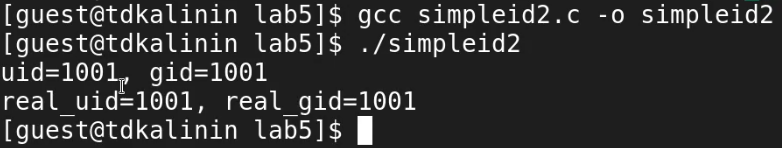


Figure 5: Компиляция и выполнение simpleid2.c

1. От имени суперпользователя выполните команды ([Рис. 6](#fig:006)).

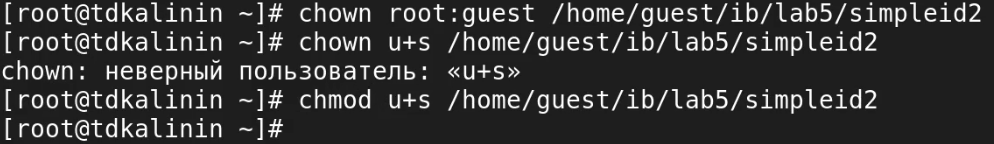


Figure 6: Установка прав

1. Используйте sudo или повысьте временно свои права с помощью su.
2. Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2 ([Рис. 7](#fig:007)).

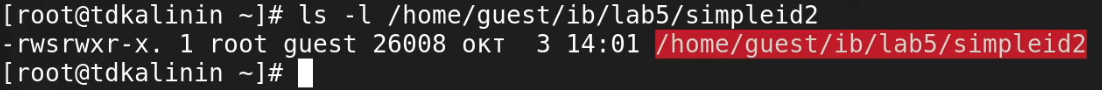


Figure 7: Проверка

1. Запустите simpleid2 ([Рис. 8](#fig:008)).

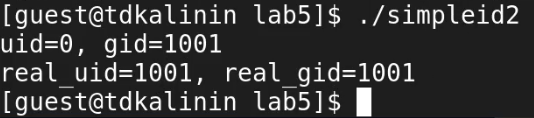


Figure 8: Запуск simpleid2

1. Проделайте тоже самое относительно SetGID-бита ([Рис. 9](#fig:009)).

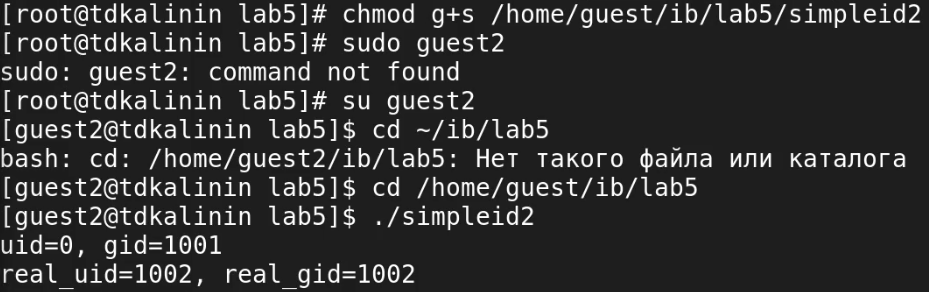


Figure 9: Установка setGID-бита

1. Создайте программу readfile.c ([Рис. 10](#fig:010)).

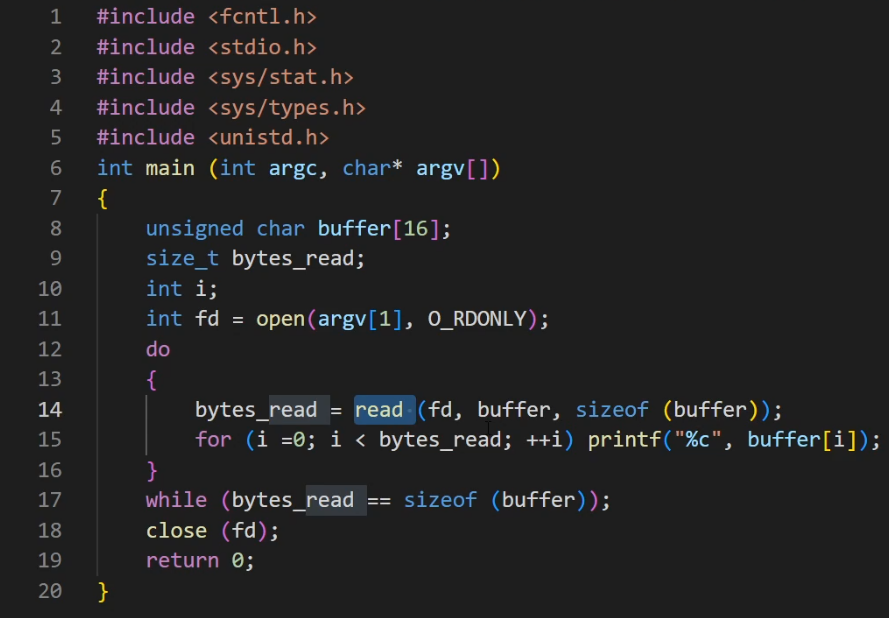


Figure 10: Код readfile.c

1. Откомпилируйте её ([Рис. 11](#fig:011)).

Figure 11: Комплиляция readfile.c

Figure 11: Комплиляция readfile.c

1. Смените владельца у файла readfile.c (или любого другого текстового файла в системе) и измените права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог ([Рис. 12](#fig:012)).

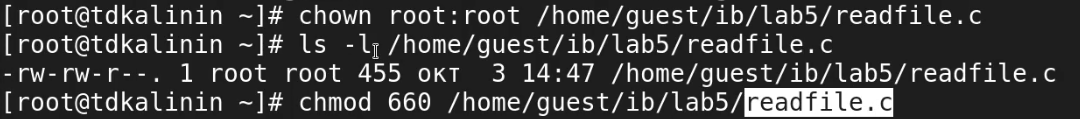


Figure 12: Изменяем владельца

1. Проверьте, что пользователь guest не может прочитать файл readfile.c ([Рис. 13](#fig:013)).

Figure 13: Проверка чтения

Figure 13: Проверка чтения

1. Смените у программы readfile владельца и установите SetU’D-бит ([Рис. 14](#fig:014), [Рис. 15](#fig:015)).

Figure 14: Смена владельца

Figure 14: Смена владельца

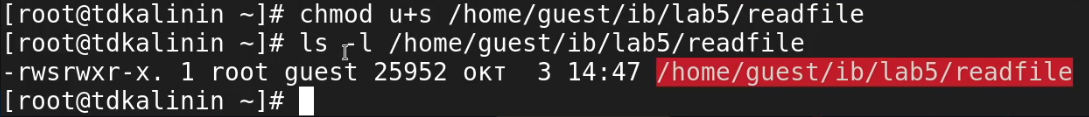


Figure 15: Установка setUID-бита

1. Проверьте, может ли программа readfile прочитать файл readfile.c? ([Рис. 16](#fig:016)). Да, может

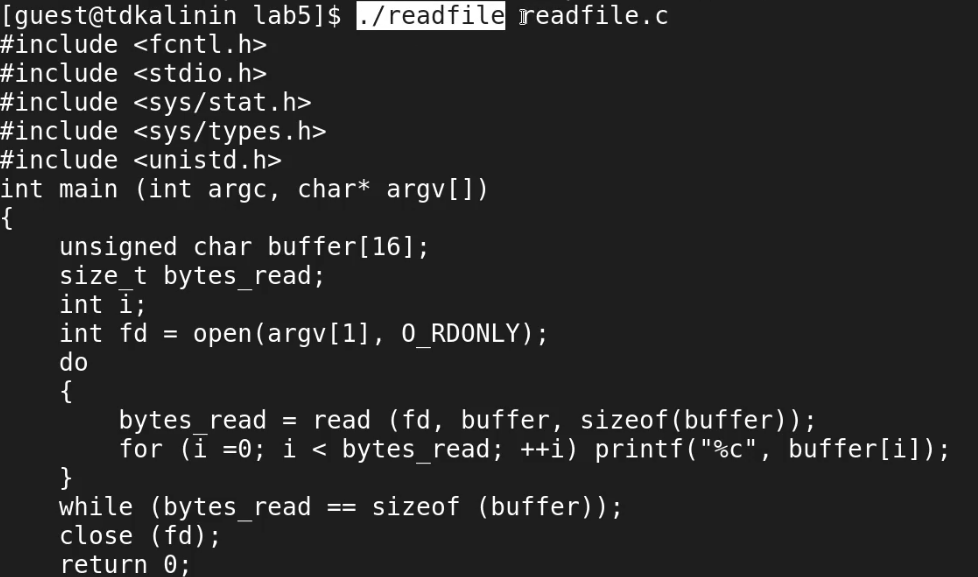


Figure 16: Проверка чтения readfile.c

1. Проверьте, может ли программа readfile прочитать файл /etc/shadow? Отразите полученный результат и ваши объяснения в отчёте ([Рис. 17](#fig:017)). Да, может, так как мы запускаем программу на исполнение от имени владельца, то есть пользователя root.

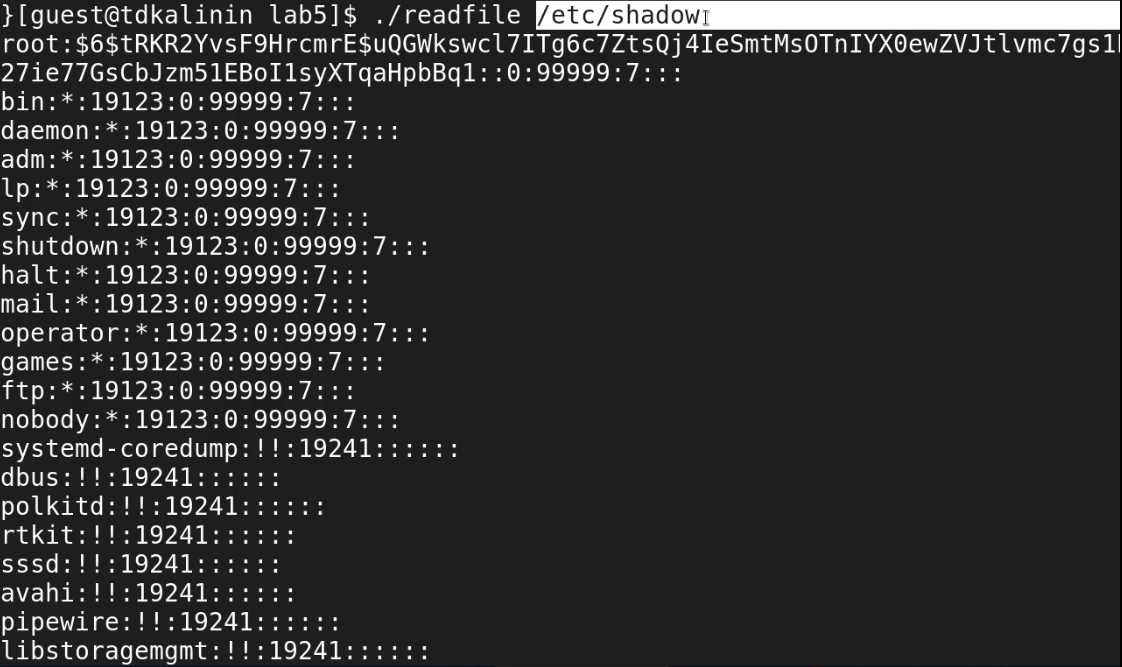


Figure 17: Проверка чтения /etc/shadow

## 2.2 Исследование Sticky-бита

1. Выясните, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду ([Рис. 18](#fig:018)). Да установлен (буква t)

Figure 18: Атрибуты

Figure 18: Атрибуты

1. От имени пользователя guest создайте файл file01.txt в директории /tmp со словом test ([Рис. 19](#fig:019)).

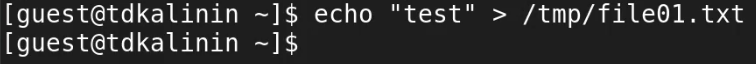


Figure 19: Создание нового файла

1. Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные» ([Рис. 20](#fig:020), [Рис. 21](#fig:021)).

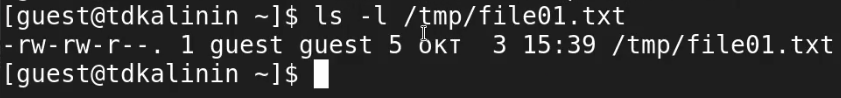


Figure 20: Просмотр атрибутов

Figure 21: Установка прав доступа

Figure 21: Установка прав доступа

1. От пользователя guest2 (не являющегося владельцем) попробуйте прочитать файл /tmp/file01.txt ([Рис. 22](#fig:022)).

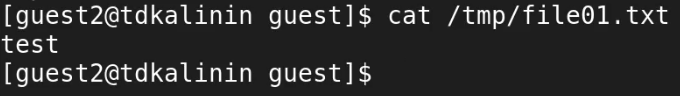


Figure 22: Чтение файла

1. От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 ([Рис. 23](#fig:023)).



Figure 23: Дозапись в файл

1. От пользователя guest2 попробуйте записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой ([Рис. 24](#fig:024)).

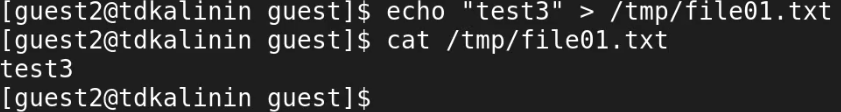


Figure 24: Перезапись файла

1. Проверьте содержимое файла командой ([Рис. 25](#fig:025)).

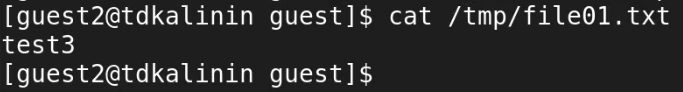


Figure 25: Проверка содержимого

1. От пользователя guest2 попробуйте удалить файл /tmp/file01.txt командой ([Рис. 26](#fig:026)).

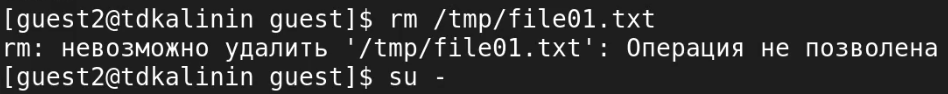


Figure 26: Попытка удаления

1. Повысьте свои права до суперпользователя следующей командой и выполните после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp ([Рис. 27](#fig:027)).

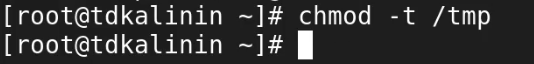


Figure 27: Снятие атрибута t

1. Покиньте режим суперпользователя
2. От пользователя guest2 проверьте, что атрибута t у директории /tmp нет ([Рис. 28](#fig:028)).

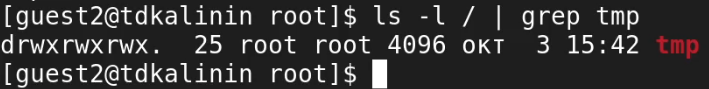


Figure 28: Проверка атрибутов

1. Повторите предыдущие шаги. Какие наблюдаются изменения? ([Рис. 29](#fig:029)). В этот раз удалось удалить файл.

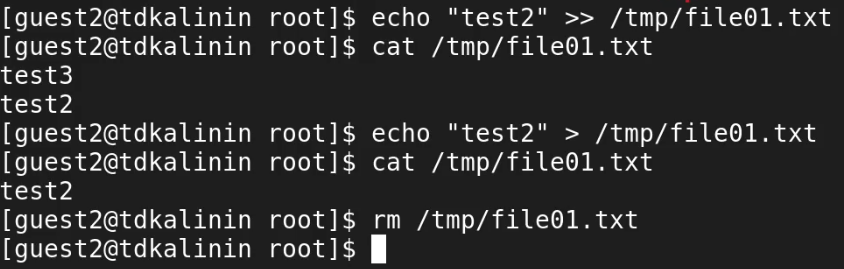


Figure 29: Повтор действий

1. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем? Да, теперь удалось.

# 3 Выводы

Мы изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получили практические навыки работы в консоли с дополнительными атрибутами. Рассмотрели работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# 4 Библиография

1. Лабораторная работа №5. - 2 с. URL: <https://esystem.rudn.ru/pluginfile.php/1651889/mod_resource/content/2/005-lab_discret_sticky.pdf>