Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Казакова Виктория Алексеевна

Содержание

# 1 Цель работы

## 1.1 ### 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.

1. Подготовила лабораторный стенд, выполнила все необходимые команды из пункта 5.2.1. (рис. [1](#fig:001))



Figure 1: Подготовка лабораторного стенда

1. Вошла в пользователя guest. Создала программу simpleid.c командой touch (рис. [2](#fig:002))

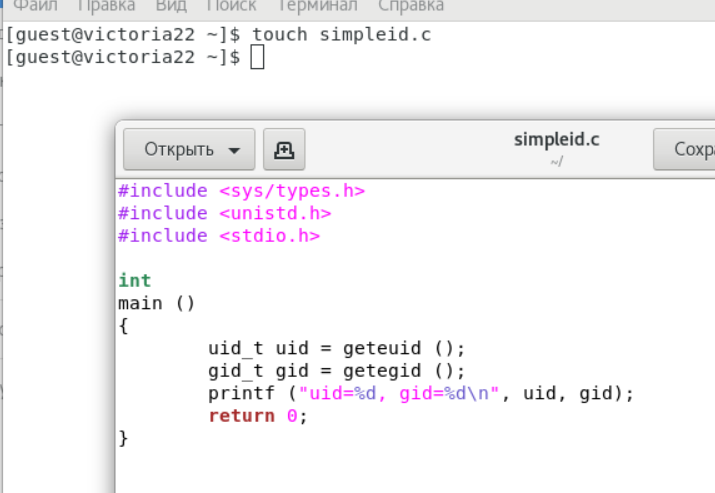


Figure 2: Файл simpleid.c

1. Скомпилировала программу и убедилась, что файл программы создан(рис. [3](#fig:003))

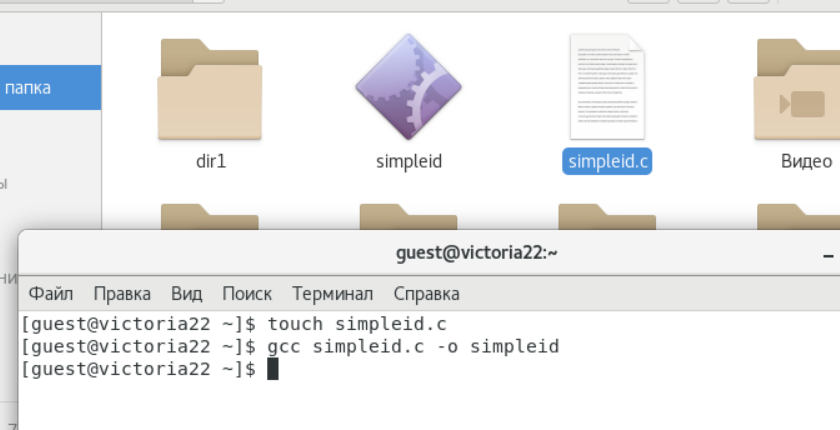


Figure 3: Файл скомпилирован

1. Выполнила программу simpleid командой ./simpleid. Выполнила системную программу id. Результат совпал(рис. [4](#fig:004))

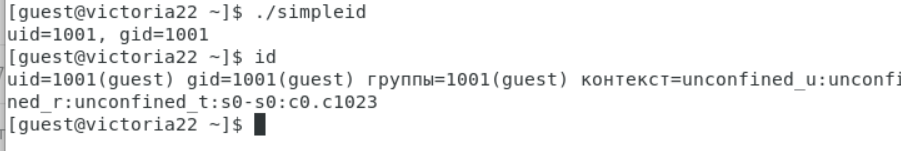


Figure 4: Результаты запуска

1. Создала программу simpleid2.c, содержащую в себе усложненый код программы simpleid.c. (рис. [5](#fig:005))

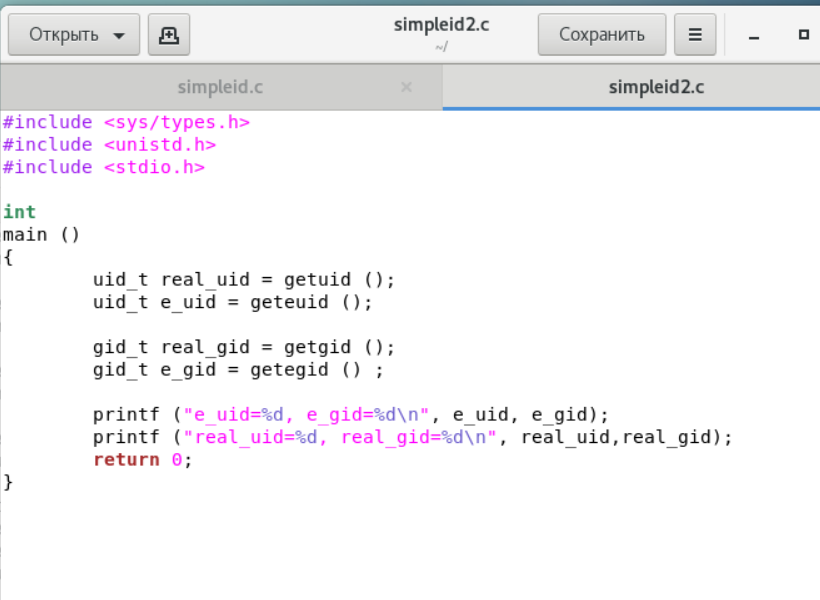


Figure 5: Программа simpleid2.c

1. Скомпилировала и запустила simpleid2.c (рис. [6](#fig:006)).

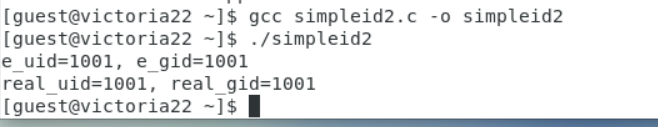


Figure 6: Результат работы simpleid2.c

1. От имени суперпользователя (перешла в него командой su) выполнила команды chown root:guest /home/guest/simpleid2 и chmod u+s /home/guest/simpleid2. Эти команды установили права над файлом суперпользователя (рис. [7](#fig:007)).

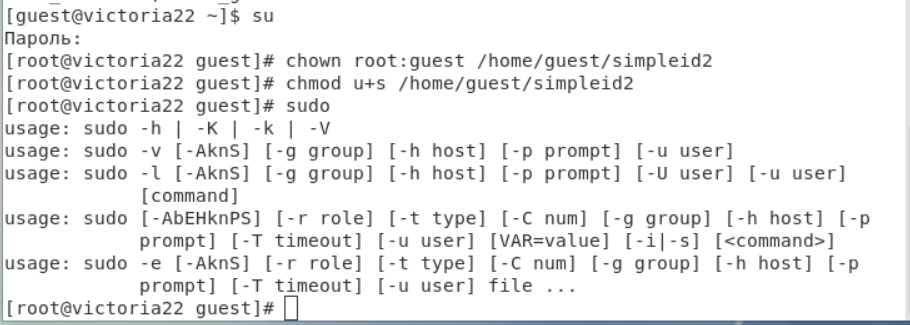


Figure 7: Чтение файла

1. Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2 (рис. [8](#fig:008)).

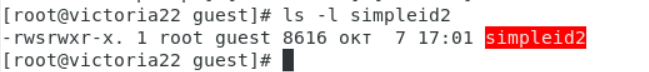


Figure 8: Проверка правильности

1. Запустила simpleid2 и id. Результат совпал (рис. [9](#fig:009)).

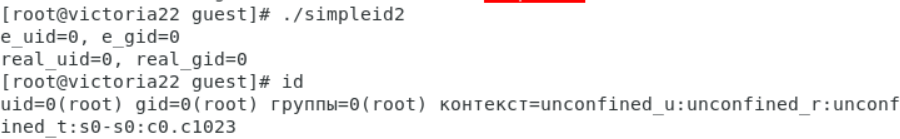


Figure 9: Попытка стереть содержимое файла

1. Проделала тоже самое относительно SetGID-бита (рис. [10](#fig:010)).

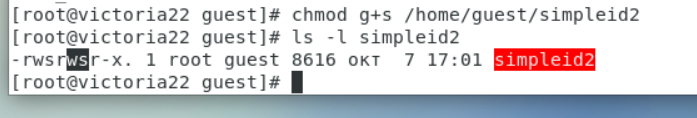


Figure 10: Изменение прав

1. Создала программу readfile.c (рис. [11](#fig:011)).

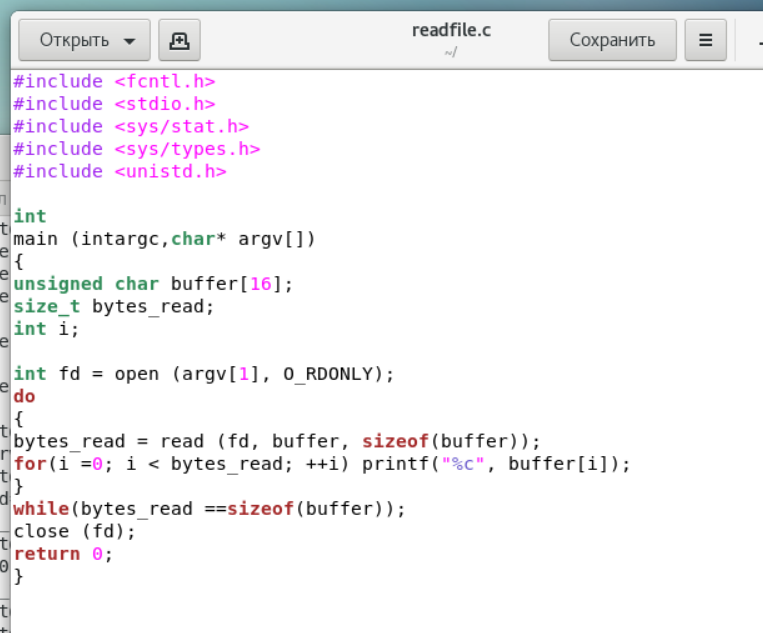


Figure 11: Программа readfile.c

1. Откомпилировала её. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог. Убедилась, что пользователь guest не может прочитать файл readfile.c (рис. [12](#fig:012))

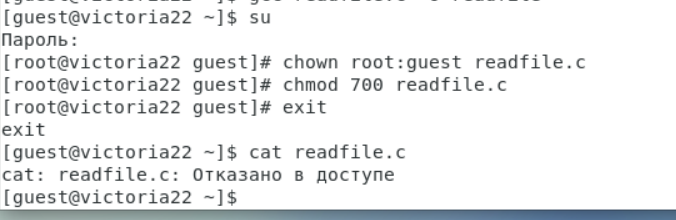


Figure 12: Применение команд

1. Сменила у программы readfile владельца и установила SetU’D-бит (рис. [13](#fig:013))

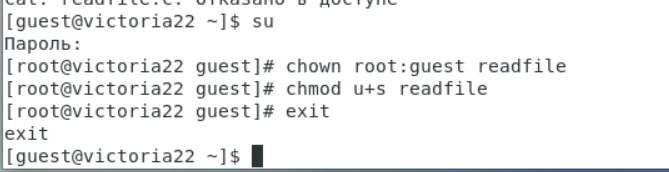


Figure 13: Смена владельца и ограничений

1. Убедилась, что программа readfile может прочитать файл readfile.c (рис. [14](#fig:014)) и файл /etc/shadow (рис. [15](#fig:015)).

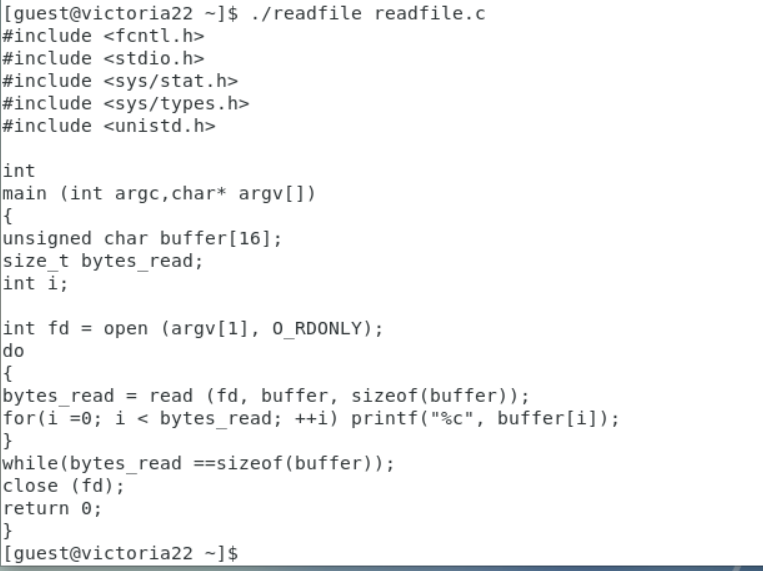


Figure 14: Чтение файла readfile.c

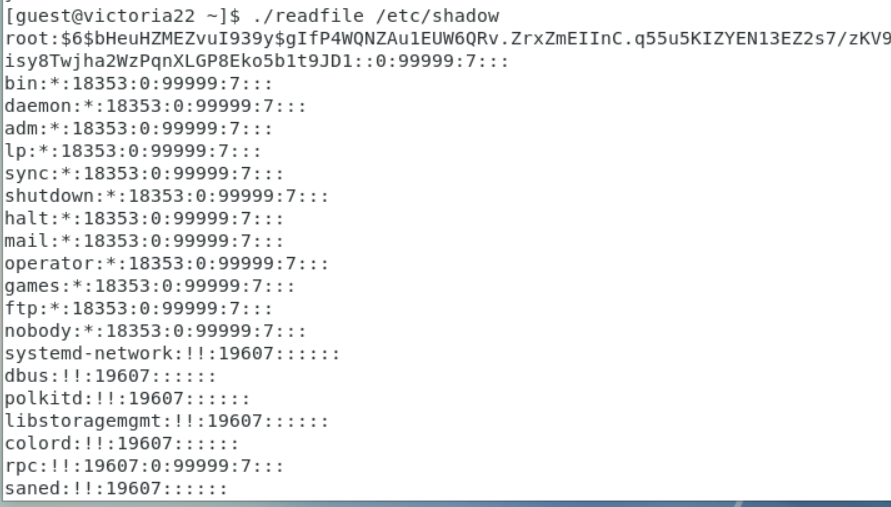


Figure 15: Чтение файла /etc/shadow

15.Приступила ко второй части работы. Выяснила, установлен ли атрибут Sticky на директории /tmp, для чего выполнила команду ls -l / | grep tmp и от имени пользователя guest создала файл file01.txt в директории /tmp со словом test(рис. [16](#fig:016)).

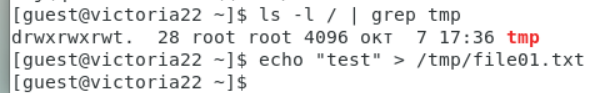


Figure 16: Применение команд, заполнение файла

1. Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные» (рис. [17](#fig:017)).

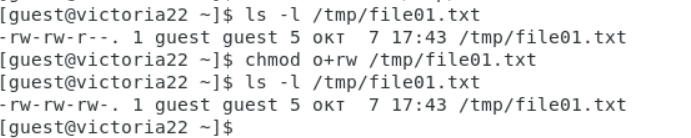


Figure 17: Просмотр и установка атрибутов

1. От пользователя guest2 попробовала прочитать файл /tmp/file01.txt и дозаписать в файл слово test2. Снова проверила содержимое файла (рис. [18](#fig:018)). Файл получается прочитать, но не получается дозаписать в него текст. Команда его стирает и пишет новый



Figure 18: Чтение и дозапись в файл

1. От пользователя guest2 записала в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой, а затем прочитала его (рис. [19](#fig:019)). Команду выполнить удалось.

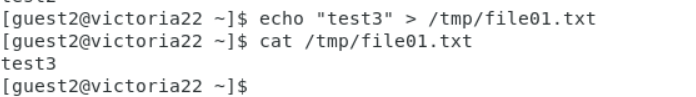


Figure 19: Чтение и дозапись в файл

1. От пользователя guest2 попробовала удалить файл /tmp/file01.txt командой rm /tmp/fileOl.txt (рис. [20](#fig:020)). Команду выполнить не удалось.

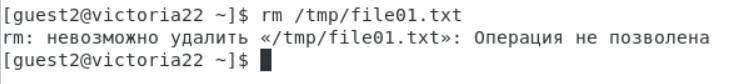


Figure 20: Попытка удалить файл

1. Повысила права до суперпользователя и выполнила после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp. Затем покинула режим суперпользователя и от пользователя guest2 проверьте, что атрибута t у директории /tmp нет. Затем снова попыталась удалить файл (рис. [19](#fig:019)). Файл удалить получилось.

## 1.2 Повторная попытка удалить файл

# 2 Выводы

В результате выполнения работы я изучила механизм изменения идентификаторов, применения SetUID- и Sticky-битов. Получила практические навыки работы в консоли с дополнительными атрибутами. Рассмотрела работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов

# 3 Библиография

1. [Методический материал] [https://esystem.rudn.ru/pluginfile.php/2090279/mod\_resource/content/2/005-lab\_discret\_sticky.pdf]
2. [Сайт для поиска команд] [https://www.ibm.com/]