Отчет по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Лебедев Ярослав Борисович

**Содержание**

[Цель работы 3](#_Toc116045683)

[Выполнение лабораторной работы 4](#_Toc116045684)

[Создание программы 4](#_Toc116045685)

[Исследование Sticky-бита 9](#_Toc116045686)

[Выводы 11](#_Toc116045687)

[Список литературы 12](#_Toc116045688)

# 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 [1].

# Выполнение лабораторной работы

## Создание программы

1. Войдите в систему от имени пользователя guest (Рис.1).
2. Создайте программу simpleid.c (Рис.1 - Рис.2).

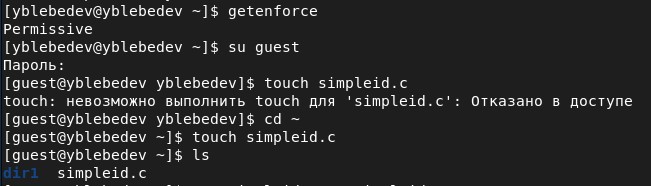


Рис.1. Пункт 1-2



Рис.2. Пункт 2. Программа

1. Скомплилируйте программу и убедитесь, что файл программы создан (Рис.3): gcc simpleid.c -o simpleid
2. Выполните программу simpleid (Рис.3): ./simpleid
3. Выполните системную программу id (Рис.3): id и сравните полученный вами результат с данными предыдущего пункта задания.
4. Усложните программу, добавив вывод действительных идентификаторов Получившуюся программу назовите simpleid2.c (Рис.3 - Рис.4).

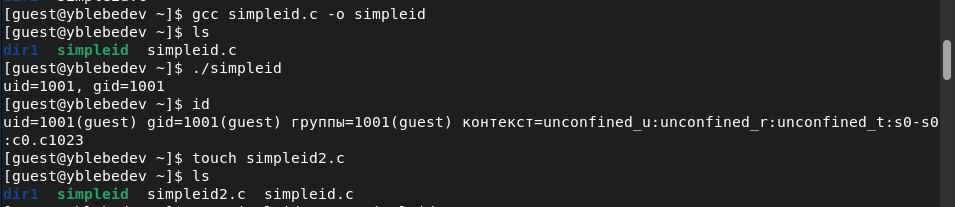


Рис.3. Пункт 3-6

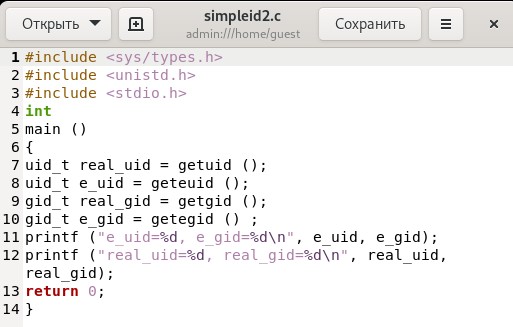


Рис.4. Пункт 6. Программа

1. Скомпилируйте и запустите simpleid2.c (Рис.5) gcc simpleid2.c -o simpleid2 ./simpleid2
2. От имени суперпользователя выполните команды (Рис.5): chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2
3. Используйте sudo или повысьте временно свои права с помощью su (Рис.5). Поясните, что делают эти команды.
4. Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2 (Рис.5): ls -l simpleid2

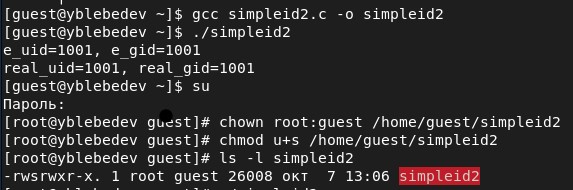


Рис.5. Пункт 7-10

1. Запустите simpleid2 и id: ./simpleid2 id Сравните результаты (Рис.6).

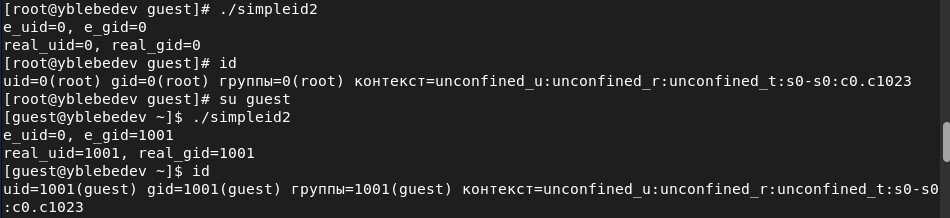


Рис.6. Пункт 11

1. Проделайте тоже самое относительно SetGID-бита (Рис.7).
2. Создайте программу readfile.c (Рис.7 - Рис.8).



Рис.7. Пункт 12-13

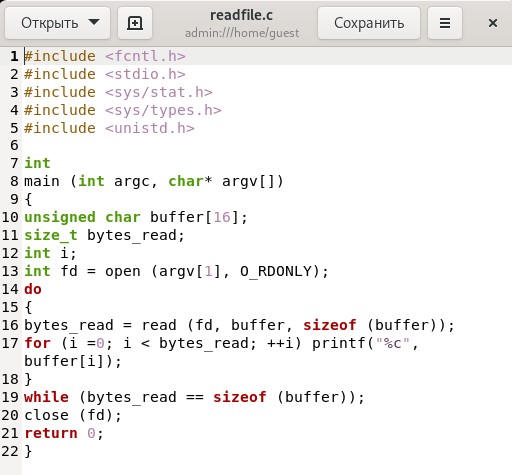


Рис.8. Пункт 13. Программа

1. Откомпилируйте её (Рис.9). gcc readfile.c -o readfile
2. 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.9).
3. Проверьте, что пользователь guest не может прочитать файл readfile.c (Рис.9).

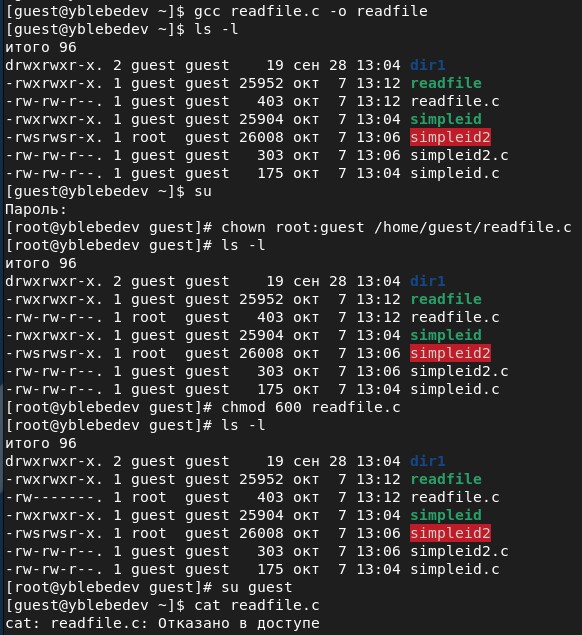


Рис.9. Пункт 14-16

1. Смените у программы readfile владельца и установите SetU’D-бит (Рис.10).
2. Проверьте, может ли программа readfile прочитать файл readfile.c? (Рис.10)

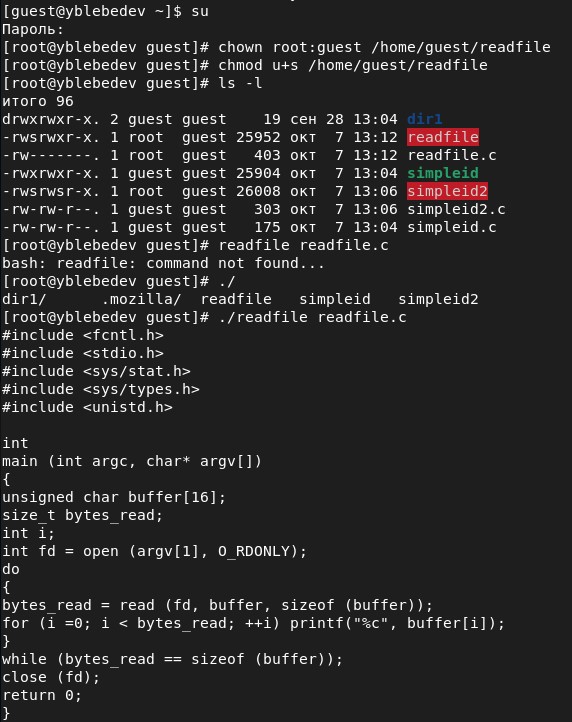


Рис.10. Пункт 17-18

1. Проверьте, может ли программа readfile прочитать файл /etc/shadow? Отразите полученный результат и ваши объяснения в отчёте (Рис.11).

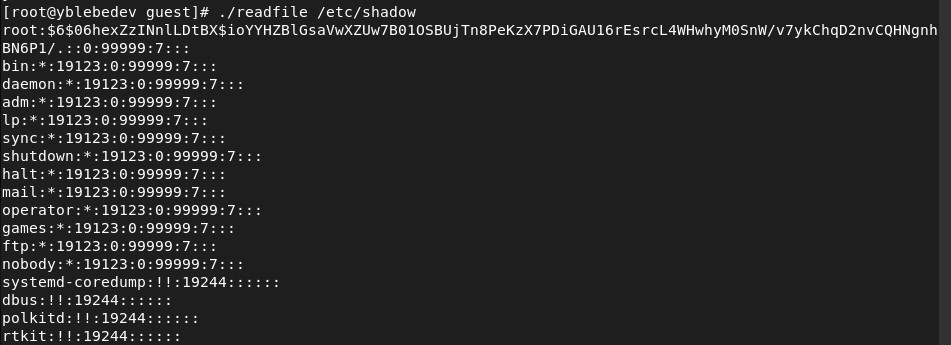


Рис.11. Пункт 19

## Исследование Sticky-бита

1. Выясните, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду (Рис.12) ls -l / | grep tmp
2. От имени пользователя guest создайте файл file01.txt в директории /tmp со словом test (Рис.12): echo “test” > /tmp/file01.txt
3. Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные» (Рис.12): ls -l /tmp/file01.txt chmod o+rw /tmp/file01.txt ls -l /tmp/file01.txt

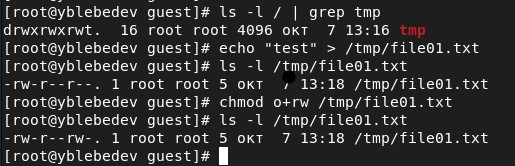


Рис.12. Пункт 1-3. Исследование Sticky-бита

1. От пользователя guest2 (не являющегося владельцем) попробуйте прочитать файл /tmp/file01.txt (Рис.13): cat /tmp/file01.txt
2. От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 командой (Рис.13) echo “test2” > /tmp/file01.txt Удалось ли вам выполнить операцию?
3. Проверьте содержимое файла командой (Рис.13) cat /tmp/file01.txt
4. От пользователя guest2 попробуйте записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой (Рис.13) echo “test3” > /tmp/file01.txt Удалось ли вам выполнить операцию?
5. Проверьте содержимое файла командой (Рис.13) cat /tmp/file01.txt
6. От пользователя guest2 попробуйте удалить файл /tmp/file01.txt командой rm /tmp/fileOl.txt Удалось ли вам удалить файл? (Рис.13)
7. Повысьте свои права до суперпользователя следующей командой (Рис.13) su - и выполните после этого команду, снимающую атрибут t(Sticky-бит) с директории /tmp: chmod -t /tmp
8. Покиньте режим суперпользователя командой (Рис.13) exit
9. От пользователя guest2 проверьте, что атрибута t у директории /tmp нет (Рис.13): ls -l / | grep tmp
10. Повторите предыдущие шаги. Какие наблюдаются изменения? (Рис.13)
11. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем? Ваши наблюдения занесите в отчёт (Рис.13).
12. Повысьте свои права до суперпользователя и верните атрибут t на директорию /tmp (Рис.13): su - chmod +t /tmp exit

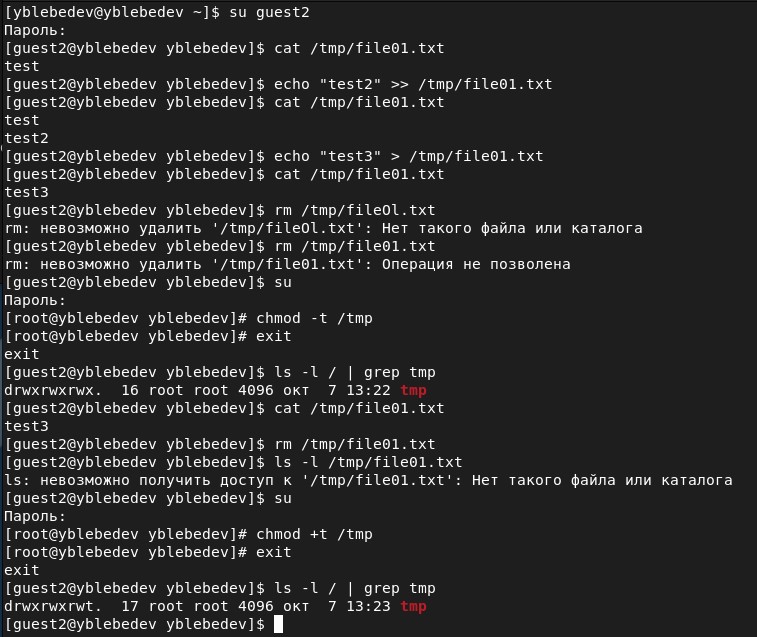


Рис.13. Пункт 4-15. Исследование Sticky-бита

# Выводы

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

# Список литературы

1. Методические материалы курса