Информационная безопасность.

Лабораторная работа №5.

Филиппова Вероника Сергеевна.

Содержание

# 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. Создание программы.
2. Исследование Sticky-бита

# Выполнение лабораторной работы

## Создание программы

Проверила версию gcc с помощью программы gcc -v

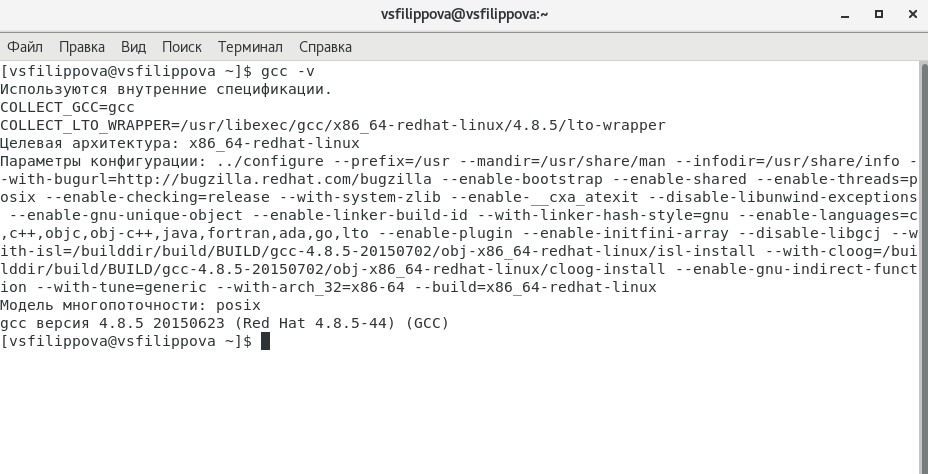


Рисунок 1

Отменила на текущую сессию SELinux командой setenforce 0 Вошла в систему от имени пользователя guest, создала программу simpleid.c

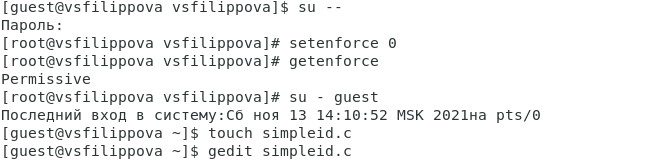


Рисунок 2

Скомпилировала программу и убедилась, что файл программы создан, командой gcc simpleid.c -o simpleid

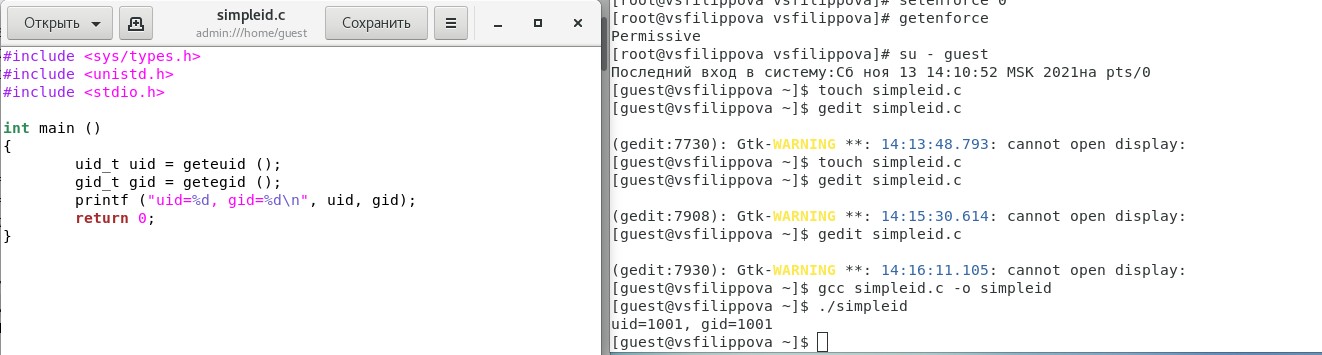


Рисунок 3

Выполнила программу simpleid: ./simpleid и программу id и сравнила полученный результат с данными предыдущего пункта. Полученные значения id совпадают

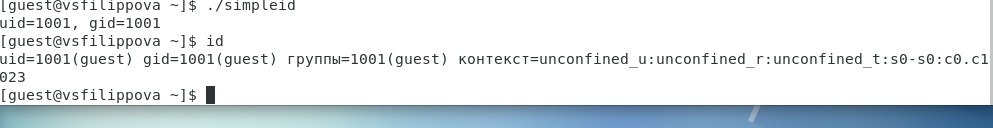


Рисунок 4

Усложнила программу, добавив вывод действительных идентификаторов, назвала программу simpleid2.c Скомпилировала и запустил simpleid2.c gcc simpleid2.c -o simpleid2, а затем ./simpleid2

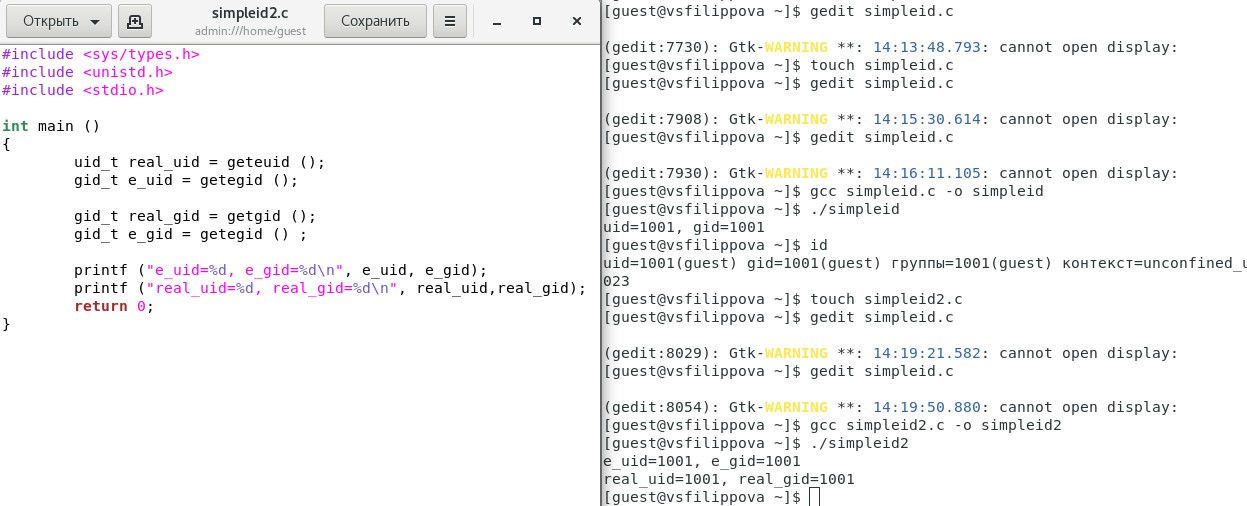


Рисунок 5

От имени суперпользователя выполнила команды: chown root:guest /home/guest/simpleid2 и chmod u+s /home/guest/simpleid2. Первая команда изменяет права на файл с guest на root. А затем устанавливает атрибут SetUID, который запускает программу не с правами пользователя, а с правами владельца файла. Затем выполнила проверку изменений с помощью команды ls -l simpleid2

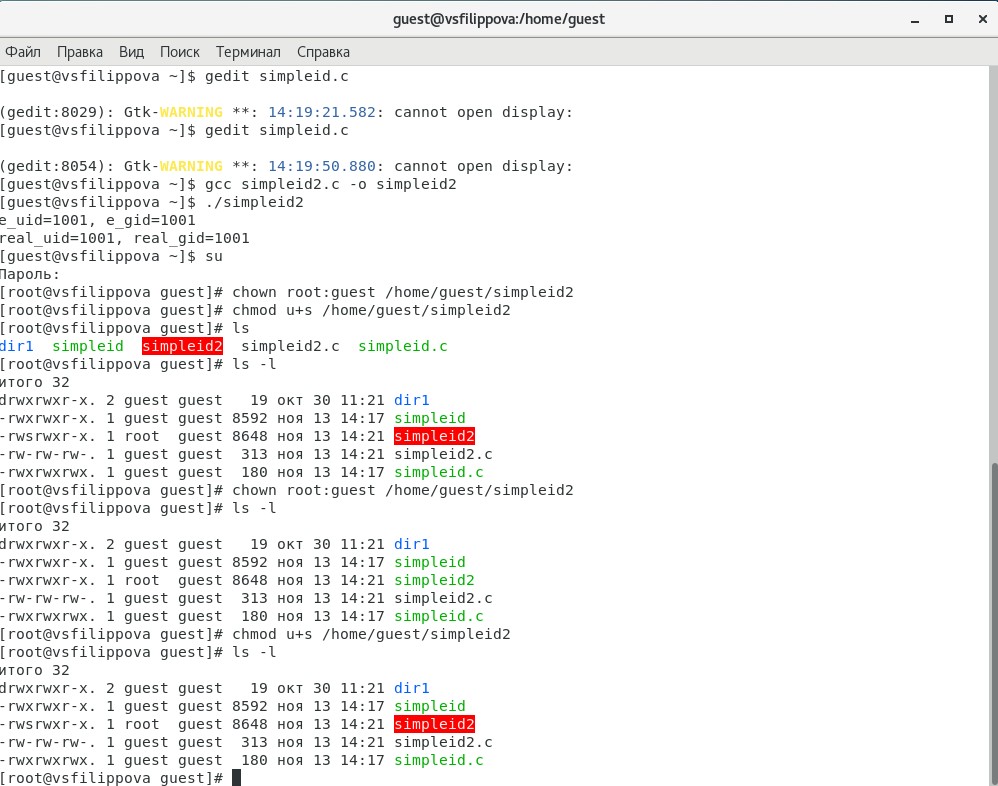


Рисунок 6

Запустила ./simpleid2, id. При данном запуске выводы совпадают.

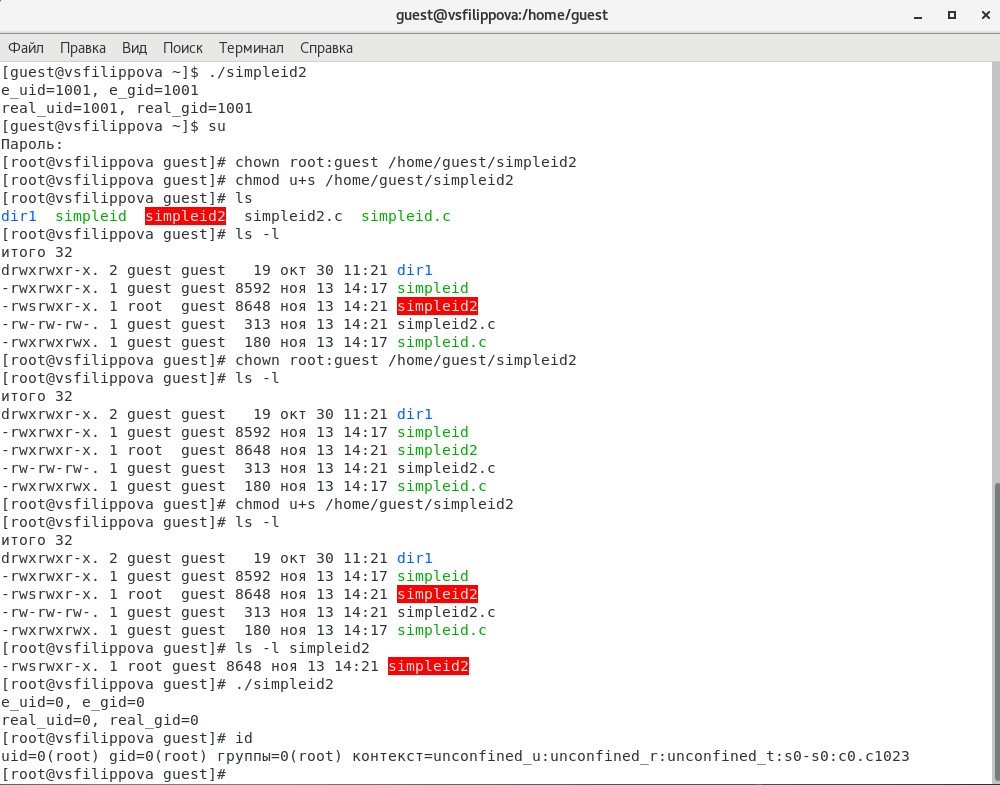


Рисунок 7

Проделала то же самое с атрибутом SetGID (установление прав для владеющей группы).

Запустила файл. Теперь выводы для группы различны.

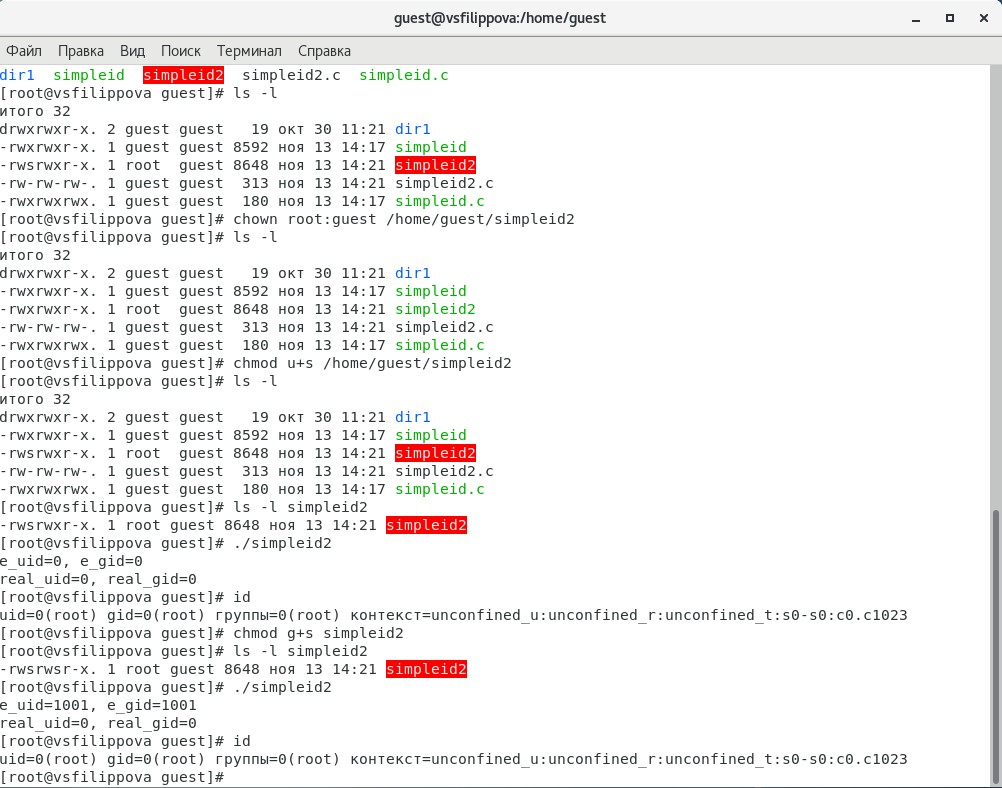


Рисунок 8

Создала программу readfile.c

Откомпилировала программу: gcc readfile.c -o readfile

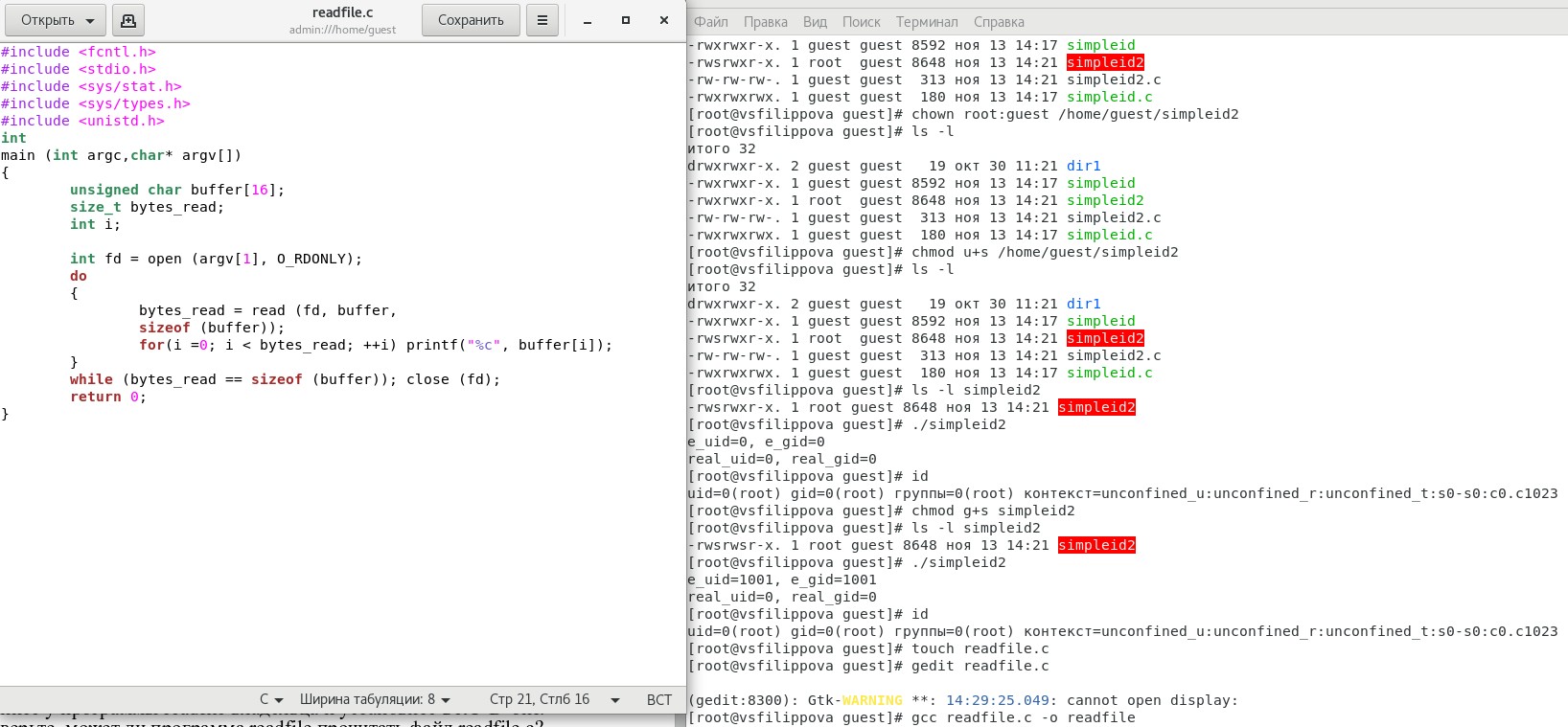


Рисунок 9

Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь(root) мог прочитать его.

Проверила, что пользователь guest не может прочитать файл readfile.с

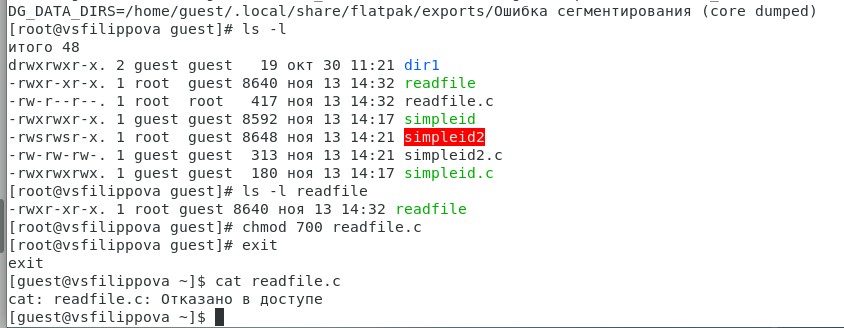


Рисунок 10

Сменила у программы readfile владельца и установила SetU’D-бит.

Проверила, может ли программа readfile прочитать файл readfile.c. Да.

Проверила, может ли программа readfile прочитать файл /etc/shadow. Да.

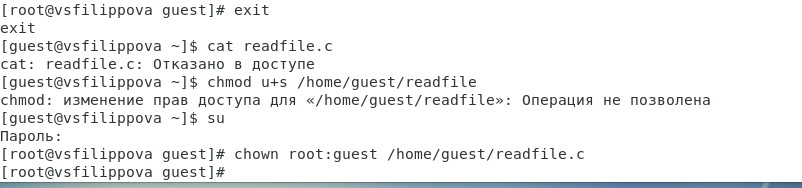


Рисунок 11

## Исследование Sticky-бита.

Узнала, установлен ли атрибут Sticky на директории /tmp, для чего выполнила команду ls -l / | grep tmp

От имени пользователя guest создала файл file01.txt в директории /tmp со словом test echo "test" > /tmp/file01.txt

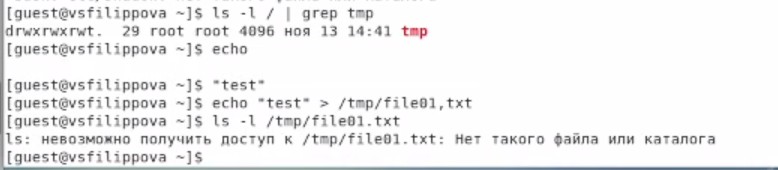


Рисунок 12

Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные»:

1. ls -l /tmp/file01.txt,
2. chmod o+rw /tmp/file01.txt,
3. ls -l /tmp/file01.txt



Рисунок 13

От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt: cat /tmp/file01.txt

Попробовала записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой echo "test3" > /tmp/file01.txt

Попробовала дозаписать в файл /tmp/file01.txt слово test2 командой echo "test2" >> /tmp/file01.txt

Проверила содержимое файла командой cat /tmp/file01.txt

[Рисунок 14](../scr/13.png{ #fig:014 width=70% }

От пользователя guest2 попробовала удалить файл /tmp/file01.txt командой rm /tmp/file01.txt Файл удалить не удалось.

[Рисунок 15](../scr/14.png{ #fig:015 width=70% }

Повысила свои права до суперпользователя командой su - и выполнила после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: chmod -t /tmp

[Рисунок 16](../scr/16.png{ #fig:016 width=70% }

Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp: su -, chmod +t /tmp, exit

[Рисунок 17](../scr/17.png{ #fig:015 width=70% }

# Выводы

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