Лабораторная работа №5

Информационная безопасность

Дьяконова Софья

Содержание

# 1 Цель работы

Целью работы является 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 Теоретическое введение

Setuid, Setgid и Sticky Bit - это специальные типы разрешений позволяют задавать расширенные права доступа на файлы или каталоги.

# 3 Выполнение лабораторной работы

## 3.1 Создание программы

Я вошла в систему от имени пользователя guest.(рис. 1)

Далее создала программу simpled.c и заполнила ее.(рис. 1)

Скомплилировала файл через **gcc simpled.c -o simpled** и выполнила программу simpled.(рис. 1)

Выполнила системную программу id. Результаты похожи. Gid и uid одинаковые, однако команда id дает больше информации.(рис. 1)

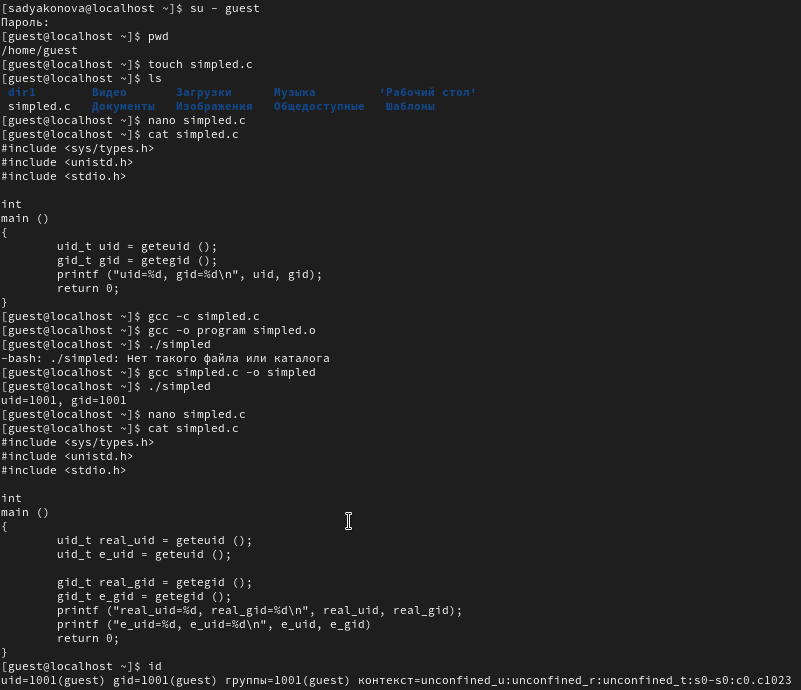


Рис. 1: simpled

Усложнила программу, добавив вывод действительных идентификаторов.(рис. 2)

Скомпилировала и запустила simpled.c.(рис. 2)

От имени суперпользователя выполнила команды **chown root:guest /home/guest/simpled, chmod u+s /home/guest/simpled**.(рис. 2)

Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpled.(рис. 2)

Запустила simpled и id. Результаты похожи. Gid и uid одинаковые, однако команда id дает больше информации.(рис. 2)

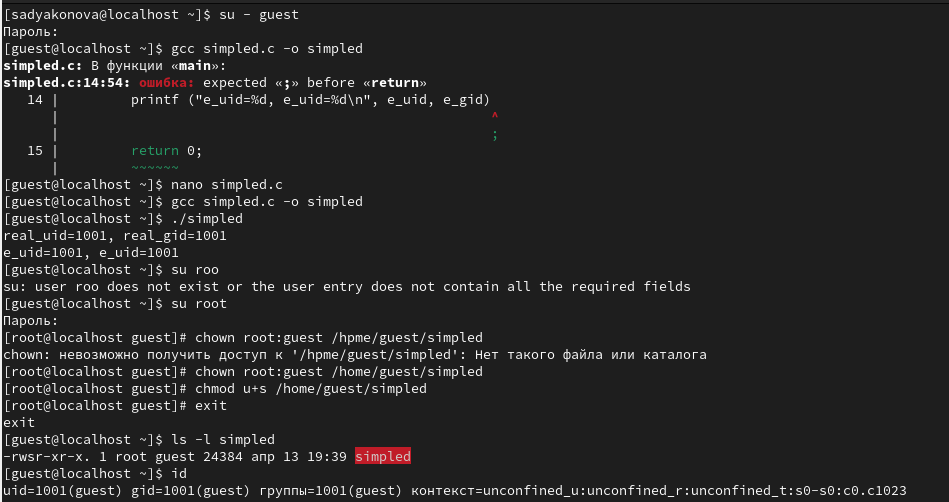


Рис. 2: simpled 2

Создала программу readfile.c.(рис. 3)

Откомпилировала её.(рис. 3)

Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, a aleksandrovauv не мог. Проверила, может ли пользователь прочитать файл readfile.c. Не может.(рис. 4)

Программа readfile в целом может прочитать файл /etc/shadow.(рис. 4)

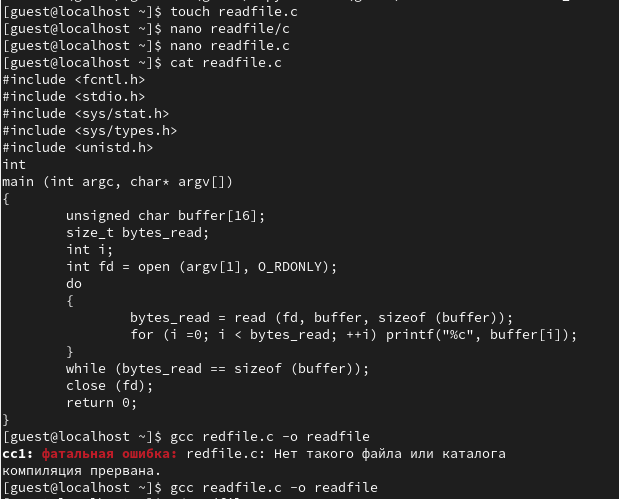


Рис. 3: readfile

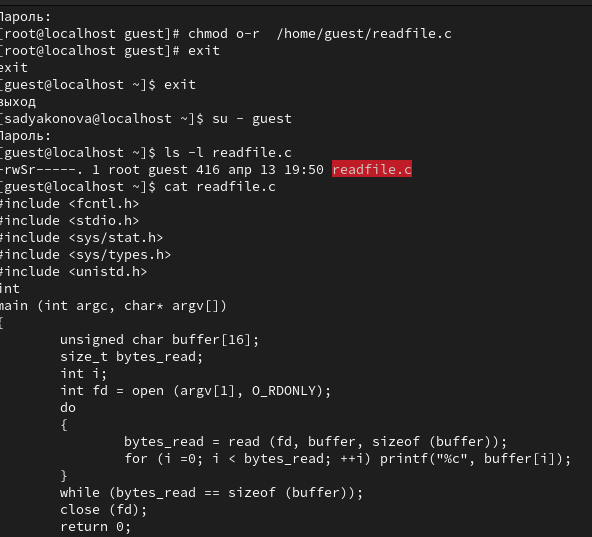


Рис. 4: readfile

## 3.2 Исследование Sticky-бита

Выяснила, установлен ли атрибут Sticky на директории /tmp. Установлен.  
От имени пользователя guest создала файл file01.txt в директории /tmp со словом test через **echo “test” > /tmp/file01.txt**. Затем просмотрите атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные» при помощи утилиты **chmod o+rw /tmp/file01.txt**.(рис. 5).

От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt. Попробовала дозаписать в файл /tmp/file01.txt слово test2 командой **echo “test2” > /tmp/file01.txt**. Мне отказано в доступе. То же самое попробовала сделать с test3, но мне снова отказано в доступе. Файл не записался.(рис. 5).

От пользователя guest2 попробовала удалить файл /tmp/file01.txt. Мне отказали в доступе. Потом я повысила свои права до суперпользователя командой **su -** и сняла атрибут t (Sticky-бит) с директории /tmp. От пользователя guest2 проверила, что атрибута t у директории /tmp нет. Повторила предыдущие шаги. Файл удалился (рис. 5).

Вернула атрибут t (рис. 5).

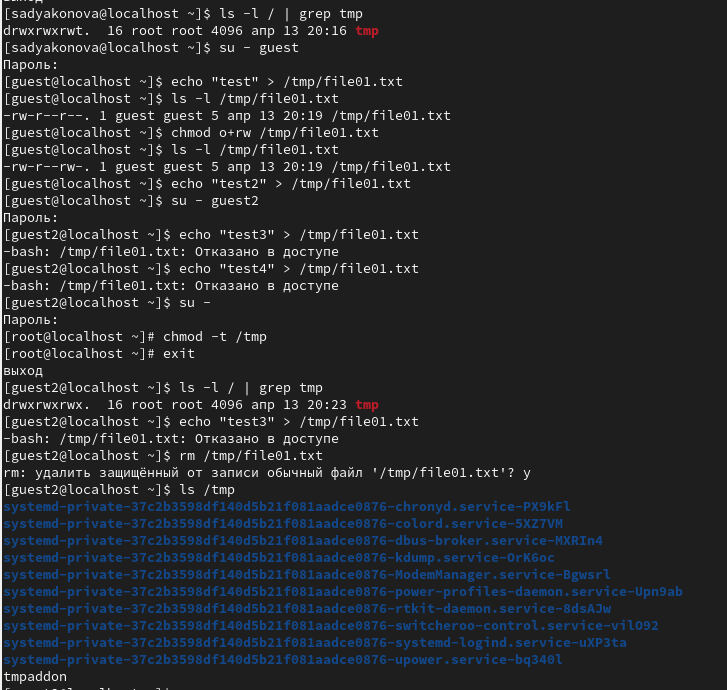


Рис. 5: Sticky

# 4 Выводы

Я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Полученила практических навыков работы в консоли с дополнительными атрибутами.