Отчёт по лабораторной работе №5

Дисциплина: Основы информационной безопасности

Дудырев Глеб Андреевич НПИбд-01-22

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. Создаю файл simpleid.c (рис. 1)

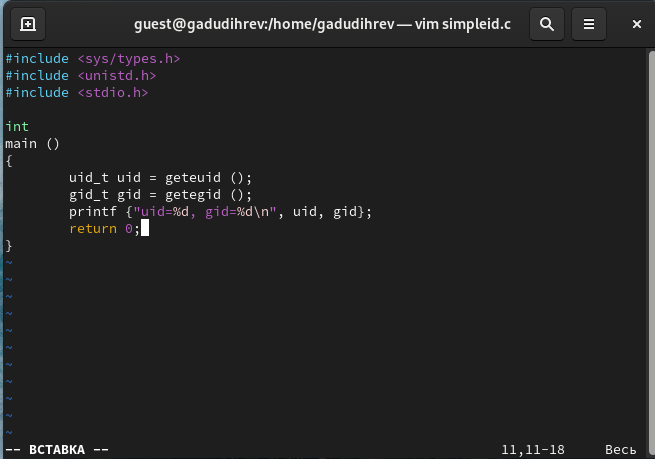


Рис. 1: Программа simpleid.c

1. Компилирую программу командой *gcc simpleid.c -o simpleid* и проверяю, что файл создан. Выполняю программу simpleid командой *./simpleid*, а зтем системную программу *id* - вывод одинаков. (рис. 2)

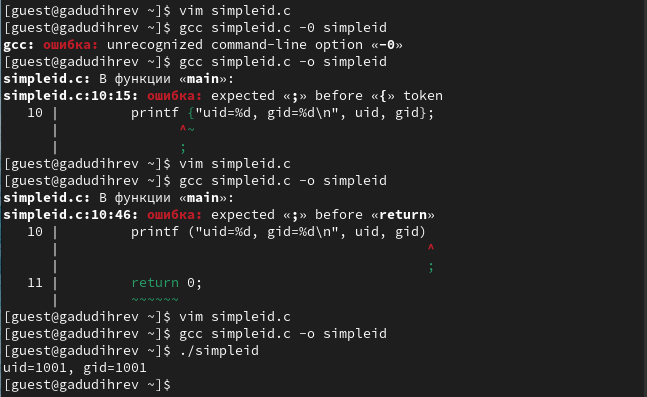


Рис. 2: Выполнение программы

1. Усложняю программу и записываю ее в файл simpleid2.c (рис. 3)

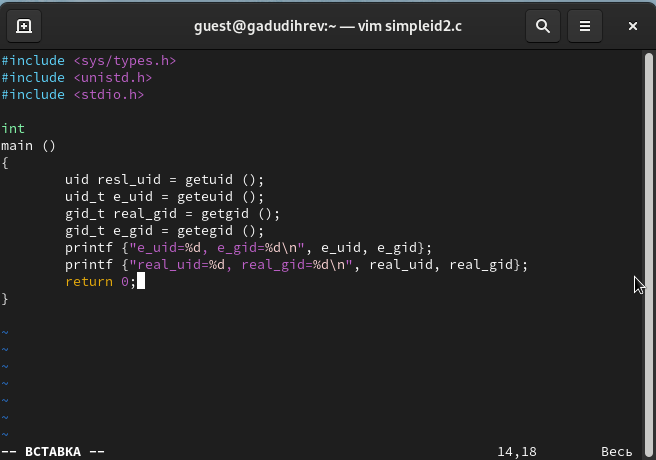


Рис. 3: Программа simpleid2.c

1. Компилирую и запускаю программу командами *gcc simpleid2.c -o simpleid2* и *./simpleid2* (рис. 4)

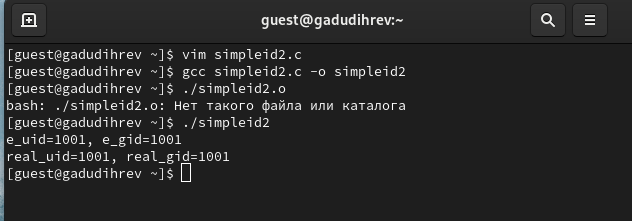


Рис. 4: Компиляция и запуск

1. От суперпользователя выполняю команды *chown root:guest /home/guest/simpleid2* и *chmod u+s /home/guest/simpleid2*. Проверяю правильность новых атрибутов командой *ls -l simpleid2*. Запускаю simpleid2 и id: *./simpleid2*, *id* (рис. 5)

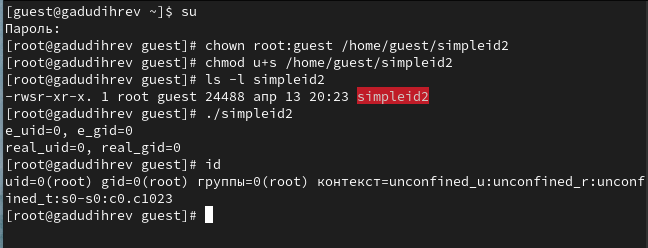


Рис. 5: Изменение атрибутов, запуск

1. Создаю программу readfile.c (рис. 6)

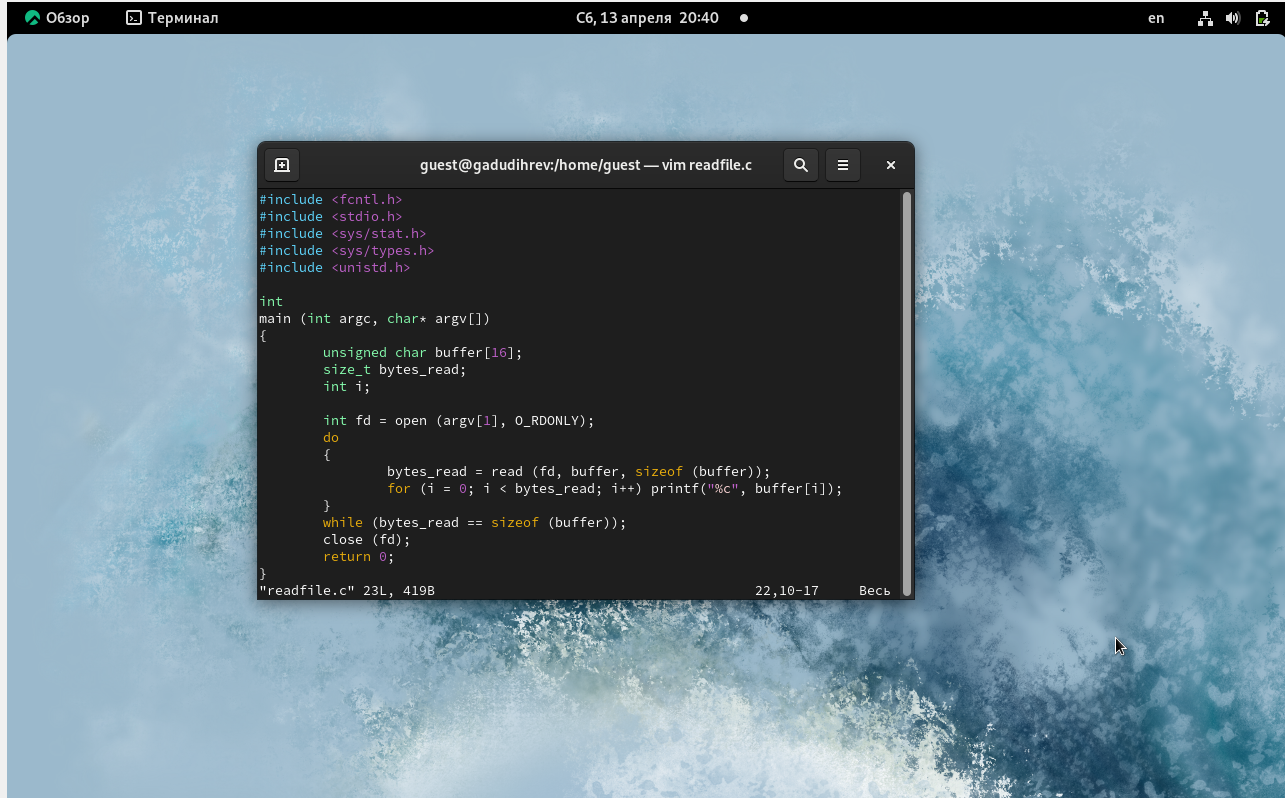


Рис. 6: Программа readfile.c

1. Компилирую ее командой *gcc readfile.c -o readfile* и изменяю права доступа так, чтобы только суперпользователь мог прочитать его, a guest не мог (рис. 7)

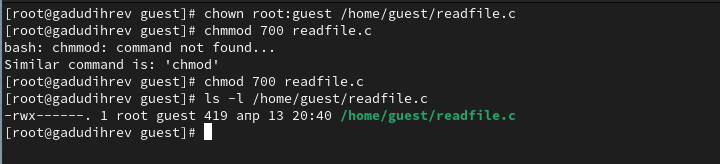


Рис. 7: Компиляция программы, смена прав доступа

1. Командой *cat readfile.c* проверяю, что пользователь guest не может прочитать файл readfile.c. Устанавливаю SetU’D-бит и теперь от пользователя guest можно прочитать файл (рис. 8)

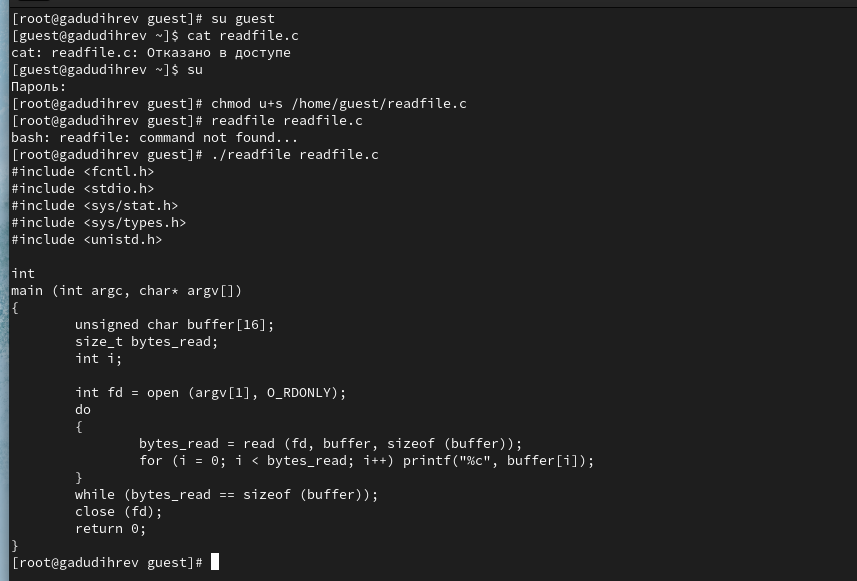


Рис. 8: Установка SetU’D-бита, проверка

1. Проверяю, может ли программа readfile прочитать файл /etc/shadow - да, может (рис. 9)

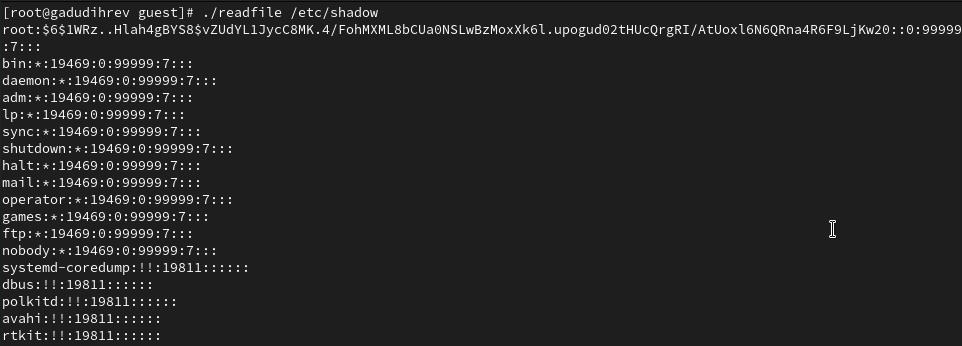


Рис. 9: Файл /etc/shadow

## 2.2 Исследование Sticky-бита

1. Проверяю, установлен ли атрибут Sticky на директории /tmp командой *ls -l / | grep tmp*. От пользователя guest создаю файл со словом test командой *echo “test” > /tmp/file01.txt*. Просматриваю атрибуты у только что созданного файла и разрешаю чтение и запись для категории пользователей «все остальные» (рис. 10)

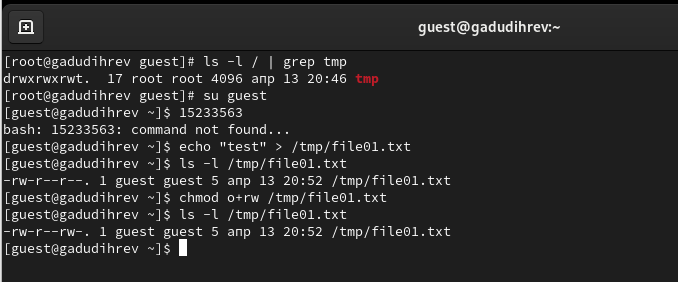


Рис. 10: Проверка атрибута, работа с файлом

1. От пользователя guest пробую прочитать файл командой *cat /tmp/file01.txt*, далее записываю в файл слово test2 и вновь читаю его - текст файла изменен (рис. 11)

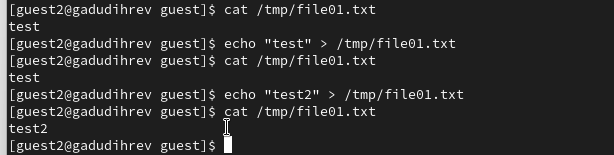


Рис. 11: Действия с файлом от другого пользователя

1. От пользователя guest2 пробую записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой *echo “test3” > /tmp/file01.txt* - операцию выполнить удалось. Просматриваю содержимое файла и пробую удалить его - удалить не удалось (рис. 12)

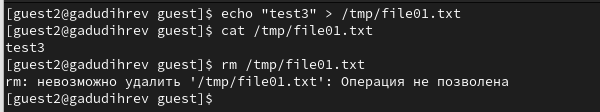


Рис. 12: Действия с файлом от другого пользователя

1. От суперпользователя ввожу команду, снимающую атрибут t (Sticky-бит) с директории /tmp: *chmod -t /tmp*. Проверяю от пользователя guest2, что атрибута t у директории /tmp нет командой *ls -l / | grep tmp* (рис. 13)

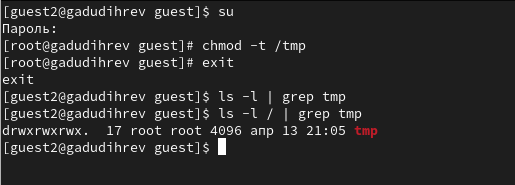


Рис. 13: Снятие Sticky-бита с директории

1. Снова пробую записать, прочитать и удалить файл - все операции выполнены успешно (рис. 14)

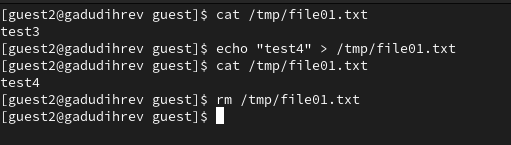


Рис. 14: Запись, чтение и удаление

1. Возвращаюсь в суперпользователя и возвращаю атрибут t на директорию /tmp командой *chmod +t /tmp* (рис. 15)

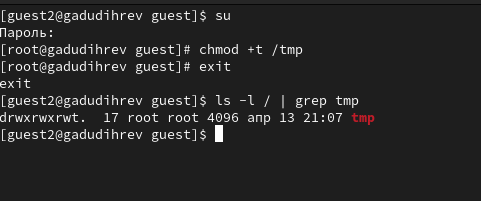


Рис. 15: Возвращение атрибута t

# 3 Выводы

Я научился применять SetUID- и Sticky-биты, поработал с дополнительными атрибутами в консоли, рассмотрел работу механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов.