Лабораторная работа №5

Дисциплина: Основы информационной безопасности

Аветисян Давид Артурович

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.

# Теоретическое введение

SetUID, SetGID и Sticky - это специальные типы разрешений позволяют задавать расширенные права доступа на файлы или каталоги. • SetUID (set user ID upon execution — «установка ID пользователя во время выполнения) являются флагами прав доступа в Unix, которые разрешают пользователям запускать исполняемые файлы с правами владельца исполняемого файла. • SetGID (set group ID upon execution — «установка ID группы во время выполнения») являются флагами прав доступа в Unix, которые разрешают пользователям запускать исполняемые файлы с правами группы исполняемого файла. • Sticky bit в основном используется в общих каталогах, таких как /var или /tmp, поскольку пользователи могут создавать файлы, читать и выполнять их, принадлежащие другим пользователям, но не могут удалять файлы, принадлежащие другим пользователям. Более подробно см. в [1].

# Выполнение лабораторной работы

1 часть: Создание программы

1. Для начала мы убеждаемся, что компилятор gcc установлен, исолпьзуя команду “gcc -v”. Затем отключаем систему запретов до очередной перезагрузки системы командой “sudo setenforce 0”, после чего команда “getenforce” выводит “Permissive” (fig. 1).

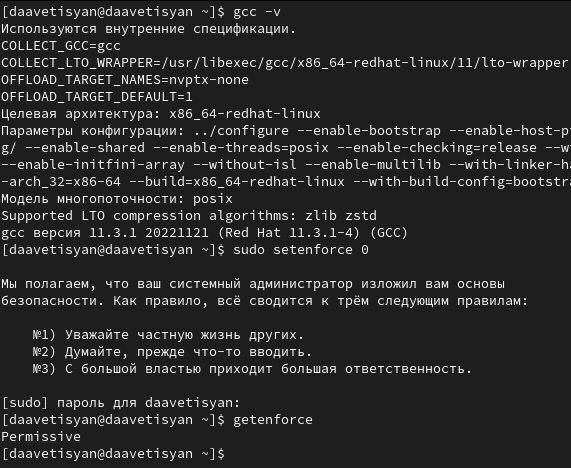


Figure 1: Предварительная подготовка

1. Проверяем успешное выполнение команд “whereis gcc” и “whereis g++” (их расположение)( fig. 2).

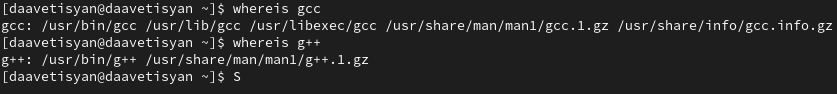


Figure 2: Команда “whereis”

1. Входим в систему от имени пользователя guest командой “su - guest”. Создаём программу simpleid.c командой “touch simpleid.c” и открываем её в редакторе командой “gedit /home/guest/lab05/simpleid.c” (fig. 3).

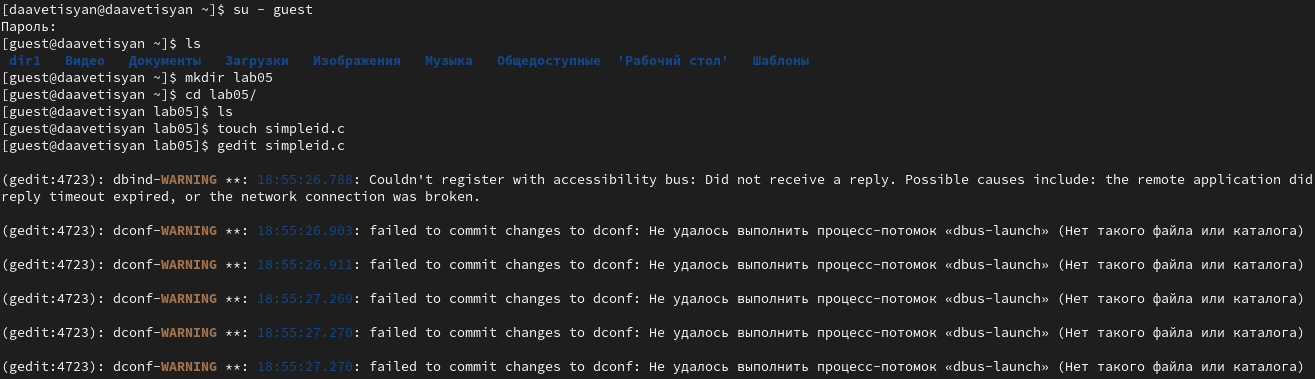


Figure 3: Вход в систему и создание программы

1. Код программы выглядит следующим образом (fig. 4).

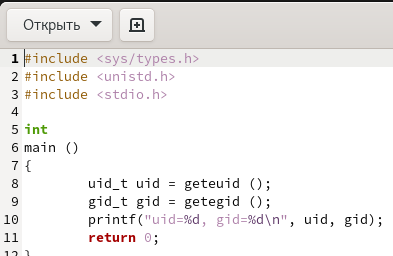


Figure 4: Код программы simpleid.c

1. Скомпилируем программу и убедимся, что файл программы был создан командой “gcc simpleid.c -o simpleid”. Выполняем программу simpleid командой “./simpleid”, а затем системную программу id командой “id”. Результаты, полученные в результате выполнения обеих команд, совпадают(uid=1001 и gid=1001) (fig. 5).

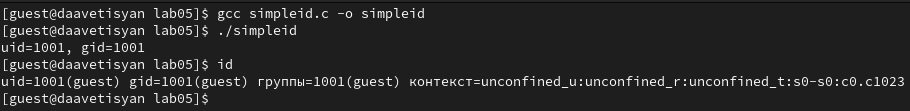


Figure 5: Компиляция и выполнение программы simpleid

1. Усложняем программу, добавив вывод действительных идентификаторов, новый файл назовём simpleid.c (fig. 6).

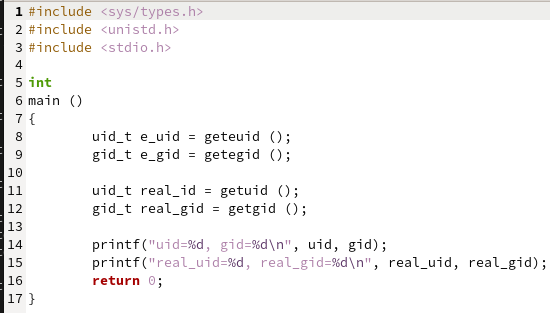


Figure 6: Усложнение программы

1. Скомпилируем и запустим simpleid2.c командами “gcc simpleid2.c -o simpleid2” и “./simpleid2” (fig. 7).

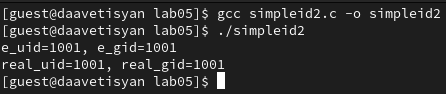


Figure 7: Компиляция и выполнение программы simpleid2

1. От имени суперпользователя выполняем команды “sudo chown root:guest /home/guest/lab05/simpleid2” и “sudo chmod u+s /home/guest/lab05/simpleid2”, затем выполняем проверку правильности установки новых атрибутов и смены владельца файла simpleid2 командой “sudo ls -l /home/guest/lab05/simpleid2” (fig. 8). Этими командами была произведена смена пользователя файла на root и установлен SetUID-бит.

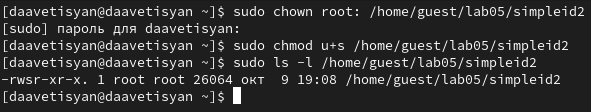


Figure 8: Установка новых атрибутов (SetUID) и смена владельца файла

1. Запускаем программы simpleid2 и id. Теперь появились различия в uid (fig. 9).

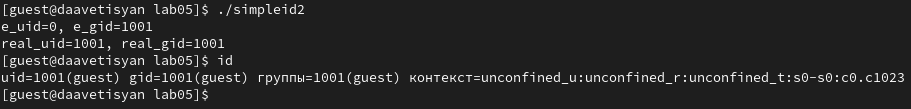


Figure 9: Запуск simpleid2 после установки SetUID

1. Проделаем тоже самое относительно SetGID-бита. Также можем заметить различия с предыдущим пунктом (fig. 10).

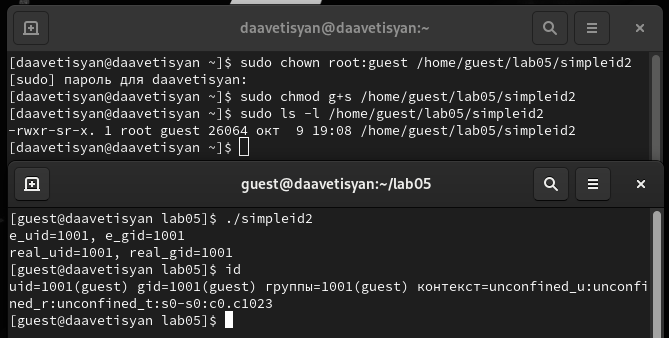


Figure 10: Запуск simpleid2 после установки SetGID

1. Создаем программу readfile.c (fig. 11).

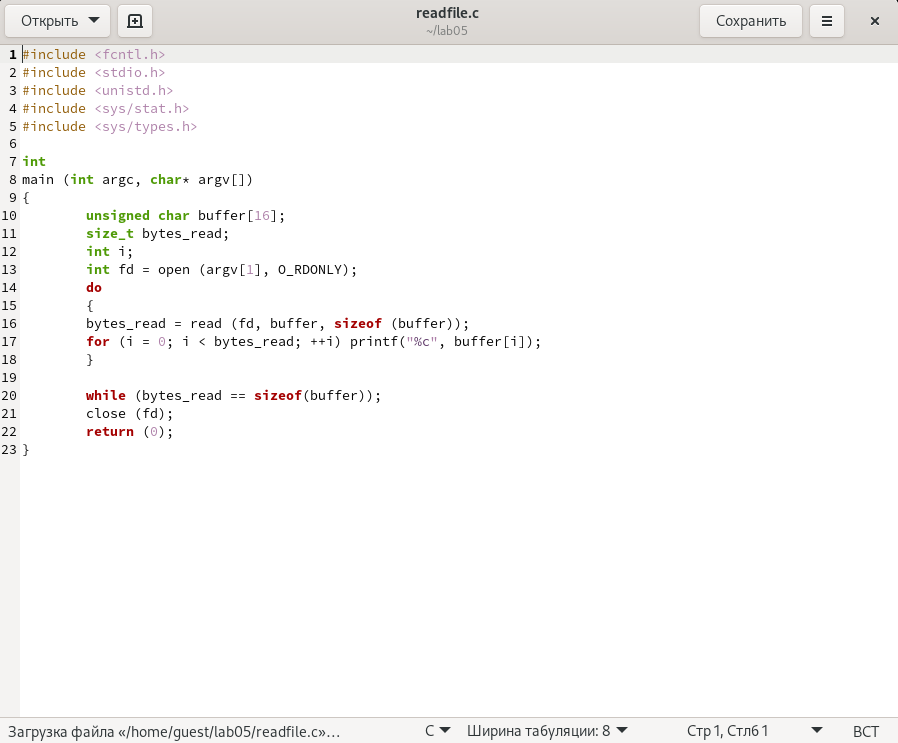


Figure 11: Код программы readfile.c

1. Скомпилируем созданную программу командой “gcc readfile.c -o readfile”. Сменим владельца у файла readfile.c командой “sudo chown root:guest /home/guest/readfile.c” и поменяем права так, чтобы только суперпользователь мог прочитать его, а guest не мог, с помощью команды “sudo chmod 700 /home/guest/readfile.c”. Убеждаемся, что пользователь guest не может прочитать файл readfile.c командой “cat readfile.c”, получив отказ в доступе (fig. 12).

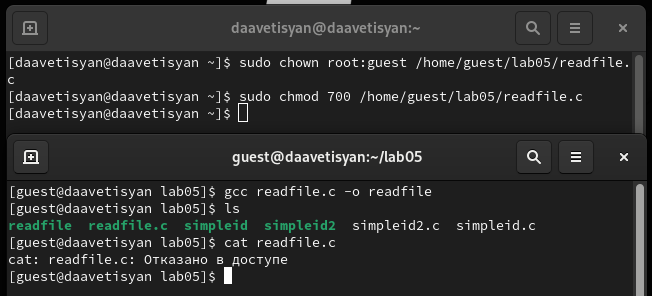


Figure 12: Смена владельца и прав доступа у файла readfile.c

13)П оменяем владельца у программы readfile и установим SetUID. Проверим, может ли программа readfile прочитать файл readfile.c командой “./readfile readfile.c”. Прочитать удалось. Аналогично проверяем, можно ли прочитать файл /etc/shadow. Прочитать удалось (fig. 13).

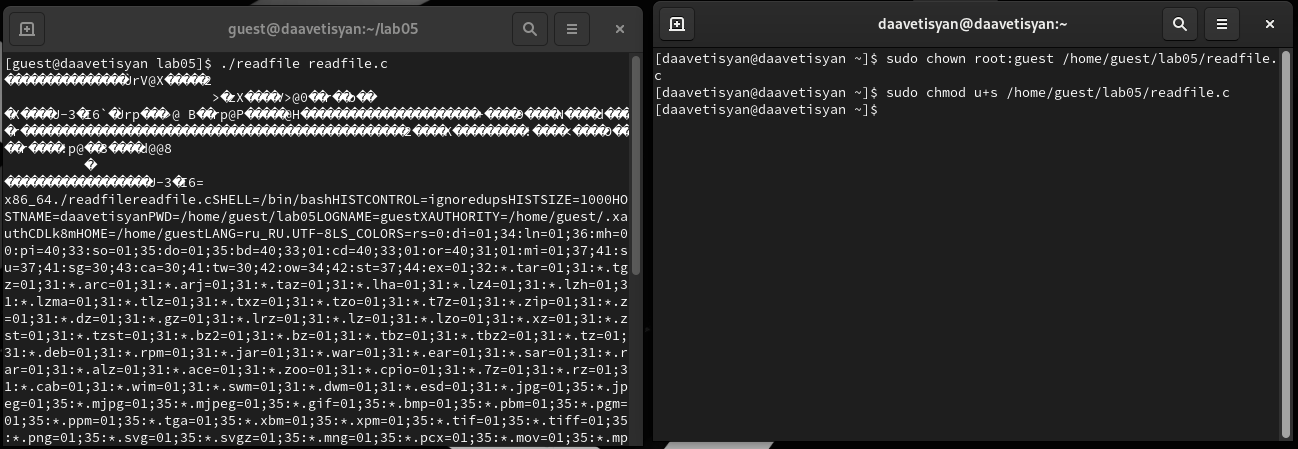


Figure 13: Запуск программы readfile

2 часть: Исследование Sticky-бита

1. Командой “ls -l / | grep tmp” убеждаемся, что атрибут Sticky на директории /tmp установлен. От имени пользователя guest создаём файл file01.txt в директории /tmp со словом test командой “echo”test” > /tmp/file01.txt”. Просматриваем атрибуты у только что созданного файла и разрешаем чтение и запись для категории пользователей “все остальные” командами “ls -l /tmp/file01.txt” и “chmod o+rw /tmp/file01.txt” (fig. 14).

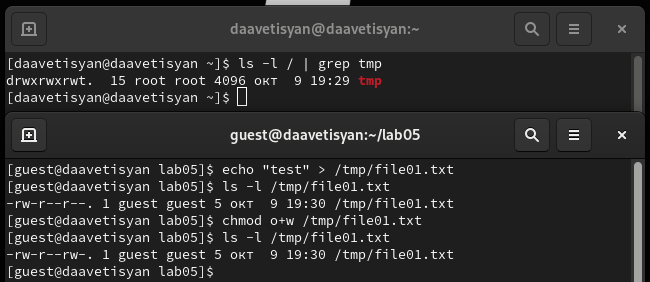


Figure 14: Создание файла file01.txt

1. От имени пользователя guest2 пробуем прочитать файл командой “cat /tmp/file01.txt” - это удалось. Далее пытаемся дозаписать в файл слово test2, проверить содержимое файла и записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию - эти операции удалось выполнить только в случае, если еще дополнительно разрешить чтение и запись для группы пользователей командой “chmod g+rw /tmp/file01.txt”. От имени пользователя guest2 пробуем удалить файл - это не удается ни в каком из случаев, возникает ошибка (fig. 15).

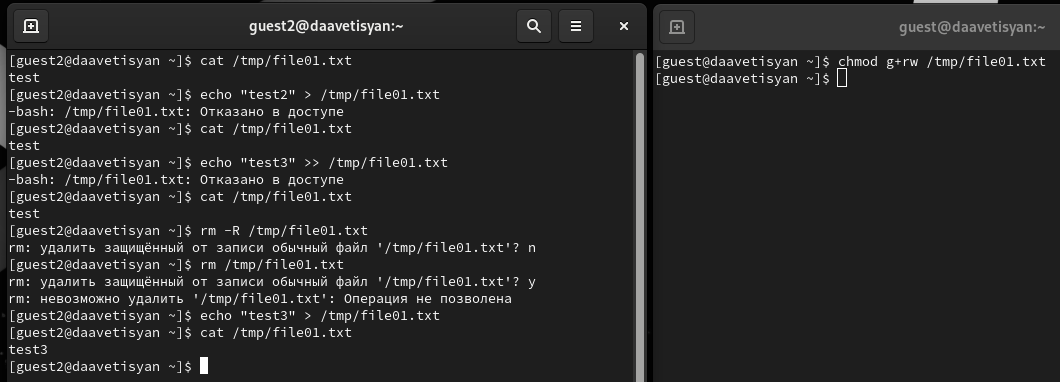


Figure 15: Попытка выполнить действия над файлом file01.txt от имени пользователя guest2

1. Повышаем права до суперпользователя командой “su -” и выполняем команду, снимающую атрибут t с директории /tmp “chmod -t /tmp”. После чего покидаем режим суперпользователя командой “exit”. Повторяем предыдущие шаги. Теперь нам удаётся удалить файл file01.txt от имени пользователя, не являющегося его владельцем (fig. 16).

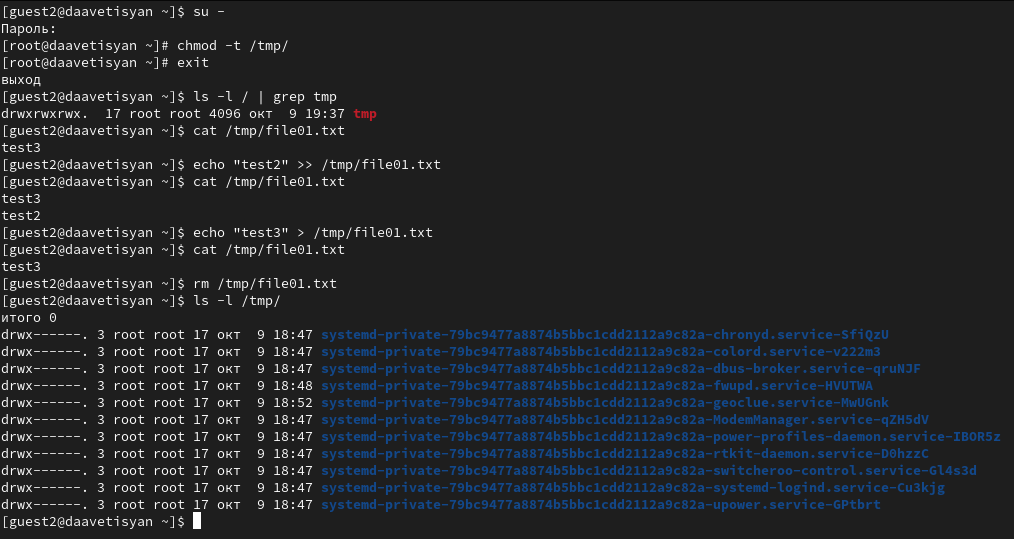


Figure 16: Удаление атрибута t (Sticky-бита) и повторение действий

1. Повышаем свои права до суперпользователя и возвращаем атрибут t на директорию /tmp (fig. 17).

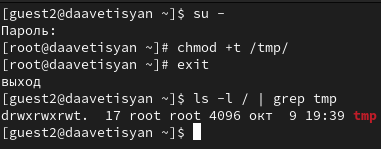


Figure 17: Возвращение атрибута t (Sticky-бита)

# Выводы

* В ходе выполнения данной лабораторной работы я изучил механизмы изменения идентификаторов, применение SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Список литературы

* Стандартные права SetUID, SetGID, Sticky в Linux [Электронный ресурс]. URL: https://linux-notes.org/standartny-e-prava-unix-suid-sgid-sticky-bity/.