Отчёт по лабораторной работе №5

Дисциплина: Основы информационной безопасности

Полиенко Анастасия Николаевна, НПМбд-01-19

Содержание

# 1 Цель работы

Изучить особенности работы с дополнительными атрибутами SetUID, SetGID и Sticky битами и их влияние на работу с файлами при их наличии и отсутствии.

# 2 Теоретическое введение

SetUID, SetGID и Sticku — это специальные типы разрешений, которые позволяют задавать расширенные права доступа на файлы и каталоги.

* SetUID — это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла. Другими словами, использование этого бита позволят поднять привилегии пользователя в случае, если это необходимо. Наличие SetUID бита выражается в том, что на месте классического бита x выставлен специальный бит s: -rwsr-xr-x
* SetGID — очень похож на SetUID с отличием, что файл будет запускаться от имени группы, который владеет файлом: -rwxr-sr-x
* Sticky — в случае, если этот бит установлен для папки, то файлы в этой папке могут быть удалены только их владельцем. Наличие этого бита показывается через букву t в конце всех прав: drwxrwxrwxt

Более подробно см. в [1].

# 3 Выполнение лабораторной работы

## 3.1 Создание программы

Создадим программу simpleid.c (рис. 1).

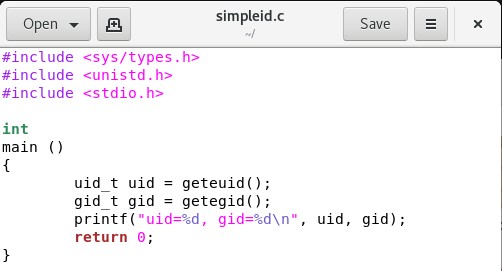


Рис. 1: Текст программы simpleid.c

Скомпилируем программу с помощью команды gcc и убеждаемся, что файл действительно создан. Далее запускаем исполняемый файл через ./. Вывод написанной программы совпадает с выводом команды id (рис 2).



Рис. 2: Компиляция и запуск simpleid

Усложним программу и назовём её simpleid2.c (рис. 3).

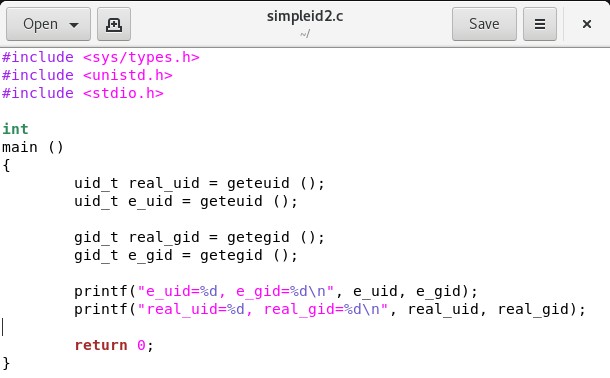


Рис. 3: Текст программы simpleid2.c

Скомпилируем и запустим файл simpleid2 (рис. 4).

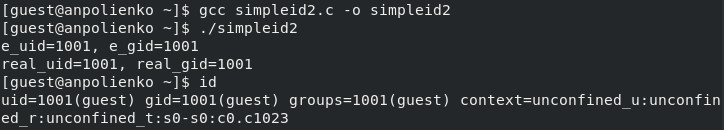


Рис. 4: Компиляция и запуск simpleid2

От имени суперпользователя сменим владельца файла simpleid2 на root и установим SetUID-бит. Далее через команду ls -l видим, что бит установился корректно (рис. 5)

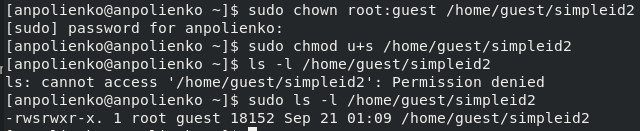


Рис. 5: Смена владельца и установка SetUID

Запускаем программу simpleid2 и комаду id. Теперь видим, что появились отличия в uid строках (рис. 6).

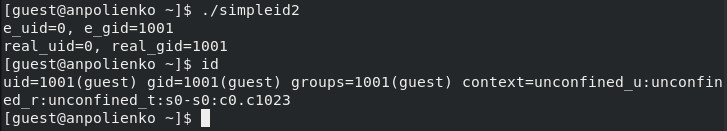


Рис. 6: Запуск simpleid2

Проделываем выше описанные действия для SetGID-бита. Теперь после запуска simpleid2 можем увидеть отличие и в gid строках (рис. 7).

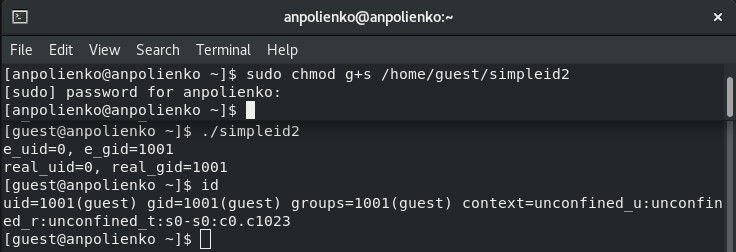


Рис. 7: SetGID-бит

Создадим программу readfile.c (рис. 8).

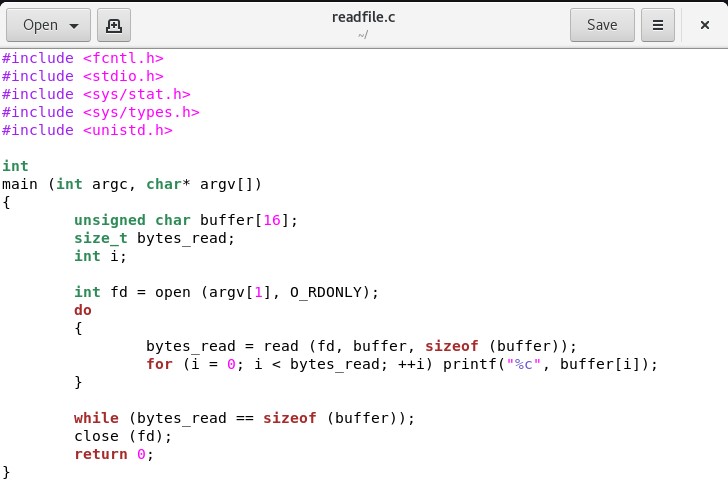


Рис. 8: Текст программы readfile.c

Откомпилируем эту программу командой gcc. Далее меняем владельца файла readfile.c и отнимаем у пользователя guest право на чтение. При попытке прочитать файл от имени пользователя guest возникает ошибка (рис. 9).

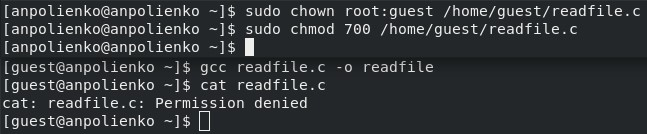


Рис. 9: Компиляция readfile.c

Меняем владельца файла readfile и устанавливаем на него SetUID-бит. Запускаем исполняемый файл и убеждаемся, что программа может прочитать файлы readfile.c и /etc/shadow (рис. 10).

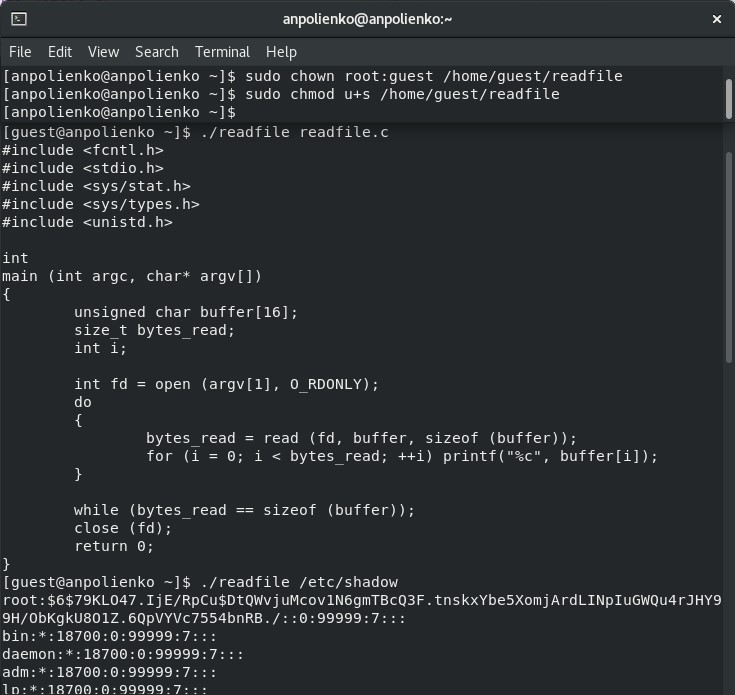


Рис. 10: Запуск readfile

## 3.2 Исследование Sticky-бита

Выполняя команду ls -l выявняем, что на каталоге /tmp установлен Sticky-бит. Это видно, т.к. в конце написана t. Далее от имени пользователя guest создаём файл /tmp/file01.txt. Потом просматриваем атрибуты только что созданного файла и даём всем пользователям право на чтение и запись (рис. 11).

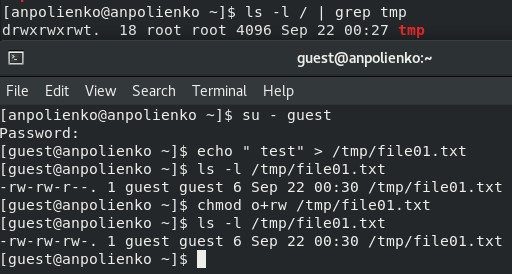


Рис. 11: Создание файла file01.txt

От имени пользователя guest2 читаем файл file01.txt командой cat. Далее успешно дозаписываем в конец файла строку “test2”, а затем успешно перезаписываем содержимое, меняя его на строку “test3”. Однако при попытке удалить файл возникла ошибка (рис. 12).

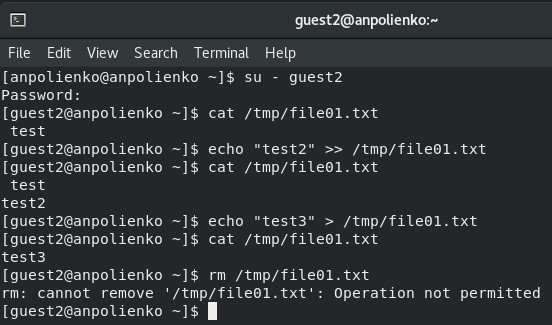


Рис. 12: Действия над file01.txt от лица guest2

Временно повышаем права до суперпользователя и снимаем с директории /tmp Sticky-бит. Покидаем режим суперпользователя командой exit (рис. 13).

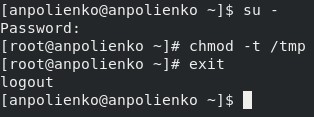


Рис. 13: Удаление Sticky-бита

Убеждаемся через команду ls -l, что Sticky-бит действительно отсутсвует. Далее повторяем действия от имени пользователя guest2. описанные выше. В этот раз удалось удалить файл file01.txt даже при условии, что guest2 не является его владельцем (рис. 14).

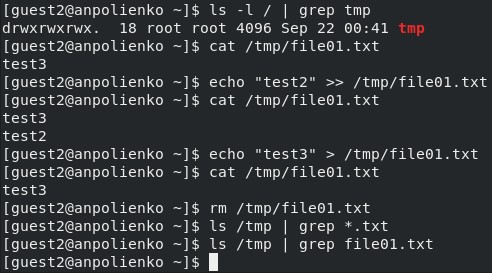


Рис. 14: Повтор действий

Временно повышаем права до суперпользователя и возвращает Sticky-бит на каталог /tmp (рис. 15).

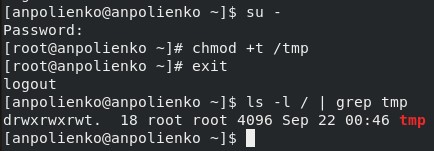


Рис. 15: Возращение Skicky-бита

# 4 Выводы

Изучила механизмы изменения идентификаторов и получила практические навыки по работе с SetUID, SetGID и Sticky битами и узнала об их особенностях и влиянии на файлы и директории.

# Список литературы

1. SETUID, SETGID and Sticky bits [Электронный ресурс]. RuVSD, 2021. URL: <https://ruvsd.com/ru/helpcenter/suid-sgid-sticky-bit-linux/>.