Лабораторная работа №5

Форис Анастасия Дмитриевна, НПМбд-02-21

Содержание

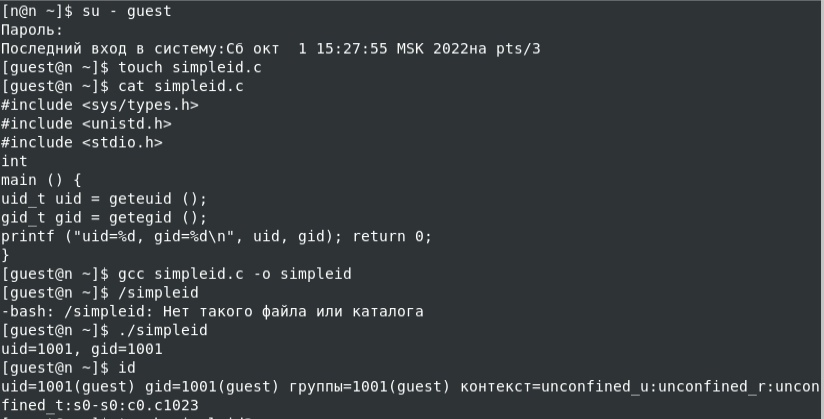
# 1 Цель работы

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

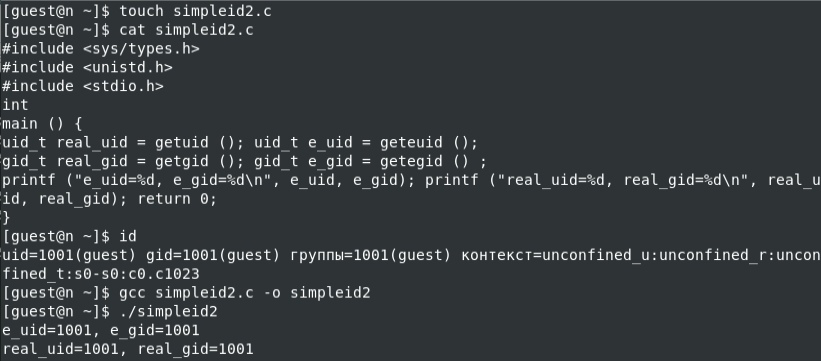
# 2 Выполнение лабораторной работы

## 2.1 Создание программы

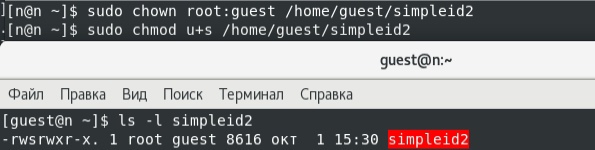
Создадим программу simpleid.c и скомпилируем ее с помощью команды gcc и убеждаемся, что файл действительно создан. Далее запускаем исполняемый файл через ./. Вывод написанной программы совпадает с выводом команды id



Усложним программу, скомпилируем и запустим (файл simpleid2)



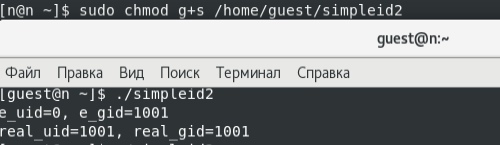
От имени суперпользователя сменим владельца файла simpleid2 на root и установим SetUID-бит.



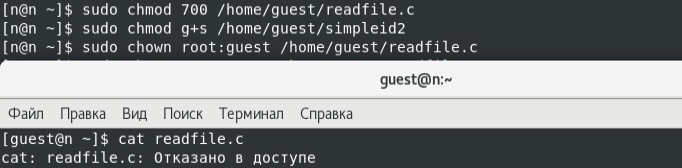
Запускаем программу simpleid2 и комаду id. Появились отличия в uid строках



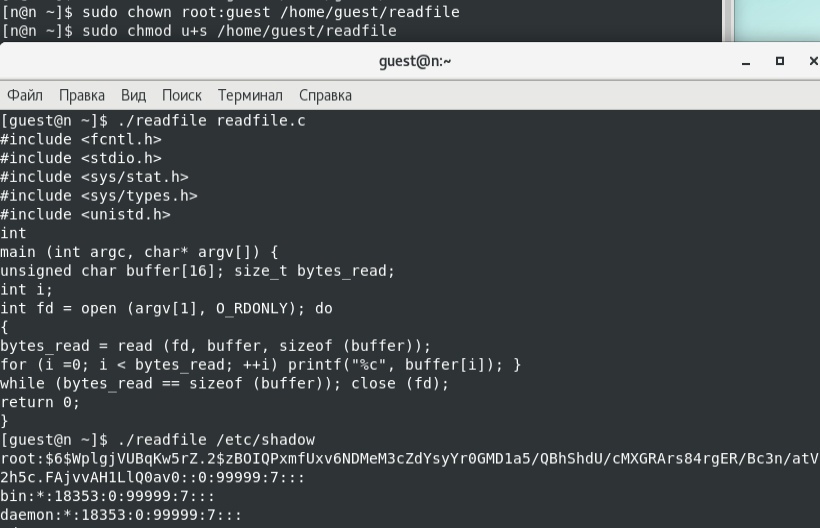
Проделываем выше описанные действия для SetGID-бита. Появились отличия в gid строках



Создадим программу readfile.c и откомпилируем эту программу командой gcc. Меняем владельца файла readfile.c и отнимаем у пользователя guest право на чтение. При попытке прочитать файл от имени пользователя guest возникает ошибка

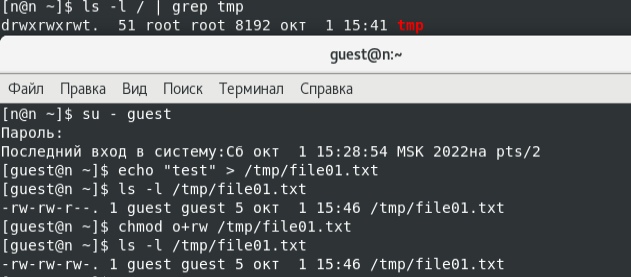


Меняем владельца файла readfile и устанавливаем на него SetUID-бит. Запускаем исполняемый файл и убеждаемся, что программа может прочитать файлы readfile.c и /etc/shadow



## 2.2 Исследование Sticky-бита

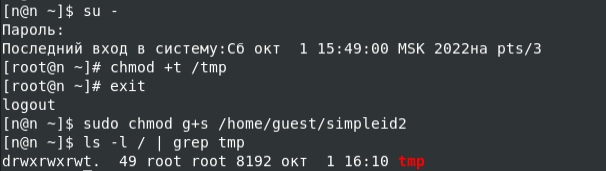
Выполняя команду ls -l выявняем, что на каталоге /tmp установлен Sticky-бит. Это видно, т.к. в конце написана t. Далее от имени пользователя guest создаём файл /tmp/file01.txt. Потом просматриваем атрибуты только что созданного файла и даём всем пользователям право на чтение и запись



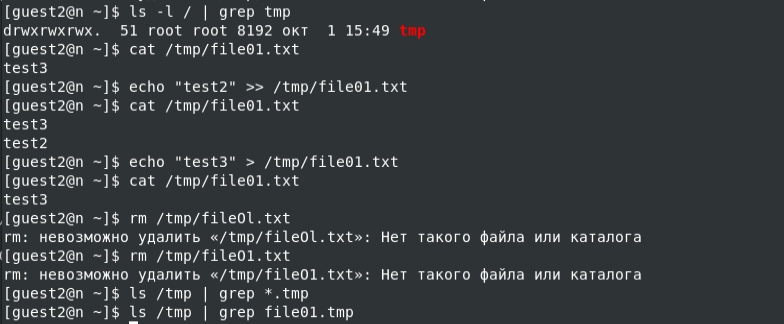
От имени пользователя guest2 читаем файл file01.txt командой cat. Повторяем предыдущие шаги. При попытке удалить файл возникла ошибка.



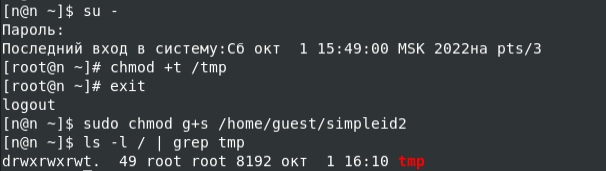
Повышаем права до суперпользователя и снимаем с директории /tmp Sticky-бит. Покидаем режим суперпользователя командой exit



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



Повышаем права до суперпользователя и возвращает Sticky-бит на каталог /tmp



# 3 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.

# 4 Список литературы

* Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: http://bugtraq.ru/library/books/attack1/index.html
* Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: http://bugtraq.ru/library/books/attack/index.html
* Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.