Отчёт по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Даниил Анатольевич Вейценфельд

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 Задание

1. Создать программу для проверки uid и gid
2. Протестировать ее от имени разных пользователей
3. Протестировать ее с разными правами доступаи и SUID/SGID-битами
4. Создать программу для чтения файла
5. Протестировать ее на файлах с разными правами доступа и SUID/SGID-битами
6. Протестировать sticky-бит

# 3 Теоретическое введение

SetUID- и SetGID-биты (они же SUID, SGID) являются “заменой” обычным битам на право выполнения (x) файла; имеют обозначения s, через ls -l отображаются на месте бита x пользователя или группы соответственно.

Эти биты позволяют выполнить файл любому пользователю от лица владельца файла. Для примера: программа sudo имеет влазельца root и SUID бит, значит любой пользователь может ее выполнить от лица root.

Sticky Bit - если он установлен для папки, то файлы в этой папке могут быть удалены только их владельцем. Пример использования этого бита в операционной системе это системная папка /tmp. Эта папка разрешена на запись любому пользователю, но удалять файлы в ней могут только пользователи, являющиеся владельцами этих файлов.

Теорию работы в \*nix-системах см. в [1–6].

# 4 Выполнение лабораторной работы

## 4.1 SetUID, SetGID

С помощью языка Си и компилятора gcc создана (рис. 1) простая программа для проверки uid и gid исполняющего пользователя (рис. 2).

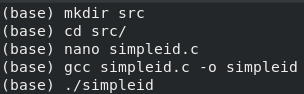


Рис. 1: Создание программы

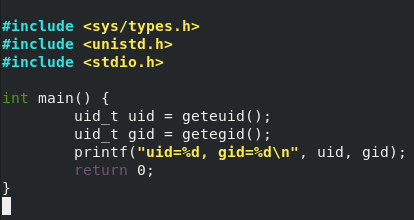


Рис. 2: Код программы получения ID

Программа верно определила id пользователя guest (рис. 3). Команда id возвращает ту же информацию.

Рис. 3: Запуск от guest

Рис. 3: Запуск от guest

Немного усложним программу для получения как отображаемых, так и реальных ID (рис. 4).

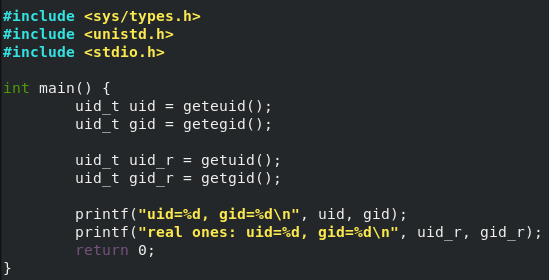


Рис. 4: Усложненный код получения ID

Установим ей владельца root и SUID-бит (рис. 5).

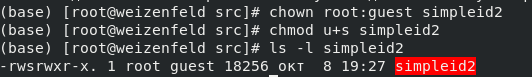


Рис. 5: Установка владельца и SUID-бита

Проверим, что она выводит для пользователя guest: рис. 6.

Рис. 6: Проверка от пользователя guest

Рис. 6: Проверка от пользователя guest

Установим ей и SGID-бит вместе с группой root. Информация верна. (suid-бит был ранее снят) (рис. 7)

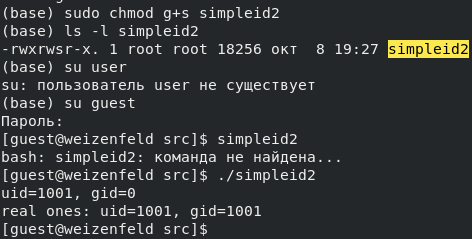


Рис. 7: Установка SGID-бита и проверка

Теперь напишем программу, которая читает файл как cat (рис. 8).

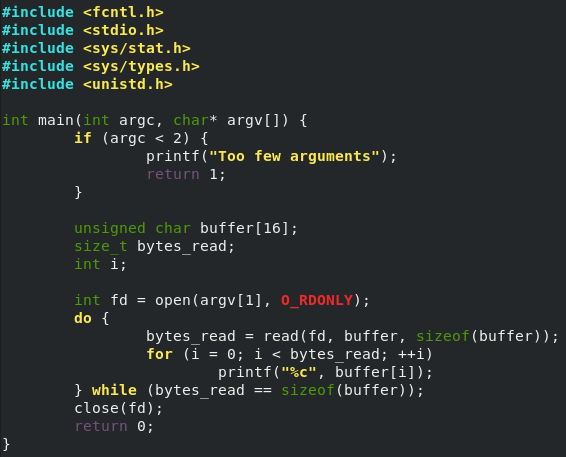


Рис. 8: Программа для чтения

Создадим текстовый файл с правами на чтение и запись тоьлко для root (рис. 9).

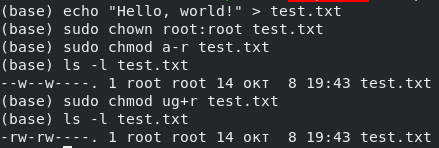


Рис. 9: Создан текстовый файл

Проверим чтение с помощью cat и с помощью программы (рис. 10). Программе ранее был установлен бит SUID.

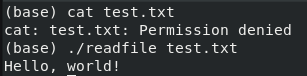


Рис. 10: Проверка чтения программой

Также, удалось считать файл /etc/shadow с помощью ./readfile /etc/shadow | less (рис. 11).

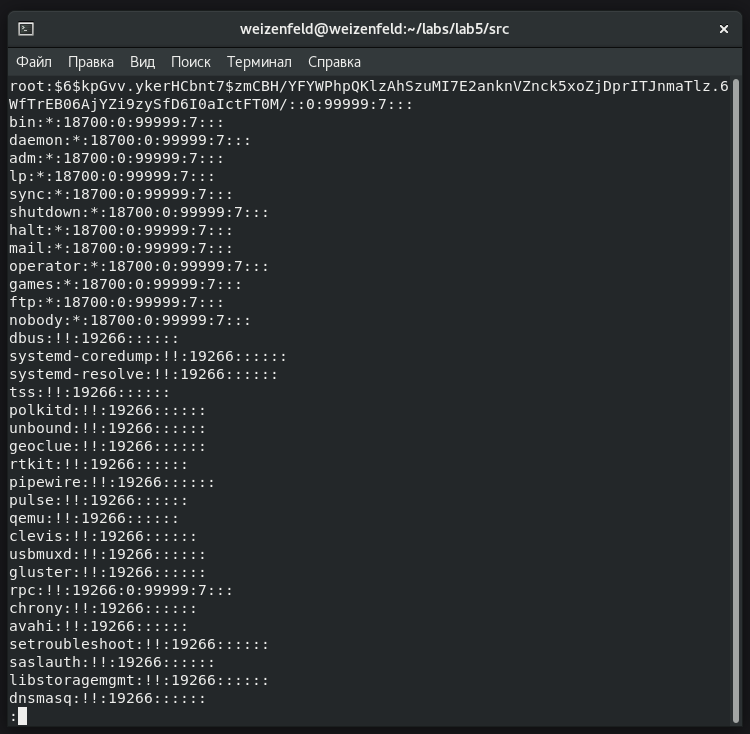


Рис. 11: Чтение /etc/shadow

## 4.2 Sticky-бит

Проверим его наличие на директории /tmp (рис. 12).

Рис. 12: Sticky-бит установлен на д-и /tmp

Рис. 12: Sticky-бит установлен на д-и /tmp

Создадим там файл с правами на чтение/запись для всех (рис. 13).

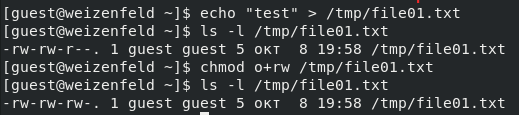


Рис. 13: Создание файла file01

Теперь попробуем чтение, запись и дозапись от другого пользователя. Все успешно. Но удалить файл нельзя (рис. 14).

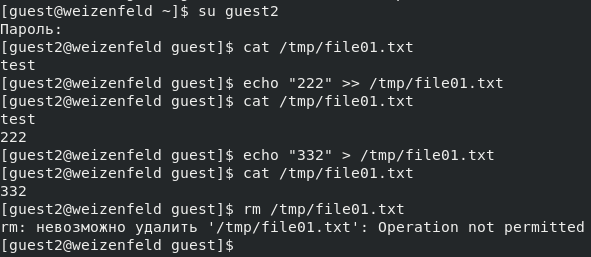


Рис. 14: Эксперименты от guest2 с файлом

Уберем от пользователя root sticky-бит с директории /tmp (рис. 15).

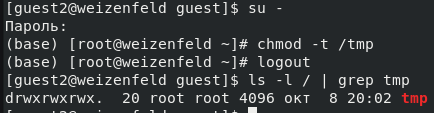


Рис. 15: Удаление sticky-бита

Файл так же можно читать/записывать, но теперь можно и удалить (рис. 16).

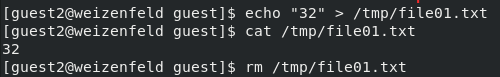


Рис. 16: Успешное удаление файла

# 5 Выводы

Изучены механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получены практические навыки работы в консоли с дополнительными атрибутами. Рассмотрена работа механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Список литературы

1. GNU Bash Manual [Электронный ресурс]. Free Software Foundation, 2016. URL: <https://www.gnu.org/software/bash/manual/>.

2. Newham C. [Learning the bash Shell: Unix Shell Programming](http://www.amazon.com/Learning-bash-Shell-Programming-Nutshell/dp/0596009658). O’Reilly Media, 2005. 354 с.

3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.

4. Robbins A. [Bash Pocket Reference](https://www.ncbi.nlm.nih.gov/pubmed/25246403). O’Reilly Media, 2016. 156 с.

5. Таненбаум Э. Архитектура компьютера. 6-е изд. СПб.: Питер, 2013. 874 с.

6. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.