Отчёт по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Кондрашина Мария Сергеевна

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 Теоретические сведения

Setuid, Setgid и Sticky Bit - это специальные типы разрешений позволяют задавать расширенные права доступа на файлы или каталоги.

Setuid – это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла. Другими словами, использование этого бита позволяет нам поднять привилегии пользователя в случае, если это необходимо.

Принцип работы Setgid похож на setuid с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.

В случае, если Sticky Bit установлен для папки, то файлы в этой папке могут быть удалены только их владельцем, тоже самое верно и для файлов.[2]

# 3 Выполнение лабораторной работы. Создание программы

1. Подготовка лабораторного стенда (fig. 1)

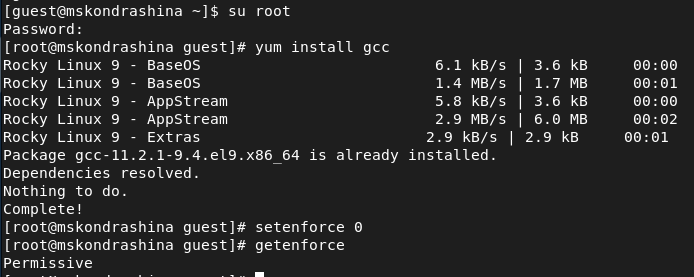


Figure 1: Подготовка лабораторного стенда

1. Вошла в систему от имени пользователя guest, создала программу simpleid.c(fig. 2). Скомплилировала программу и выполнила ее, также выполнила системную программу id т сравнила вывод двух программ - вывелись одинаковые значения.(fig. 3)

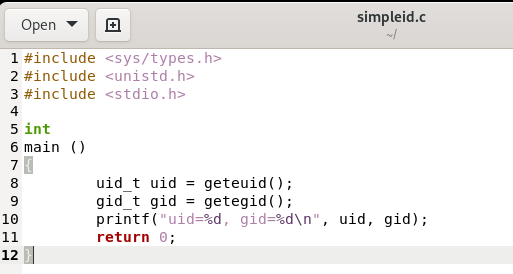


Figure 2: Программа simpleid.c

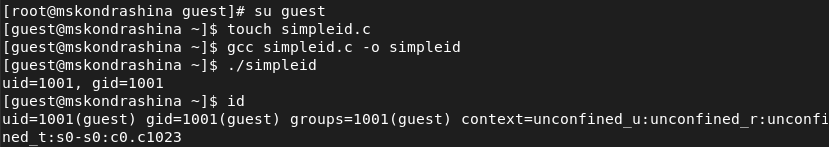


Figure 3: Пункт 1-5

1. Усложнила программу, добавив вывод действительных идентификаторов тила (fig. 4), скомпилировала и запустила (fig. 5)

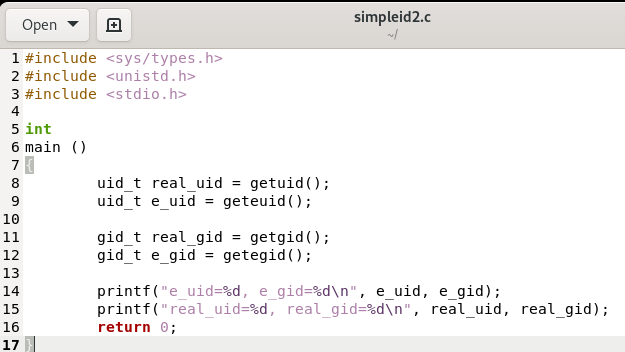


Figure 4: Программа simpleid2.c

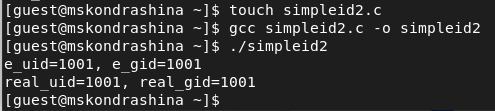


Figure 5: Компилирование и запуск simpleid2.c

1. От имени суперпользователя выполнила команды: chown root:guest /home/guest/simpleid2, chmod u+s /home/guest/simpleid2. Также выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2: ls -l simpleid2, запустила simpleid2 и id, результаты которых оказались одинаковыми.(fig. 6)



Figure 6: SetUID-бит

1. Проделала тоже самое относительно SetGID-бита.(fig. 7)

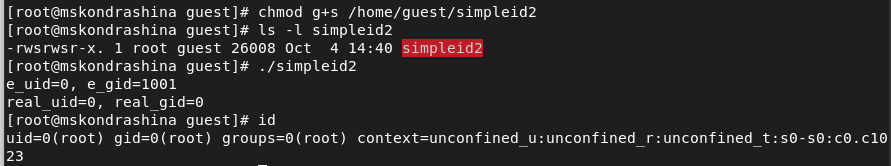


Figure 7: SetGID-бит

1. Создала программу readfile.c (fig. 8)(fig. 9)

Figure 8: Создание файла readfile.c

Figure 8: Создание файла readfile.c

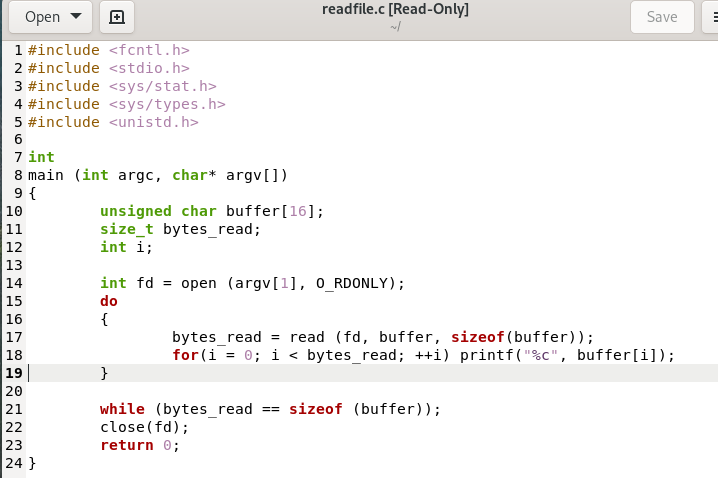


Figure 9: Программа readfile.c

1. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог.(fig. 10)

Figure 10: Смена прав так, чтобы только суперпользователь мог прочесть файл

Figure 10: Смена прав так, чтобы только суперпользователь мог прочесть файл

1. Проверила, что пользователь guest не может прочитать файл readfile.c (fig. 11)

Figure 11: Проверка

Figure 11: Проверка

1. Сменила у программы readfile владельца и установила SetUID-бит. (fig. 12)

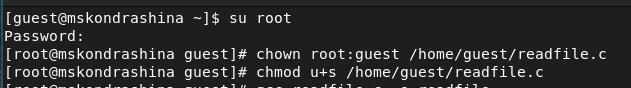


Figure 12: readfile SetUID-бит

1. Проверила, может ли программа readfile прочитать файл readfile.c - Да, может. (fig. 13)

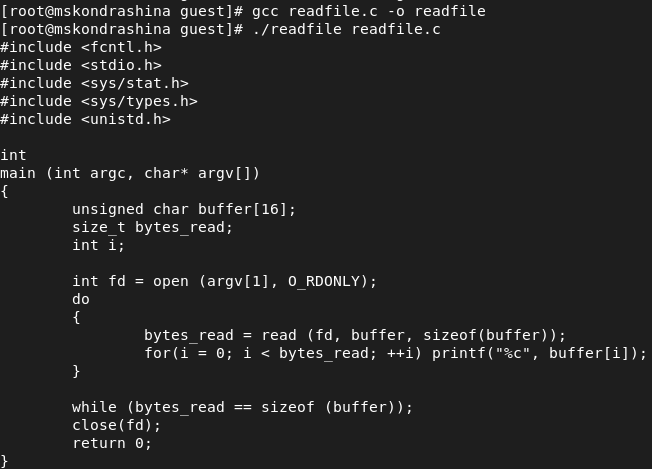


Figure 13: Проверка чтения файла readfile.c

1. Проверила, может ли программа readfile прочитать файл /etc/shadow. - Да, может. (fig. 14)

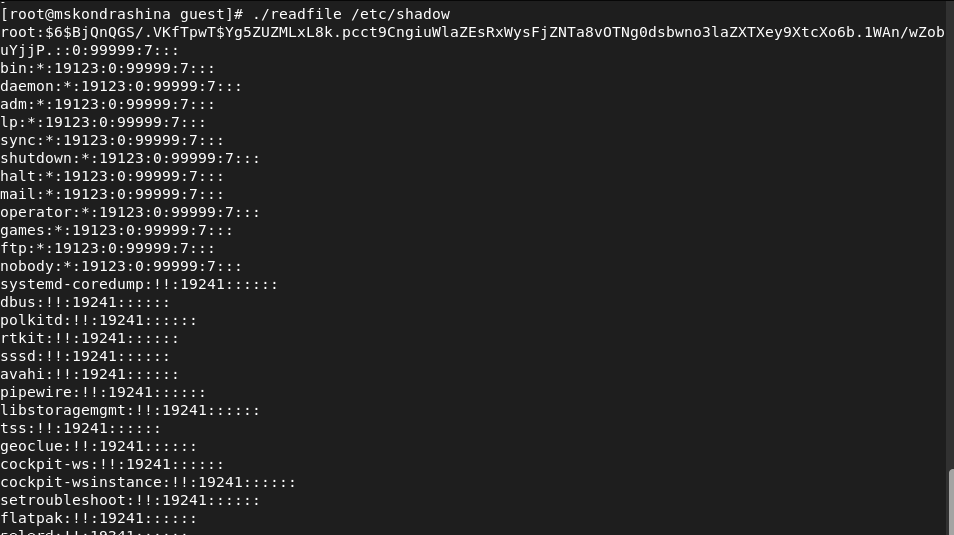


Figure 14: Проверка чтения файла /etc/shadow

# 4 Исследование Sticky-бита

1. Выяснила, установлен ли атрибут Sticky на директории /tmp. От имени пользователя guest создала файл file01.txt в директории /tmp со словом test. Просмотрела атрибуты у только что созданного файла и разрешила чтение и запись для категории пользователей «все остальные» (fig. 15)



Figure 15: Атрибут Sticky на директории /tmp и файл file01.txt

1. От пользователя guest2 попробовала прочитать файл /tmp/file01.txt, дозаписать в файл, записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию, удалить файл.(fig. 16)

Все удалось кроме удаления файла.

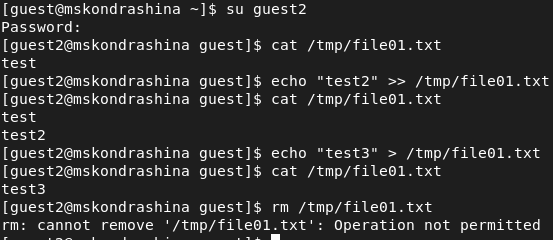


Figure 16: guest2 и file01

1. Повысила свои права до суперпользователя и выполнила после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp, покинула режим суперпользователя.(fig. 17)

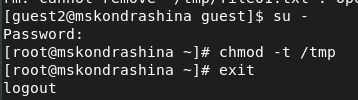


Figure 17: Снятие атрибута t (Sticky-бит) с директории /tmp

1. От пользователя guest2 проверила, что атрибута t у директории /tmp нет, повторила предыдущие шаги.(fig. 18)

Удалось удалить файл от имени пользователя, не являющегося его владельцем



Figure 18: Взаимодействие guest2 с файлом, когдан атрибута t (Sticky-бит) снят с директории /tmp

1. Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp.(fig. 19)

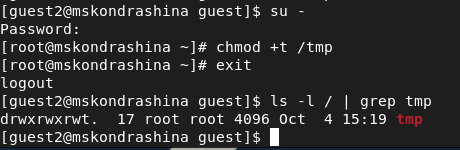


Figure 19: Возвращение атрибута t (Sticky-бит) на директорию /tmp

# 5 Выводы

Выполнила лабораторную работу №5.

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

# 6 Список литературы

1. Методические материалы курса. “Информационная безопасность компьютерных сетей” Кулябов Д. С., Королькова А. В., Геворкян М. Н.
2. https://ruvds.com/ru/helpcenter suid-sgid-sticky-bit-linux/