Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Калинина Кристина Сергеевна

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.

# Теоретические сведения

В операционных системах Linux используются 3 базовых права доступа – на чтение (read), запись (write) и исполнение (execute). Соответственно, права назначаются пользователю (user), группе (group) и всем остальным (world). [1]

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. Классический пример использования этого бита в операционной системе это команда sudo. На месте, где обычно установлен классический бит x (на исполнение), выставлен специальный бит s. Это позволяет обычному пользователю системы выполнять команды с повышенными привилегиями без необходимости входа в систему как root, разумеется зная пароль пользователя root. Для установки используется команда “chmod u+s ”. [1]

Принцип работы Setgid очень похож на setuid с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом. Аналогично setuid, бит setgid выставляется с помощью команды chmod g + s. Удалить эти биты можно также командой chmod, только вместо « + » используется « – » . [1]

Третий из специальных разрешений — sticky bit. Это разрешение полезно для защиты файлов от случайного удаления в среде, где несколько пользователей имеют права на запись в один и тот же каталог. Если применяется закрепленный sticky bit, пользователь может удалить файл, только если он является пользователем-владельцем файла или каталога, в котором содержится файл. По этой причине он применяется в качестве разрешения по умолчанию для каталога /tmp и может быть полезен также для каталогов общих групп. [2]

При использовании ls -ld, вы можете видеть sticky bit как t в позиции, где вы обычно видите разрешение на выполнение для других. Для sticky bit используйте chmod +t, а затем имя файла или каталога, для которого вы хотите установить разрешения. [2]

# Выполнение лабораторной работы

1. Вошла в систему от имени пользователя guest. Создала программу simpleid.c (fig. 1, fig. 2).

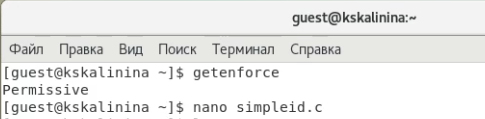


Figure 1: Создание программы simpleid.c



Figure 2: Код программы simpleid.c

1. Скомпилировала и выполнила программу. Выполнив системную программу id убедилась в правильности выведенных данных (fig. 3).

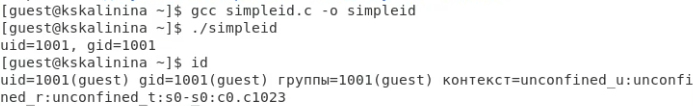


Figure 3: Выполнение программы и сравнение результата с выводом команды id

1. Усложнила программу, добавив вывод действительных идентификаторов, назвала её simpleid2.c (fig. 4).

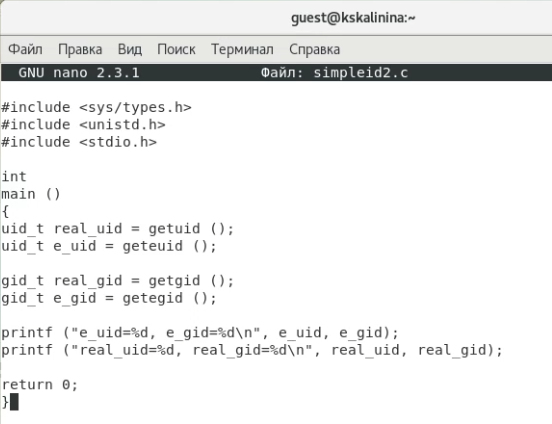


Figure 4: Код программы simpleid2.c

1. Скомпилировала и запустила программу (fig. 5).

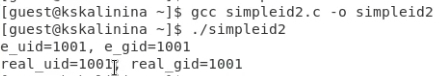


Figure 5: Выполнение программы simpleid2.c

1. От имени суперпользователя установила новые атрибуты и сменила владельца файла simpleid2 (fig. 6).

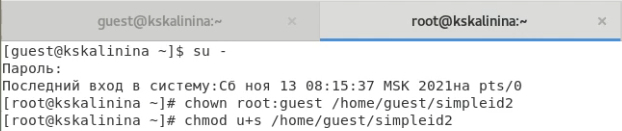


Figure 6: Смена владельца и установка атрибутов

1. Выполнила проверку и запустила программу (fig. 7).

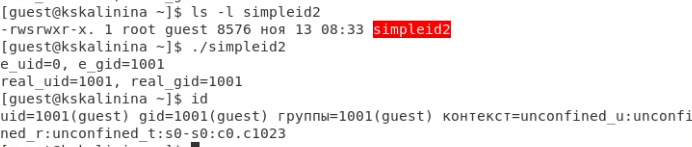


Figure 7: Проверка и запуск программы

1. Проделала тоже самое относительно SetGID-бита (fig. 8, fig. 9).

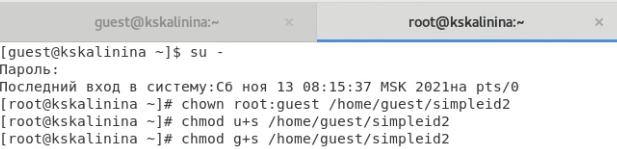


Figure 8: Установка атрибутов

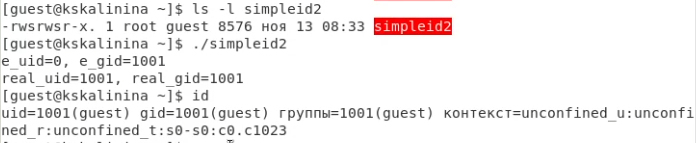


Figure 9: Повтор действий с SetGID-битом

1. Создала программу readfile.c (fig. 10).

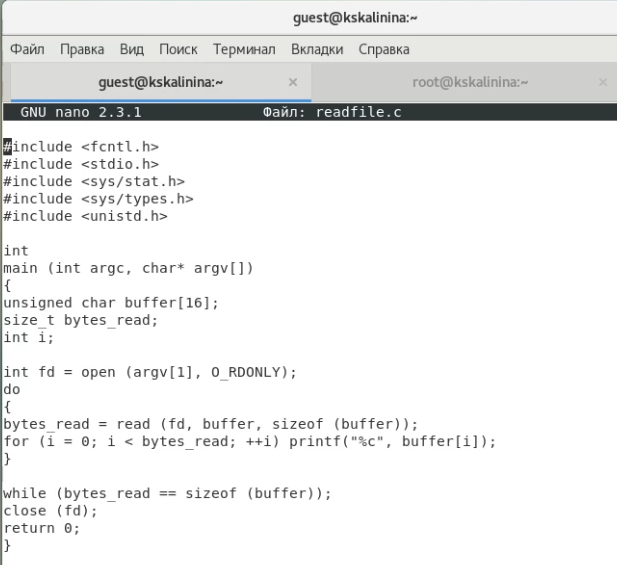


Figure 10: Код программы readfile.c

1. Откомпилировала её (fig. 11).

Figure 11: Компиляция программы readfile.c

Figure 11: Компиляция программы 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. 12).

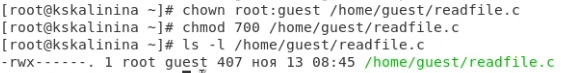


Figure 12: Смена владельца файла readfile.c и прав на него

1. Убедилась, что guest не может прочитать файл readfile.c (fig. 13).

Figure 13: Отказ в чтении readfile.c

Figure 13: Отказ в чтении readfile.c

1. Смените у программы readfile владельца и установите SetU’D-бит (fig. 14).

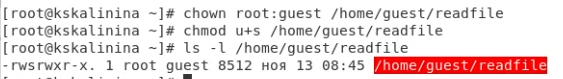


Figure 14: Смена владельца файла readfile и установка SetU’D-бит

1. Убедилась, что readfile может прочитать файлы readfile.c и “/etc/shadow” (fig. 15).

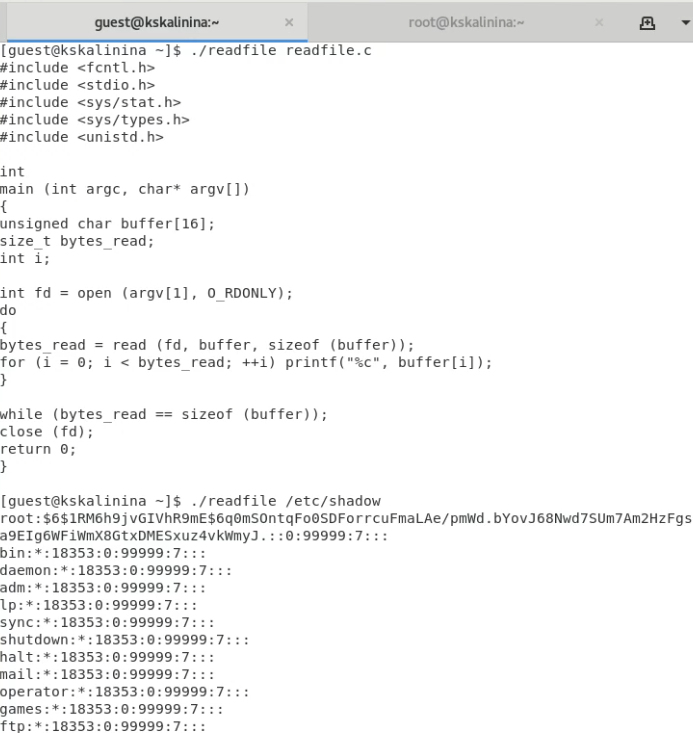


Figure 15: Чтение readfile.c и “/etc/shadow”

1. Убедилась, что атрибут Sticky установлен на директории “/tmp” (fig. 16).

Figure 16: Атрибут Sticky на директории /tmp

Figure 16: Атрибут Sticky на директории /tmp

1. От имени пользователя guest создала файл file01.txt в директории “/tmp” со словом test. Разрешила чтение и запись для категории пользователей «все остальные» (fig. 17).

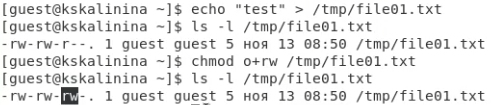


Figure 17: Создание file01.txt и смена атрибутов

1. От пользователя guest2 просмотрела файл, успешно дозаписала и переписала его. Но не смогла его удалить (fig. 18).

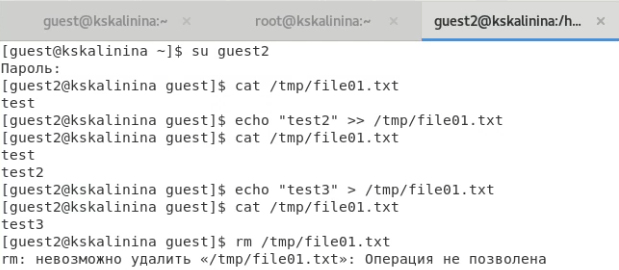


Figure 18: Работа с file01.txt от guest2

1. От суперпользователя сняла атрибут t (Sticky-бит) с директории “/tmp” (fig. 19).

Figure 19: Снятие атрибута Sticky с директории /tmp

Figure 19: Снятие атрибута Sticky с директории /tmp

1. Убедилась в правильности снятия атрибута и повторила предыдущие шаги. В этот раз удаление также прошло успешно (fig. 20).



Figure 20: Повторное выполнение команд от guest2

1. От суперпользователя вернула атрибут t (Sticky-бит) на директорию “/tmp” (fig. 21).

Figure 21: Возвращение атрибута Sticky на директорию /tmp

Figure 21: Возвращение атрибута Sticky на директорию /tmp

# Выводы

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

# Список литературы

1. Использование SETUID, SETGID и Sticky bit. // ruvds.com 2021. URL: https://ruvds.com/ru/helpcenter/suid-sgid-sticky-bit-linux/ (дата обращения 13.11.2021).
2. ИПрава в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask). // habr.com 2019. URL: https://habr.com/ru/post/469667/ (дата обращения 13.11.2021).
3. Д. С. Кулябов, А. В. Королькова, М. Н. Геворкян. Информационная безопасность компьютерных сетей: лабораторные работы. // Факультет физико-математических и естественных наук. M.: РУДН, 2015. 64 с..