**Лабораторная работа №5**

**Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов**

Гудиева Мадина Куйраевна

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**

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]

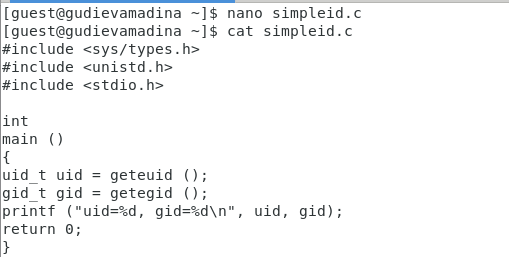
Setuid – это бит разрешения, который позволяет пользователю запускать исполняемый файл с правами владельца этого файла. Другими словами, использование этого бита позволяет нам поднять привилегии пользователя в случае, если это необходимо. Классический пример использования этого бита в операционной системе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

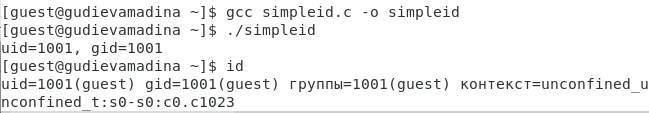
Третий из специальных разрешений — sticky bit. Это разрешение полезно для защиты файлов от случайного удаления в среде, где несколько пользователей имеют права на запись в один и тот же каталог. Если применяется закрепленный sticky bit, пользователь может удалить файл, только если он является пользователем-владельцем 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**

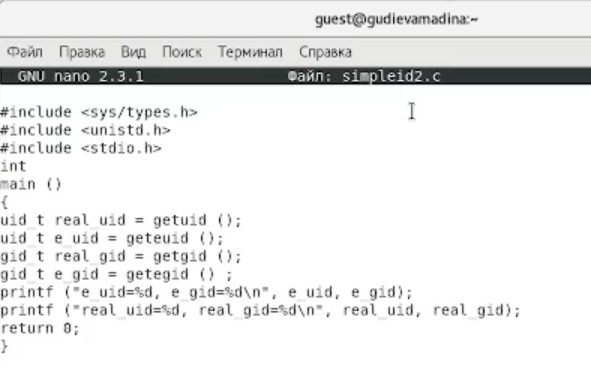
Вошла в систему от имени пользователя guest. Создала программу simpleid.c.  


Скомпилировала и выполнила программу. Выполнив системную программу id убедилась в правильности выведенных данных



Усложнила программу, добавив вывод действительных идентификаторов, назвала её simpleid2.c



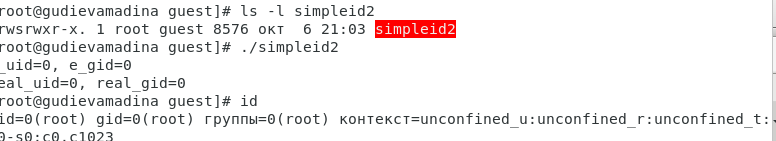


Скомпилировала и запустила программу

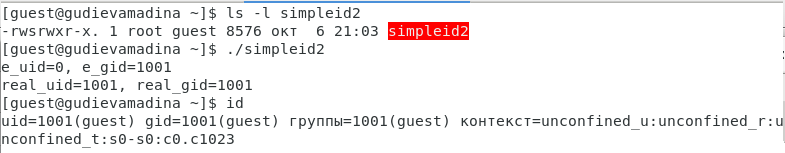


От имени суперпользователя установила новые атрибуты и сменила владельца файла simpleid2



Выполнила проверку и запустила программу   


Проделала тоже самое относительно SetGID-бита

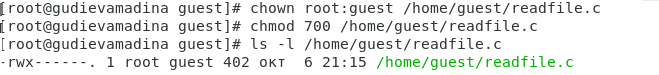
fig:  


Создала программу readfile.c



Откомпилировала её

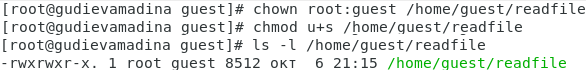


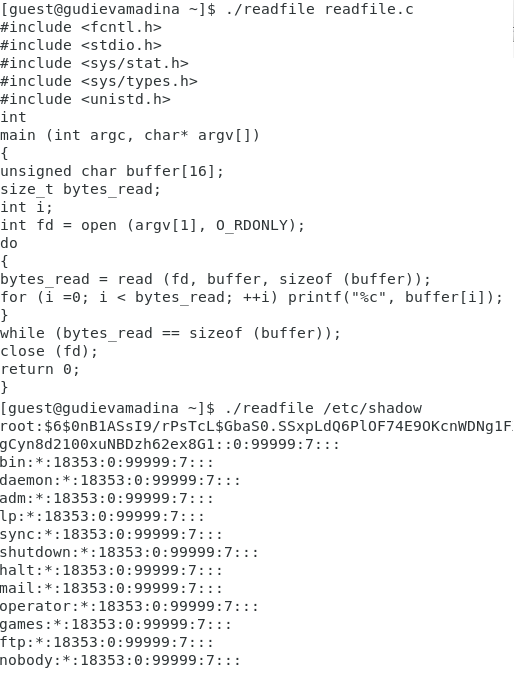
Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог  


Убедилась, что guest не может прочитать файл readfile.c

fig:  
Смените у программы readfile владельца и установите SetU’D-бит

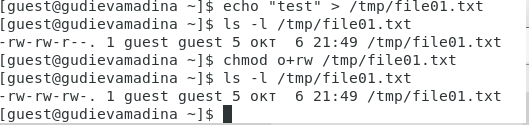
Убедилась, что readfile может прочитать файлы readfile.c и "/etc/shadow"

  
Убедилась, что атрибут Sticky установлен на директории "/tmp"

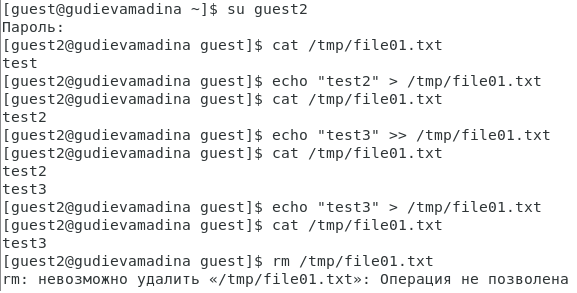


От имени пользователя guest создала файл file01.txt в директории "/tmp" со словом test. Разрешила чтение и запись для категории пользователей «все остальные»   
fig:

От пользователя guest2 просмотрела файл, успешно дозаписала и переписала его. Но не смогла его удалить



От суперпользователя сняла атрибут t (Sticky-бит) с директории "/tmp"

  
Убедилась в правильности снятия атрибута и повторила предыдущие шаги. В этот раз удаление также прошло успешно  
От суперпользователя вернула атрибут t (Sticky-бит) 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  
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).

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).

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..