Отчёт по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ханина Ирина Владимировна, НБИбд-02-18

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.

# Задание

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

# Теоретическое введение

Чтобы получить доступ к файлам и директориям в Linux, используются разрешения. Эти разрешения назначаются трем объектам: владельцу, группе и остальным пользователям. При создании файла или директории тот пользователь, от имени которого был создан файл или директория, становится его владельцем, а группой устанавливается основная группа владельца. Но владельца файла и группу можно менять, для этого используются команды chown.

Система разрешений Linux была изобретена в 1970-х годах. Поскольку вычислительные потребности были ограничены в те годы, базовая система разрешений была довольно ограничена. Эта система разрешений использует три разрешения, которые можно применять к файлам и каталогам:

* r - разрешение на чтение;
* w - разрешение на запись;
* x - разрешение на выполнение. [[1]](https://habr.com/ru/post/469667/)

Помимо основных разрешений в Linux также есть набор расширенных разрешений:

* SUID - разрешение на установку идентификатора пользователя. 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.
* SGID - разрешение на установку идентификатора группы. Принцип работы очень похож на SUID с отличием, что файл будет запускаться пользователем от имени группы, которая владеет файлом.
* Sticky bit - в случае, если этот бит 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. Когда вы применяете sticky bit, пользователь может удалять файлы, только если выполняется одно из следующих условий: пользователь является владельцем файл или пользователь является владельцем каталога, в котором находится файл. [[2]](https://ruvds.com/ru/helpcenter/suid-sgid-sticky-bit-linux/)

Чтобы применить SUID, SGID и sticky bit, можно использовать команду chmod. Для SUID используйте chmod u+s. Для SGID используйте chmod g+s. Для sticky bit используйте chmod +t, а затем имя файла или каталога, для которого вы хотите установить разрешения. [[1]](https://habr.com/ru/post/469667/)

# Выполнение лабораторной работы

1. Выполнила подготовку лабораторного стенда. ([рис. 1](image/1.png))

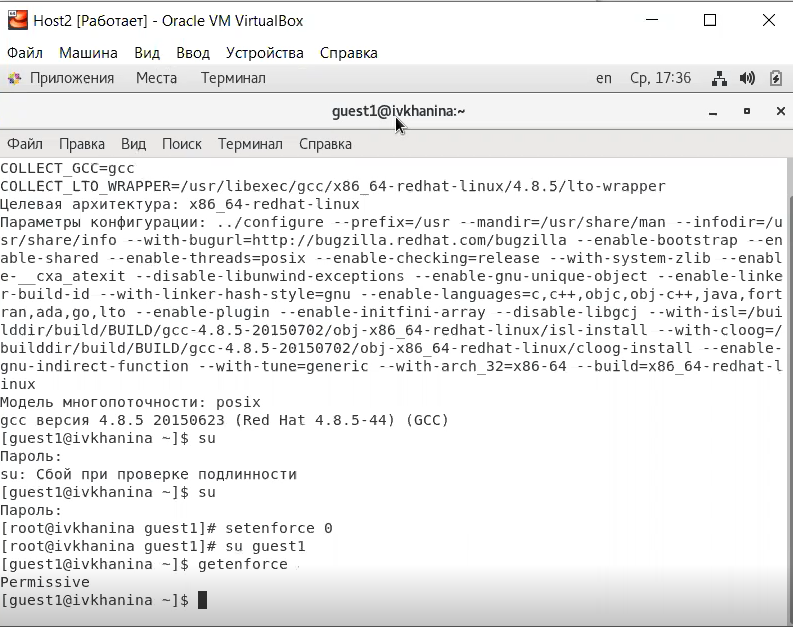


Рис 1. Подготовка лабораторного стенда

1. Я вошла в систему от имени пользователя guest1 и создала программу simpleid.c. ([рис. 2](image/2.png)). Скомплилировала программу с помощью команды gcc simpleid.c -o simpleid и убедилась, что файл программы был создан. Выполнила программу simpleid. Затем я выполнила системную программу id и сравнила полученный результат: вывод uid и gid одинаковый. ([рис. 3](image/3.png))

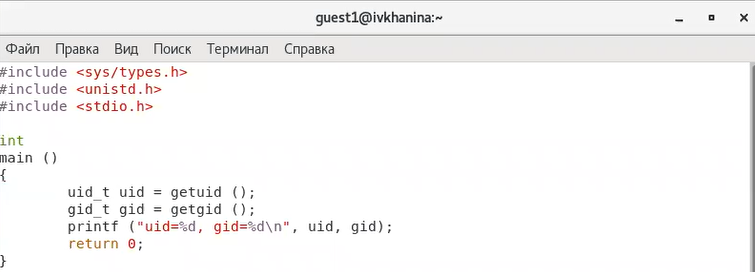


Рис 2. Создание файла simpleid.c



Рис 3. Выполнение программ simpleid и id

1. Усложнила программу, добавив вывод действительных идентификаторов. Получившуюся программу назвала simpleid2.c. ([рис. 4](image/4.png)). Скомпилировала и запустила simpleid2.c. ([рис. 5](image/5.png)).

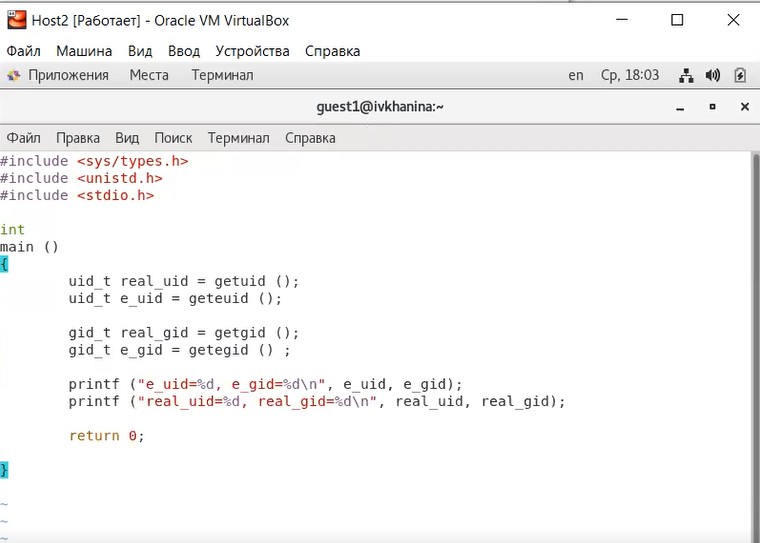


Рис 4. Создание файла simpleid2.c

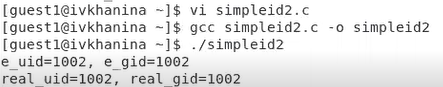


Рис 5. Выполнение программы simpleid2

1. От имени суперпользователя выполнила команды chown root:guest1 /home/guest1/simpleid2 и chmod u+s /home/guest1/simpleid2. Использовала команду su, чтобы временно повысить свои права. Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2, введя команду ls -l simpleid2. Запустила simpleid2 и id, сравнила результаты. Программа simpleid2 была запущена с правами суперпользователя - владьца файла, хотя действительный uid пользователя guest1 другой. ([рис. 6](image/6.png))



Рис 6. Установление SetUID-бита

1. Проделала те самые действия относительно SetGID-бита. ([рис. 7](image/7.png))



Рис 7. Установление SetGID-бита

1. Создала программу readfile.c. ([рис. 8](image/8.png)). Скомпилировала её при помощи команды gcc readfile.c -o readfile. ([рис. 9](image/9.png))

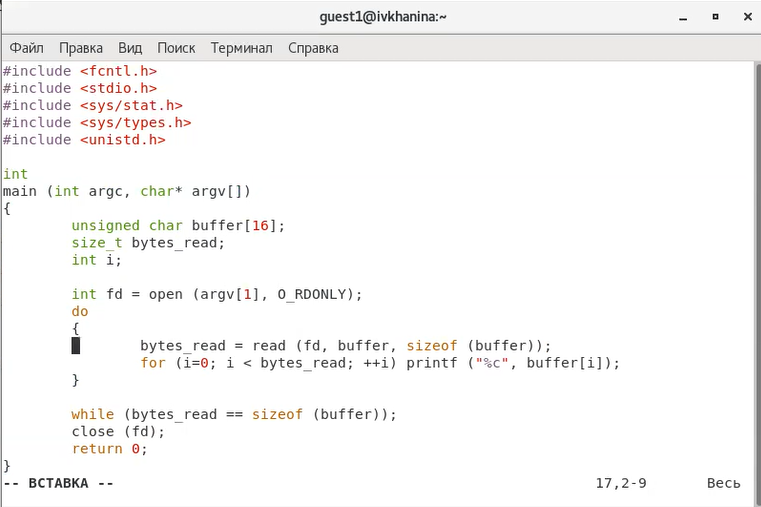


Рис 8. Создание файла readfile.c

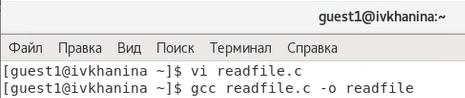


Рис 9. Компиляция readfile.c

1. Далее я сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, a guest1 не мог. После этого я проверила, что пользователь guest1 не может прочитать файл readfile.c. Сменила у программы readfile владельца и установила SetU’D-бит. ([рис. 10](image/10.png))



Рис 10. Смена владельцев файлов readfile.c и readfile, установление SetU’D-бита

1. Я проверила, может ли программа readfile прочитать файл readfile.c ([рис. 11](image/11.png)), а также может ли программа readfile прочитать файл /etc/shadow. ([рис. 12](image/12.png)) Программа смогла их прочитать.

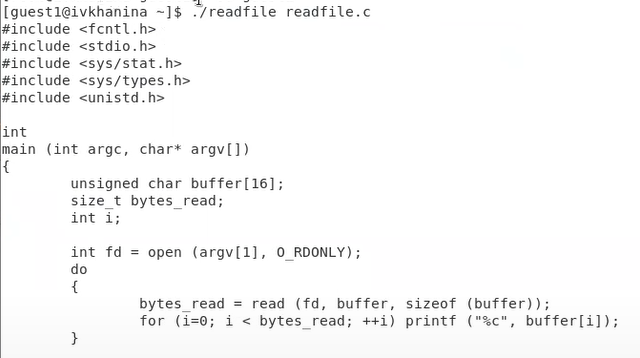


Рис 11. Проверка чтения файла readfile.c программой readfile

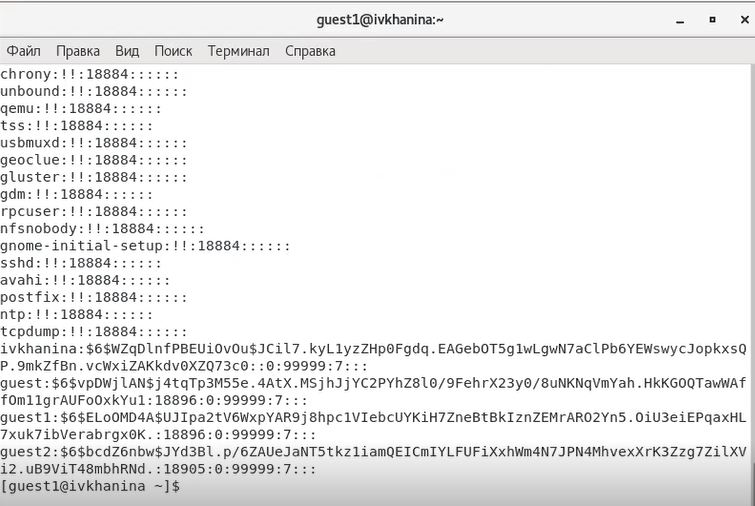


Рис 12. Проверка чтения файла /etc/shadow программой readfile

1. Выяснила, установлен ли атрибут Sticky на директории /tmp, для чего выполнила команду ls -l / | grep tmp. Да, данный атрибут установлен. От имени пользователя guest1 создала файл file01.txt в директории /tmp со словом test. Затем я просмотрела атрибуты у созданного файла и разрешила чтение и запись для категории пользователей «все остальные». От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt, а так же сделать дозапись слова test2 в файл /tmp/file01.txt командой echo “test2” > /tmp/file01.txt. Мне удалось выполнить операцию. Далее я распечатала содержимое файла командой cat /tmp/file01.txt. От пользователя guest2 попробовала записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой echo “test3” > /tmp/file01.txt. Я смогла это сделать. Затем я проверила содержимое файла командой cat /tmp/file01.txt.([рис. 13](image/13.png))



Рис 13. Создание файла file01.txt и выполнение различных команд от пользователя guest2

1. От пользователя guest2 попробовала удалить файл /tmp/file01.txt командой rm /tmp/fileOl.txt. Я не смогла удалить файл. Повысила свои права до суперпользователя, введя команду su -, и выполните после этого команду chmod -t /tmp. Покинула режим суперпользователя командой exit, после чего от пользователя guest2 проверила, что атрибута t у директории /tmp нет. Повторила предыдущие шаги. Мне удалось удалить файл от имени пользователя, не являющегося его владельцем. ([рис. 14](image/14.png)).

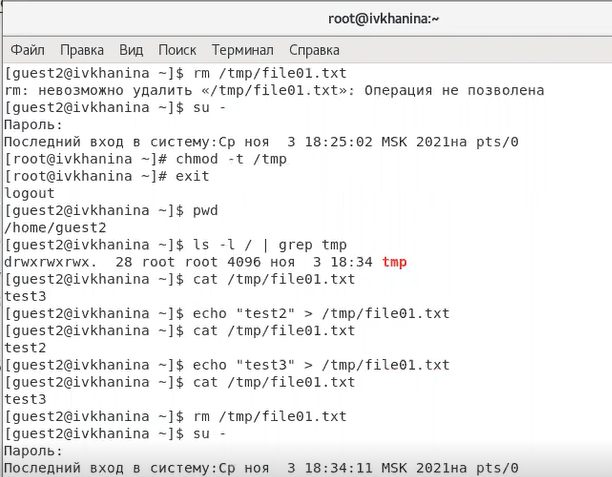


Рис 14. Попытка удаления файла файл от имени пользователя, не являющегося его владельцем

1. Я вновь повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp. ([рис. 15](image/15.png))

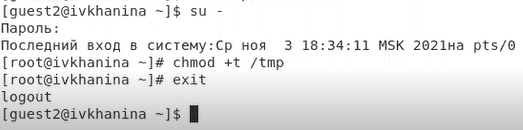


Рис 15. Возвращение атрибута t на директорию /tmp

# Выводы

В результате выполнения лабораторной работы я 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. [Права в Linux (chown, chmod, SUID, GUID, sticky bit, ACL, umask)](https://habr.com/ru/post/469667/)
2. [Использование SETUID, SETGID и Sticky bit для расширенной настройки прав доступа в операционных системах Linux](https://ruvds.com/ru/helpcenter/suid-sgid-sticky-bit-linux/)