Лабораторная работа №5

Основы информационной безопасности

Колчева Юлия Вячеславовна

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

Часть 1

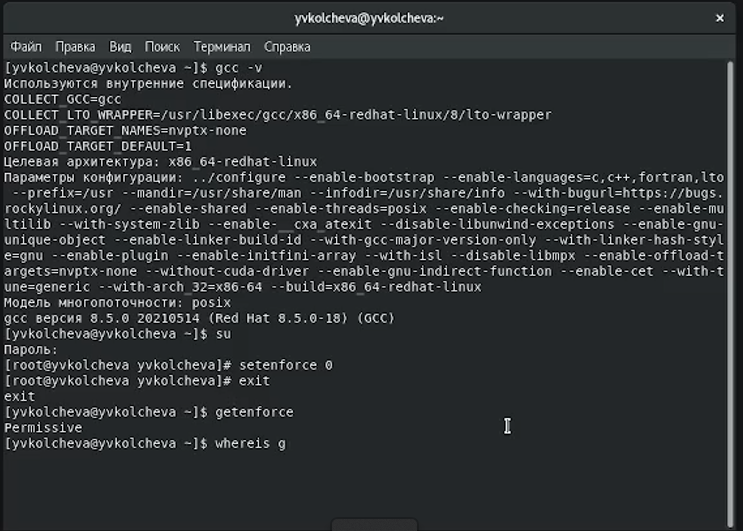
Создание программы

Часть 2

Исследование Sticky-бита

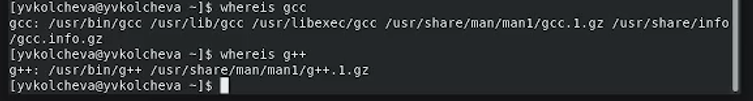
# 3 Выполнение лабораторной работы

Для начала я убедилась, что компилятор gcc установлен, исолпьзуя команду “gcc -v”. Затем отключила систему запретов до очередной перезагрузки системы командой “sudo setenforce 0”, после чего команда “getenforce” вывела “Permissive”(рис. [??])



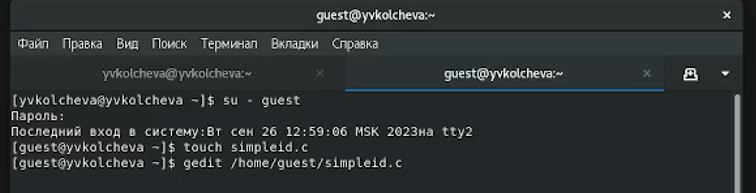
Работа с консолью

Проверила успешное выполнение команд “whereis gcc” и “whereis g++” (их расположение) (рис. [??])



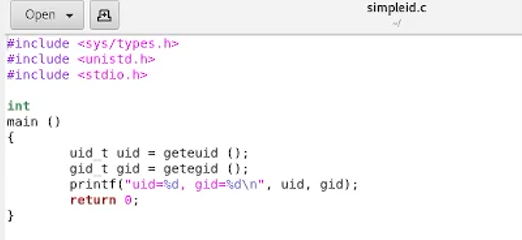
Работа с консолью

Вошла в систему от имени пользователя guest командой “su - guest”. Создала программу simpleid.c командой “touch simpleid.c” и открыла её в редакторе командой “gedit /home/guest/simpleid.c” (рис. [??])



Работа с консолью

Код программы выглядит следующим образом (рис. [??])



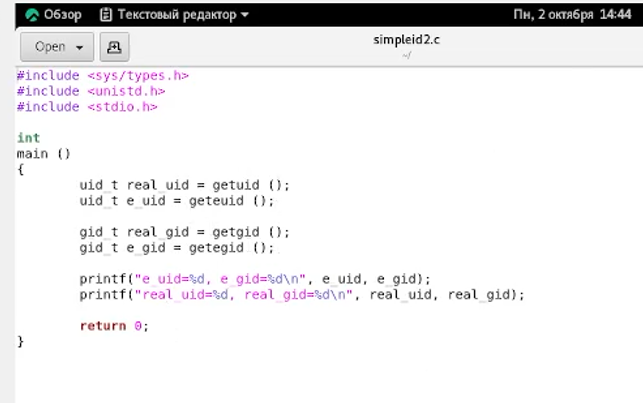
Код первой программы

Скомпилировала программу и убедилась, что файл программы был создан командой “gcc simpleid.c -o simpleid”. Выполнила программу simpleid командой “./simpleid”, а затем выполнила системную программу id командой “id”. Результаты, полученные в результате выполнения обеих команд, совпадают (uid=1001 и gid=1001) (рис. [??])



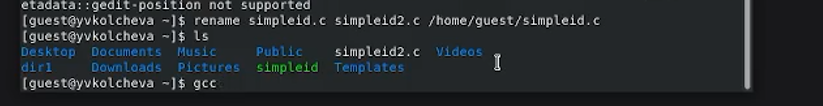
Работа с консолью

Усложнила программу, добавив вывод действительных идентификаторов (рис. [??])



Вторая программа

Получившуюся программу назвала simpleid2.c (рис. [??])



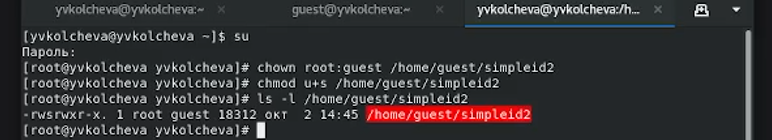
Работа с консолью

Скомпилировала и запустила simpleid2.c командами “gcc simpleid2.c -o sipleid2” и “./simpleid2” (рис. [??])



Работа с консолью

От имени суперпользователя выполнила команды “sudo chown root:guest /home/guest/simpleid2” и “sudo chmod u+s /home/guest/simpleid2”, затем выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2 командой “sudo ls -l /home/guest/simpleid2” (рис. 3.9). Этими командами была произведена смена пользователя файла на root и установлен SetUID-бит. (рис. [??])



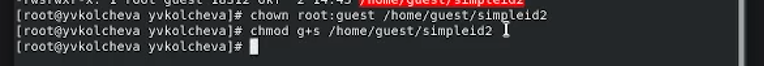
Работа с консолью

Запустила программы simpleid2 и id. Теперь появились различия в uid (рис. [??])



Работа с консолью

Проделала тоже самое относительно SetGID-бита. Также можем заметить различия с предыдущим пунктом (рис. [??]) (рис. [??])

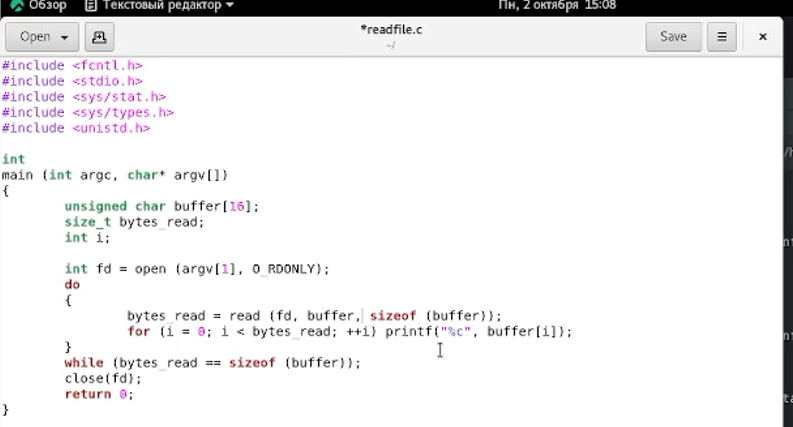


Работа с консолью



Работа с консолью

Создаем программу readfile.c (рис. [??])



Работа с консолью

Скомпилировала созданную программу командой “gcc readfile.c -o readfile”. Сменила владельца у файла readfile.c командой “sudo chown root:guest /home/guest/readfile.c” и поменяла права так, чтобы только суперпользователь мог прочитать его, а guest не мог, с помощью команды “sudo chmod 700 /home/guest/readfile.c”. Теперь убедилась, что пользователь guest не может прочитать файл readfile.c командой “cat readfile.c”, получив отказ в доступе (рис. [??]) (рис. [??])

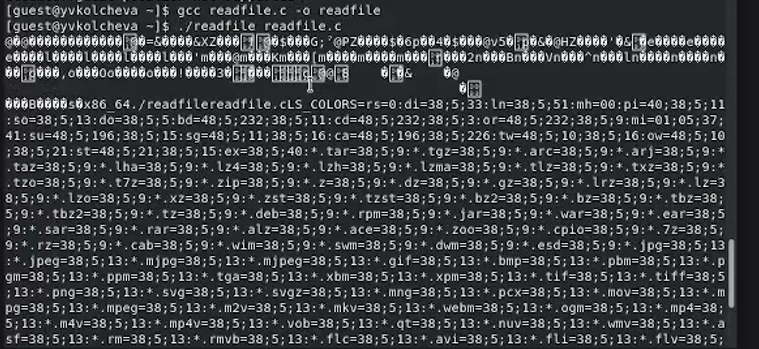
Работа с консолью

Работа с консолью

Работа с консолью

Работа с консолью

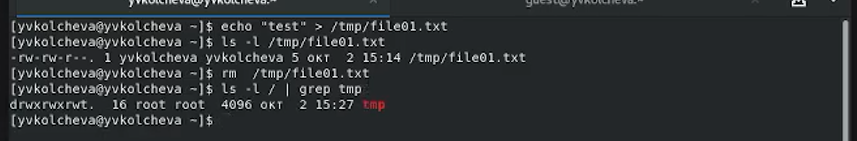
Поменяла владельца у программы readfile и устанавила SetUID. Проверила, может ли программа readfile прочитать файл readfile.c командой “./readfile readfile.c”. Прочитать удалось.Аналогично проверила, можно ли прочитать файл /etc/shadow. Прочитать удалось (рис. [??])



Работа с консолью

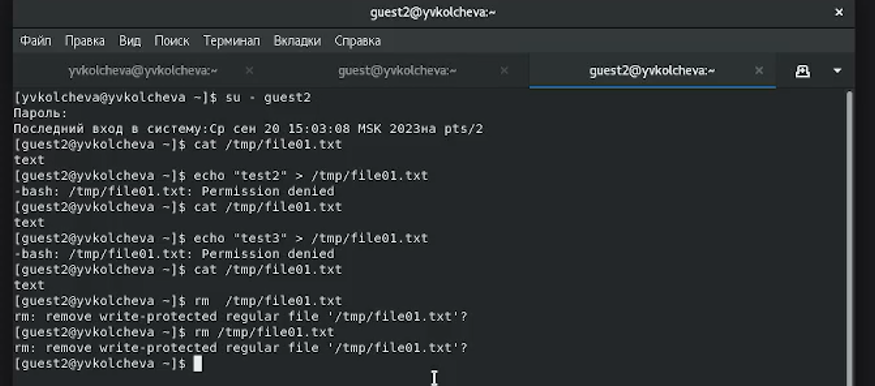
2 часть

Командой “ls -l / | grep tmp” убеждилась, что атрибут Sticky на директории /tmp установлен. От имени пользователя guest создала файл file01.txt в директории /tmp со словом test командой “echo”test” > /tmp/file01.txt”. Просматрела атрибуты у только что созданного файла и разрешаем чтение и запись для категории пользователей “все остальные” командами “ls -l /tmp/file01.txt” и “chmod o+rw /tmp/file01.txt” (рис. [??])



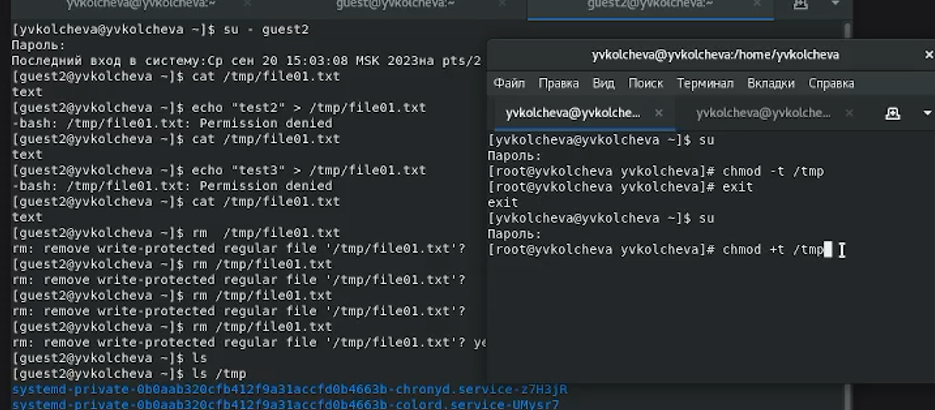
Работа с консолью

От имени пользователя guest2 попробовала прочитать файл командой “cat /tmp/file01.txt” - это удалось. Далее попыталась дозаписать в файл слово test2, проверить содержимое файла и записать в файл слово test3, стерев при этом всю имеющуюся в файле информацию - эти операции удалось выполнить только в случае, если еще дополнительно разрешить чтение и запись для группы пользователей командой “chmod g+rw /tmp/file01.txt”. От имени пользователя guest2 попробовала удалить файл - это не удается ни в каком из случаев, возникает ошибка (рис. [??])



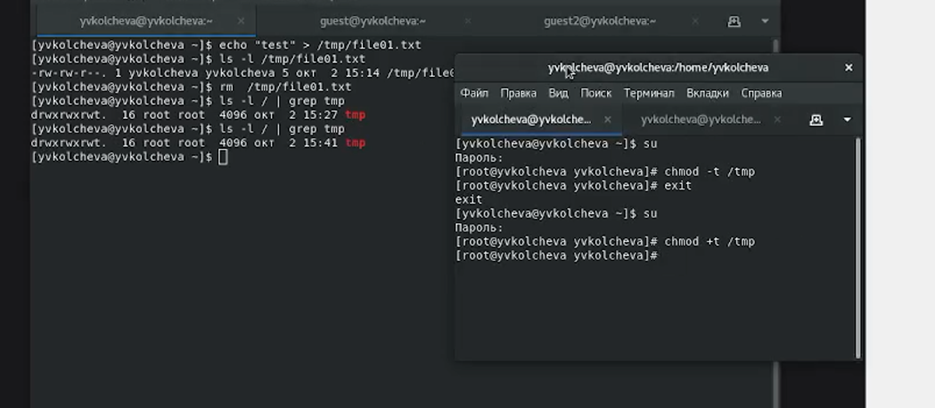
Работа с консолью

Повысила права до суперпользователя командой “su -” и выполнила команду, снимающую атрибут t с директории /tmp “chmod -t /tmp”. После чего покинула режим суперпользователя командой “exit”. Повторила предыдущие шаги. Теперь мне удалось удалить файл file01.txt от имени пользователя, не являющегося его владельцем (рис. [??])



Работа с консолью

Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp (рис. [??])



Работа с консолью

# 4 Выводы

В ходе выполнения данной лабораторной работы я изучила механизмы изменения идентификаторов, применение 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.

# 5 Список литературы

Лабораторная работа №5

Стандартные права SetUID, SetGID, Sticky в Linux [Электронный ресурс]. URL: https://linux-notes.org/standartny-e-prava-unix-suid-sgid-sticky-bity/