Лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Щербак Маргарита Романовна, НПИбд-02-21

2024

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 [1].

# Теоретическое введение

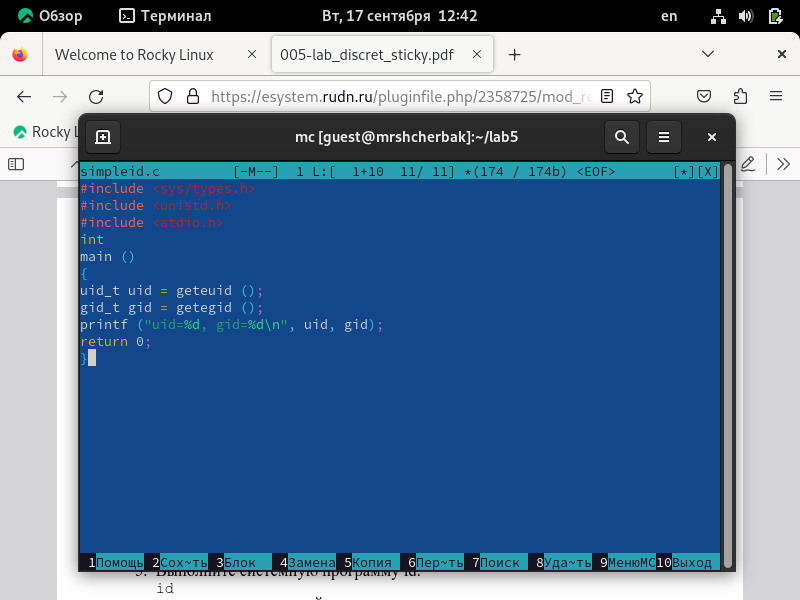
Информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.

Права доступа в системах управляют тем, какие операции может выполнять пользователь с определенными файлами и папками. Правильная настройка прав доступа помогает создать безопасную среду, где никто не сможет изменять ваши данные или нарушать работу важных системных файлов. Помимо групп root и users, в системе существует множество других, которые созданы для управления доступом программ к общим ресурсам. Участники каждой группы получают права на чтение или изменение конкретных файлов и каталогов, что регулирует их доступ и действия. Эти же права передаются процессам, которые запускает пользователь [2].

# Выполнение лабораторной работы

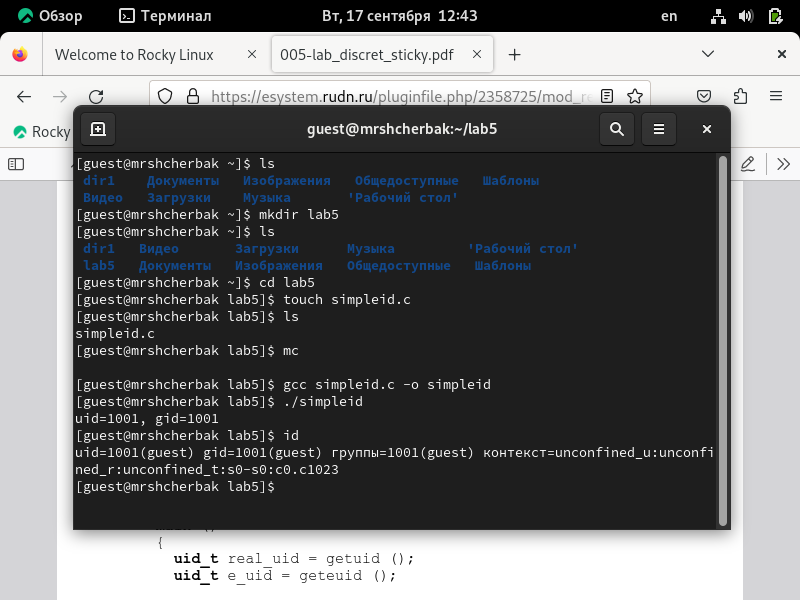
## Создание программы

1. Я подготовила лабораторный стенд. У меня был установлен gcc. Я вошла в систему от имени пользователя guest. Создала программу simpleid.c (рис.1).



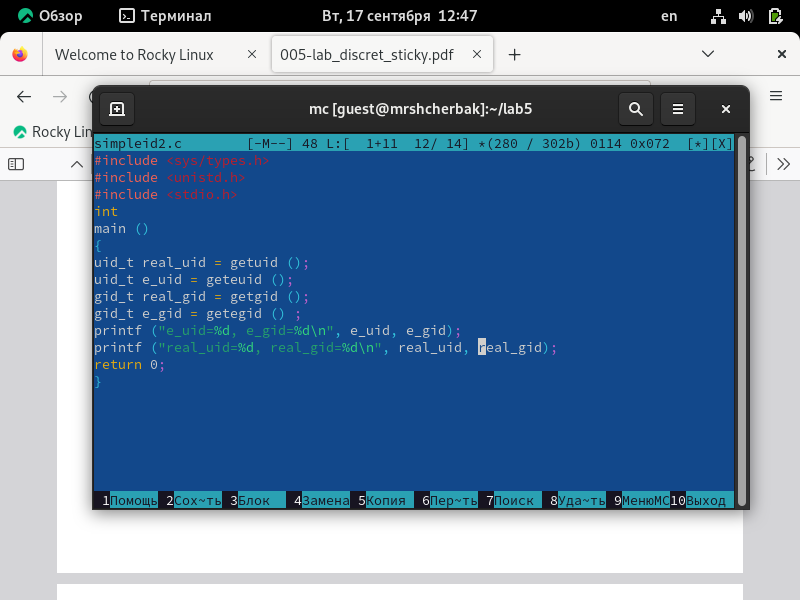
Содержимое программы simpleid.c

1. Скомплилировала программу и убедилась, что файл программы создан. Выполнила программу simpleid. Выполнила системную программу id и сравнила полученный результат с данными предыдущего пункта задания. Результаты совпадают (рис.2).



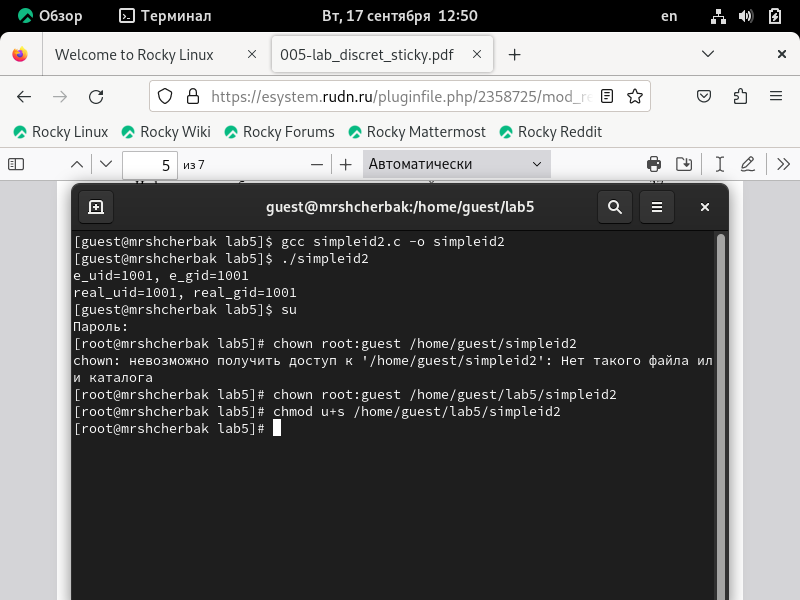
Выполнение команд

1. Усложнила программу, добавив вывод действительных идентификаторов. Получившуюся программу назвала simpleid2.c (рис.3).



Усложненная программа

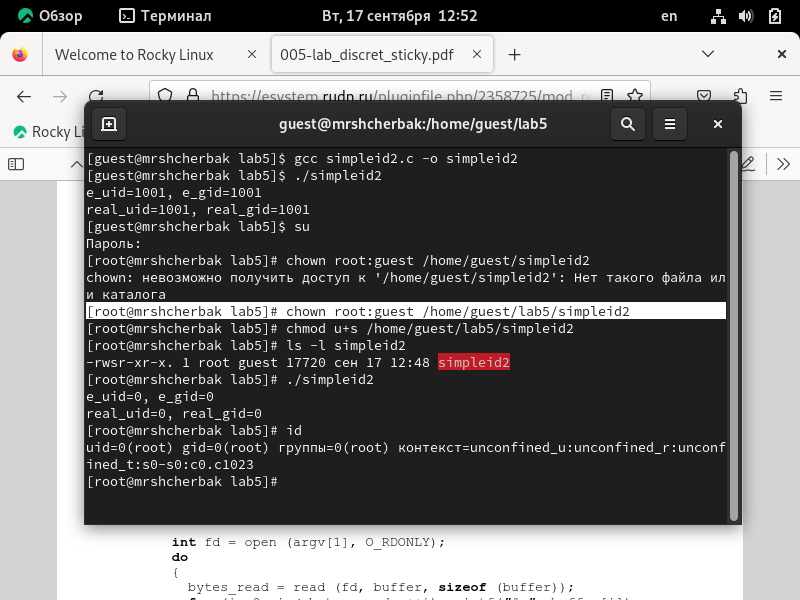
1. Скомпилировала и запустила simpleid2.c. От имени суперпользователя выполнила команды: chown root:guest /home/guest/simpleid2 и chmod u+s /home/guest/simpleid2 (рис.4).



Выполнение команд

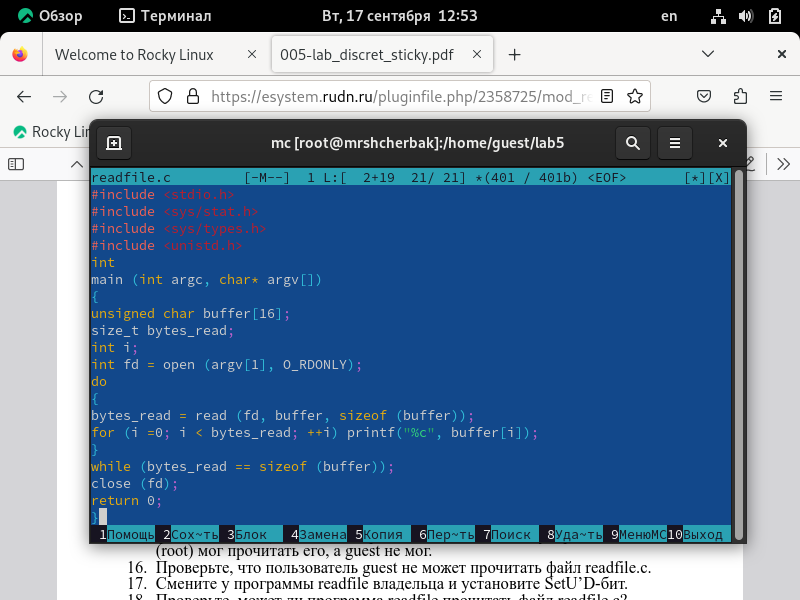
* sudo: выполняет одну команду с правами суперпользователя (root) без полного переключения на него. Требует пароль.
* su: полностью переключает на другого пользователя (обычно root) с его окружением, требуя пароль этого пользователя.

1. Выполнила проверку правильности установки новых атрибутов и смены владельца файла simpleid2. Запустила simpleid2 и id. Результаты совпадают (рис.5).



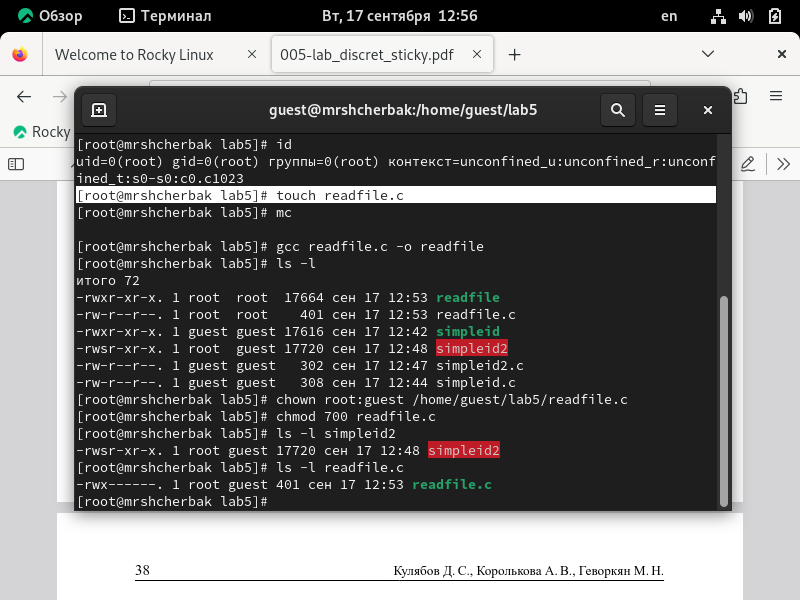
Выполнение команд

1. Проделала то же самое относительно SetGID-бита. Создала программу readfile.c (рис.6).



Содержимое программы readfile.c

1. Откомпилировала её. Сменила владельца у файла readfile.c и изменила права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог (рис.7).



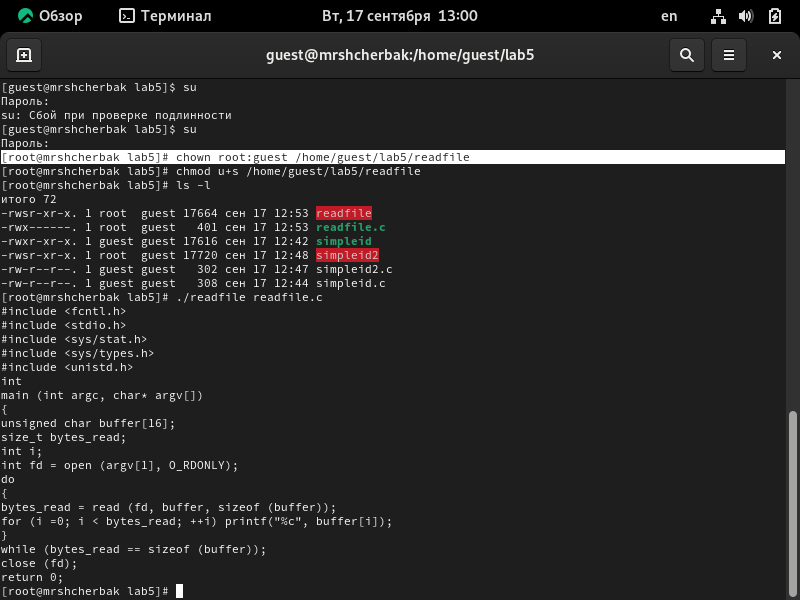
Смена владельца

1. Проверила, что пользователь guest не может прочитать файл readfile.c (рис.8).

Проверка

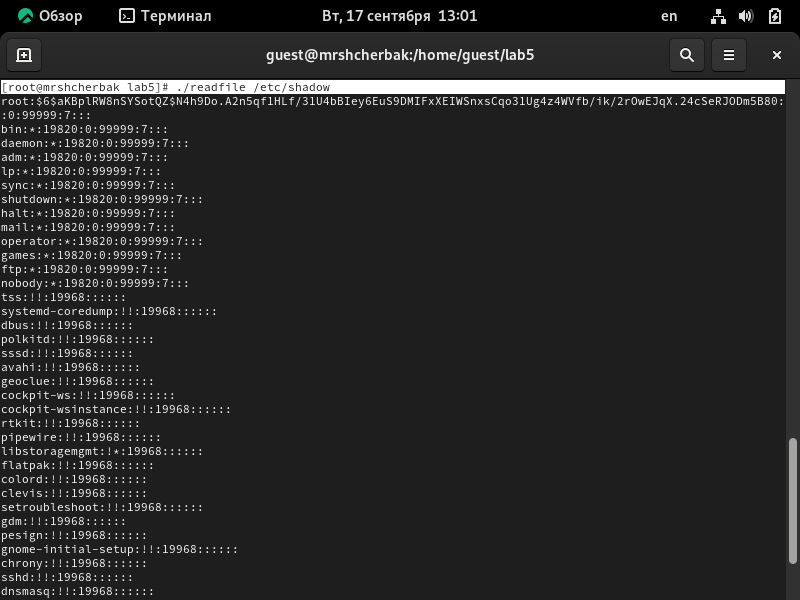
Проверка

1. Сменила у программы readfile владельца и установила SetU’D-бит Проверила, может ли программа readfile прочитать файл readfile.c (рис.9).



Проверка

1. Проверила, может ли программа readfile прочитать файл /etc/shadow (рис.10).

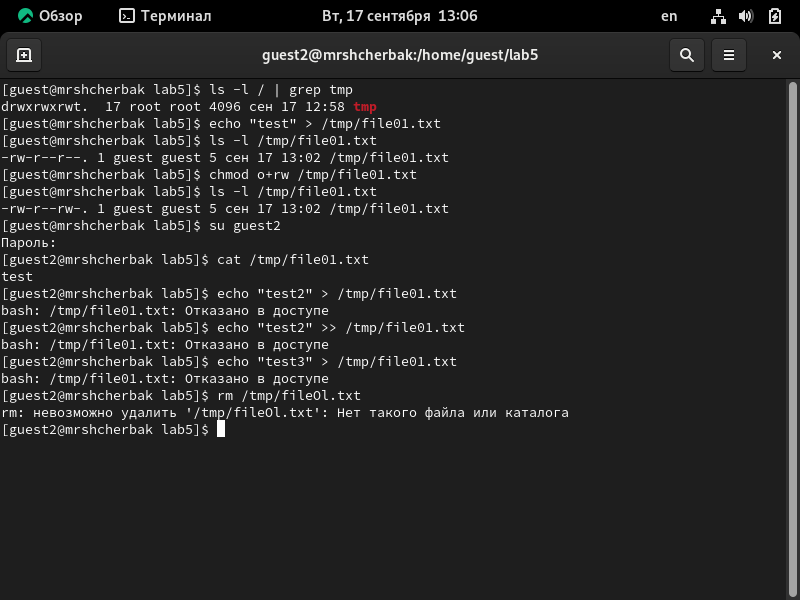


Проверка

Программа может прочитать оба файла.

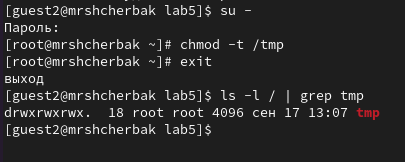
## Исследование Sticky-бита

1. Выяснила, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду ls -l / | grep tmp. Атрибут “t” установлен. 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». От пользователя guest2 (не являющегося владельцем) попробовала прочитать файл /tmp/file01.txt. От пользователя guest2 попробовала дозаписать в файл /tmp/file01.txt слово test2. От пользователя guest2 попробовала удалить файл /tmp/file01.txt командой rm /tmp/fileOl.txt (рис.11). Операции выполнить не удалось.



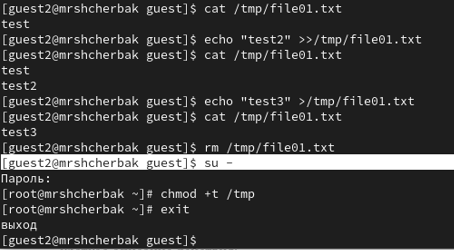
Выполнение команд

1. Повысила свои права до суперпользователя следующей командой su - и выполнила после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp. Покинула режим суперпользователя командой exit. От пользователя guest2 проверила, что атрибута t у директории /tmp нет (рис.12).



Снятие Sticky-бита

1. Повторила предыдущие шаги. Повысила свои права до суперпользователя и вернула атрибут t на директорию /tmp (рис.13).



Возвращение Sticky-бита

# Вывод

Таким образом, в ходе ЛР№5 я изучила механизмы изменения идентификаторов, применения SetUID- и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Библиография

1. Методические материалы курса.
2. Chmod. [Электронный ресурс]. М. URL: [Файловая система](https://ru.wikipedia.org/wiki/Chmod) (Дата обращения: 17.09.2024).