Отчёт по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Артамонов Тимофей Евгеньевич

Содержание

# 1 Цель работы

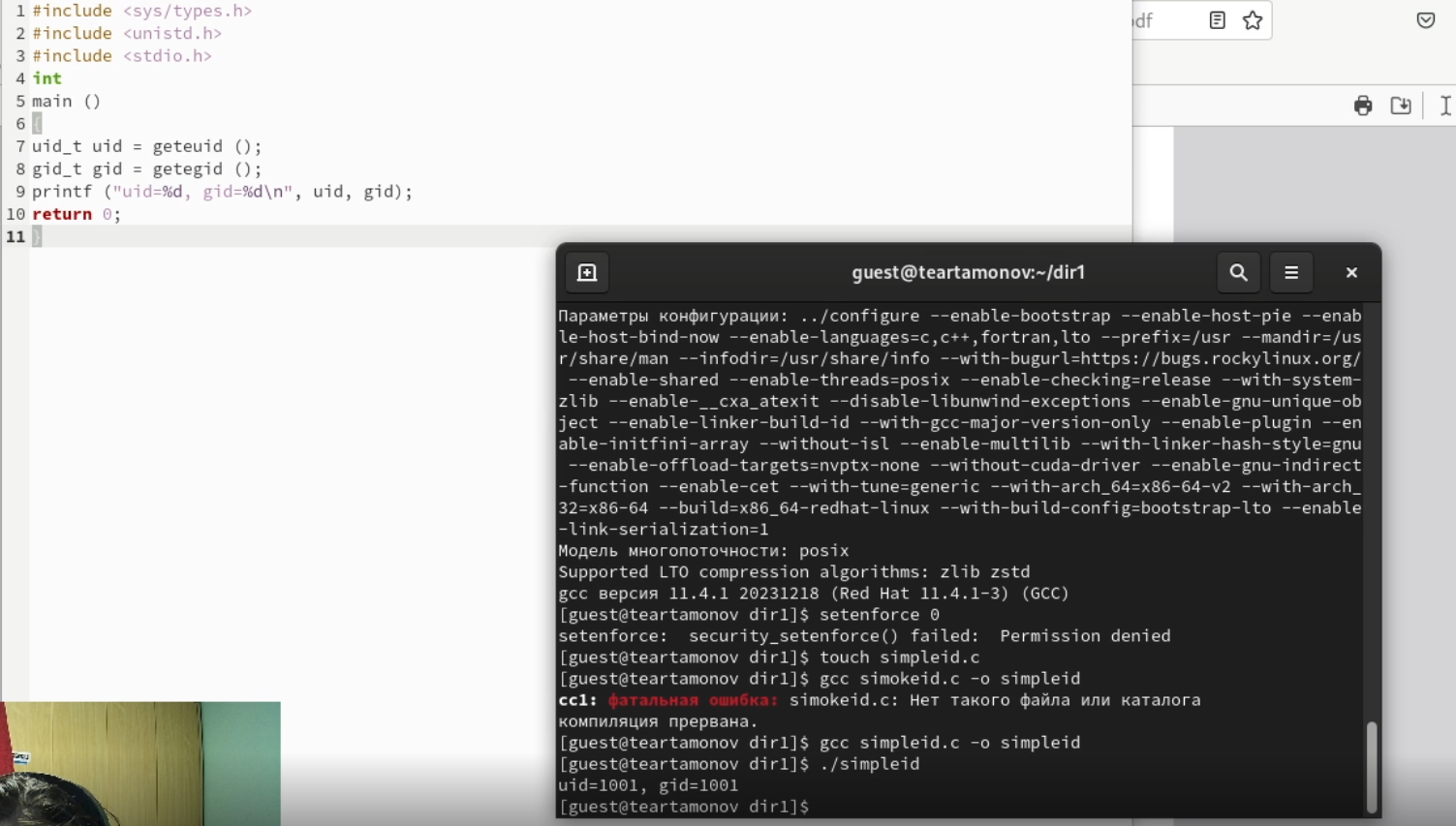
Изучение механизмов изменения идентификаторов, применения SetUID и Sticky-битов. Получение практических навыков работы в консоли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# 2 Теоретическое введение

В настоящее время sticky bit используется в основном для каталогов, чтобы защитить в них файлы. Из такого каталога пользователь может удалить только те файлы, владельцем которых он является. Примером может служить каталог /tmp, в который запись открыта для всех пользователей, но нежелательно удаление чужих файлов. Установка атрибута производится утилитой chmod. [1]

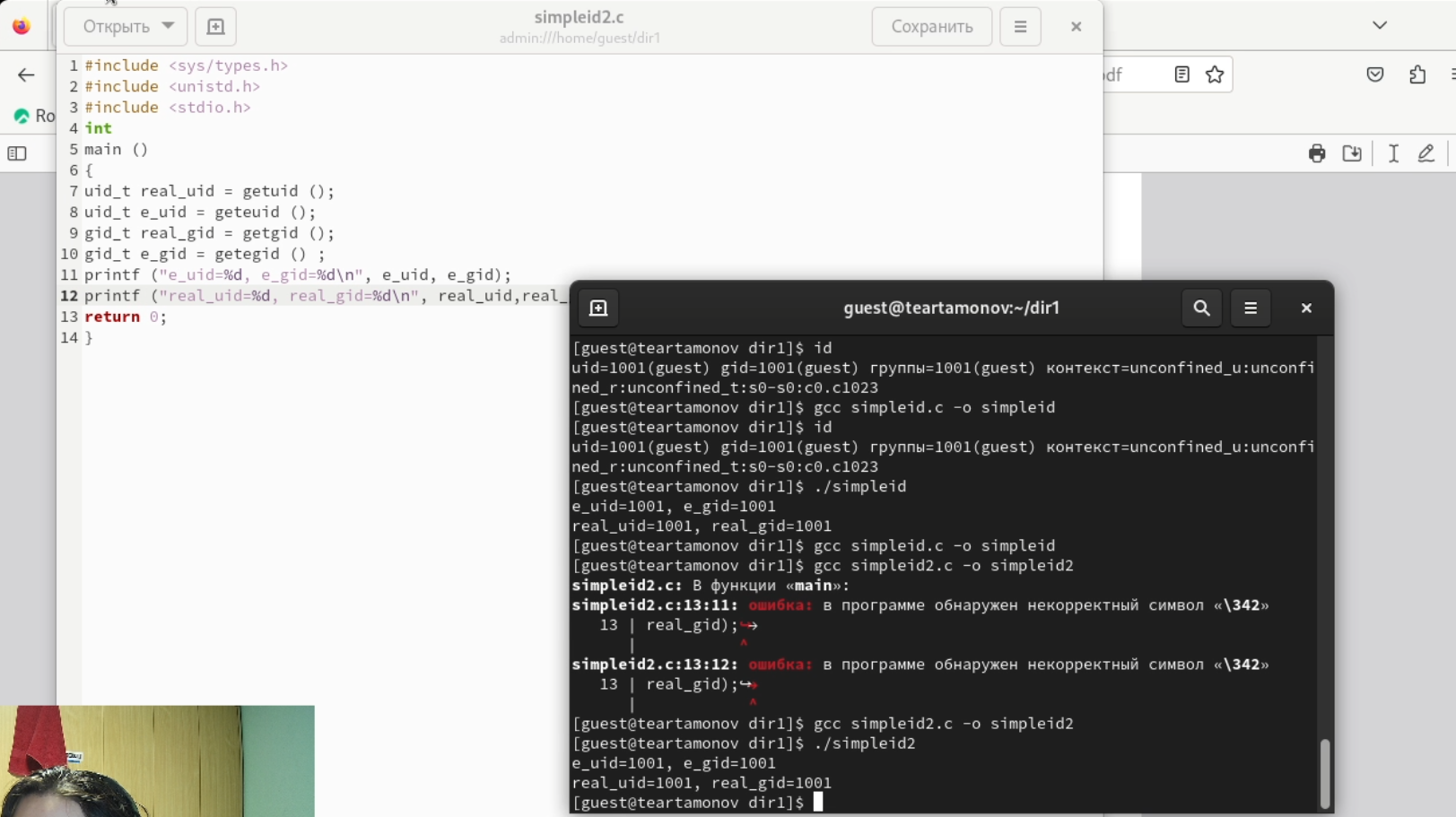
# 3 Выполнение лабораторной работы

Создали файл simple.id и записали в него код из лабораторной. (рис. [??])



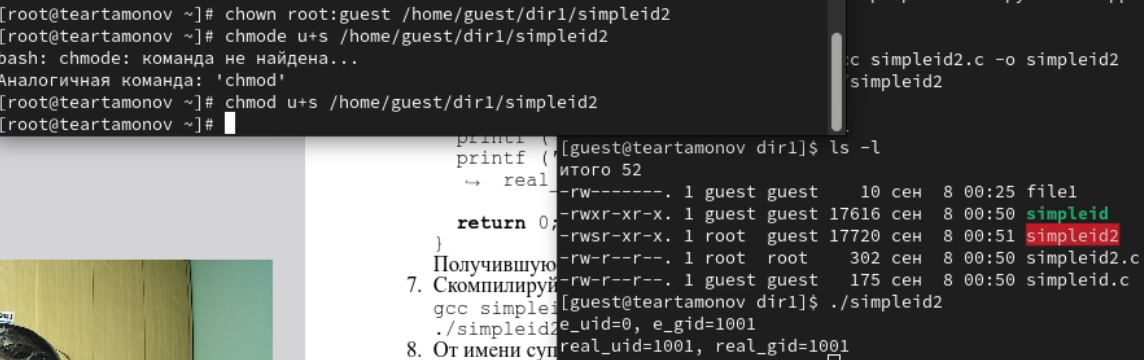
После запуска получили uid и gid нашего пользователя

Усложним скрипт, добавив вывод real uid и gid. (рис. [??])



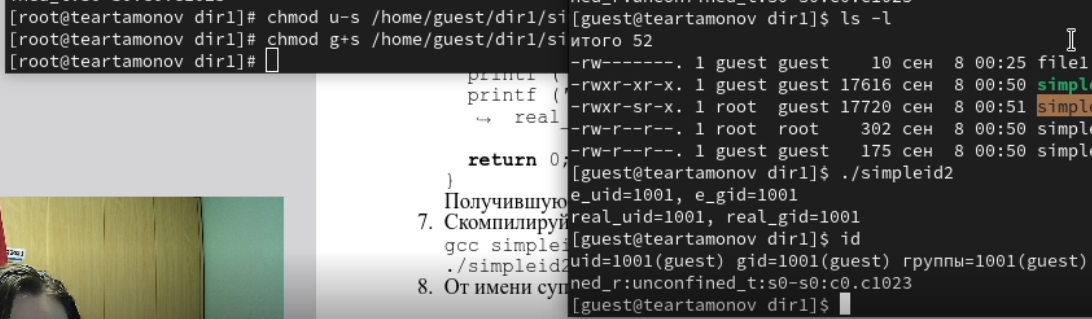
Теперь выводятся и real uid и gid, все совпадает с результатами предыдущих шагов

Пропишем chown и chmod. (рис. [??])



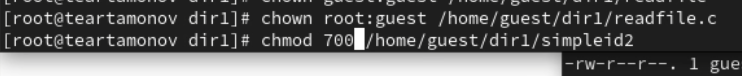
chown изменяет владельца файла, а chmod u+s позволяет запускать файл с правами владельца. Теперь при запуске файла от имени guest получаем e\_uid root

Проделаем то же самое с SetGID-битом. (рис. [??])



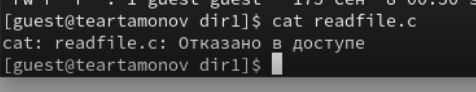
Вывод такой же

Создадим файл readfile.c как в лабораторной и скомпилируем его. (рис. [??])



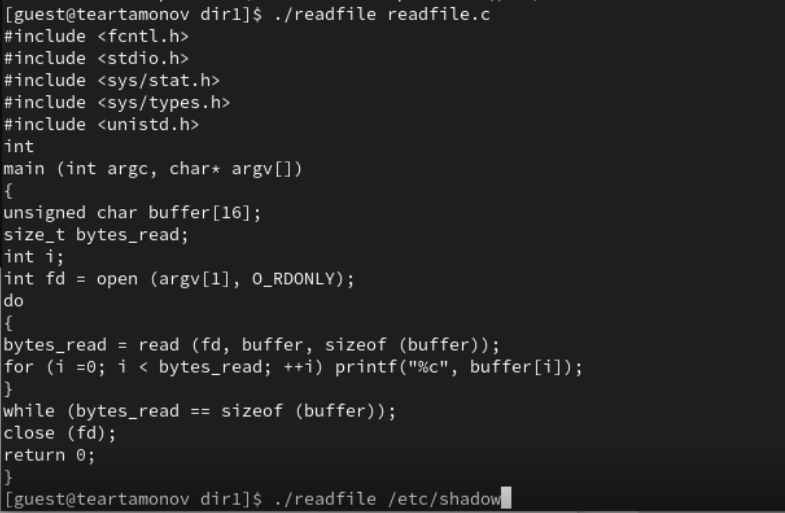
Меняем владельца на root и забираем все права у всех кроме владельца

Проверяем. (рис. [??])



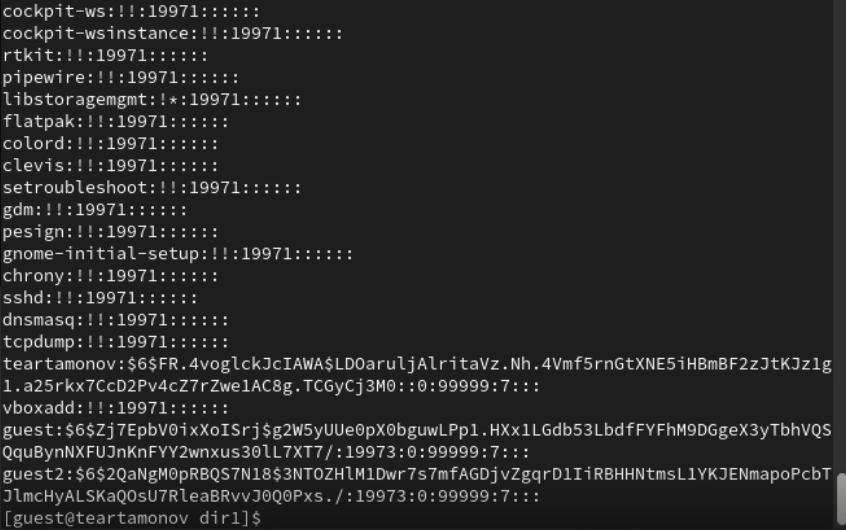
guest не может прочесть readfile.c

Попробуем прочитать readfile.c с помощью readfile. (рис. [??])



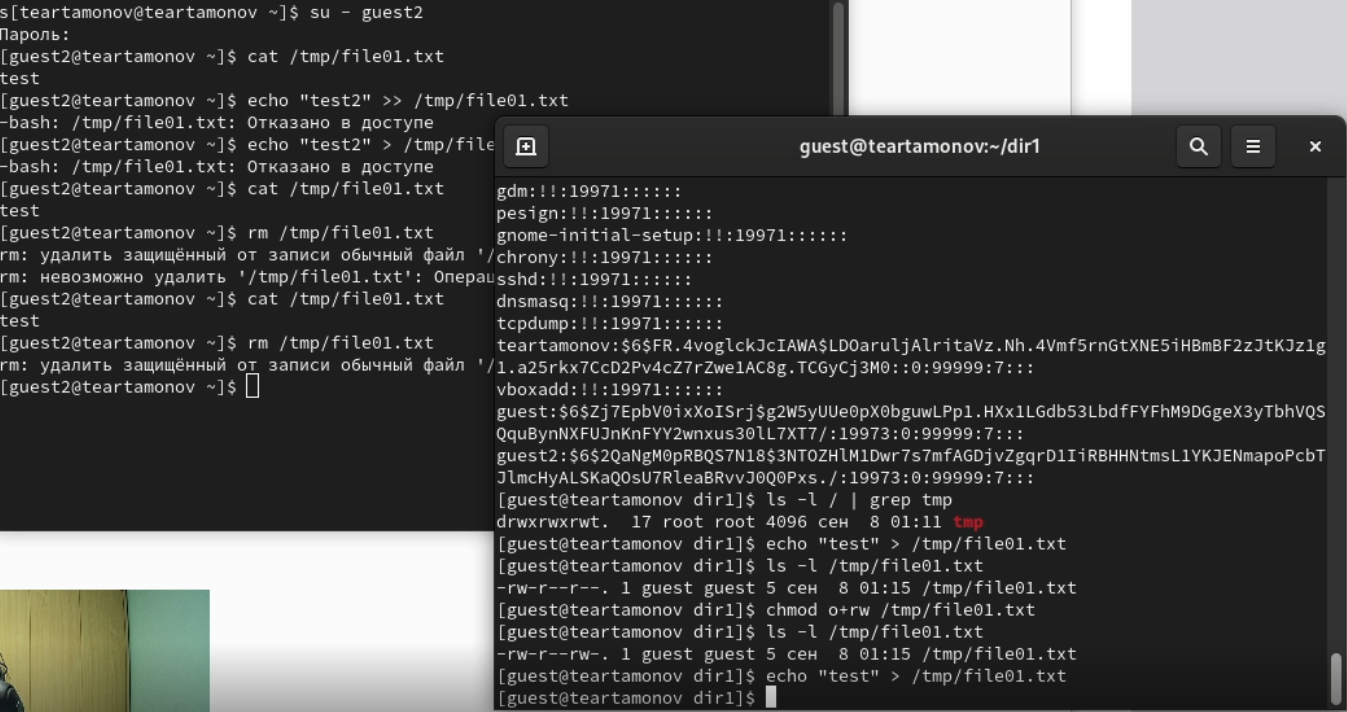
Успешно

Попробуем прочитать /etc/shadow с помощью readfile. (рис. [??])



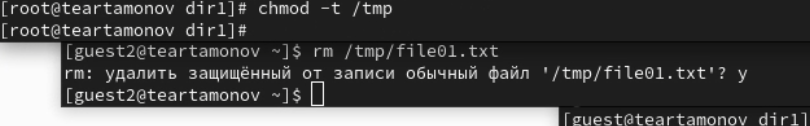
Успешно

Найдем директорию tmp, создадим там файл от имени guest и от имени guest2 попробуем выполнит с ним разные действия. (рис. [??])



Можем только читать файл, все что связано с изменением запрещено

Уберем параметр -t и попробуем еще раз. (рис. [??])



Теперь изменение не для владельца открыто

# 4 Выводы

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

# Список литературы

1. Sticky bit [Электронный ресурс]. Wikimedia Foundation, 2024. URL: <https://ru.wikipedia.org/wiki/Sticky_bit>.