Отчет по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния расширенных атрибутов

Евсеева Дарья Олеговна

8 октября, 2022

Содержание

# Цель работы

Целью данной работы является изучение механизмов изменения идентификаторов и применения SetUID-, SetGID- 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

1. Провести работу с SetUID- и SetGID-битами.
2. Провести работу со Sticky-битом.

# Теоретическое введение

Дискреционное разграничение доступа — подход к разграничению доступа, предполагающий назначение владельцев объектов, которые по собственному усмотрению определяют права доступа субъектов (других пользователей) к объектам (файлам), которыми владеют.

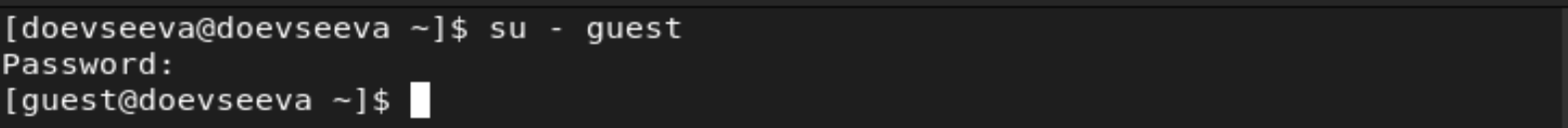
Дискреционные механизмы разграничения доступа используются для разграничения прав доступа процессов как обычных пользователей, так и для ограничения прав системных программ (например, служб операционной системы), которые работают от лица псевдопользовательских учетных записей.

# Выполнение лабораторной работы

Выполнять работу будем в операционной системе, установленной при выполнении первой лабораторной работы.

## 1. Работа с SetUID- и SetGID-битами

Для начала войдем в систему от имени пользователя guest.



Вход в систему от имени пользователя guest

Далее создадим файл simpleid.c и запишем в него код программы.

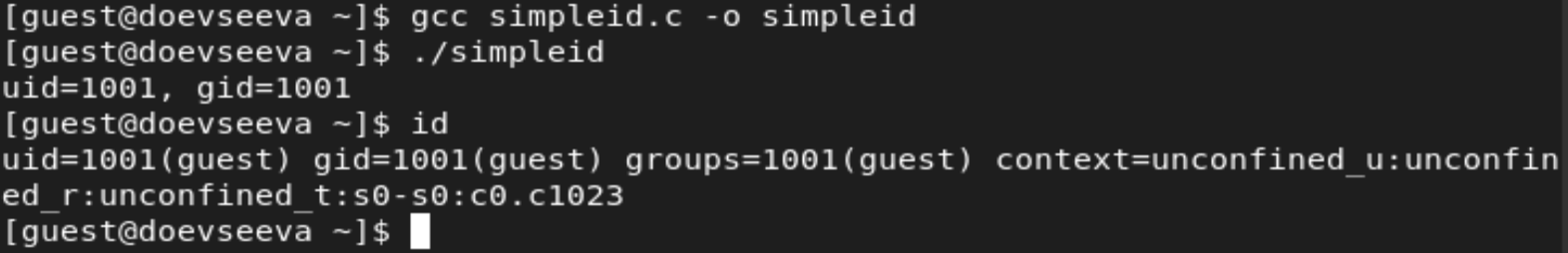


Создание файла



Код программы

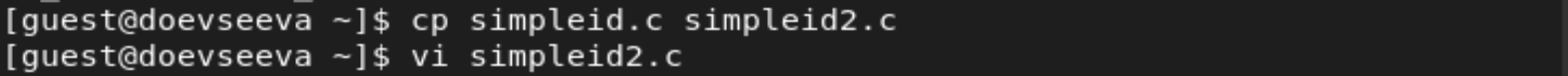
Скомпилируем программу и выполним ее, сравнив результаты с выводом команды id.



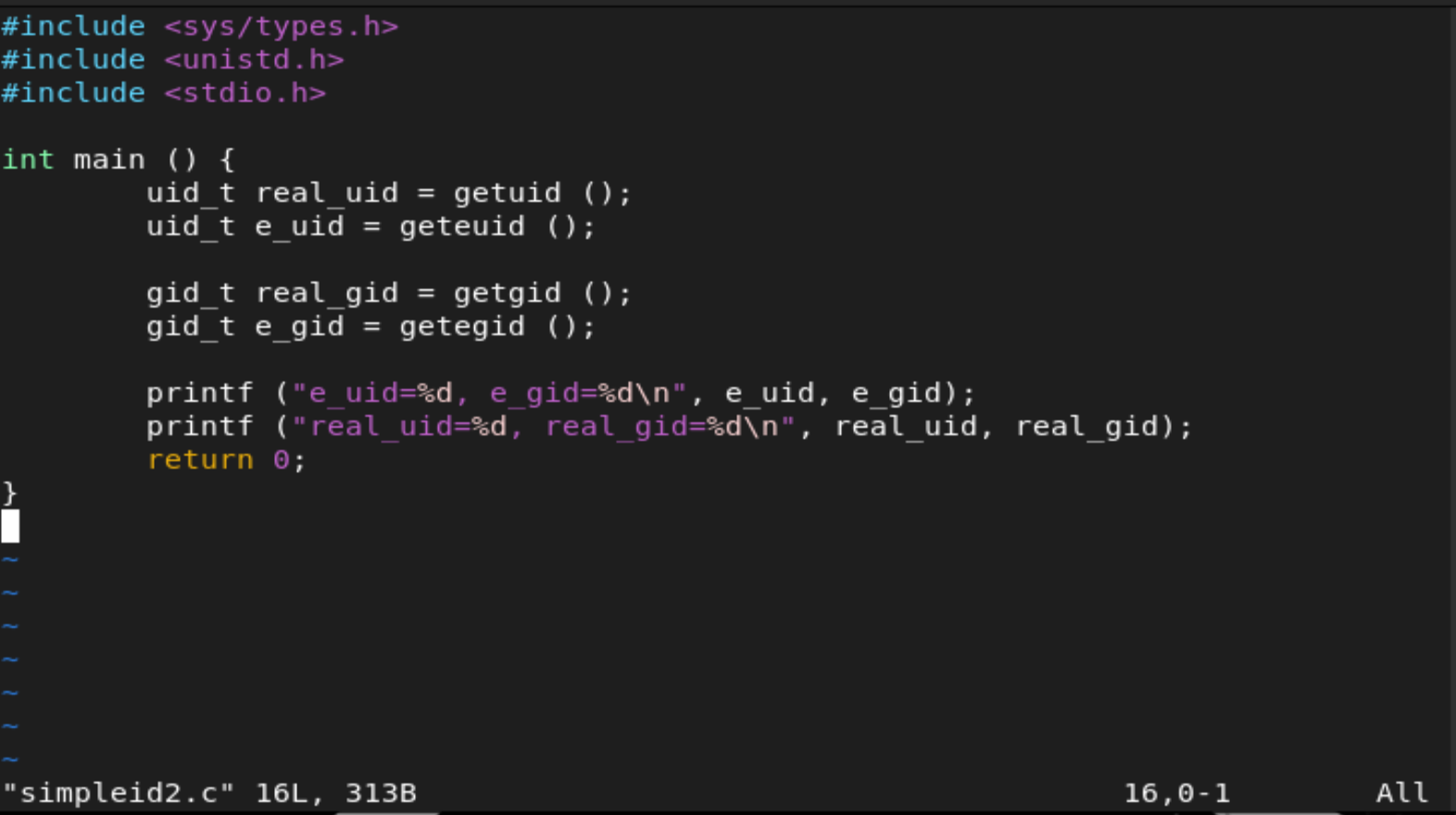
Выполнение программы и команды id

Мы видим, что результаты вывода программы и команды совпадают и соответствуют действительности.

Далее создадим файл simpleid2.c и запишем в него ранее написанную программу, добавив вывод действительных идентификаторов.

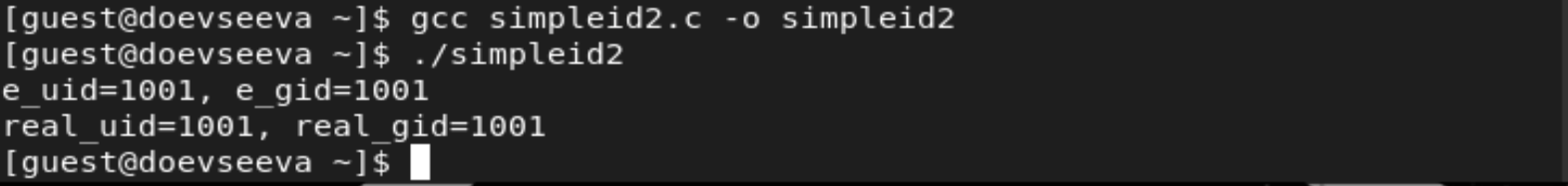


Создание файла



Код программы

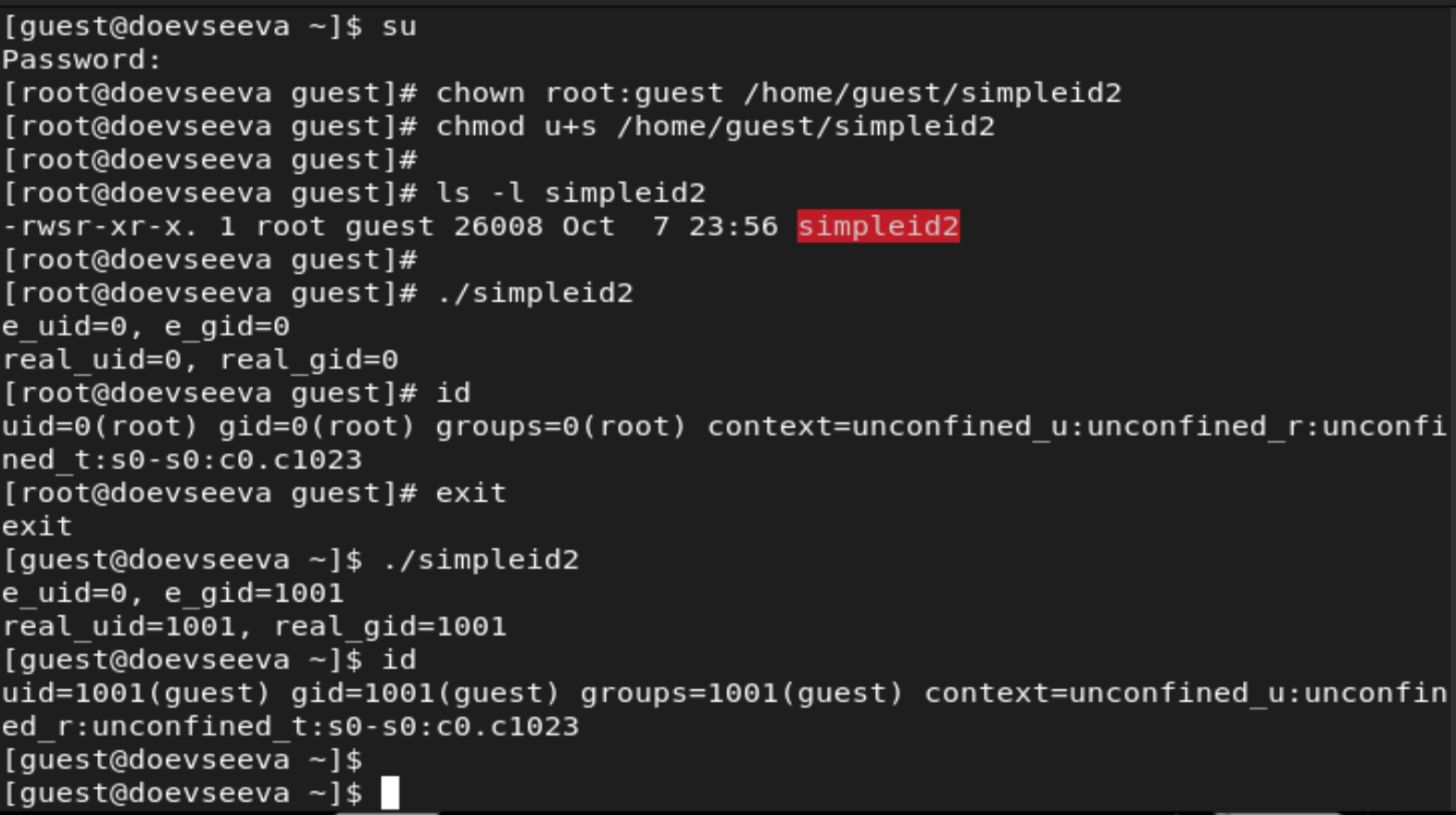
Скомпилируем и запустим программу.



Результаты запуска программы

Здесь мы видим, что полученные значения для пар uid и gid совпадают.

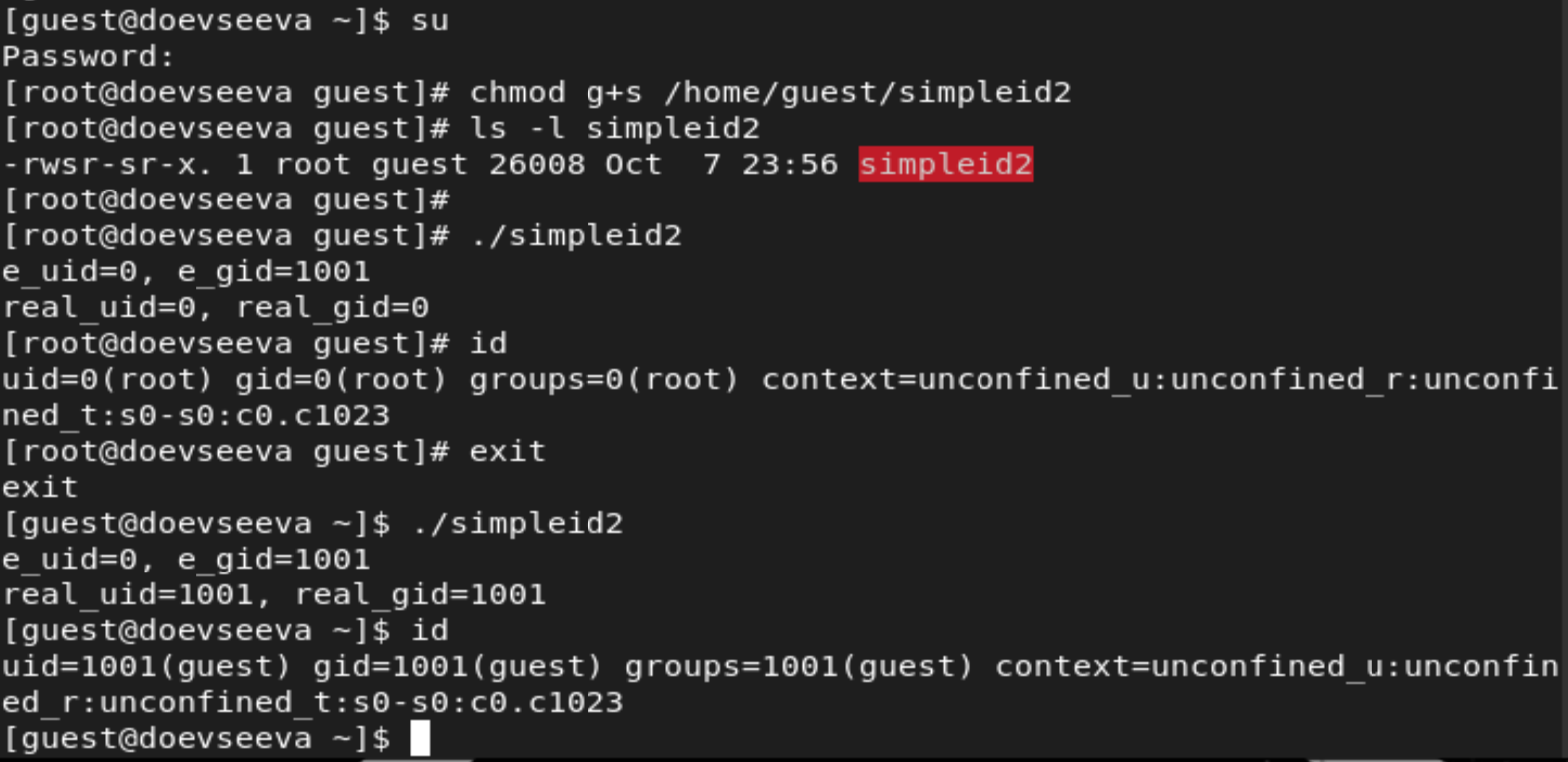
Далее от имени суперпользователя сменим владельца файла simpleid2 и установим на него атрибут s для пользователя, после чего проверим правильность выполненных команд и сравним результат запуска simpleid2 с выводом команды id для суперпользователя и для пользователя guest.



Установка атрибута s для пользователя

Мы видим, что при выводе результатов от имени суперпользователя все результаты совпадают по значениям, однако при выводе результатов от имени пользователя guest можно заметить, что значение e\_uid остается соответствующим суперпользователю, а остальные значения соответствуют значениям для пользователя guest.

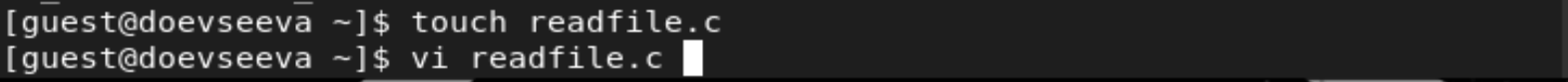
Далее проделаем те же действия, установив на файл от имени суперпользователя атрибут s для группы.



Установка атрибута s для группы

Здесь мы видим, что при выводе результатов от имени суперпользователя все результаты совпадают по значениям, кроме значения g\_uid, которое соответствует группе guest, а при выводе результатов от имени пользователя guest значение e\_uid остается соответствующим суперпользователю, а значение g\_uid с остальными результатами также соответствует группе и пользователю guest.

Теперь создадим программу readfile.c и откомпилируем ее.



Создание файла

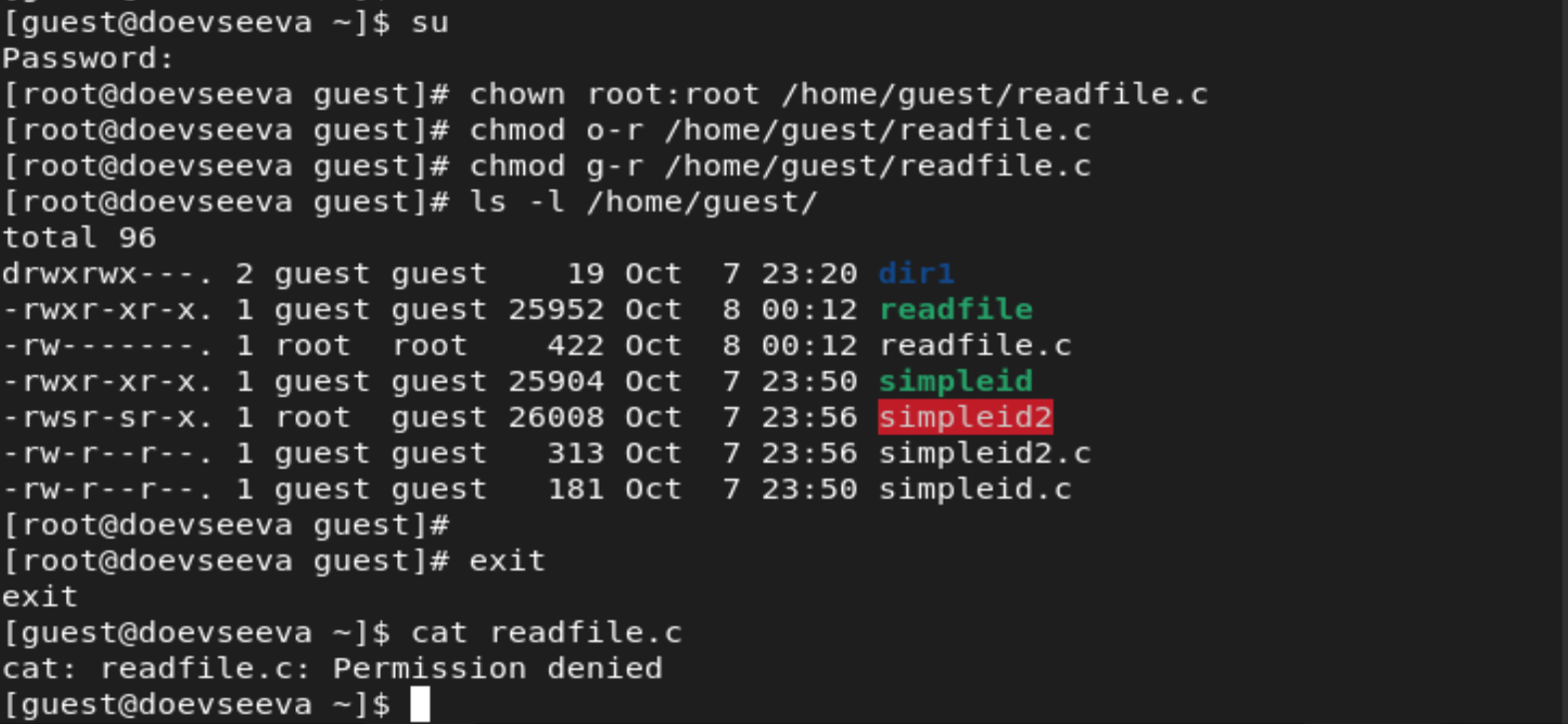


Код программы

Компиляция программы

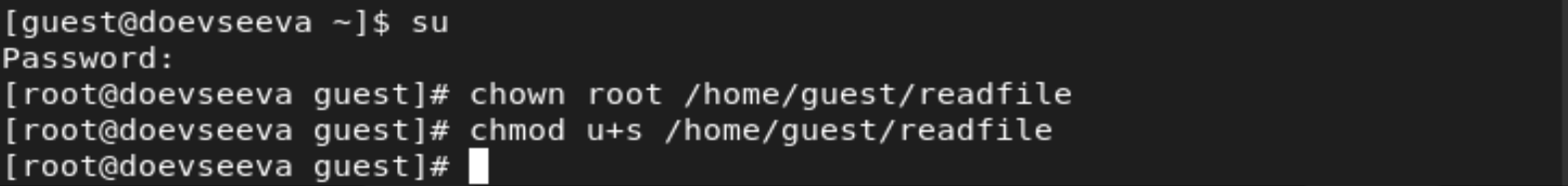
Компиляция программы

Сменим владельца у файла readfile.c и изменим права так, чтобы только суперпользователь мог прочитать его, а guest не мог, и проверим успешность изменения прав.



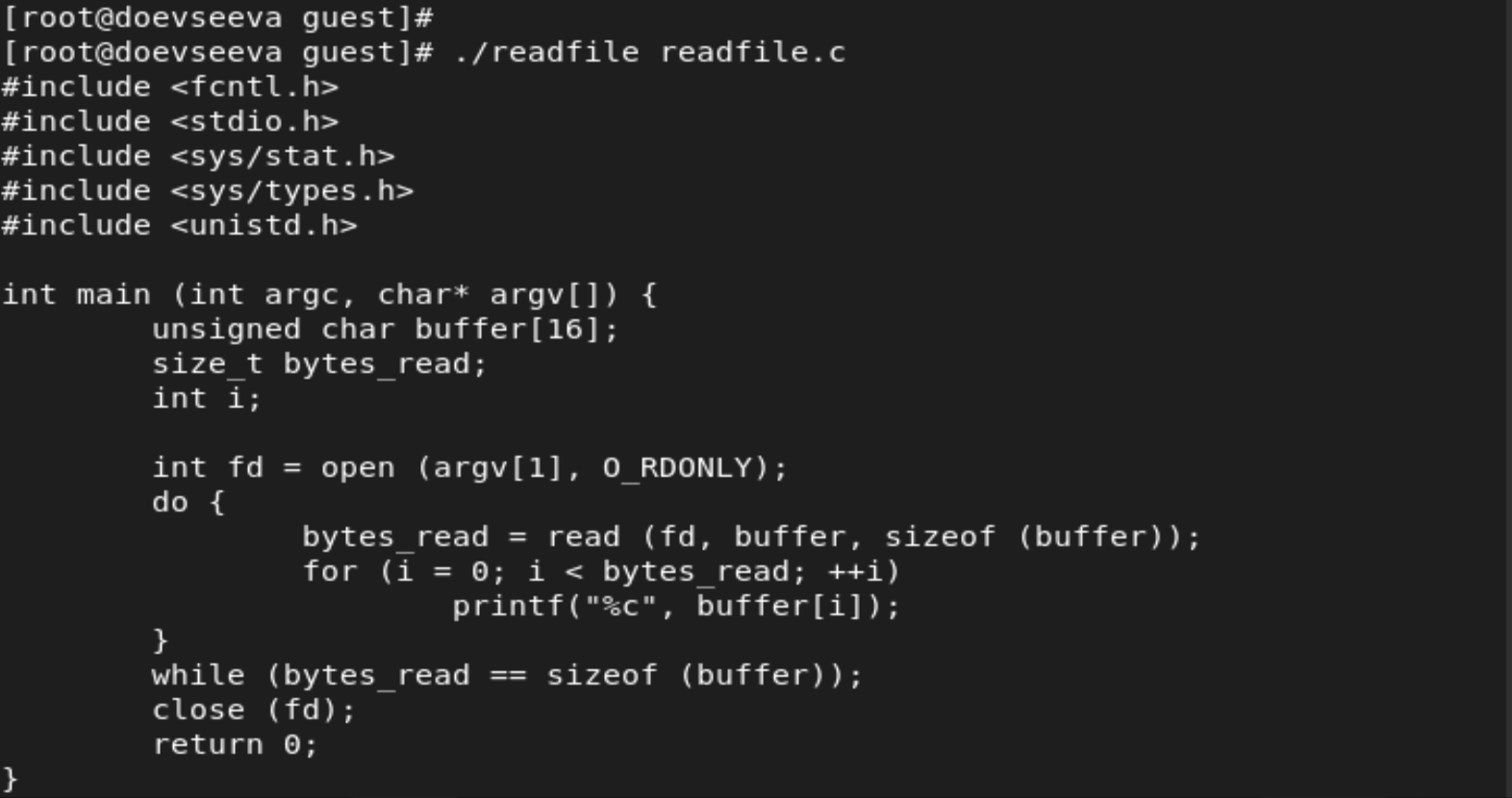
Смена владельца файла и изменение прав

Далее сменим у программы readfile владельца и установим SetUID-бит.

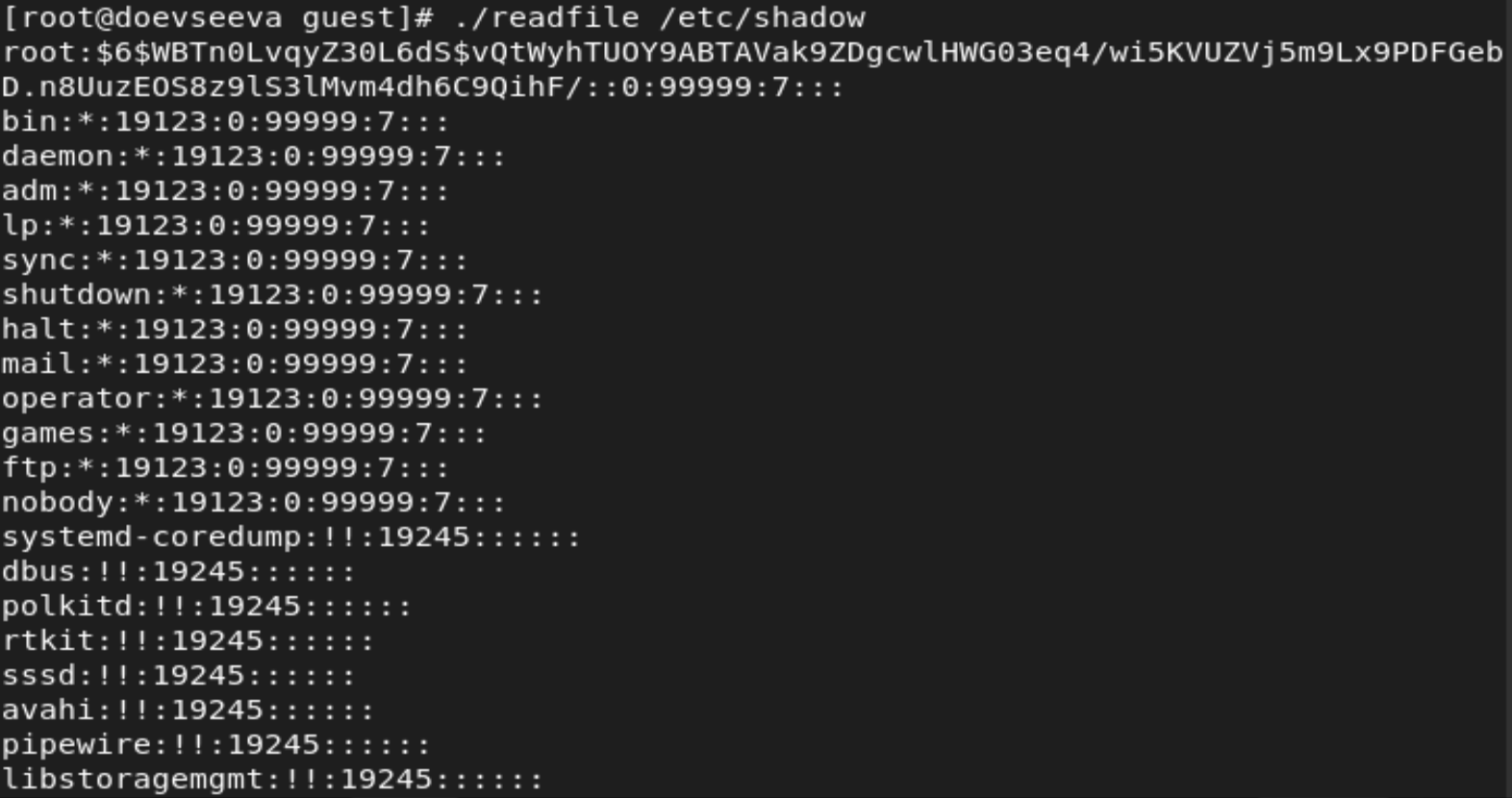


Смена владельца и установка SetUID-бита

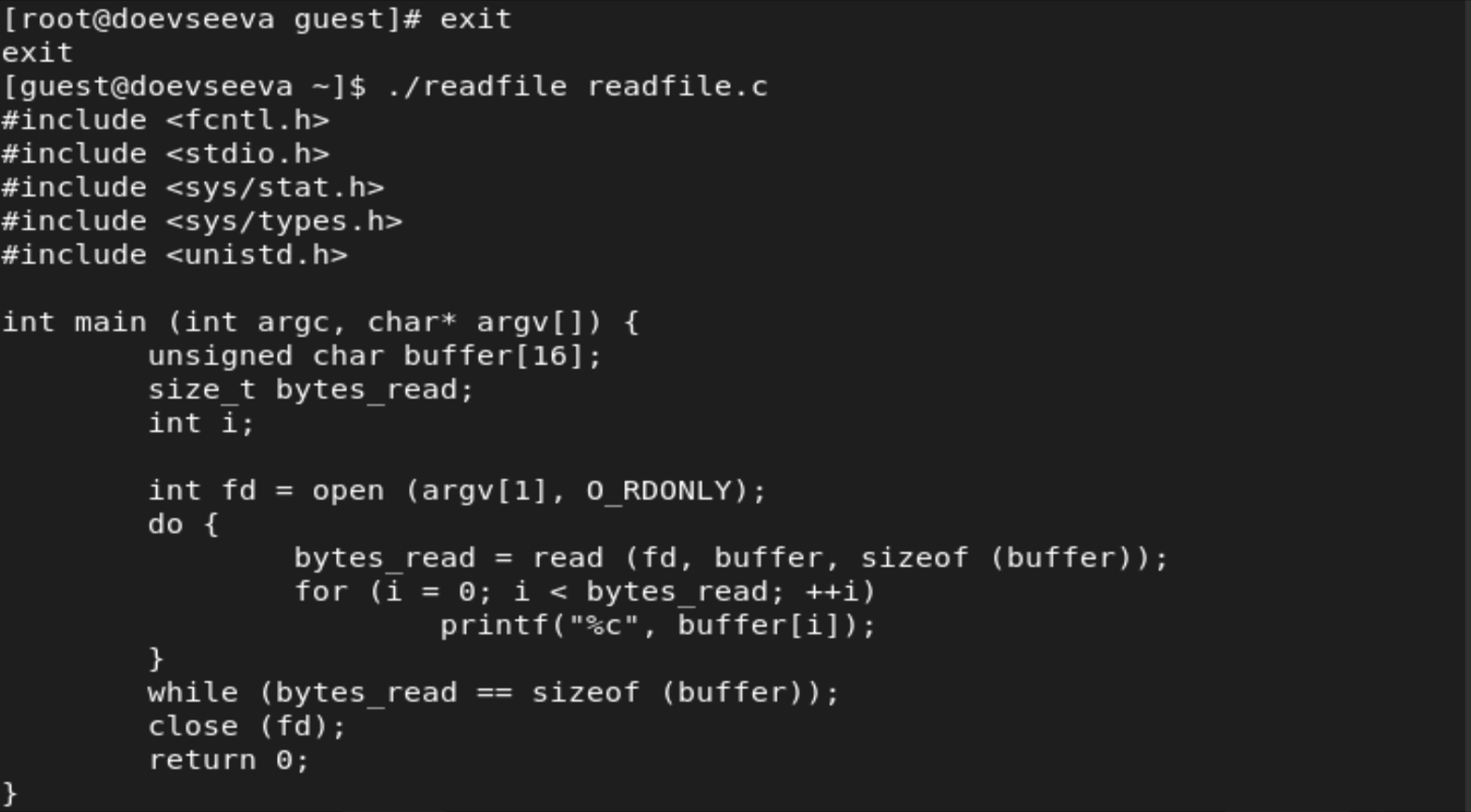
Проверим возможность чтения программой readfile файлов readfile.c и /etc/shadow от имени суперпользователя и пользователя guest.



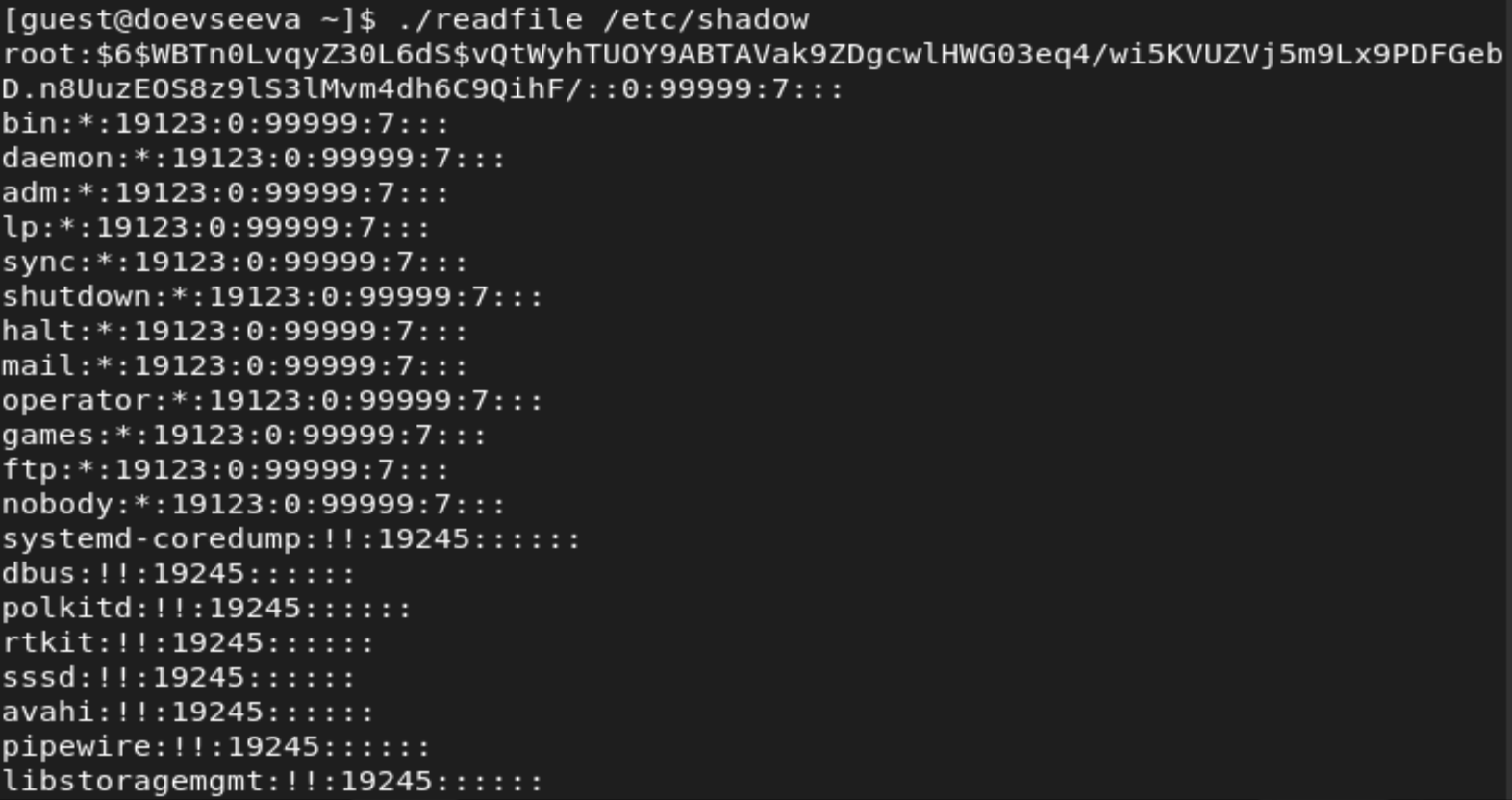
Чтение readfile.c от имени суперпользователя



Чтение /etc/shadow от имени суперпользователя



Чтение readfile.c от имени пользователя guest

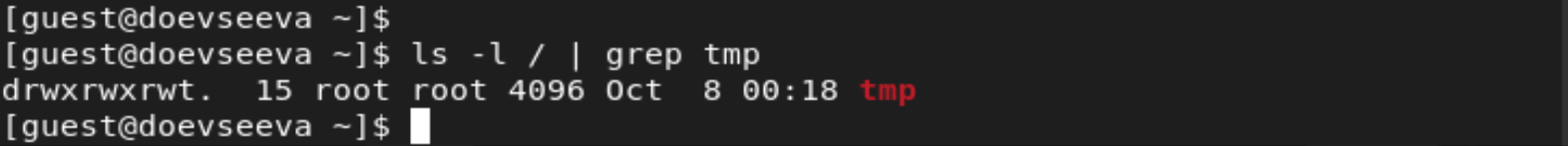


Чтение /etc/shadow от имени пользователя guest

Как мы видим, файлы были успешно прочитаны в обоих случаях.

## 2. Работа со Sticky-битом

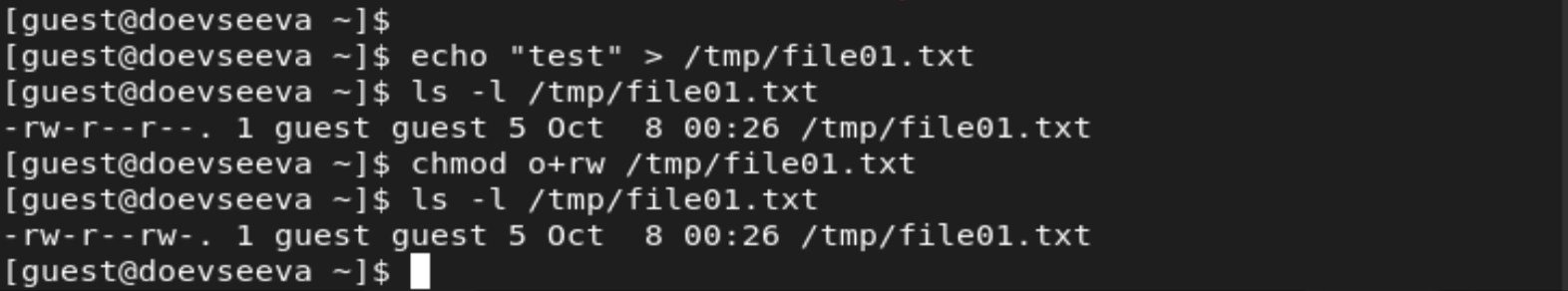
Выясним, установлен ли атрибут Sticky на директории /tmp.



Проверка наличия атрибута Sticky

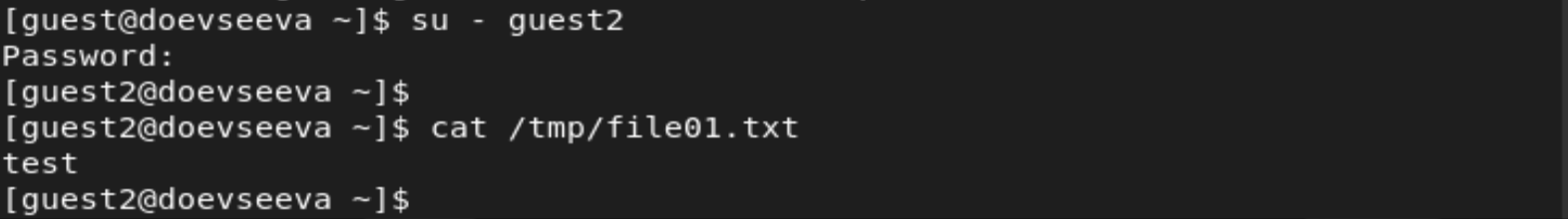
Мы видим, что атрибут t установлен на директории.

От имени пользователя guest создадим файл file01.txt в директории /tmp со словом test, просмотрим его атрибуты и разрешим чтение и запись для категории пользователей ‘все остальные’.



Создание файла и изменение прав

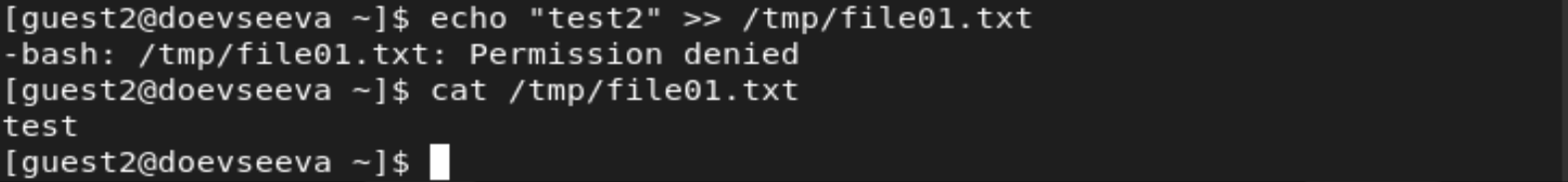
От имени пользователя guest2 попробуем прочитать созданный файл.



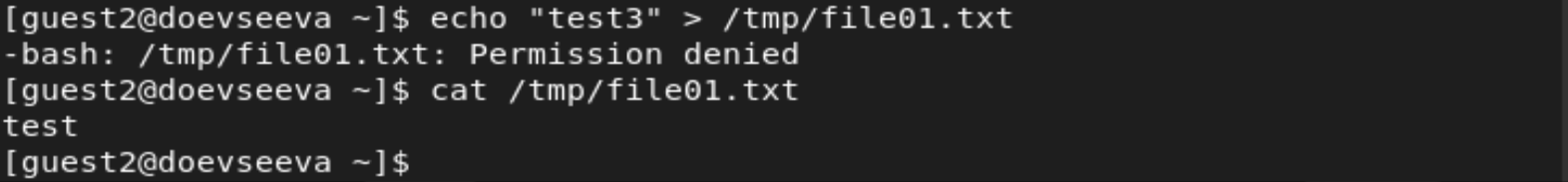
Чтение файла от имени пользователя guest2

Файл был успешно прочитан.

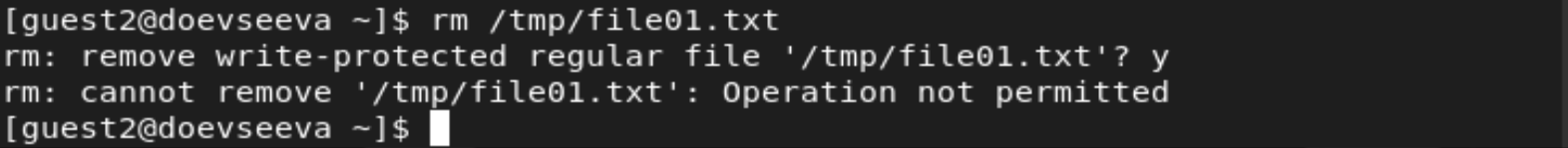
Далее попробуем сделать дозапись в файл, перезаписать его содержимое и удалить файл.



Попытка дозаписи в файл



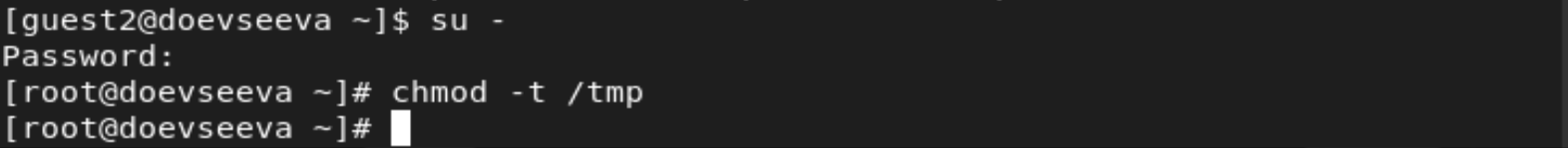
Попытка перезаписи файла



Попытка удаления файла

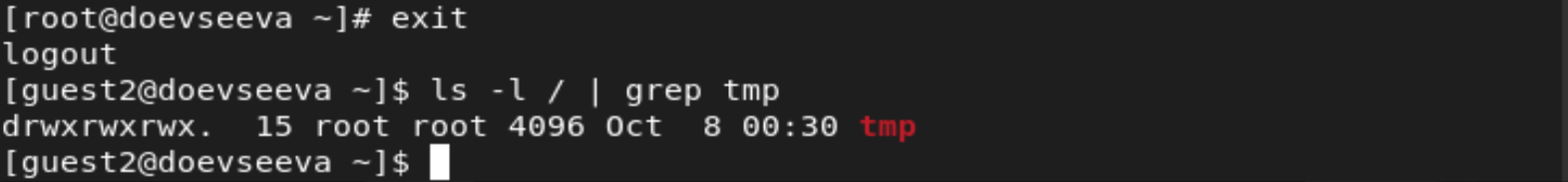
При попытке выполнения каждой из команд было отказано в доступе, соответственно выполнить их не удалось.

Повысим свои права до суперпользователя и снимем атрибут t с директории /tmp.



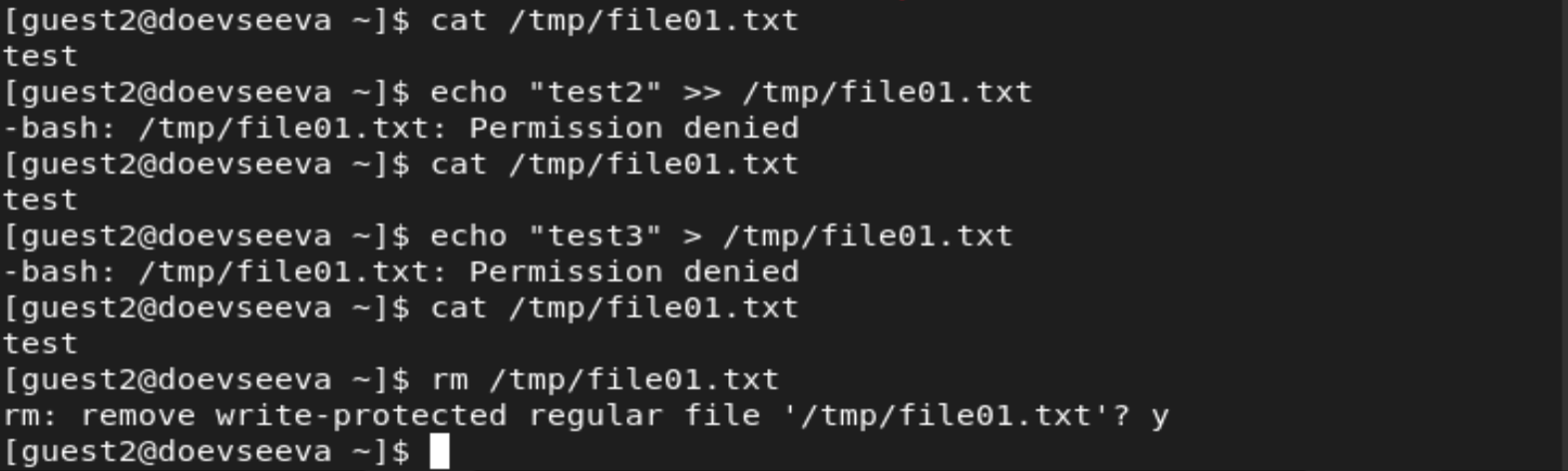
Снятие атрибута Sticky

Покинем режим суперпользователя и проверим успешность снятия атрибута.



Проверка атрибутов

Далее попробуем выполнить команды, которые не удалось выполнить ранее.



Попытка повторного выполнения команд

Итак, мы можем видеть, что при попытке дозаписи в файл или перезаписи его содержимого в доступе снова было отказано, однако на этот раз удалось успешно удалить файл от имени пользователя, не являющегося его владельцем.

Повысим свои права до суперпользователя и вернем атрибут t на директорию /tmp.



Возвращение атрибута Sticky

# Выводы

В результате проделанной работы мы изучили механизмы изменения идентификаторов и применения SetUID-, SetGID- 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

* Методические материалы к лабораторной работе, представленные на сайте “ТУИС РУДН” https://esystem.rudn.ru/