Основы информационной безопасности

Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Нзита Диатезилуа Катенди

Содержание

# ПЦель 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.

# Теоретические сведения

При работе с командой chmod важно понимать основные разрешения, назначаемые файлам или каталогам. В Linux[@scott\_linux\_2019] существует три основных типа разрешений:

* Чтение — обозначается буквой «r». Предоставляет возможность просмотра содержимого файла или каталога.
* Запись — обозначается буквой «sh». Позволяет создавать, изменять и удалять файлы в каталоге, а также изменять содержимое файла.
* Выполнение — обозначается буквой «x». Предоставляет разрешение на выполнение файла или вход в каталог.

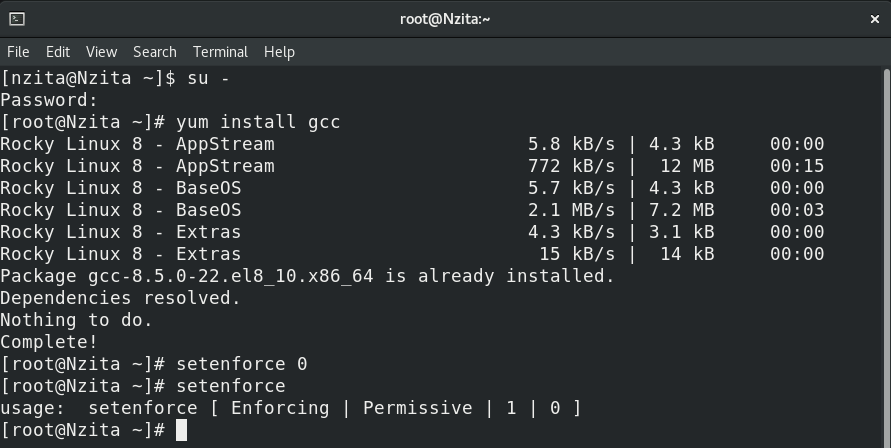
Каждый из вышеперечисленных типов разрешений может быть назначен трем группам пользователей:

* Владелец — пользователь, которому принадлежит файл или каталог.
* Группа — группа пользователей, к которой принадлежит файл или каталог.
* Другие — все остальные пользователи в системе.

Комбинация этих основных разрешений для каждой группы пользователей определяет полный набор разрешений для файла или каталога.

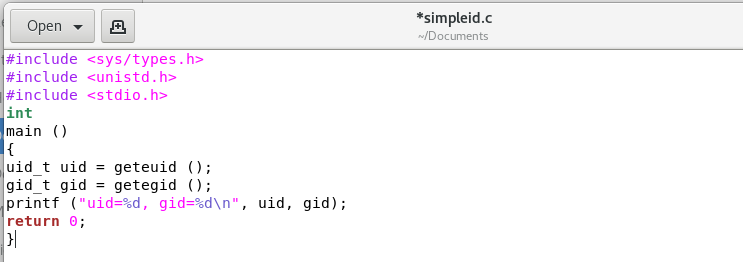
# Выполнение лабораторной работы

Проверим установлен ли компилятора gcc, а также отклочим SELinux (рис. @fig:001)



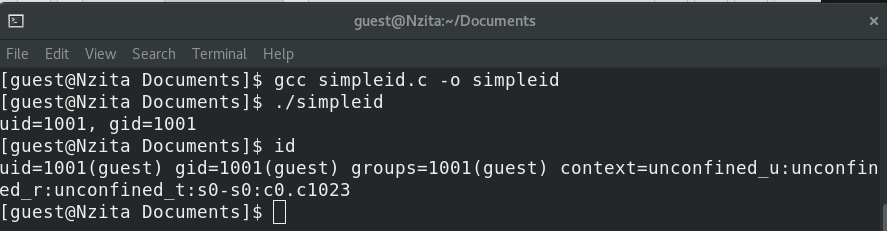
Подготовка лабораторного стенда

Войдем в систему от имен пользователя guest и создадим программу simpleid.c, которая выводит идентификатор пользователя и группы(рис. @fig:002)



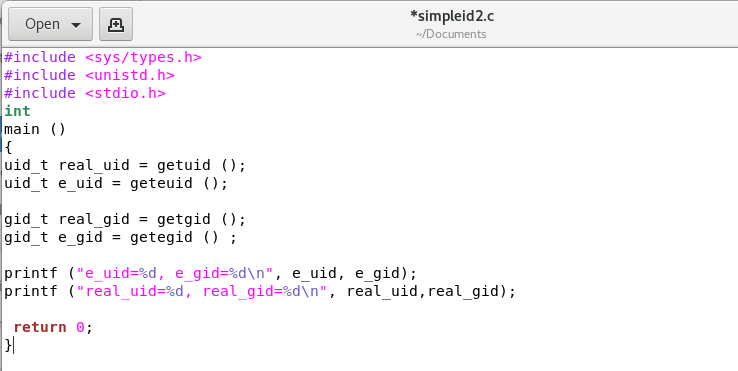
Текст прораммы simpleid.c

Теперь скомпириуем программу с помощью gcc, затем, запустив её, увидим, что она выводит идентификаторы пользователя и группы 1001 и 1001 для guest, что совпадает с выводом команды id(рис. @fig:003)



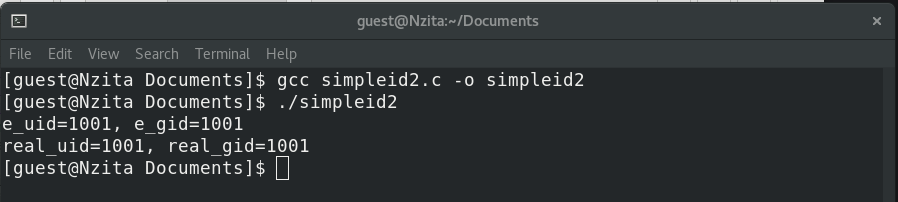
Запуск програмы simpleid.c

Усложним программу, добавив вывод действительных идентификаторов(рис. @fig:004).



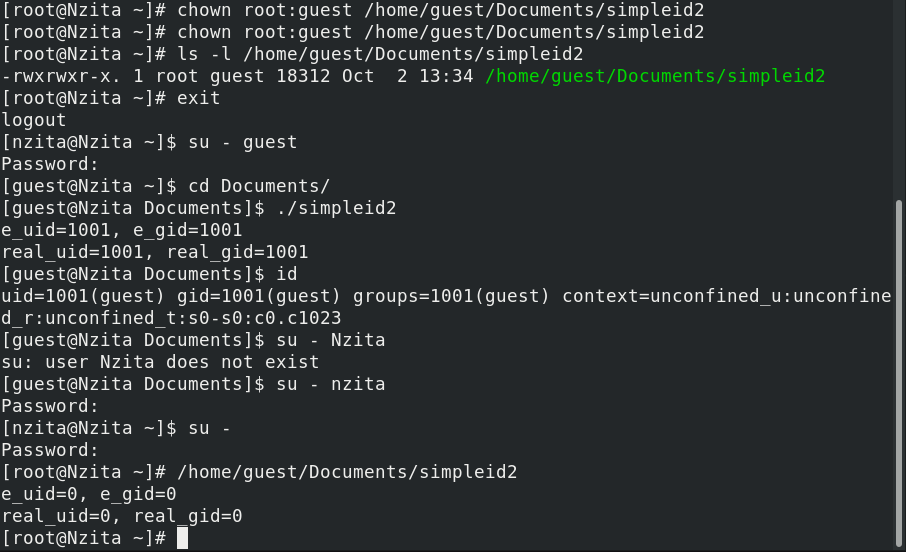
Текст прораммы simpleid2

Теперь скомпириуем программу с помощью gcc, затем, запустив её, увидим, что она выводит идентификаторы пользователя и группы 1001 и 1001 для guest, что совпадает с выводом команды id(рис. @fig:005).



Запуск програмы simpleid2.c

От имени суперпользователя изменим владельца файла /home/guest/simpleid2 и установим SetUID-бит. Проверим корректность установленных прав и опять запустим simpleid2(рис. @fig:006).

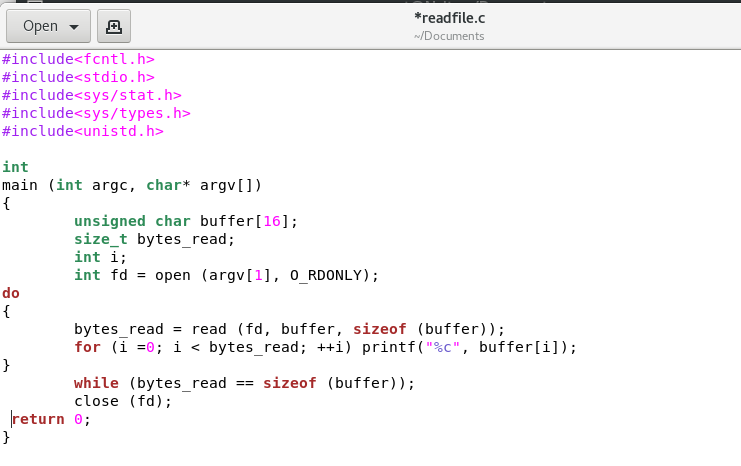


Изменение владельца и запуск программы simpleid2 с установленным SetUID-битом

Проделаем аналогичные действия относительно SetGID-бита(рис. @fig:007):

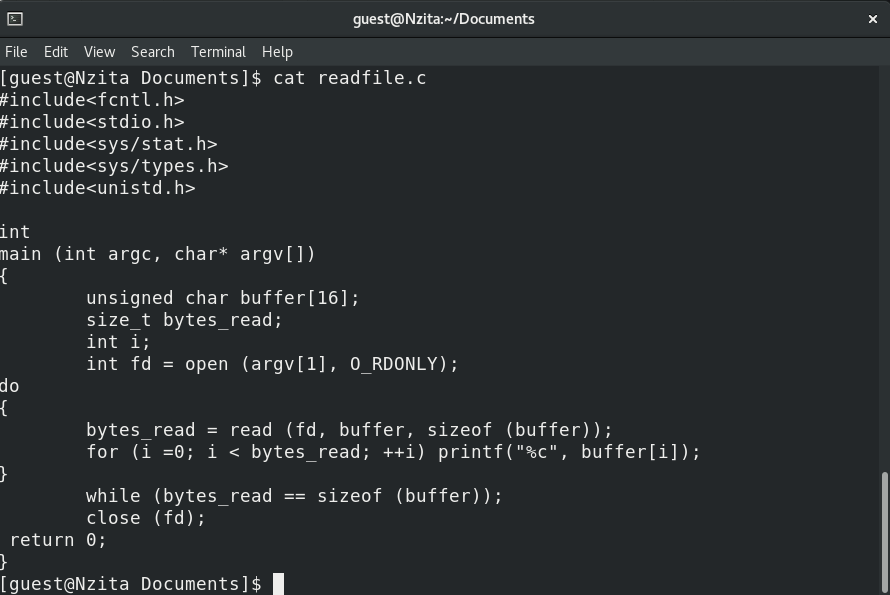
![[Запуск программы simpleid2 с установленным SetGID-битом](image/7.png)

Создадим программу для чтения файлов readfile.c(рис. @fig:008):



Текст программы readfile.c

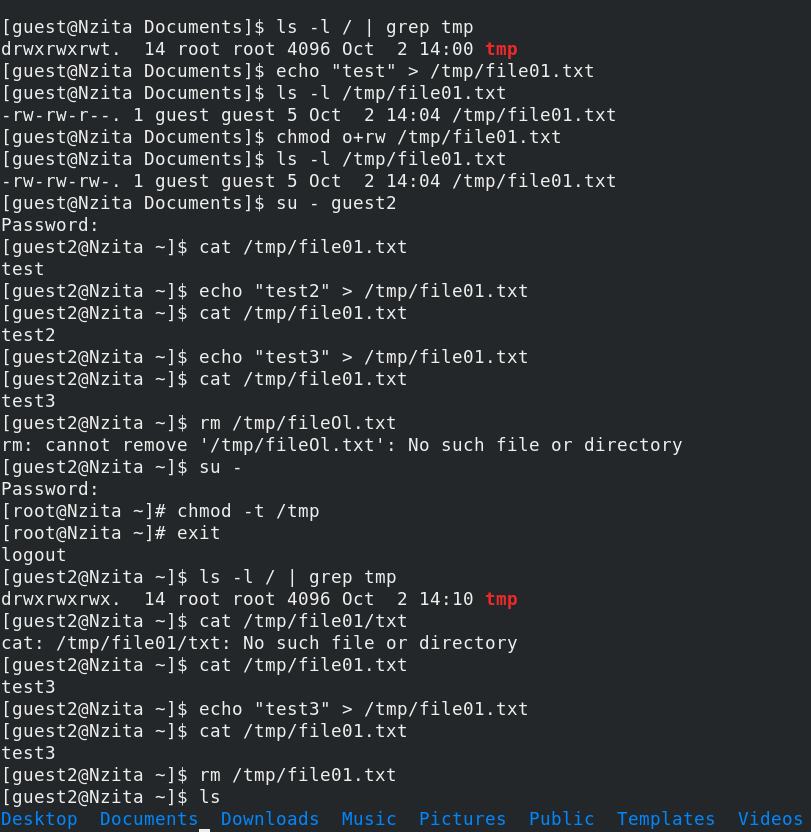
Скомпилируем её и сменим владельца у файла с текстом программы, затем изменим права так, чтобы только суперпользователь (root) мог прочитать его, и проверим корректность настроек(рис. @fig:009):



Изменение владельца и прав файла readfile.c

После завершения установки операционной системы корректно перезапустим виртуальную машину и при запросе примем условия лицензии.

Проверим, что установлен атрибут Sticky на директории /tmp(в конце стоит t). Затем от имени пользователя guest создадим файл file01.txt в директории /tmp со словом test, затем просмотрим атрибуты у только что созданного файла и разрешим чтение и запись для категории пользователей «все остальные». После этого от пользователя guest2 попробуем дозаписать в этот файл новое слово, однако получим отказ, также нам отказано в перезаписи и удалении этого файла. Если же убрать Sticky бит, то нам будет разрешено удаление этого файла(рис. @fig:010):



Подключение образа диска дополнений

# Выводы

В результате выполнения работы были выполнены:

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

# Список литературы