Информационная безопасность лабораторная работа №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Ким Илья Владиславович НФИбд-01-21

Содержание

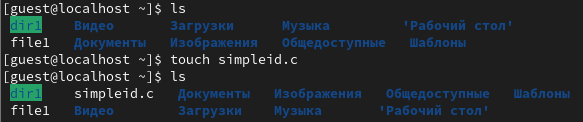
# Цель работы

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

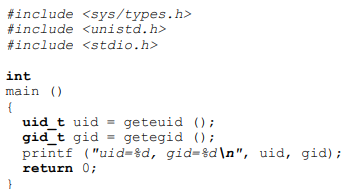
# Выполнение лабораторной работы

## Создание программы

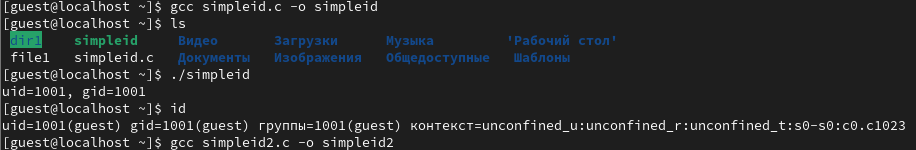
1. Создал программу simpleid.c (рис. [-@fig:001])



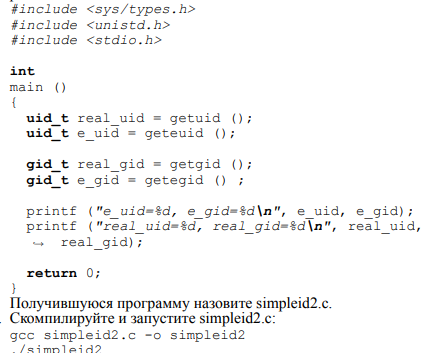
1. Записал код программы в simpleid.c (рис. [-@fig:002])



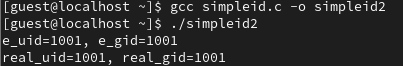
1. Скомпилировал и выполнил программу simpleid.c (рис. [-@fig:003])



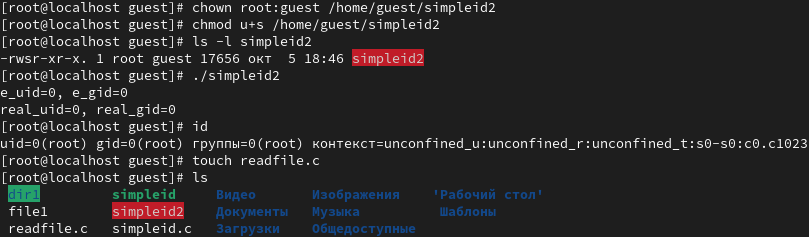
1. Изменил код программы в simpleid.c (рис. [-@fig:004])



1. Скомпилировал и выполнил программу simpleid2.c (рис. [-@fig:005])

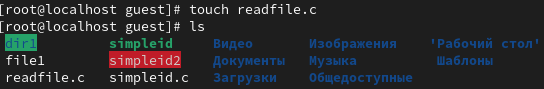


1. От имени суперпользователя поменял права на файл simpleid2.c, поменял владельца файла и выполнил программу (рис. [-@fig:006])

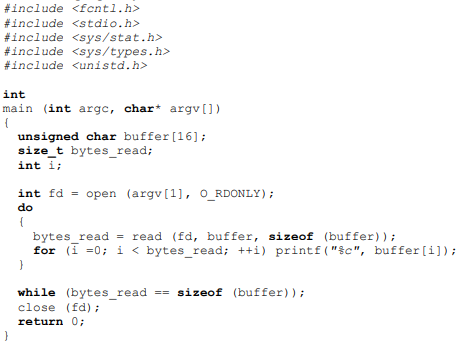


* Результаты выполнения отличаются.

1. Создал файл readfile.c (рис. [-@fig:007])



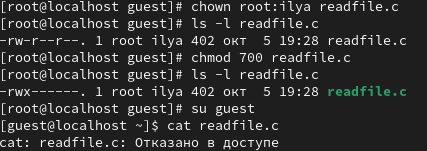
1. Записал код программы в readfile.c (рис. [-@fig:008])



1. Скомпилировал readfile.c (рис. [-@fig:009])



1. Сменил права и владельца readfile.c, попрбовал от имени пользователя guest прочитать файл, получил отказ (рис. [-@fig:010])

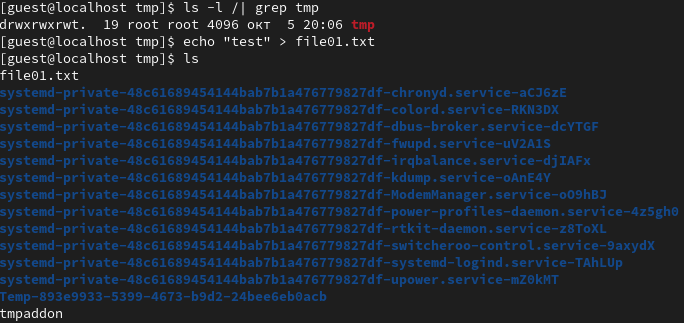


1. С помощью программы readfile прочитал файл /etc/shadow (рис. [-@fig:011])

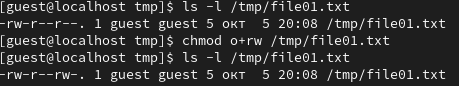


## Исследование Sticky-бита

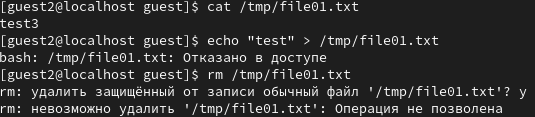
1. Проверил установлен ли атрибут Sticky на директории /tmp , создал в ней файл file91.txt(рис. [-@fig:012])



1. Проверил атрибуты у файла file01.txt , поменял атрибуты на чтение и запись для остальных пользователей (рис. [-@fig:013])



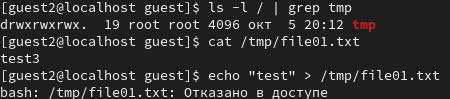
1. От пользователя guest 2 попробовал прочитать, изменить и удалить file01.txt, получилось только прочитать (рис. [-@fig:014])



1. От имени суперпользователя снял атрибут t у /tmp (рис. [-@fig:015])



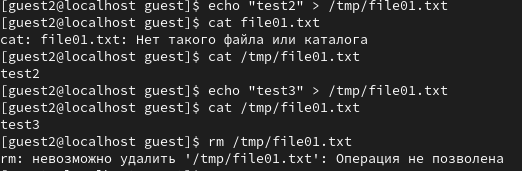
1. От имени guest 2 проверил, что у директории /tmp нет атрибута t. Попробовал сделать команды еще раз, ничего не поменялось. (рис. [-@fig:016])



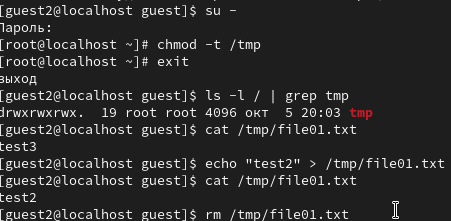
1. Поменял права файла file01.txt на 666 (рис. [-@fig:017])



1. Попробовал выполнить команды еще раз, получилось сделать все, кроме удаления (рис. [-@fig:018])



1. Удалил атрибут t и выполнил команды, получилось выполнить все, включая удаление (рис. [-@fig:019])



# Выводы

Изучил механизм изменения идентификаторов, применяя SetUID и Sticky-битов. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работу механизма смены идентификатора процессов пользователей, а также влияния бить Sticky на запись и удаление файлов.