Отчёт по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Косолапов Степан Эдуардович НПИбд-01-20

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 Выполнение работы

1. Входим в систему от имени пользователя guest. Создаем программу simpleid.c:



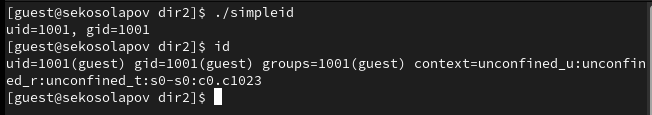
simpleid.c

1. Компилируем программу и убеждаемся, что файл программы создан.

компиляция simpleid.c

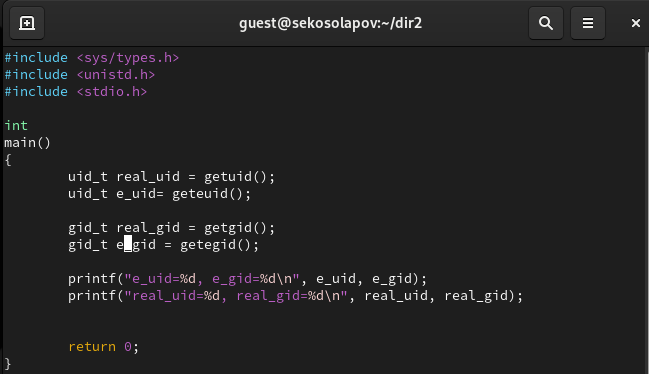
компиляция simpleid.c

1. Выполняем программу simpleid и выполняем системную программу id. Видим, что айдишники показываются такие же, но id показывает более расширеную информацию.



сравнение вывода simpleid.c и id

1. Усложняем программу, добавив вывод действительных идентификаторов. Получившуюся программу называем simpleid2.c.



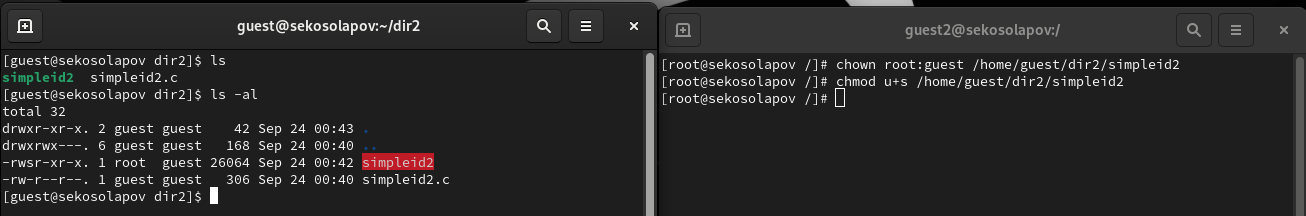
simpleid2.c

1. Компилируем и запускаем simpleid2.c.



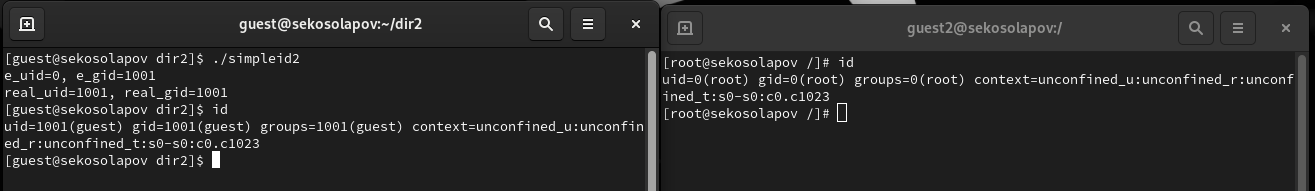
компиляция и запуск simpleid2.c

1. От имени суперпользователя выполняем команды: chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2
2. Выполняем проверку правильности установки новых атрибутов и смены владельца файла simpleid2



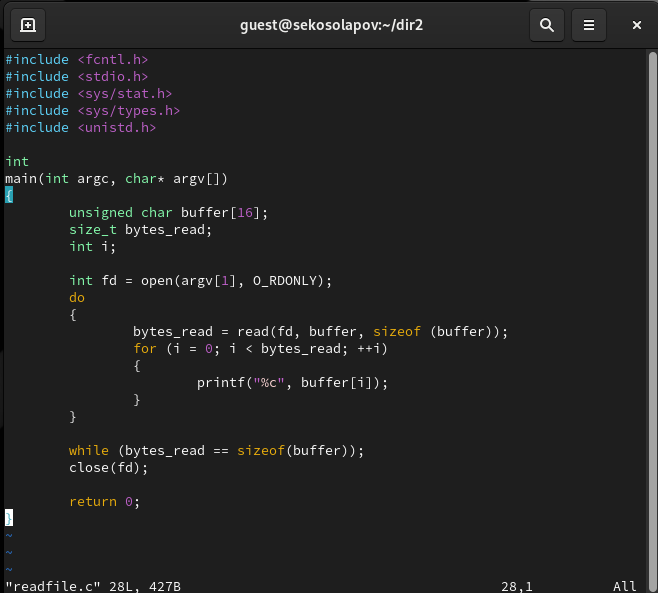
устанавливаем владельца файла simpleid2 и добавляем setuid бит

1. Запускаем программы simpleid2 и id. Видим, что при выполнении файла simpleid2 он берет id владельца.



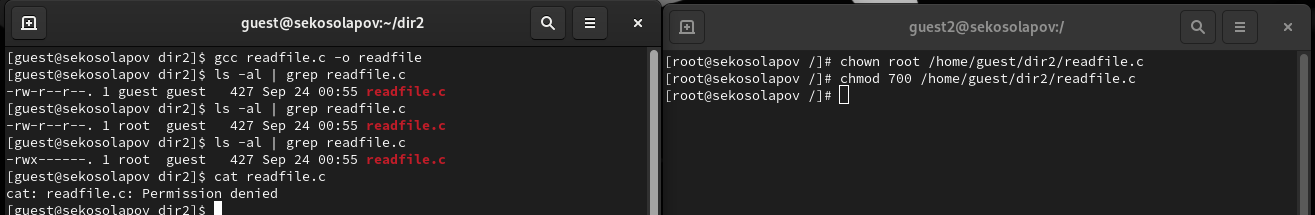
выполняем simpleid2 с битом setuid

1. Создаём программу readfile.c:



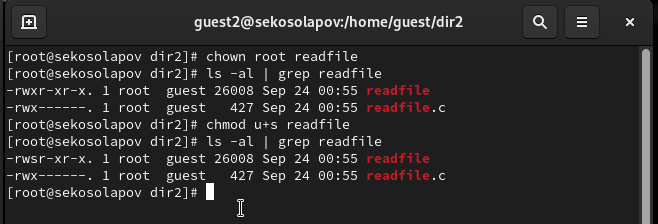
readfile.c

1. Компилируем ее командой: gcc readfile.c -o readfile
2. Меняем владельца у файла readfile.c на root и выделяем права на чтение только для владельца. Проверяем, что пользователь guest не может прочитать файл readfile.c.



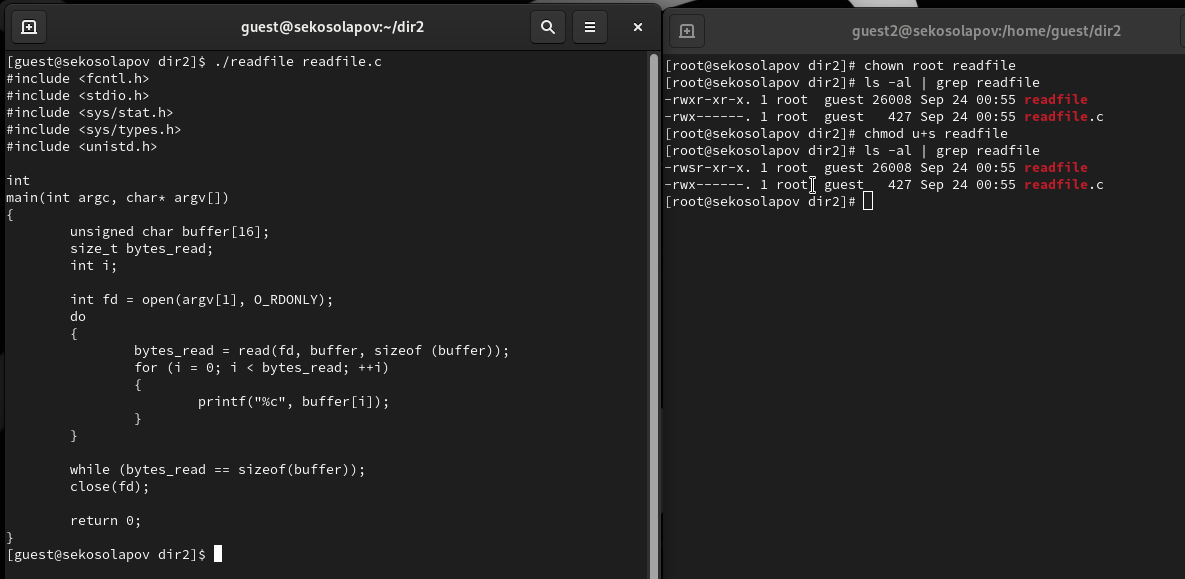
установка прав на файл readfile.c только для root

1. Меняем у программы readfile владельца на root и устанавливаем SetUID-бит.



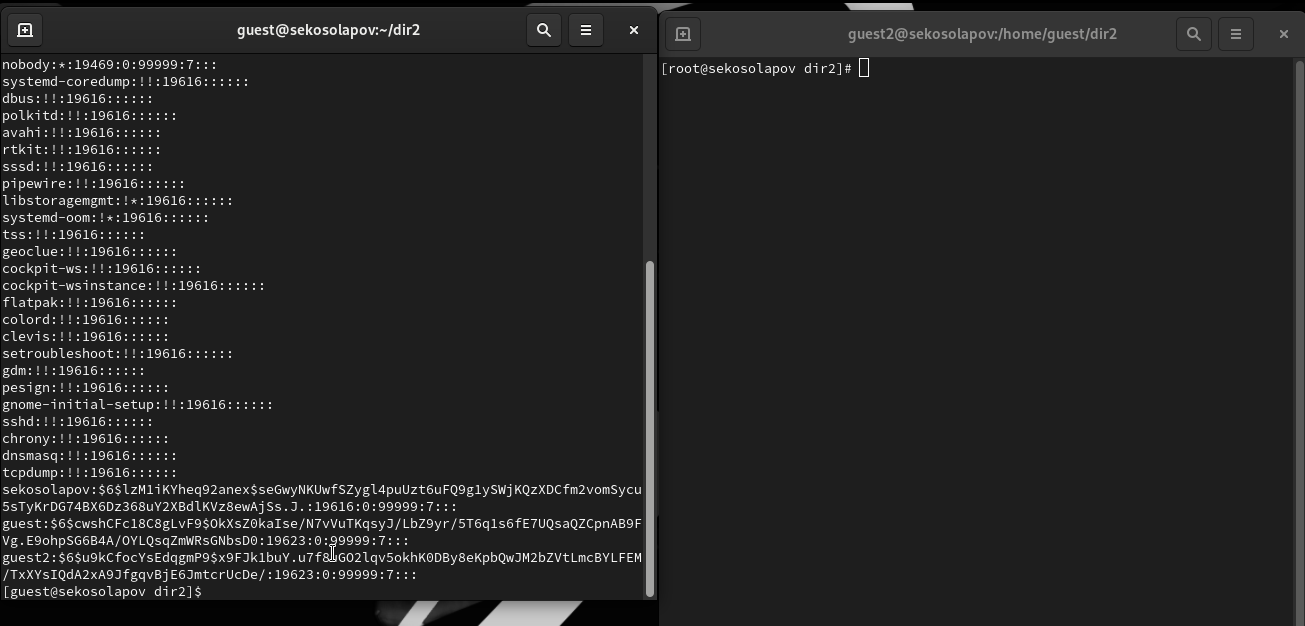
установка setuid бита на файл readfile

1. Проверяем, может ли программа readfile прочитать файл readfile.c. Видим, что программа может прочитать файл, потому что установлен SetUID бит, который позволяет программе при запуске получать права своего владельца, которым установлен root.



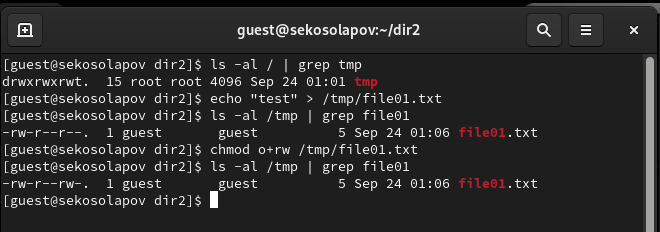
чтение readfile.c с помощью readfile с установленным setuid битом

1. Проверяем, может ли программа readfile прочитать файл /etc/shadow. Ситуация аналогичная предыдущему пункту. Мы можем прочитать этот файл, потому что у root есть к нему доступ на чтение.



чтение /etc/shadow с помощью readfile с установленным setuid битом

1. Выясняем, установлен ли атрибут Sticky на директории /tmp. Видим, что атрибут установлен (атрибут t). От имени пользователя guest создаём file01.txt в директории /tmp со словом test. Смотрим атрибуты у только что созданного файла и разрешаем чтение и запись для категории пользователей «все остальные».

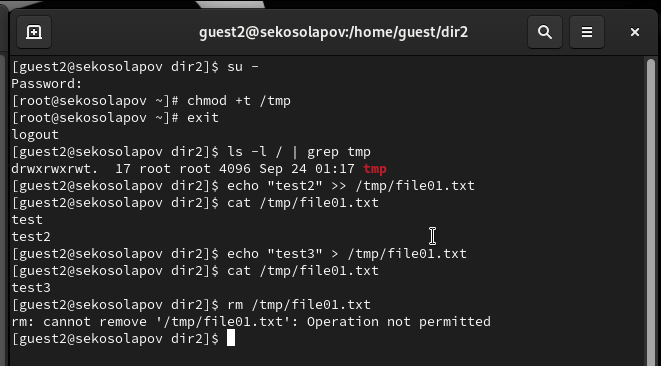


создание файла в sticky директории

На самом деле, тут у пользователя guest2 не будет прав, потому что он находится в группе владельца файла и нам нужно добавить права на чтение для группы, а не для всех остальных.

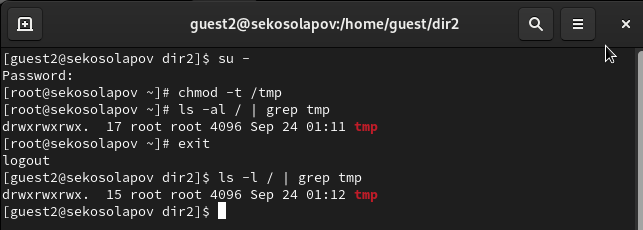
chmod g+rw /tmp/file01.txt

1. От пользователя guest2 пробуем выполнить привычные опреации с файлом /tmp/file01.txt. У нас получлось выполнить - чтение, дозапись, перезапись. Не получилось сделать удаление файла. Как раз из-за установленного на директории tmp атрибута tmp.



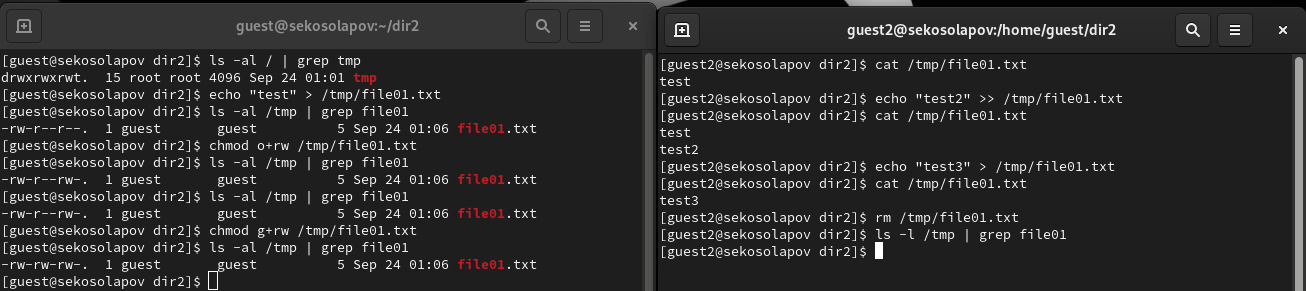
операции над файлом в sticky директории

1. От имени суперпользователя убираем атрибут sticky.



снятие атрибута sticky

1. Пробуем повторить операции без атрибтуа sticky у директории tmp. Теперь мы можем выполнять все операции, которые разрешены для группы владельца файла, в нашем случае это дозапись, перезапись, чтение и удаление файла.



операции над файлом в директории без sticky

1. В конце возвращаем атрибут sticky директории tmp.

# 3 Выводы

В данной работе мы изучили атрибуты sticky, и биты setgid и setuid и их влияние на различные аспекты работы системы. Атрибут sticky, применяемый к директориям, позволяет ограничить доступ к файлам в них, предотвращая удаление или переименование файлов другими пользователями. Бит setgid позволяет устанавливать группу-владельца для новых файлов, созданных в директории, что может быть полезно для обеспечения совместного доступа к файлам между пользователями. Бит setuid, с другой стороны, позволяет запускать исполняемые файлы с привилегиями владельца файла, что может быть полезно для выполнения определенных задач, требующих повышенных привилегий.