Лабораторная работа № 5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибуто

Алади Принц Чисом

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 лабораторной работы

1. Я создал файл “simpleid.c” и внёс в него программу.

Первая программа 

1. Скомпилировал программу и убедился, что файл создан правильно.



Рис. 1: Компиляция первой программы

1. Запустил программу и посмотрел, как она работает. Затем прописал команду “id”, чтобы сравнить данные. Все данные сходятся.

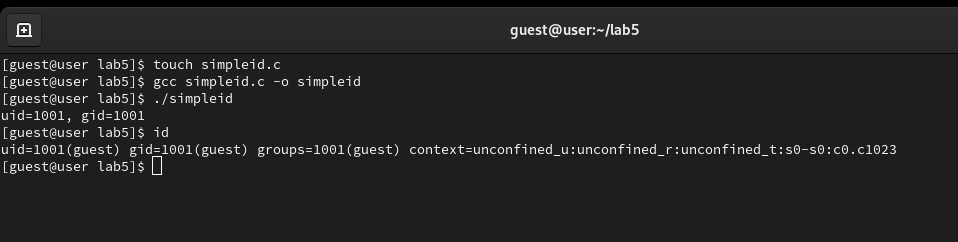


Рис. 2: Запуск первой программы

1. Создал второй файл и назвал его “simlpeid2.c”. Усложнил первую программу и внёс ее в файл.

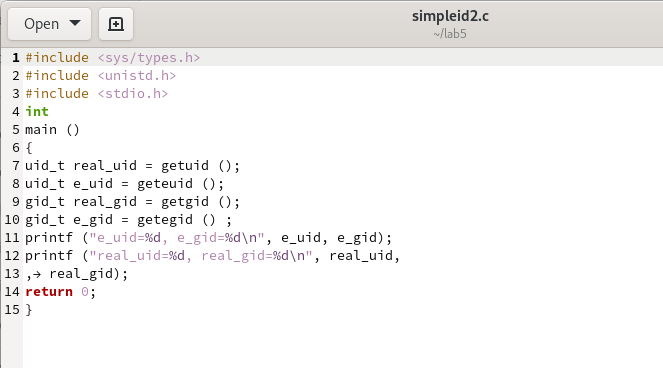


Рис. 3: Вторая программа

1. Скомпилировал и посмотрел вторую программу. Проверил как она работает.



Рис. 4: Запуск второй программы

1. От имени суперпользователя я выполнил команды и временно повысил свои права. Команды сменили пользователя файла на root и установили SetUID-бит. Я запустил файл от имени root-пользователя и проверил сходство с командой “id”.

Рис. 5: Изменение прав для root

Рис. 5: Изменение прав для root

Рис. 6: Проверка работы для root

Рис. 6: Проверка работы для root

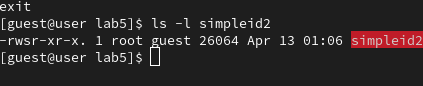


Рис. 7: Установка SetUID-бита

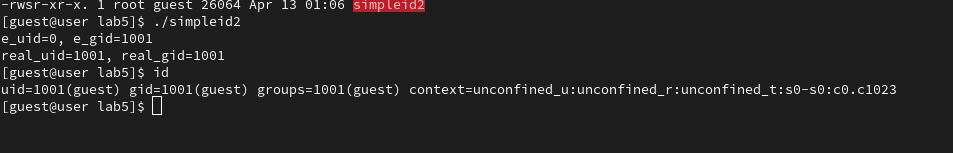


Рис. 8: Установка SetUID-бита

1. Я создал файл “readfile.c”. Внёс туда программу.

Рис. 9: Программа readfile

1. Скомпилировал программу readfile.

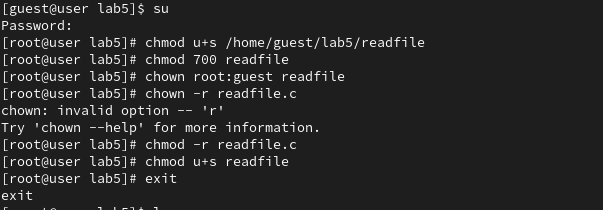


Рис. 10: Компиляция readfile

1. Я выдал программе “readfile” права так, чтобы root пользователь мог прочитать файл, а простой пользователь нет.

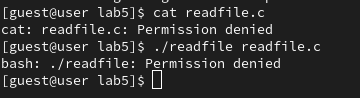


Рис. 11: Проверка на root u guest пользователях

1. Я сменил владельца программы “readfile” на root-пользователя.

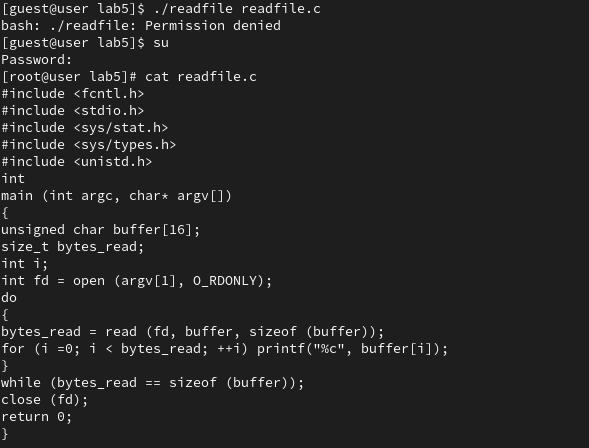


Рис. 12: Смена владельца

1. Попытался запустить программу и прочитать два файла с простого пользователя, но программа выдала ошибку. А если запускать с аккаунта root, то программа запускается нормально и работает. Связано это с тем, что владельцем программы является root-пользователь, а у других пользователей нет доступа и прав на использование программы.

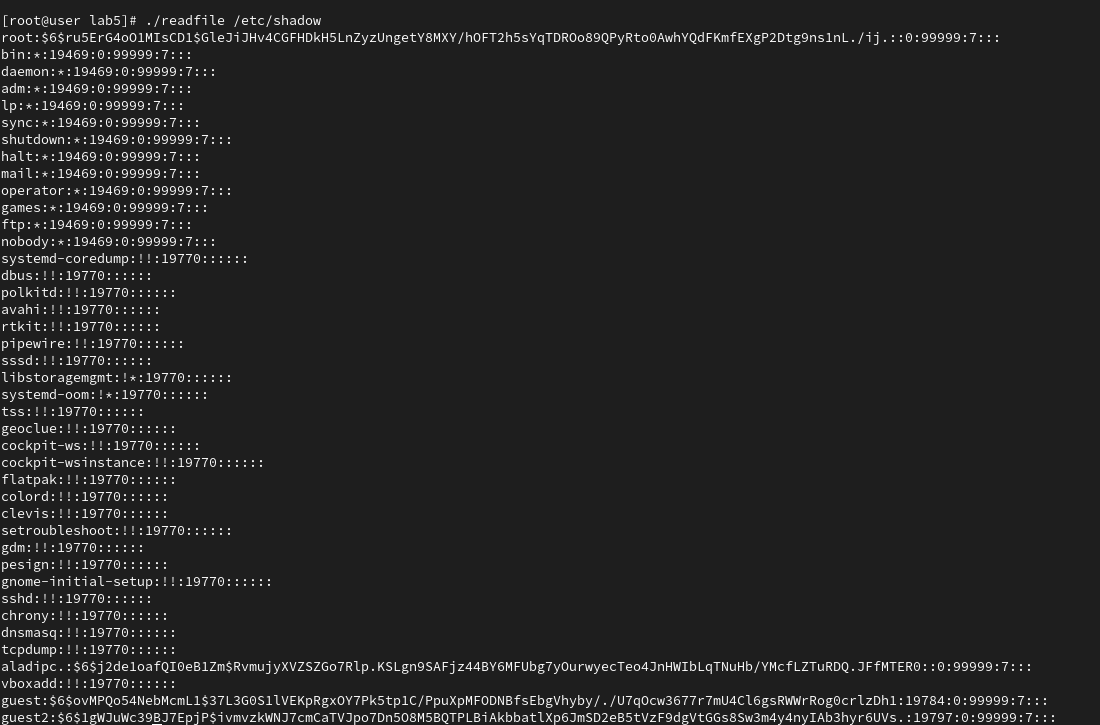


Рис. 13: Запуск с guest

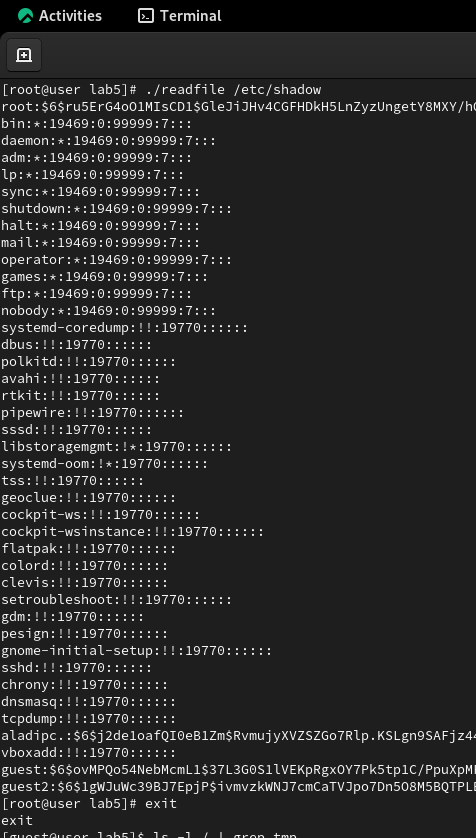


Рис. 14: Запуск с root

# 3 Исследование Sticky-бита.

1. Я выяснил, установлен ли атрибут Sticky (t) на директории “/tmp”. Атрибут установлен.

Рис. 15: Проверка наличия атрибута

Рис. 15: Проверка наличия атрибута

1. От пользователя “guest” я создал файл “file01.txt” в директории “/tmp”. Вписал в файл слово “test”. И дал права на чтение и запись для категории “все остальные (о)”.

Рис. 16: Выдача прав для файла

Рис. 16: Выдача прав для файла

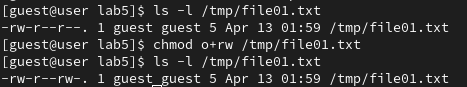


Рис. 17: Выдача прав для файла

1. От пользователя “guest2”, который не явлется владельцем, я попробовал прочитать файл. Я могу прочитать файл. Но не могу дописывать содержимое, вписывать новое или удалять этот файл.

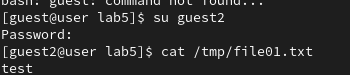


Рис. 18: Проверка от второго пользователя

1. я отключил атрибут “t” у директории “/tmp”. Попробовал повторить все предыдущие действия. Я так же не смог вписать в файл данные или дописать их. Но смог прочитать файл и удалить его.



Рис. 19: Проверка без атрибута

1. Чтобы в дальнейшем у меня не было проблем в работе с директорией “/tmp” я вернул атрибут на директорию, используя суперпользователя.



Рис. 20: Возвращение атрибута

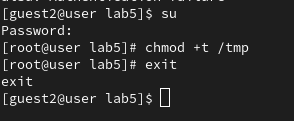


Рис. 21: Возвращение атрибута

# 4 ВАЖНОЕ ПРИМЕЧАНИЕ

По итогам лабораторной работы я понял, что Sticky-бит создан для защиты файла от удаления. Даже не смотря на то, что я дал права на запись и чтение файлов для категории “все остальные”, я не смог вписать в файл данные с пользователя “guest2”. А не смог я это сделать, так как этот аккаунт у меня находится в группе с “guest”. То есть я не дал права на вписывание для категории “группа”, но дал права для категории “все остальные”. Из-за этого Sticky-бит не влиял на возможность записи, а влиял только на возможность удаления. А изменять файл я не мог, так как мой аккаунт находился не в той группе. Если бы я использовал другой аккаунт, который не находится в группе, результаты бы были другие.

# 5 Выводы

Я изучил механизмы изменения идентификатора, применил SetUID-бит и Stickу-бит. Получил практические навыки работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователя, а так же влияние бита Sticky на запись и удаление файлов.

# Список литературы