Отчет по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Динькиев Валерий

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

1. Создание программы

1.1. Вошел в систему от имени пользователя guest.

1.2. Создал программу по шаблону из методички. (рис. 1)

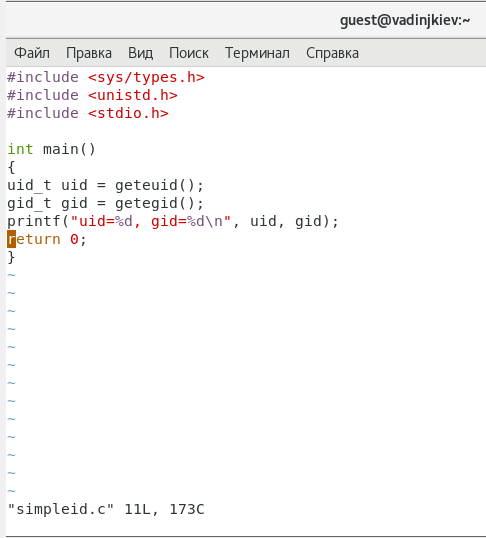


Figure 1: Программа simpleid.c

1.3. Скомплилировал программу и убедился, что файл программы создан (рис. 2)

1.4. Выполнил программу simpleid: (рис. 2)

1.5. Выполнил системную программу id (рис. 2)

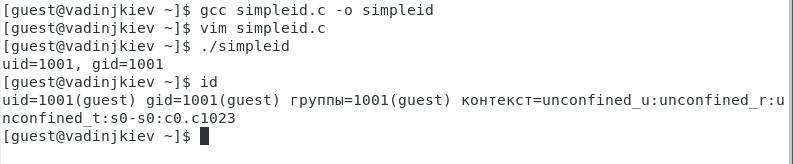


Figure 2: Компиляция и выполнение программы simpleid

1.6. Усложнил программу, добавив вывод действительных идентификаторов. Я отредактировал программу simpleid.c (рис. 3)



Figure 3: Отредактированная программа simpleid.c

1.7. Скомпилировал и запустил simpleid2.c (рис. 4)

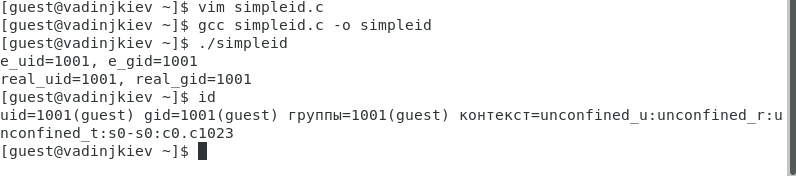


Figure 4: Компиляция и выполнение программы simpleid

1.8. От имени суперпользователя выполнил команды (рис. 5)

1.9. Повысил временно свои права с помощью su. (рис. 5) Первая команда меняет владельца файла, а вторая добавляет SetUID-бит.

1.10. Выполнил проверку правильности установки новых атрибутов и смены владельца файла simpleid2 (рис. 5) (рис. 6)

1.11. Запустил simpleid2 и id (рис. 5). Результаты совпадают.

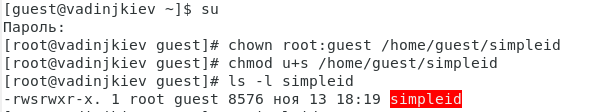


Figure 5: Смена пользователя, установка SetUID-бита



Figure 6: Выполнение программы simpleid и команды id

1.12. Проделал то же самое относительно SetGID-бита

1.13. Создал программу readfile.c по шаблону из методички. (рис. 7)

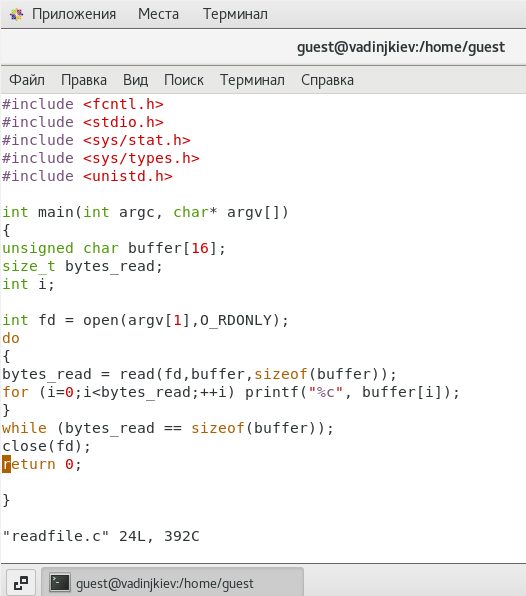


Figure 7: Программа readfile.c

1.14. Откомпилировал её (рис. 8)

1.15. Сменил владельца у файла readfile.c и изменил права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог. (рис. 8)

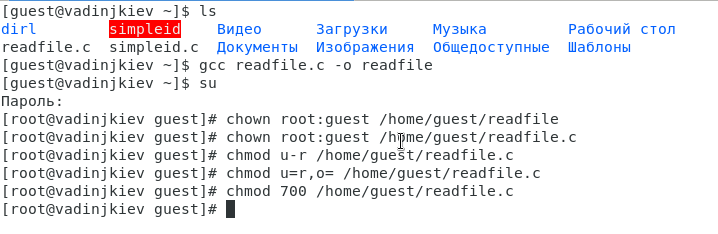


Figure 8: Работа с программой readfile.c

1.16. Проверил, что пользователь guest не может прочитать файл readfile.c. (рис. 9)

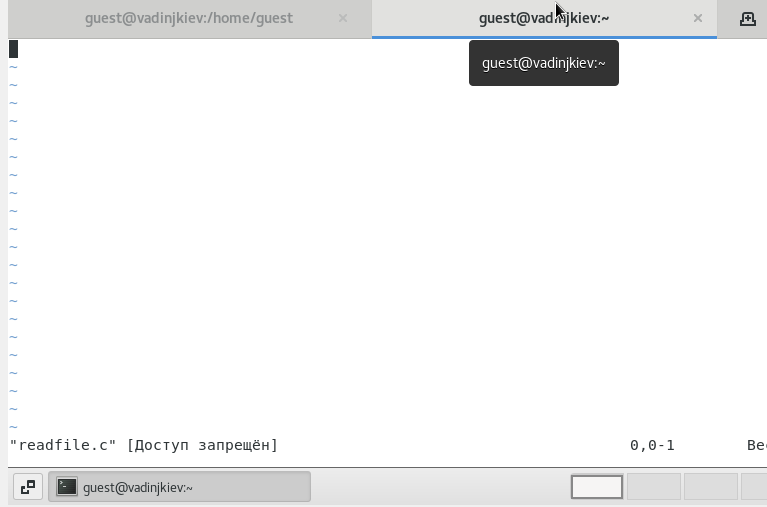


Figure 9: Проверка файла на чтение

1.17. Сменил у программы readfile владельца (рис. 8) и установил SetUID-бит (рис. **¿fig:010?**).

1.18. Проверил, может ли программа readfile прочитать файл readfile.c. (рис. 10)



Figure 10: Проверка чтения файла readfile.c и установка SetUid-бита

1.19. Проверил, может ли программа readfile прочитать файл /etc/shadow. (рис. 11)

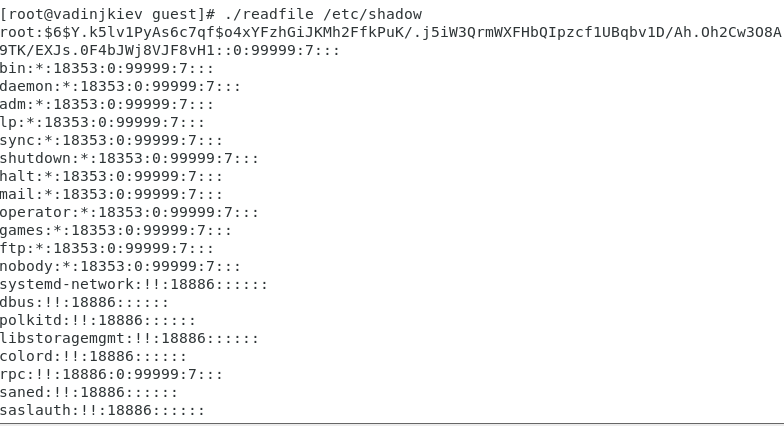


Figure 11: Проверка чтения файла /etc/shadow

1. Исследование Sticky-бита

2.1. Выяснил, установлен ли атрибут Sticky на директории /tmp, для чего выполнил команду (рис. 12)

2.2. От имени пользователя guest создал файл file01.txt в директории /tmp со словом test (рис. 12)

2.3. Просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные» (рис. 12)

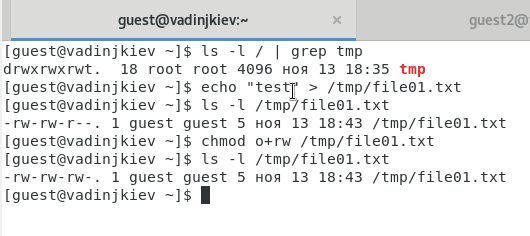


Figure 12: Исследование Sticky-бита от имени guest

2.4. От пользователя guest2 (не являющегося владельцем) попробовал прочитать файл /tmp/file01.txt. (рис. 13)

2.5. От пользователя guest2 попробовал дозаписать в файл /tmp/file01.txt слово test2 командой. (рис. 13) Операция прошла успешно.

2.6. Проверил содержимое файла командой (рис. 13)

2.7. От пользователя guest2 попробовал записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой (рис. 13) Операция прошла успешно.

2.8. Проверил содержимое файла командой (рис. 13)

2.9. От пользователя guest2 попробовал удалить файл /tmp/file01.txt командой (рис. 13) Операция была не позволена.

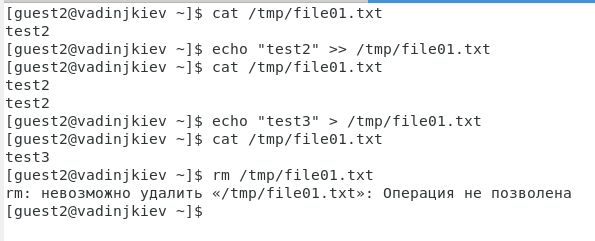


Figure 13: Работа с file01.txt от имени guest2 при наличии Sticky-бита

2.10. Повысил свои права до суперпользователя следующей командой и выполнил после этого команду, снимающую атрибут t (Sticky-бит) с директории (рис. 14)

2.11. Покинул режим суперпользователя командой. (рис. 14)

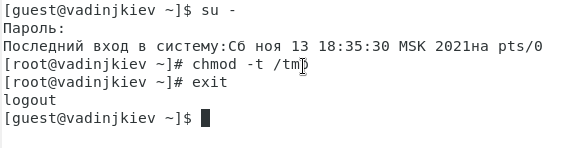


Figure 14: Снятие Sticky-бита c директории /tmp

2.12. От пользователя guest2 проверил, что атрибута t у директории /tmp. (рис. 15)

2.13. Повторил предыдущие шаги. (рис. 15) Теперь удалось удалить файл.

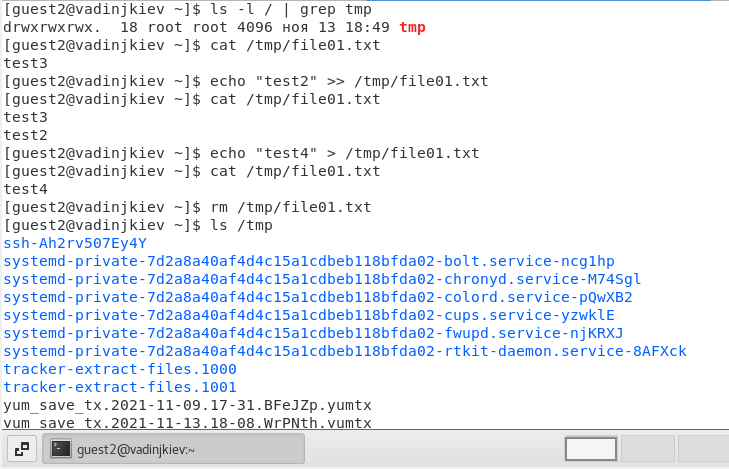


Figure 15: Работа с file01.txt от имени guest2 без Sticky-бита

2.14. Удалось удалить файл от имени пользователя, не являющегося его владельцем.

2.15. Повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp (рис. 16)

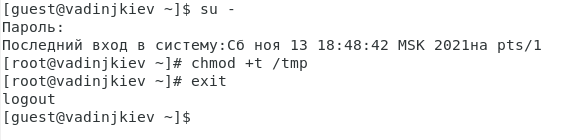


Figure 16: Возвращение Sticky-бита на /tmp

# Выводы

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