Отчет по лабораторной работе №5

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Каримов Зуфар НПИ-01-18

Содержание

[Цель работы 1](#_Toc87713473)

[Последовательность выполнения работы 1](#_Toc87713474)

[Создание программы 1](#_Toc87713475)

[Исследование Sticky-бита 9](#_Toc87713476)

[Выводы 12](#_Toc87713477)

# 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.

# Последовательность выполнения работы

## Создание программы

Для начала нам следовало установить компилятор gcc. (рис. 1)

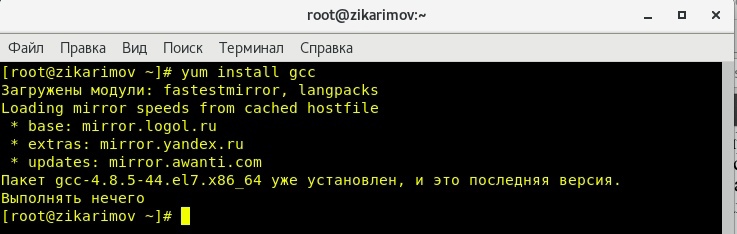


Figure 1: Компилятор gcc

Чтобы защита SELinux не мешала выполнению заданий работы, мы отключили ее. (рис. 2)

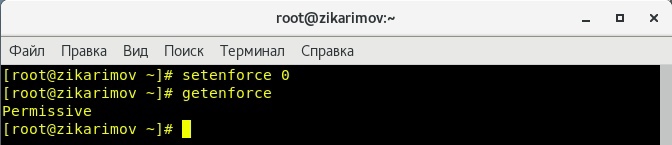


Figure 2: Отключение защиты

1. Войдите в систему от имени пользователя guest.
2. Создайте программу simpleid.c: (рис. 3) (рис. 4)

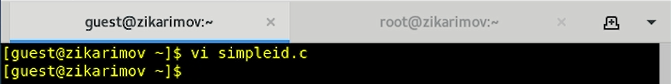


Figure 3: Программа simpleid.c

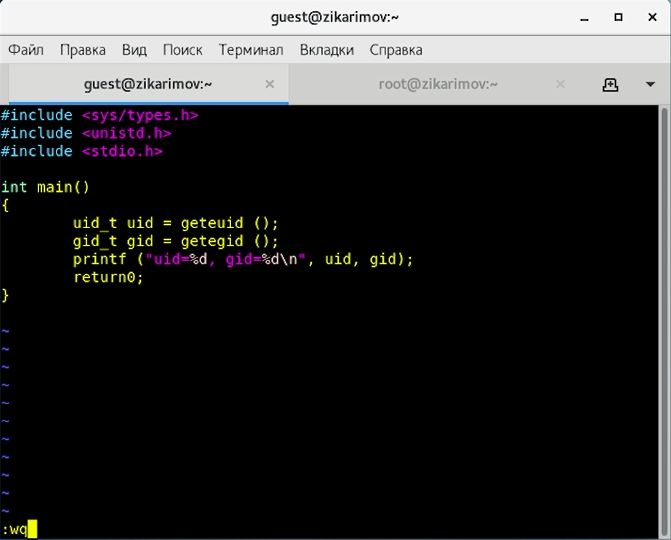


Figure 4: Программа simpleid.c

1. Скомплилируйте программу и убедитесь, что файл программы создан:

gcc simpleid.c -o simpleid

1. Выполните программу simpleid:

./simpleid

1. Выполните системную программу id:

id

и сравните полученный вами результат с данными предыдущего пункта задания. (рис. 5)

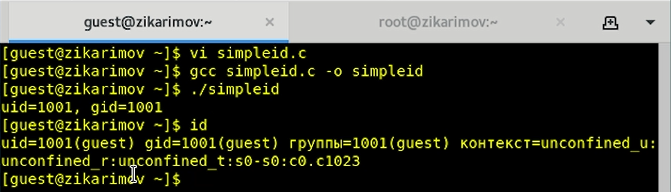


Figure 5: Компиляция и выполнения программы

1. Усложните программу, добавив вывод действительных идентификаторов: (рис. 6) (рис. 7)

Figure 6: Программа simpleid2.c

Figure 6: Программа simpleid2.c

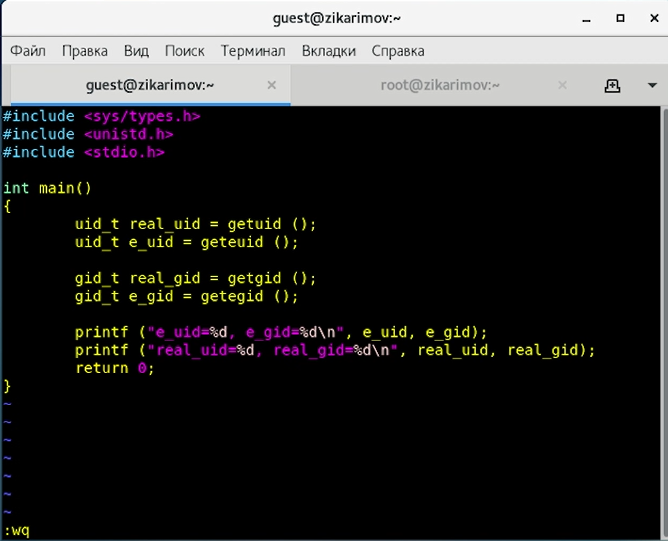


Figure 7: Программа simpleid2.c

1. Скомпилируйте и запустите simpleid2.c:

gcc simpleid2.c -o simpleid2

./simpleid2 (рис. 8)

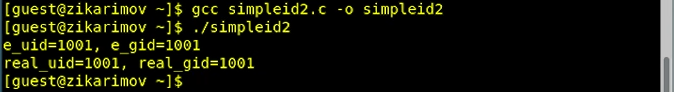


Figure 8: Компиляция и выполнения программы

1. От имени суперпользователя выполните команды:

chown root:guest /home/guest/simpleid2

chmod u+s /home/guest/simpleid2 (рис. 9)

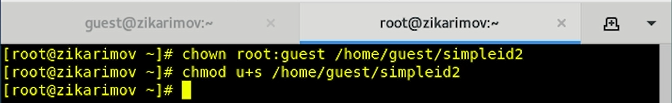


Figure 9: Смена пользователя и установка SetU’D-бита

1. Используйте sudo или повысьте временно свои права с помощью su. Поясните, что делают эти команды.

Команда sudo позволяет пользователям выполнять указанные программы с административными привилегиями без ввода пароля суперпользователя root.

1. Выполните проверку правильности установки новых атрибутов и смены владельца файла simpleid2:

ls -l simpleid2

1. Запустите simpleid2 и id:

./simpleid2

id

Сравните результаты. (рис. 10)

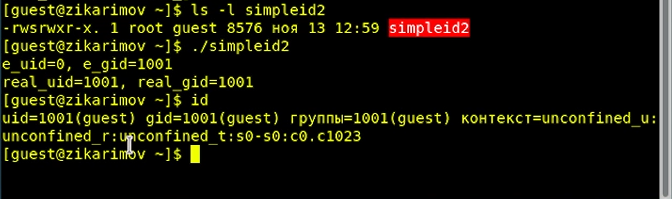


Figure 10: Проверка правильности установки новых атрибутов

1. Проделайте тоже самое относительно SetGID-бита. (рис. 11) (рис. 12)

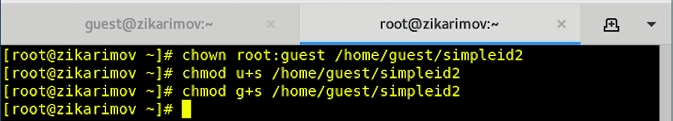


Figure 11: Проверка правильности установки новых атрибутов

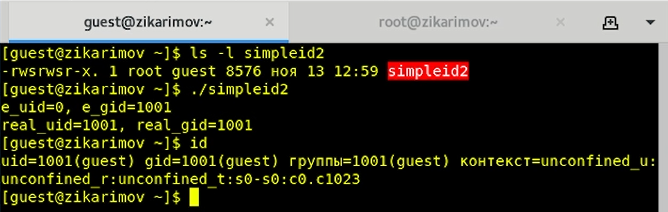


Figure 12: Проверка правильности установки новых атрибутов

1. . Создайте программу readfile.c: (рис. 13)

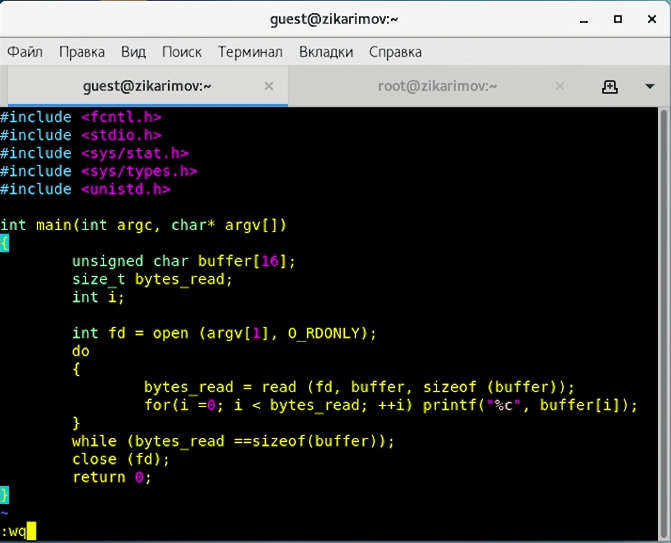


Figure 13: Программа readfile.c

1. Откомпилируйте её.

gcc readfile.c -o readfile (рис. 14)

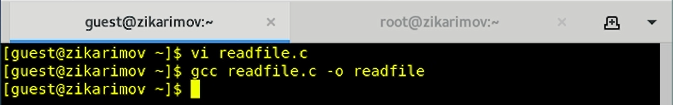


Figure 14: Программа readfile

1. Смените владельца у файла readfile.c (или любого другого текстового файла в системе) и измените права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог (рис. 15)

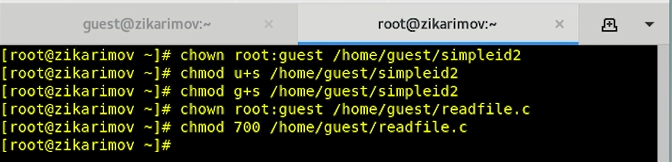


Figure 15: Смена владельца и изменения прав

1. Проверьте, что пользователь guest не может прочитать файл readfile.c. (рис. 16)

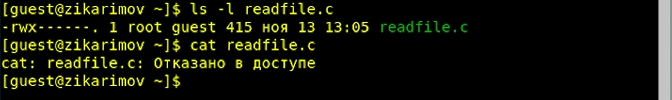


Figure 16: Проверка на правильность

1. Смените у программы readfile владельца и установите SetU’D-бит. (рис. 17)

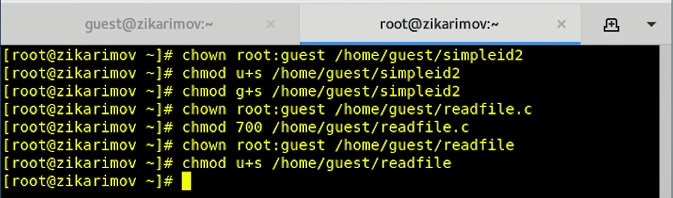


Figure 17: Смена пользователя и установка SetU’D-бита

1. Проверьте, может ли программа readfile прочитать файл readfile.c? (рис. 18) (рис. 19)

Figure 18: Проверка на правильность

Figure 18: Проверка на правильность

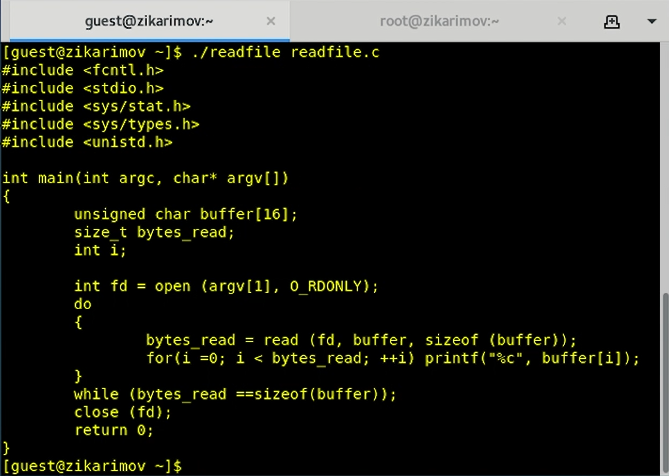


Figure 19: Чтения файла

1. Проверьте, может ли программа readfile прочитать файл /etc/shadow?

Отразите полученный результат и ваши объяснения в отчёте. (рис. 20)

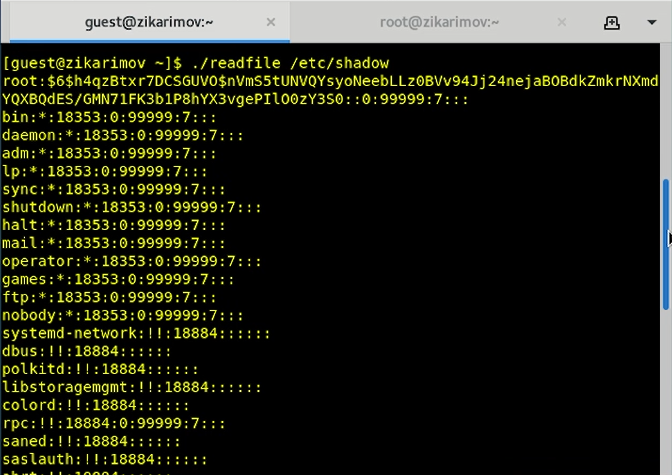


Figure 20: Чтения файла

## Исследование Sticky-бита

1. Выясните, установлен ли атрибут Sticky на директории /tmp, для чего выполните команду

ls -l / | grep tmp

1. От имени пользователя guest создайте файл file01.txt в директории /tmp со словом test:

echo “test” > /tmp/file01.txt

1. Просмотрите атрибуты у только что созданного файла и разрешите чтение и запись для категории пользователей «все остальные»:

ls -l /tmp/file01.txt

chmod o+rw /tmp/file01.txt

ls -l /tmp/file01.txt (рис. 21)

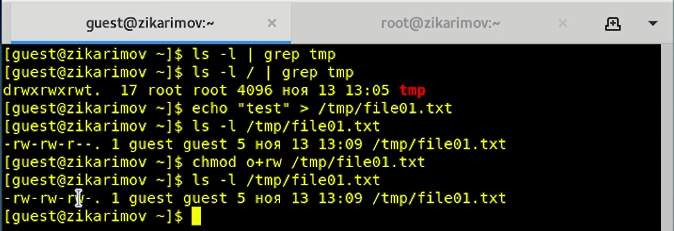


Figure 21: Просмотр атрибутов и разрешения прав

1. От пользователя guest2 (не являющегося владельцем) попробуйте прочитать файл /tmp/file01.txt:

cat /tmp/file01.txt

1. От пользователя guest2 попробуйте дозаписать в файл /tmp/file01.txt слово test2 командой

echo “test2” > /tmp/file01.txt

Удалось ли вам выполнить операцию? Да, удалось.

1. Проверьте содержимое файла командой

cat /tmp/file01.txt

1. От пользователя guest2 попробуйте записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой

echo “test3” > /tmp/file01.txt

Удалось ли вам выполнить операцию? Да, удалось выполнить операцию.

1. Проверьте содержимое файла командой

cat /tmp/file01.txt

1. От пользователя guest2 попробуйте удалить файл /tmp/file01.txt командой

rm /tmp/fileOl.txt

Удалось ли вам удалить файл? Нет, не удалось удалить файл. (рис. 22)

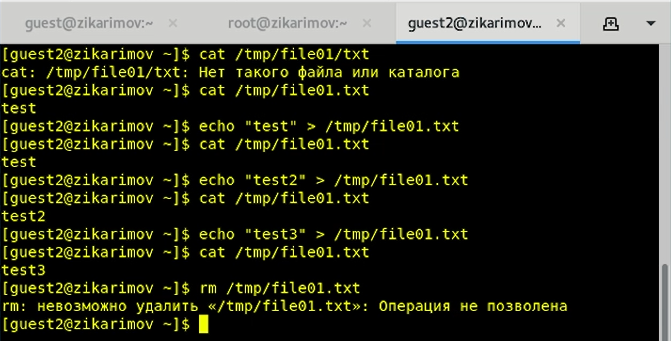


Figure 22: Просмотр атрибутов и разрешения прав

1. Повысьте свои права до суперпользователя следующей командой

su -

и выполните после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp:

chmod -t /tmp (рис. 23)

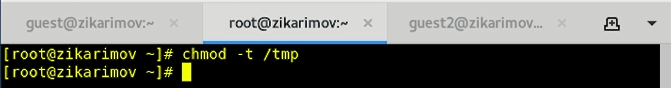


Figure 23: Просмотр атрибутов и разрешения прав

1. Покиньте режим суперпользователя командой

exit

1. От пользователя guest2 проверьте, что атрибута t у директории /tmp нет:

ls -l / | grep tmp (рис. 24)

Figure 24: Просмотр атрибутов и разрешения прав

Figure 24: Просмотр атрибутов и разрешения прав

1. Повторите предыдущие шаги. Какие наблюдаются изменения?
2. Удалось ли вам удалить файл от имени пользователя, не являющегося его владельцем? Ваши наблюдения занесите в отчёт. (рис. 25)

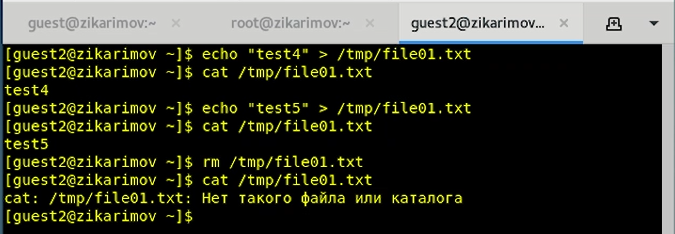


Figure 25: Просмотр атрибутов и разрешения прав

Да, удалось удалить файл от имени пользователя, не являющегося его владельцем.

1. Повысьте свои права до суперпользователя и верните атрибут t на директорию /tmp:

su -

chmod +t /tmp

exit (рис. 26)

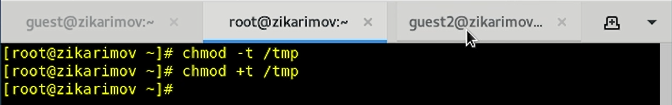


Figure 26: Просмотр атрибутов и разрешения прав

# Выводы

Изучил механизмы изменения идентификаторов, примененив SetUID- и Sticky-биты. Получил практические навыкы работы в консоли с дополнительными атрибутами. Рассмотрел работы механизмов смены идентификаторов процесса пользователей, а также влияние бита Sticky на запись и удаление файлов.