Лабораторная работа №5

Основы информационной безопасности

Сабралиева Марворид Нуралиевна

Содержание

# 1 Цель работы

Изучение механизмов изменения идентификаторов, применения SetUID- и Sticky-битов. Получение практических навыков работы в кон- соли с дополнительными атрибутами. Рассмотрение работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# 2 Выполнение лабораторной работы

## 2.1 Подготовка

1. Для выполнения части заданий потребуются средства разработки приложений. В частности, при подготовке стенда следует убедиться, что в системе установлен компилятор gcc. У меня его не было, поэтому я установила компилятор
2. Система защиты SELinux не должна мешать выполнению заданий работы. Если вы не знаете, что это такое, просто отключите систему запретов до очередной перезагрузки системы командой setenforce 0
3. Команда getenforce выводит Permissive.



Figure 1: Подготовка

## 2.2 Изучение механики SetUID

1. Вошли в систему от имени пользователя guest. (рис. [2](#fig:002)).



Figure 2: Создание программы

1. Создаем программу simpleid.c: (рис. [3](#fig:003)).

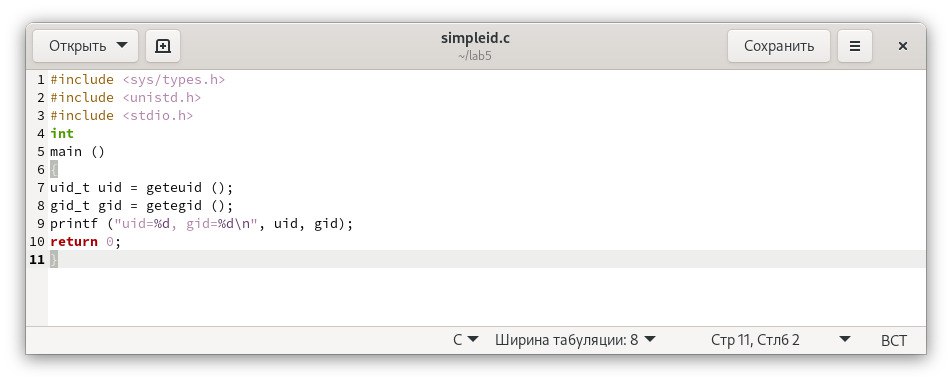


Figure 3: Заполнение программы

1. Скомплилируем программу и убедимся, что файл программы создан: gcc simpleid.c -o simpleid
2. Выполним программу simpleid: ./simpleid
3. Выполним системную программу id: id и сравните полученный вами результат с данными предыдущего пункта задания. uid и gid совпадают в обеих программах (рис. [4](#fig:004)).



Figure 4: Результат программы simpleid

1. Усложним программу, добавив вывод действительных идентификаторов Получившуюся программу назовем simpleid2.c. (рис. [5](#fig:005)).

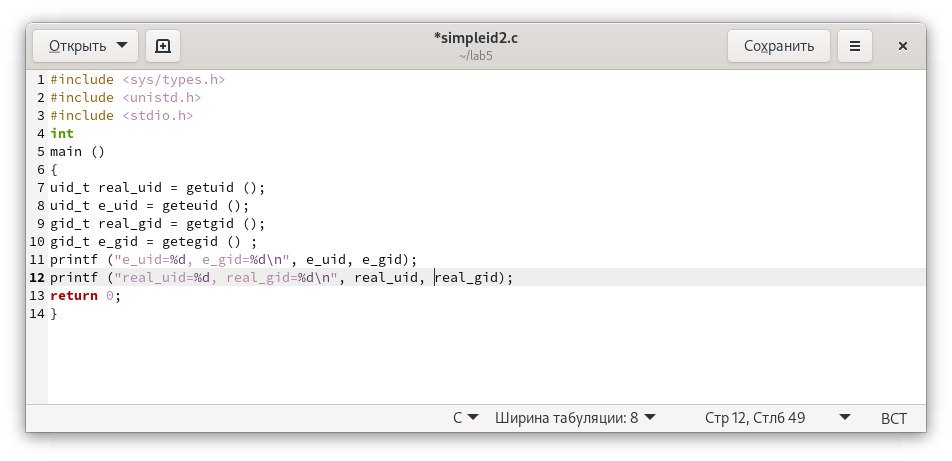


Figure 5: Программа simpleid2

1. Скомпилируем и запустим simpleid2.c: gcc simpleid2.c -o simpleid2 ./simpleid2 (рис. [6](#fig:006)).

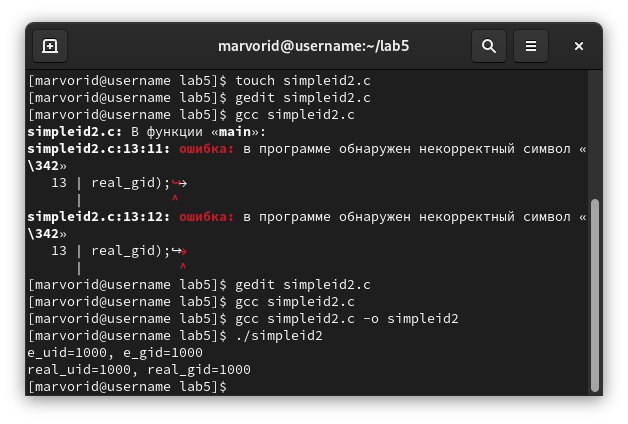


Figure 6: Результат программы simpleid2

1. От имени суперпользователя выполним команды (рис. [7](#fig:007)): chown root:guest /home/guest/simpleid2 chmod u+s /home/guest/simpleid2

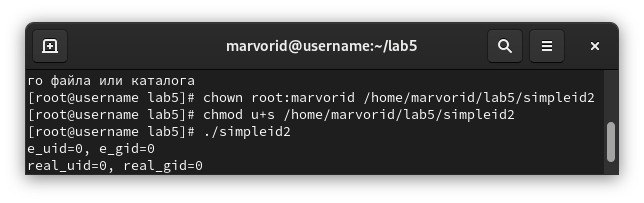


Figure 7: Выполнение команд

1. Используем su для повышения своих прав.
2. Выполним проверку правильности установки новых атрибутов и смены владельца файла simpleid2: ls -l simpleid2
3. Запустим simpleid2 и id: ./simpleid2 id Результаты выполнения теперь немного отличаются
4. Проделаем тоже самое относительно SetGID-бита. (рис. [8](#fig:008)).

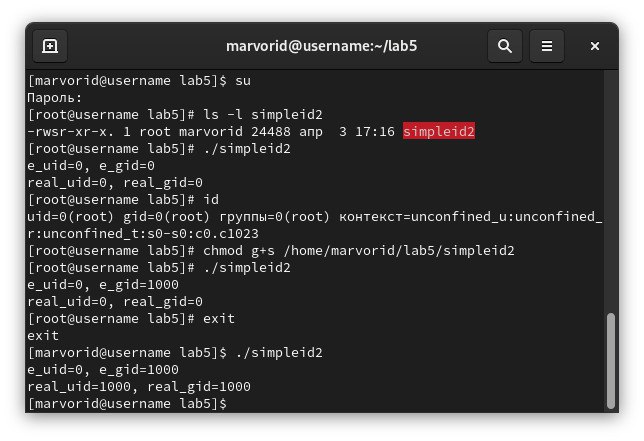


Figure 8: Выполнение команд

1. Создадим программу readfile.c (рис. [9](#fig:009)).

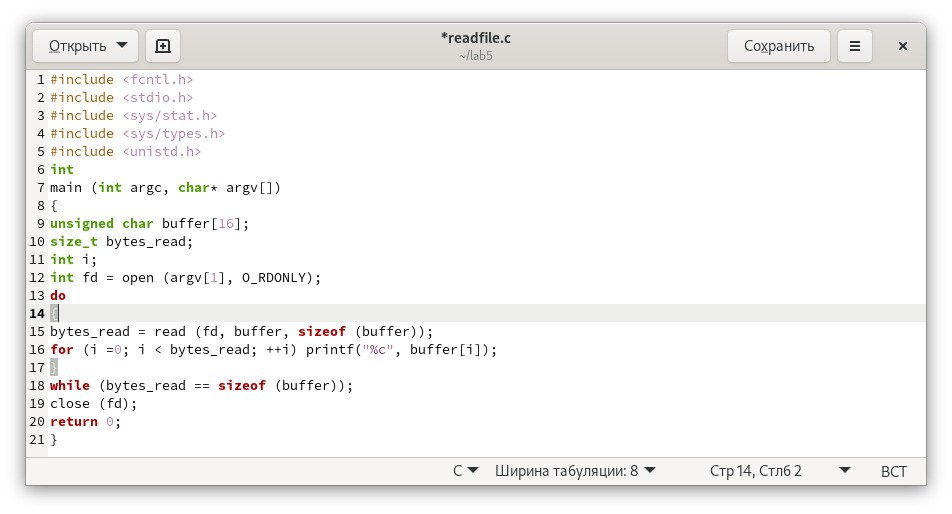


Figure 9: программа readfile.c

1. Откомпилируем её. gcc readfile.c -o readfile (рис. [10](#fig:010)).
2. Смениим владельца у файла readfile.c и изменим права так, чтобы только суперпользователь (root) мог прочитать его, a пользователь не мог.
3. Проверили, что пользователь не может прочитать файл readfile.c.
4. Сменим у программы readfile владельца и установим SetU’D-бит.
5. Проверили, может ли программа readfile прочитать файл readfile.c?
6. Проверили, может ли программа readfile прочитать файл /etc/shadow

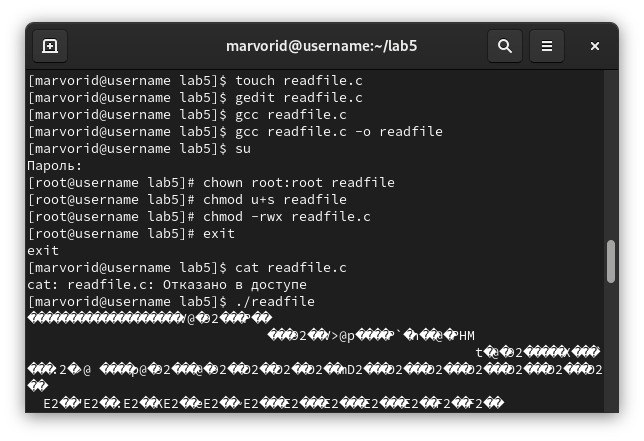


Figure 10: Скомпилируем программу readfile.c

## 2.3 Исследование Sticky-бита

1. Выяснили, что установлен атрибут Sticky на директории /tmp, для чего выполните команду ls -l / | grep tmp
2. От имени пользователя создали файл file01.txt в директории tmp со словом test: echo “test” > /tmp/file01.txt
3. Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные»: ls -l /tmp/file01.txt chmod o+rw /tmp/file01.txt ls -l /tmp/file01.txt
4. От пользователя guest2 (не являющегося владельцем) попробовали прочитать файл /tmp/file01.txt: cat /tmp/file01.txt
5. От пользователя guest2 попробовали дозаписать в файл /tmp/file01.txt слово test2 командой echo “test2” > /tmp/file01.txt операцию не удалась
6. Проверили содержимое файла командой cat /tmp/file01.txt
7. От пользователя guest2 попробовали записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию ко- мандой echo “test3” > /tmp/file01.txt
8. Проверили содержимое файла командой cat /tmp/file01.txt
9. От пользователя guest2 попробовали удалить файл /tmp/file01.txt командой rm /tmp/fileOl.txt, но получили отказ
10. Повысили свои права до суперпользователя следующей командой su - и выполнили после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp: chmod -t /tmp
11. Покинули режим суперпользователя командой exit
12. От пользователя guest2 проверили, что атрибута t у директории /tmp нет: ls -l / | grep tmp
13. Повторили предыдущие шаги.
14. Удалось удалить файл от имени пользователя не являющегося владельцем.

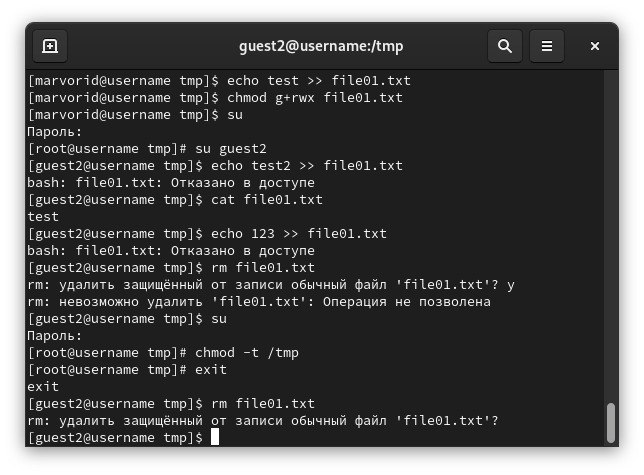


Figure 11: Выполнение команд

1. Повысили свои права до суперпользователя и вернули атрибут t на директорию /tmp: su - chmod +t /tmp exit



Figure 12: Повышение прав

# 3 Выводы

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

# Список литературы