Лабораторная работа № 5

Дисциплина: Информационная безопасность

Сулицкий Богдан Романович

Содержание

# 1 Цель работы

Целью данной лабораторной работы является 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

## 2.1 Создание программы

1. Я вошёл в систему от имени пользователя guest(??).

Создание файла и и последующее редактирование в emacs

Рис. 1: Создание файла и и последующее редактирование в emacs

И создал программу simpleid.c(??).



Рис. 2: Код программы в редакторе Emacs

1. Я скомпилировал и выполнил программу simpleid. Далее я выполнил системную программу id(??).

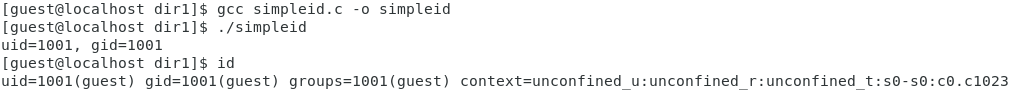


Рис. 3: Успешная компиляция и запуск simpleid. Запуск системной программы id

Данные, выведенные simpleid и id совпадают.

1. Я скопировал файл simpleid.c для последующего редактирования(??). Копирование файла и и последующее редактирование в emacs

И усложнил программу, добавив вывод действительных идентификаторов(??).

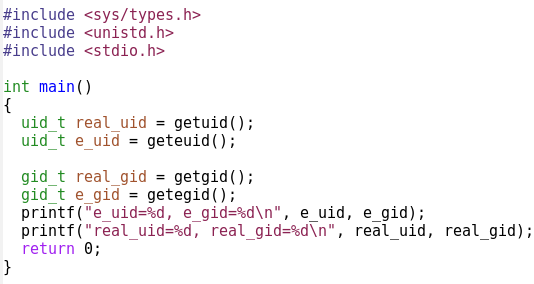


Рис. 4: Код программы в редакторе Emacs

1. Я скомпилировал и запустил simpleid2.c(??).

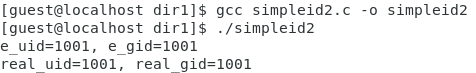


Рис. 5: Успешная компиляция

1. От имени суперпользователя я выполнил команды:

chown root:guest /home/guest/simpleid2  
chmod u+s /home/guest/simpleid2

Далее я выполнил проверку правильности установки новых атрибутов и смены владельца файла simpleid2, после чего запустил simpleid2 и id. И проделал то же самое относительно SetGID-бита(??).

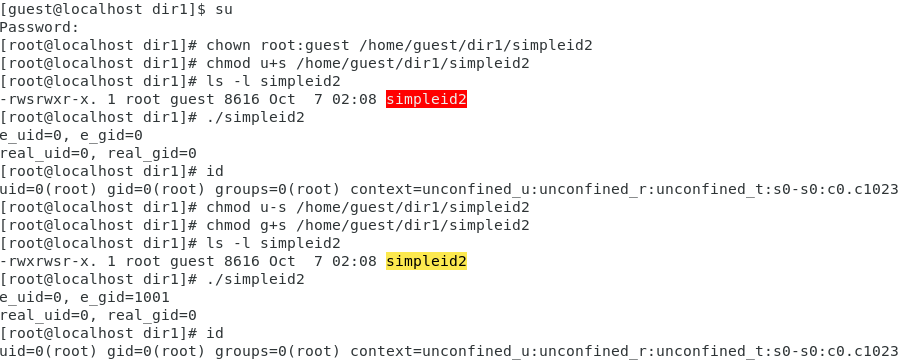


Рис. 6: Успешная компиляция с новым владельцем файла

1. Я создал программу readfile.c(??).

Создание файла и и последующее редактирование в emacs

Рис. 7: Создание файла и и последующее редактирование в emacs

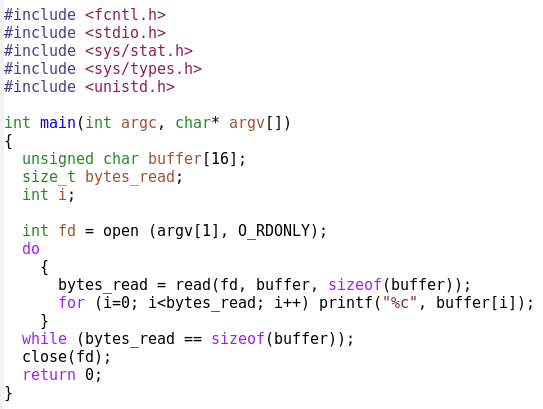


Рис. 8: Код программы в редакторе Emacs

И успешно скомпилировал её (??).

Успешная компиляция

Рис. 9: Успешная компиляция

1. Я сменил владельца у файла readfile.c и изменил права так, чтобы только суперпользователь (root) мог прочитать его, a guest не мог, после чего проверил, что пользователь guest не может прочитать файл readfile.c(??).

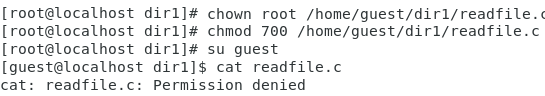


Рис. 10: Смена прав и владельца и проверка чтения файла

1. Я сменил у программы readfile владельца и установил SetU’D-бит, после чего проверил, может ли программа readfile прочитать файлы readfile.c и /etc/shadow(??).

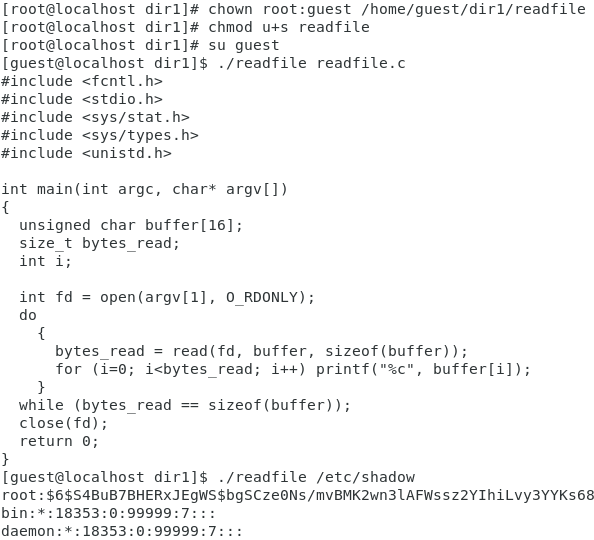


Рис. 11: Смена прав и владельца и проверка функционала файла

## 2.2 Исследование Sticky-бита

1. Я выяснил, установлен ли атрибут Sticky на директории /tmp(??).

Смена прав и владельца и проверка функционала программы

Рис. 12: Смена прав и владельца и проверка функционала программы

1. От имени пользователя guest я создал файл file01.txt в директории /tmp со словом test, далее просмотрел атрибуты у только что созданного файла и разрешил чтение и запись для категории пользователей «все остальные»(??).

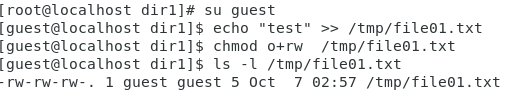


Рис. 13: Создание файла и проверка его атрибутов

1. От пользователя guest2 я прочитал файл /tmp/file01.txt и дозаписал в файл слово test. Далее я записал в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию и проверил содержимое файла командой. Я попробовал удалить файл file01.txt(??).

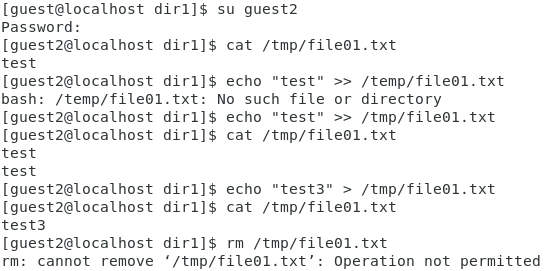


Рис. 14: Редактирование файла

Однако в ответ я получил отказ от выполнения операции.

1. Я повысил свои права до суперпользователя, затем снял атрибут t с директории /tmp, после чего покинул режим суперпользователя командой exit(??).

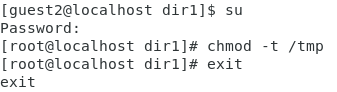


Рис. 15: Удаление атрибута /tmp в режиме суперпользователя

1. Я от имени пользователя guest2 проверил, что атрибута t у директории /tmp нет, после чего повторил те же действия. Теперь я могу удалить файл file01.txt(??).

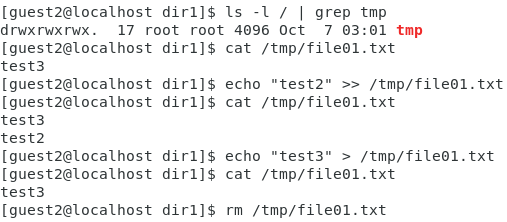


Рис. 16: Редактирование файла в режиме суперпользователя

1. Я повысил свои права до суперпользователя и вернул атрибут t на директорию /tmp(??).

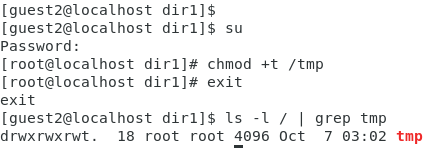


Рис. 17: Добавление атрибута /tmp в режиме суперпользователя

# 3 Вывод

В ходе проделанной работы я изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, получил практических навыков работы в консоли с дополнительными атрибутами, а также рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# Список литературы

[1] (https://esystem.rudn.ru/pluginfile.php/2090279/mod\_resource/content/2/005-lab\_discret\_sticky.pdf)