Лабораторная работа №5

Основы информационной безопасности

Серёгина Ирина Андреевна

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. Проверяю, установлен ли у меня gcc (рис. 2.1).

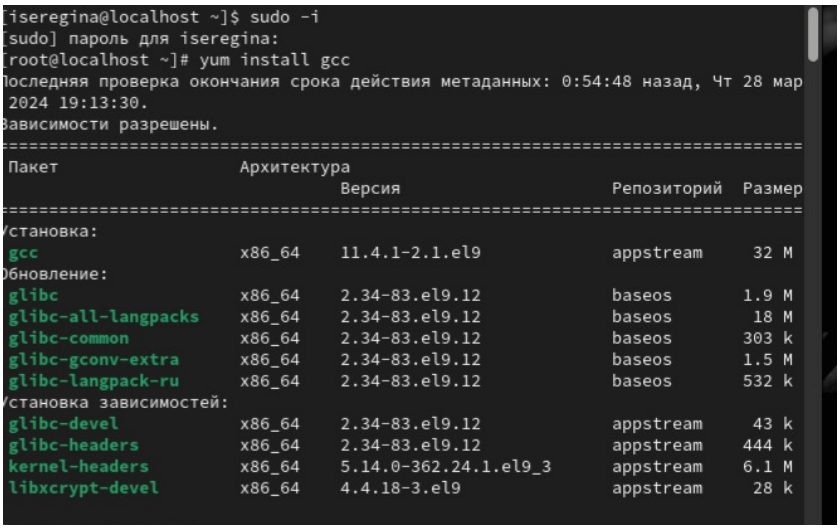

Рис. 2.1: gcc установлен

2. Отключаю систему запретов до следующей перезагрузки системы (рис. 2.2).

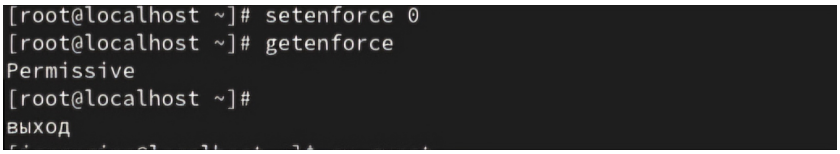

Рис. 2.2: отключаю систему запретов

3. Вхожу от имени пользователя guest (рис. 2.3).

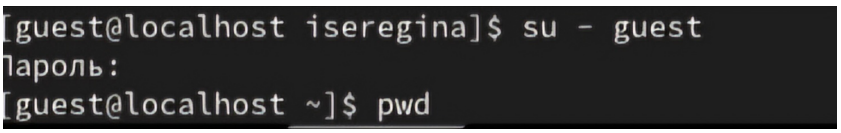

Рис. 2.3: пользователь guest

4. Создаю программу simpleid.c (рис. 2.4).

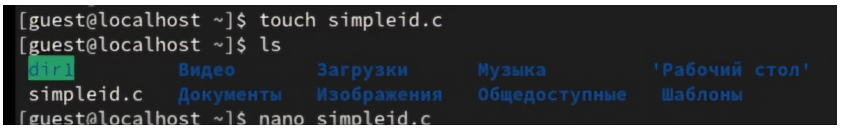

Рис. 2.4: создание программы

5. Заполняю программу (рис. 2.5).

Рис. 2.5: simpleid.c

6. Компилирую файл и выполняю системную программу id (рис. 2.6).

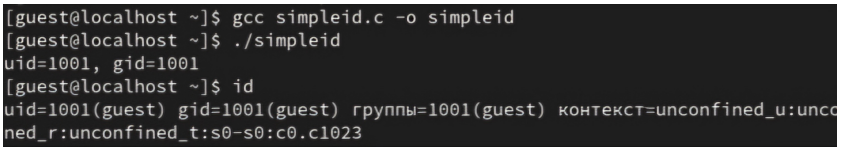

Рис. 2.6: запускаю программу

7. Усложняю программу (рис. 2.7).

Рис. 2.7: измененная программа

8. Компилирую и запускаю программу (рис. 2.8).

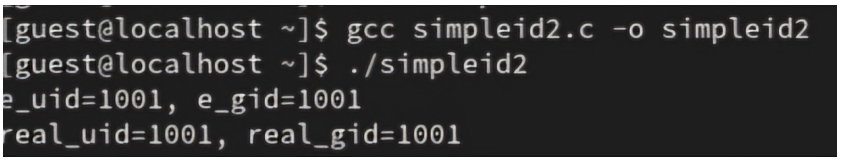

Рис. 2.8: запускаю программу

9. Выполняю следующие команды от лица суперпользователя, после чего выполняю проверку правильности запуска (рис. 2.9).

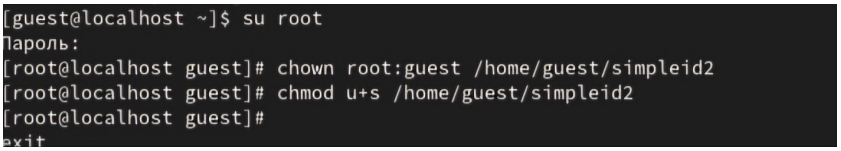

Рис. 2.9: выполняю команды от имени суперпользователя

10. Запускаю simpleid и id (рис. 2.10).

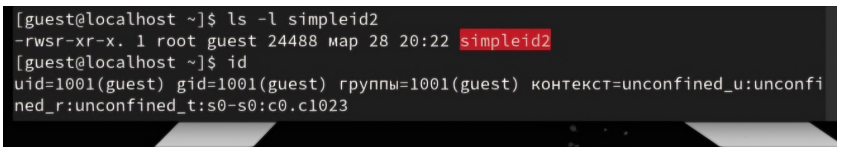

Рис. 2.10: simpleid.c и id

11. Создаю программу readfile.c, компилирую её (рис. 2.11).

Рис. 2.11: readfile.c

12. Меняю владельца файла, чтобы прочитать можно было только от лица суперпользователя (рис. 2.12).

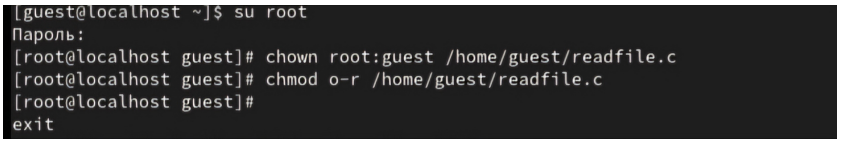

Рис. 2.12: меняю владельца файла

13. Readfile может прочитать файл /etc/shadow (рис. 2.13).

Рис. 2.13: /etc/shadow

14. Выясняю, установлен ли атрибут sticky на /tmp, создаю файл file01.txt, просматриваю его атрибуты (рис. 2.14).

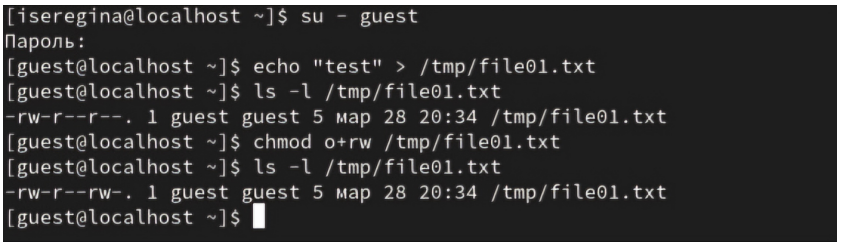

Рис. 2.14: проверяю наличие атрибута

15. От имени пользователя, не являющегося владельцем пробую прочитать и изменить файл. Не могу также удалить его (рис. **??**).

пробую выполнить действия с файлом

16. От имени суперпользователя убираю атрибут t с директории (рис. 2.15).

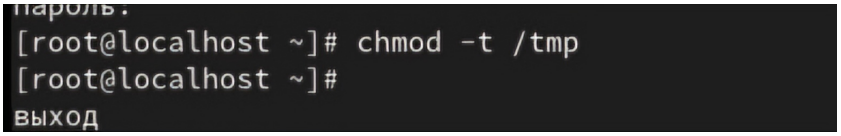

Рис. 2.15: убираю атрибут с директории

17. Файл удалился (рис. 2.16).

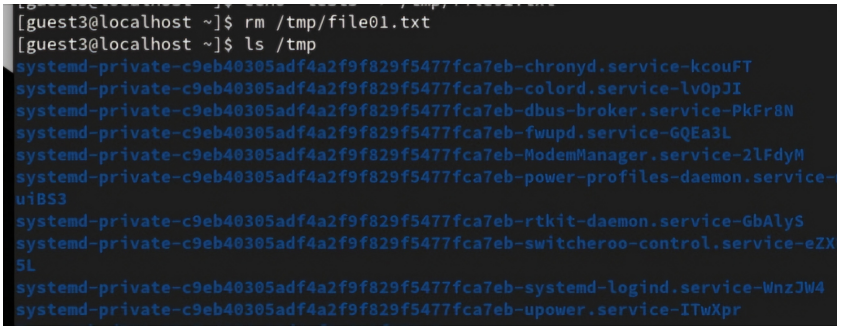

Рис. 2.16: файл удален

18. Возвращаю атрибут t (рис. 2.17).

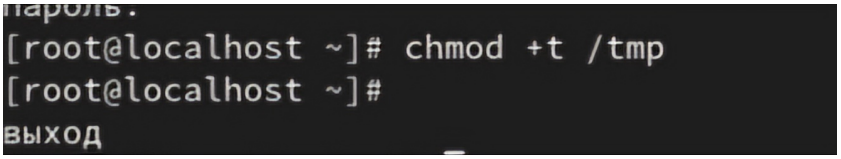

Рис. 2.17: возвращаю атрибут

3 Выводы

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

Список литературы