Лабораторная работа 5

Попов Дмитрий Павлович, НФИбд-01-19

Содержание

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

дисциплина: Информационная безопасность

Преподователь: Кулябов Дмитрий Сергеевич

Студент: Попов Дмитрий Павлович

Группа: НФИбд-01-19

МОСКВА

2022 г.

# 1 **Цель работы**

Изучение механизмов изменения идентификаторов, применения SetUID и Sticky-битов.

# 2 **Выполнение лабораторной работы**

1. Создал программу simpleid.c (Рис fig. 1).

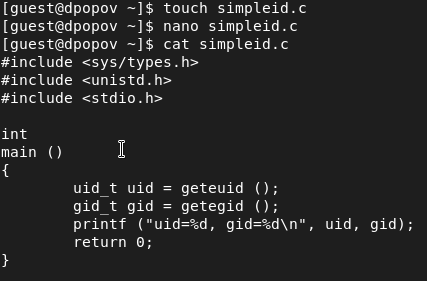


Figure 1: simpleid

1. Скомпилировал и выполнил программу. Сравнил с id. Как видим, результат работы команд - одинаковый (Рис fig. 2).

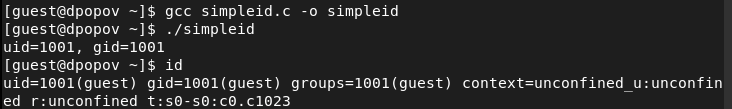


Figure 2: compile and run

1. Усложнил программу, добавив вывод действительных идентификаторов (Рис fig. 3).

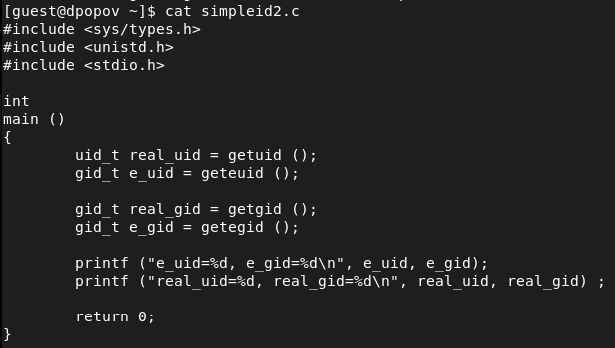


Figure 3: simpleid2.c

1. Скомпилировал и запустил simpleid2.c (Рис fig. 4).

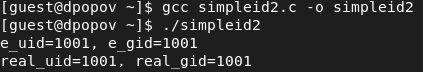


Figure 4: simpleid2

1. От имени суперпользователя выполнил команды (Рис fig. 5)

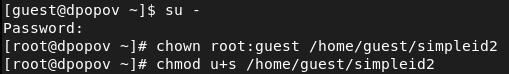


Figure 5: chmod

1. Запустил simpleid2 и id (Рис fig. 6)

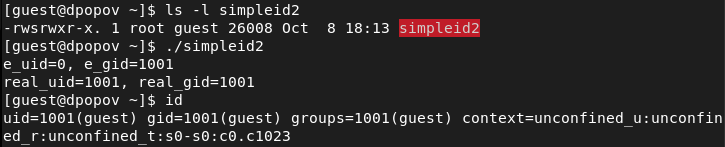


Figure 6: simpleid2 run

1. Создал программу readfile.c: (Рис fig. 7)

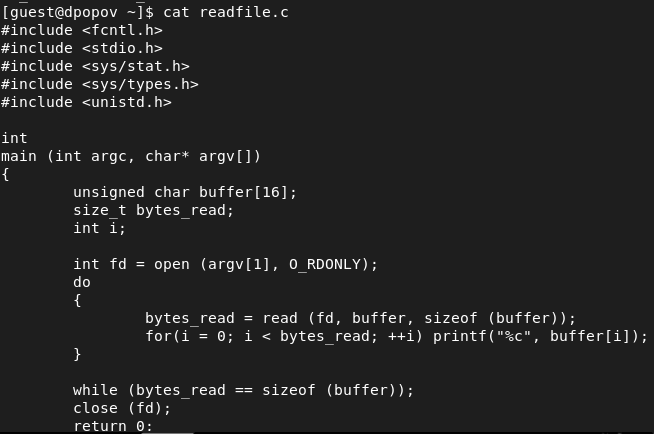


Figure 7: readfile.c

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

Figure 8: chown

Figure 8: chown

1. guest не может прочитать файл readfile.c (Рис fig. 9)

Figure 9: can not read

Figure 9: can not read

1. Сменил у программы readfile владельца и установил SetU’D-бит (Рис fig. 10)

Figure 10: readfile

Figure 10: readfile

1. Проверил прочитать файл readfile и /etc/shadow (Рис fig. 11 и fig. 12)

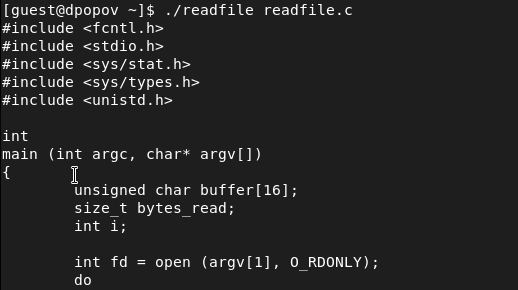


Figure 11: readfile read

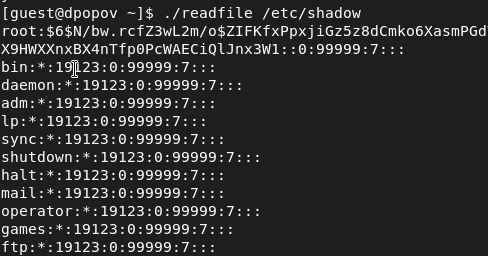


Figure 12: /etc/shadow read

1. readfile удалось прочитать, /etc/shadow - тоже удалось
2. Проверил sticky бит на категории tmp. Создал файл в tmp от guest и посмотерл атрибуты (Рис fig. 13).

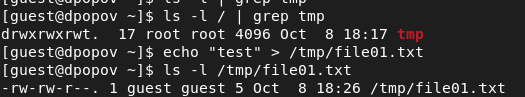


Figure 13: sticky

1. От guest2 попробовал выполнить различные операции (Рис fig. 14)

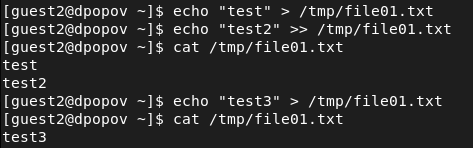


Figure 14: guest2 file01

1. Не удалось выполнить только rm
2. Снял атрибут t (Sticky-бит) сдиректории /tmp (Рис fig. 15)

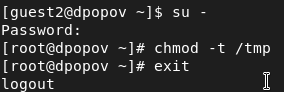


Figure 15: -t

1. Повторил предыдущие шаги. rm теперь работает (Рис fig. 16)

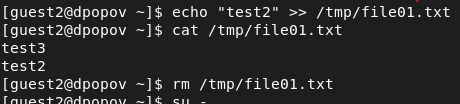


Figure 16: guest2 file01 try 2

# 3 Вывод

Выполнив данную лабораторную работу, я получение практические навыков работы в консоли с дополнительными атрибутами. Рассмотрел работы механизма смены идентификатора процессов пользователей, а также влияние бита Sticky на запись и удаление файлов.

# 4 Список литературы

1. Кулябов, Д.С. - Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов https://esystem.rudn.ru/pluginfile.php/1651889/mod\_resource/content/2/005-lab\_discret\_sticky.pdf