РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 5

дисциплина: Основы информационной безопасности

Студент: Невзоров Дмитрий

**МОСКВА**

2021г.

**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  
**Ход работы:**

1. Установим компилятор gcc (Рис. 1)

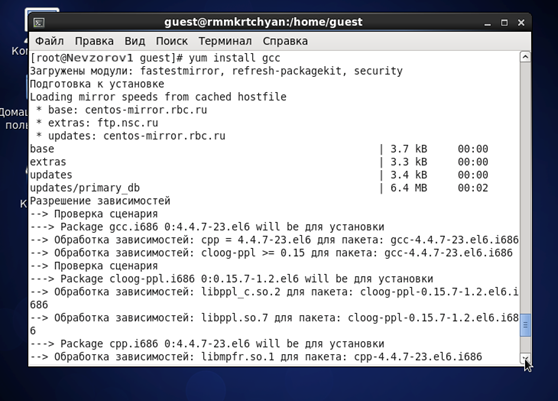


Рис. 1

1. Создадим программу simpleid.c (Рис. 2)

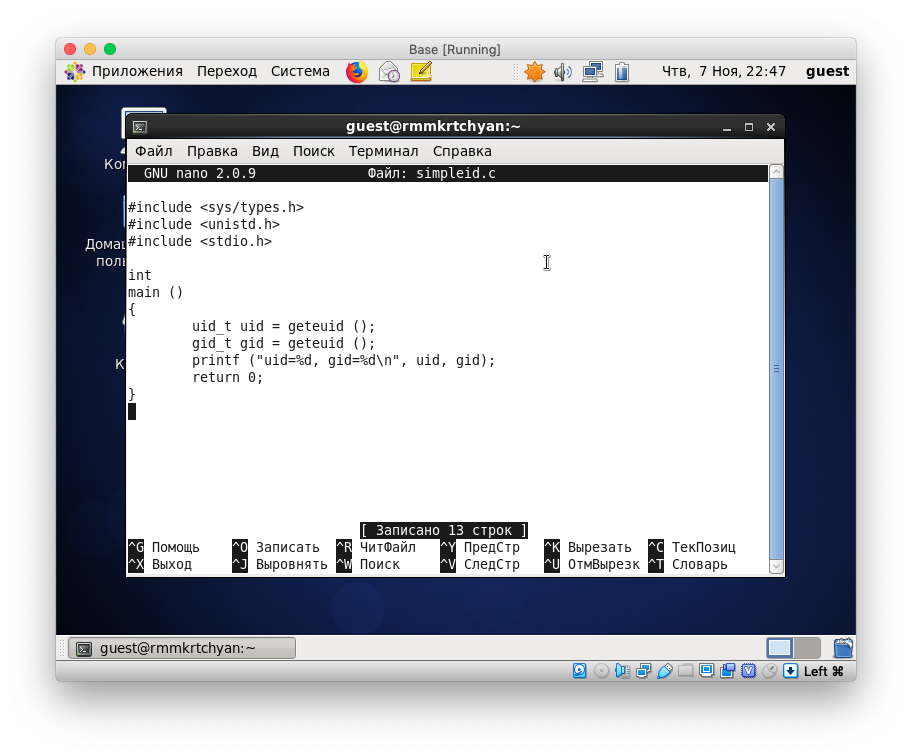


Рис. 2

1. Скомпилируем программу (Рис. 3)  
   gcc simpleid.c –o simpleid
2. Выполним програму simpleid (Рис. 3)  
   ./simpleid
3. Выполним системную программу id (Рис. 3)

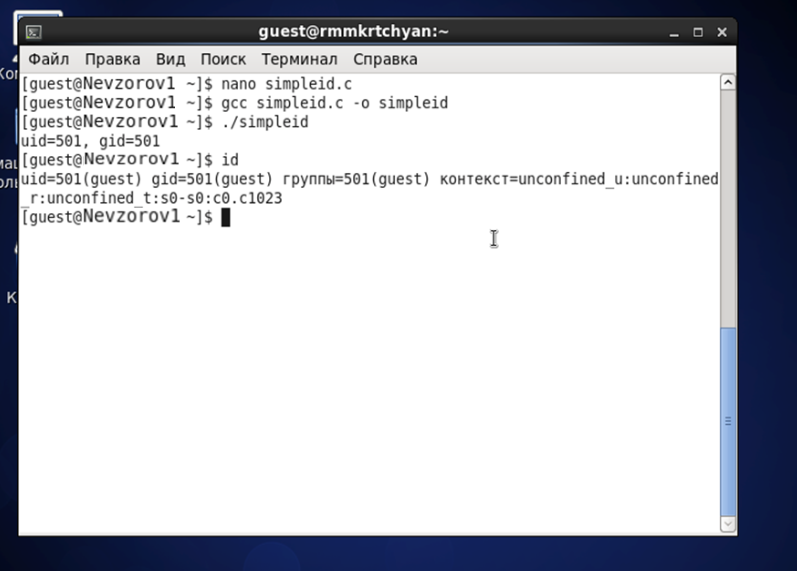


Рис. 3

Результаты совпадают

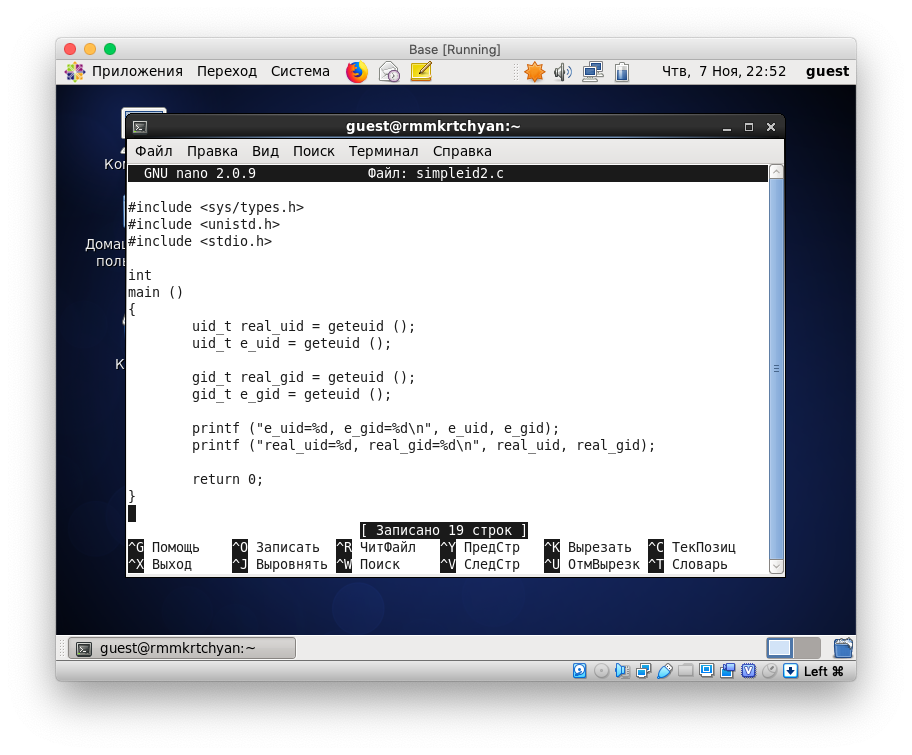
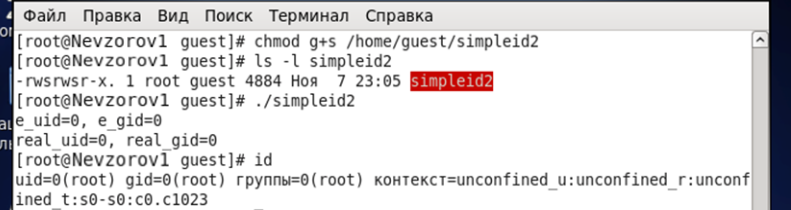
1. Усложним программу, добавив вывод действительных идентификаторов, сохранив как simpleid2.c (Рис. 4)  
   

Рис. 4

1. Скомпилируем и запустим simpleid2.c (Рис. 5)  
   gcc simpleid2.c –o simpleid  
   ./simpleid2
2. От имени суперпользователя выполним команды (Рис. 5)  
   chown root:guest /home/guest/simpleid2  
   chmod u+s /home/guest/simpleid2  
   С помощью этих команд файлу simpleid2 изменяем владельца и группу на root и guest соответственно, а также устанавливаем на файл SetUID-бит
3. Выполним проверку правильности установки новых атрибутов и смены владельца файла simpleid2 (Рис. 5)  
   ls –l simpleid2
4. Запустим simpleid2 и id (Рис. 5)  
   ./simpleid2  
   id  
   Результаты также одинаковы
5. Проделаем тоже самое относительно SetGID-бита



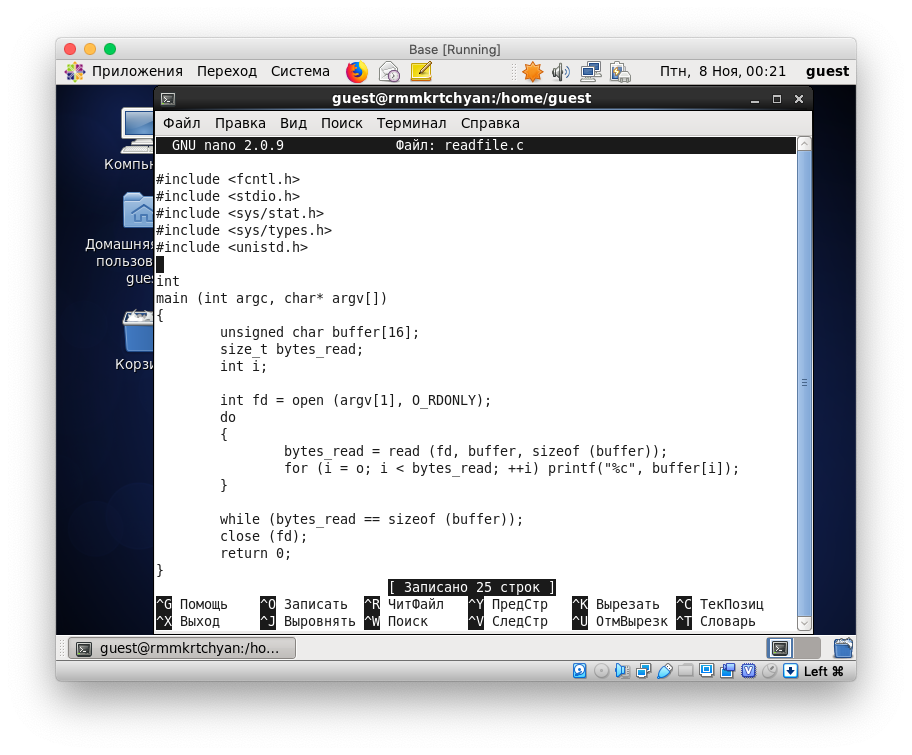
1. Создадим readfile.c (Рис. 7)  
   

Рис. 5

1. Откомпилируем ее (Рис. 8)  
   gcc readfile.c –o readfile
2. Сменим владельца у файла readfile.c и изменим права так, чтобы только root мог прочитать его (Рис. 8)
3. Проверим, что пользователь guest не может прочитать файл readfile.c (Рис. 8)
4. Сменим у программы readfile владельца и установим SetUID-бит (Рис. 8)

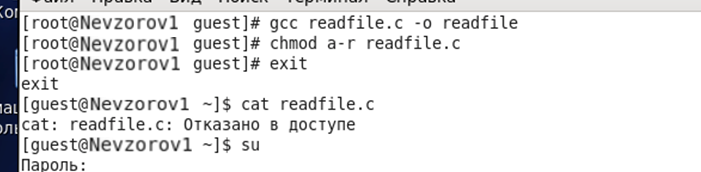


Рис. 6

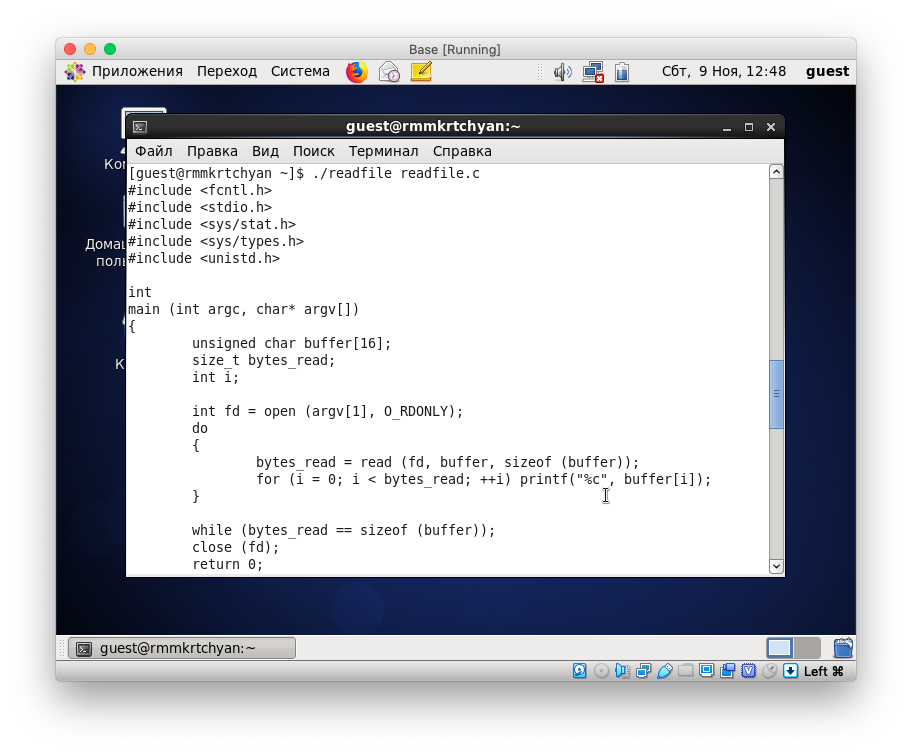
1. Проверим, может ли программа readfile прочитать файл readfile.c (Рис. 9)  
   

Рис. 7

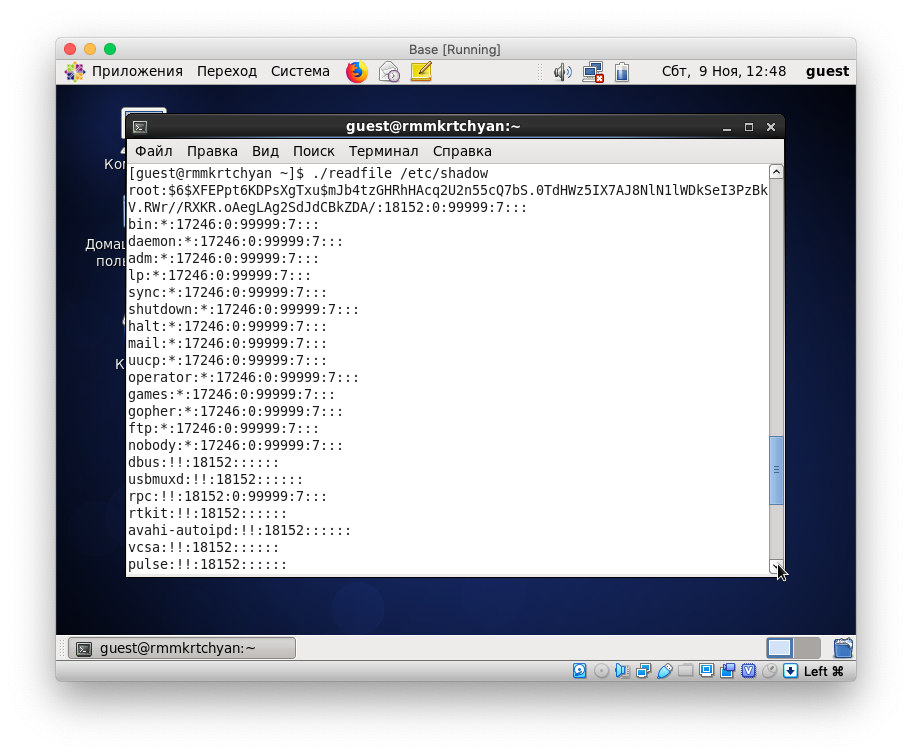
1. Проверим, может ли программа readfile прочитать файл /etc/shadow (Рис. 10)  
   

Рис. 8

1. Выясним, установлен ли атрибут Sticky на директории /tmp (Рис. 11)  
   ls –l / | grep tmp
2. От имени пользователя guest создайте файл file01.txt в директории /tmp со словом test (Рис. 11)  
   echo “test” > /tmp/file01.txt
3. Просмотрим атрибуты у только что созданного файла и разрешим чтение и запись для категории пользователей «все остальные» (Рис. 11)  
   ls –l /tmp/file01.txt  
   chmod o+rw /tmp/file01.txt  
   ls –l /tmp/file01.txt

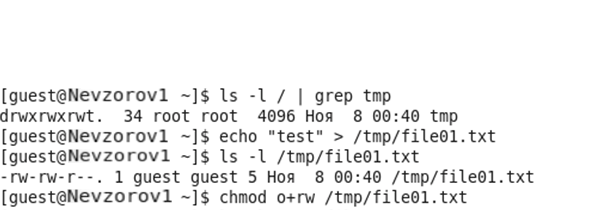


Рис. 9

1. От пользователя guest2 (не являющегося владельцем) попробуйте прочитать файл /tmp/file01.txt   
   cat /tmp/file01.txt
2. От пользователей guest2 попробуем дозаписать в файл /tmp/file01.txt слово test2   
   echo “test2” > /tmp/file01.txt  
   Дозаписать не получилось
3. Проверим содержимое файла   
   cat /tmp/file01.txt
4. От пользователей guest2 попробуем записать в файл /tmp/file01.txt слово test3, стерев всю информацию в файле   
   echo “test3” > /tmp/file01.txt  
   Перезаписать информацию получилось
5. Проверим содержимое файла   
   cat /tmp/file01.txt
6. От пользователя guest2 попробуйте удалить файл /tmp/file01.txt   
   rm /tmp/file01.txt  
   Файл не удалился
7. Повысим свои права до суперпользователя   
   su –

И выполним после этого команду снимающую атрибут Sticky-бита с директории /tmp  
chmod –t /tmp

1. Покинем режим суперпользователя   
   exit
2. От пользователя guest2 проверим, что атрибут t у директории /tmp нет   
   ls –l / | grep tmp
3. Повторим предыдущие шаги   
   Файл удалось удалить от имени пользователя, не являющегося его владельцем
4. Повысим свои права до суперпользователя и вернем атрибут t на директорию /tmp   
   su -  
   chmod +t /tmp  
   exit

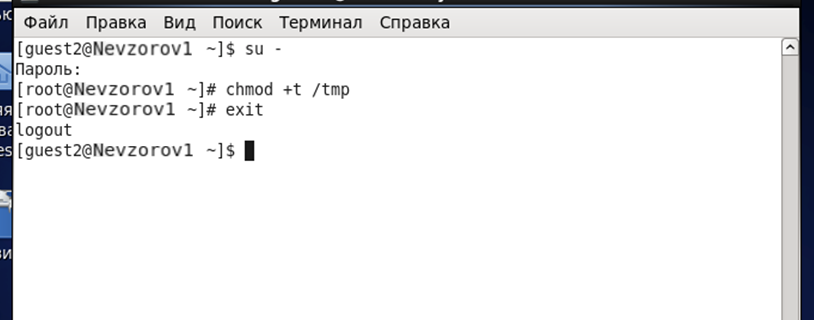


Рис. 10

**Вывод:**   
Я изучил механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, получил практические навыки работы в консоли с дополнительными атрибутами, а также рассмотрели работы механизма смены идентификатора процессов пользователей и влияние бита Sticky на запись и удаление файлов