Лабораторная работа №5.

Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов

Стариков Данила Андреевич

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 Порядок выполнения работы

## 2.1 Создание программы

1. Вошли в систему от имени пользователя guest.
2. Создали программу simpleid.c (Листинг 1):

Листинг 1: Текст программы simpleid.c

#include<sys/types.h>  
#include<unistd.h>  
#include<stdio.h>  
  
int main(){  
 uid\_t uid = geteuid();  
 gid\_t gid = getegid();  
 printf("uid=%d, gid=%d\n", uid, gid);  
 return 0;  
}

1. Скомплилировали программу и убедились, что файл программы создан:

gcc simpleid.c -o simpleid

1. Выполнили программу simpleid (Рис. 1):

./simpleid

1. Выполнили системную программу id (Рис. 1):

id

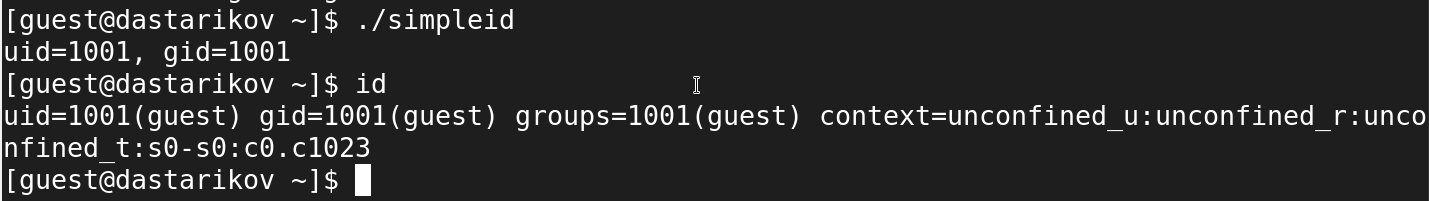


Рис. 1: Сравнение выводов программ id и simpleid.

1. Усложнили программу, добавив вывод действительных идентификаторов (Листинг 2):

Листинг 2: Текст программы simpleid2.c

#include<sys/types.h>  
#include<unistd.h>  
#include<stdio.h>  
  
int main(){  
 uid\_t real\_uid = getuid();  
 uid\_t e\_uid = geteuid();  
 gid\_t real\_gid = getgid();  
 gid\_t e\_gid = getegid() ;  
 printf("e\_uid=%d, e\_gid=%d\n", e\_uid, e\_gid);  
 printf("real\_uid=%d, real\_gid=%d\n", real\_uid, real\_gid);  
 return 0;  
}

Подробнее об отличиях geteuid, getuid, getegid и getgid можно прочитать в разделе 10.7 [1].

1. Скомпилировали и запустили simpleid2.c:

gcc simpleid2.c -o simpleid2  
./simpleid2

1. Получили права суперпользователя и выполнили команды (Рис. 2):

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

1. Выполнили проверку правильности установки новых атрибутов и смены владельца файла simpleid2 (Рис. 2):

ls -l simpleid2

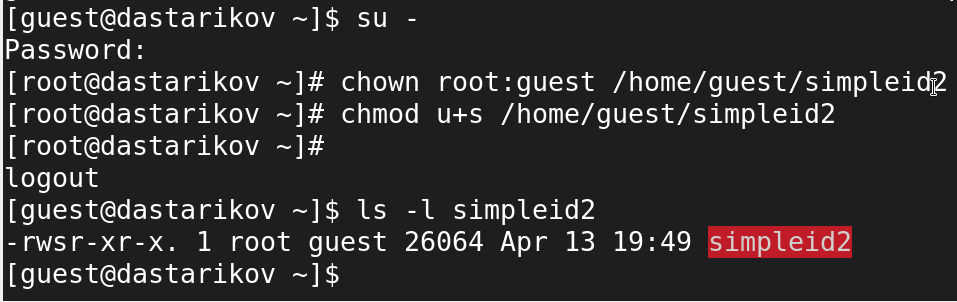


Рис. 2: Изменение владельца файла simpleid2 и добавление SUID-бита.

1. Запустили simpleid2 и id (Рис. 3):

./simpleid2  
id

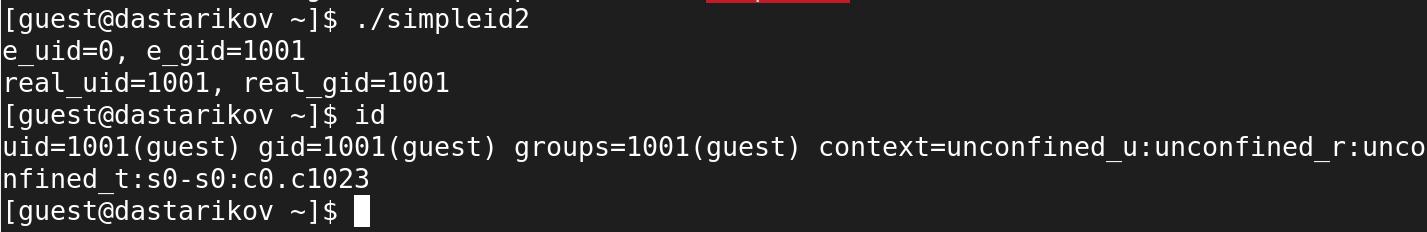


Рис. 3: Сравнение выводов программ id и simpleid2.

1. Проделайте тоже самое относительно SGID-бита (Рис. 4):

su -  
chown root:root /home/guest/simpleid2  
chmod u-s /home/guest/simpleid2  
chmod g+s /home/guest/simpleid2  
ls -l simpleid2

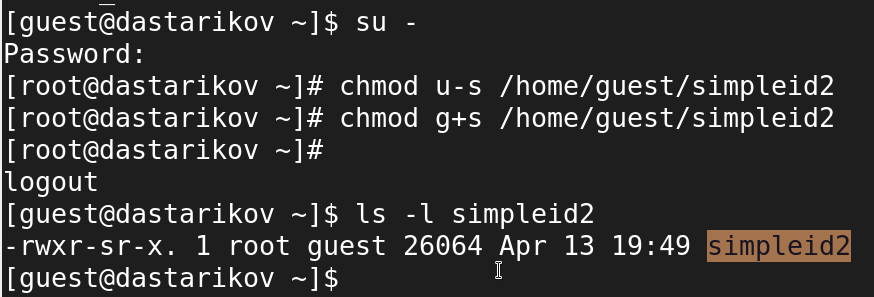


Рис. 4: Изменение группы-владельца файла simpleid2 и добавление GUID-бита.

1. Запустили simpleid2 и id (Рис. 5):

./simpleid2  
id

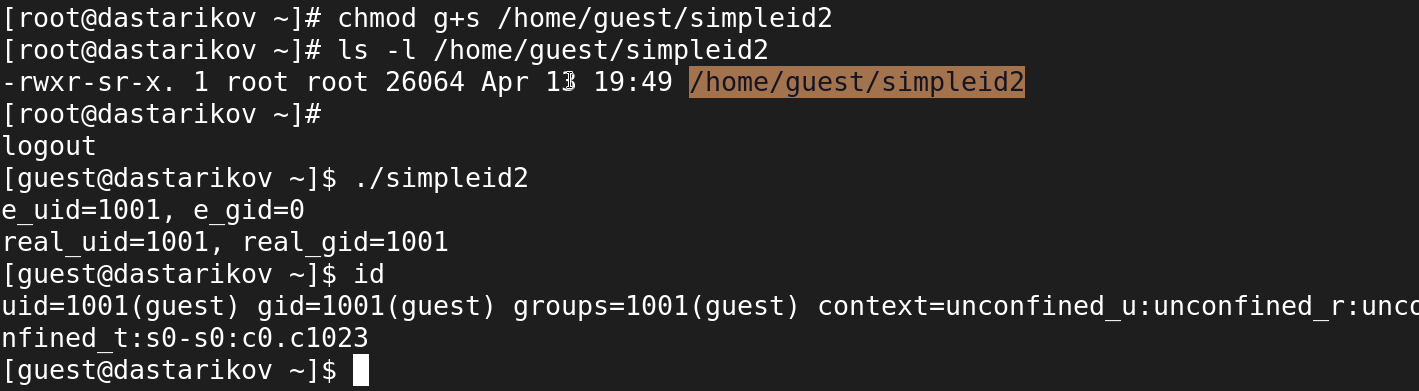


Рис. 5: Сравнение выводов программ id и simpleid2 для SGID-бита.

1. Создали программу readfile.c (Листинг 2):

Листинг 3: Текст программы readfile.c

#include<fcntl.h>  
#include<stdio.h>  
#include<sys/stat.h>  
#include<sys/types.h>  
#include<unistd.h>  
  
int main(int argc, char\* argv[]){  
 unsigned char buffer[16];  
 size\_t bytes\_read;  
 int i;  
 int fd = open(argv[1], O\_RDONLY);  
 do{  
 bytes\_read = read(fd, buffer, sizeof (buffer));  
 for (i=0;i<bytes\_read;++i) printf("%c", buffer[i]);  
 } while (bytes\_read == sizeof(buffer));  
 close(fd);  
 return 0;  
}

1. Откомпилировали её.

gcc readfile.c -o readfile

1. Сменили владельца у файла readfile.c на root и изменили права так, чтобы только суперпользователь мог прочитать его, a guest не мог (Рис. 6).
2. Проверили, что пользователь guest не может прочитать файл readfile.c (Рис. 5).

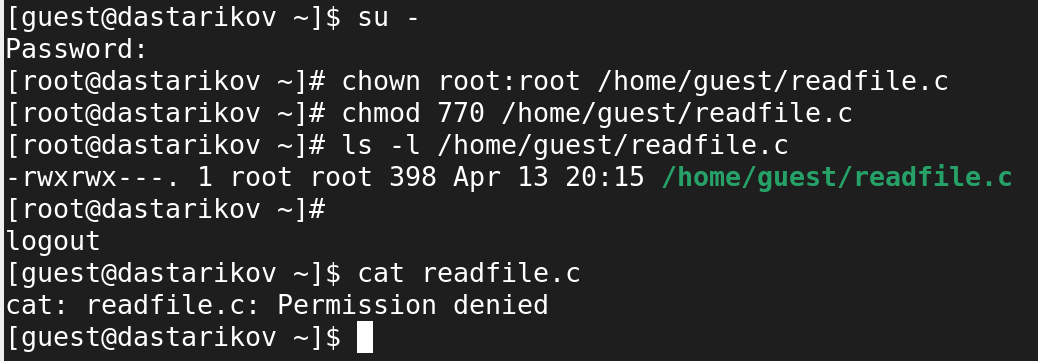


Рис. 6: Изменение прав файла readfile.c и проверка изменений.

1. Сменили у программы readfile владельца и установите SetUID-бит (Рис. 7).
2. Проверили, что программа readfile прочитать файл readfile.c (Рис. 7):

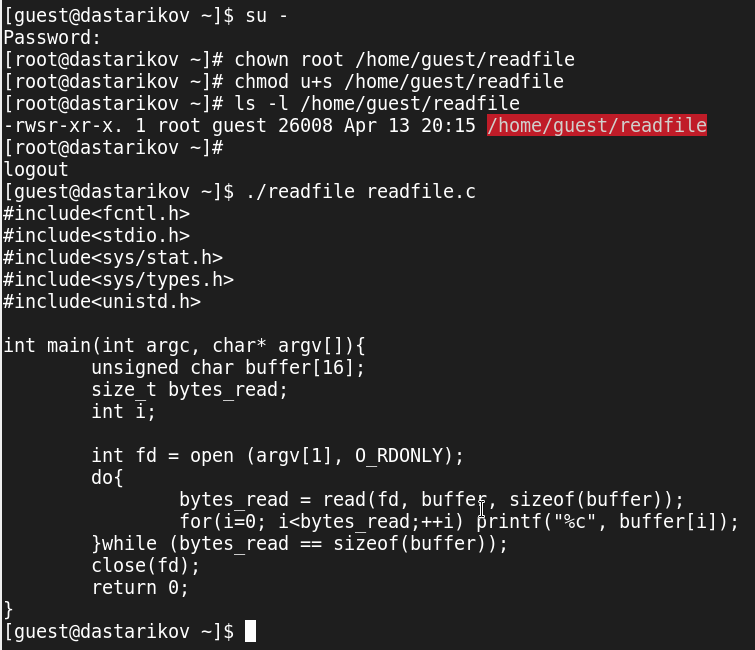


Рис. 7: Сравнение выводов программ id и simpleid2 для SGID-бита.

1. Проверили, что программа readfile прочитать файл /etc/shadow (Рис. 8)?

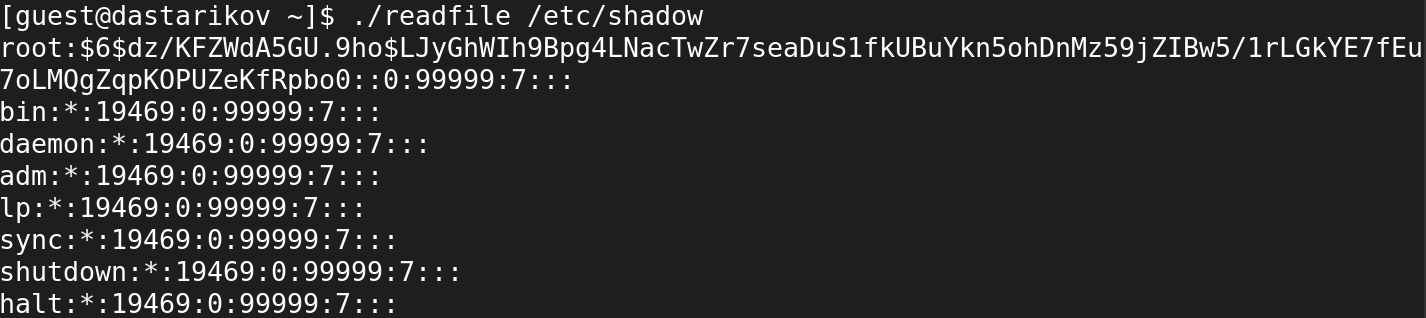


Рис. 8: Сравнение выводов программ id и simpleid2 для SGID-бита.

## 2.2 Исследование Sticky-бита

1. Выяснили, что установлен атрибут Sticky на директории /tmp (Рис. 9), выполнив команду

ls -l / | grep tmp

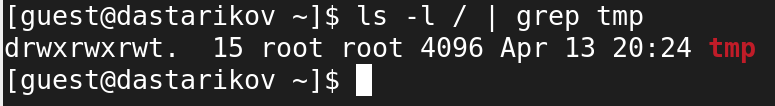


Рис. 9: Проверка атрибута Sticky на /tmp.

1. От имени пользователя guest создали файл file01.txt в директории /tmp со словом test (Рис. 10):

echo "test" > /tmp/file01.txt

1. Просмотрели атрибуты у только что созданного файла и разрешили чтение и запись для категории пользователей «все остальные» (Рис. 10):

ls -l /tmp/file01.txt  
chmod o+rw /tmp/file01.txt  
ls -l /tmp/file01.txt

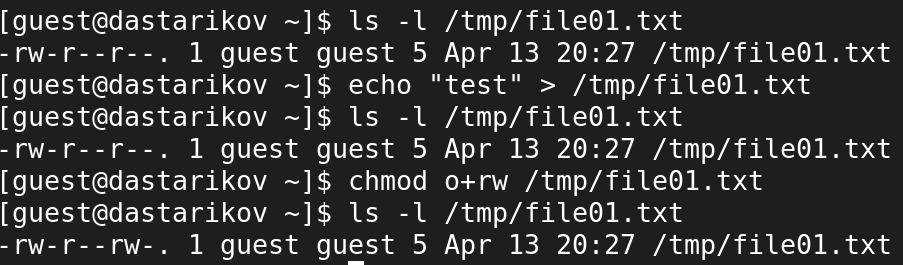


Рис. 10: Изменeние атрибутов файла file01.txt.

1. От пользователя guest2 (не являющегося владельцем) попробовали прочитать файл /tmp/file01.txt (Рис. 11):

su guest2  
cat /tmp/file01.txt

1. От пользователя guest2 попробовали дозаписать в файл /tmp/file01.txt слово test2 командой (Рис. 11)

echo "test2" >> /tmp/file01.txt

1. Проверили содержимое файла командой (Рис. 11)

cat /tmp/file01.txt

1. От пользователя guest2 попробовали записать в файл /tmp/file01.txt слово test3, стерев при этом всю имеющуюся в файле информацию командой (Рис. 11)

echo "test3" > /tmp/file01.txt

1. Проверили содержимое файла командой

cat /tmp/file01.txt

1. От пользователя guest2 попробуйте удалить файл /tmp/file01.txt командой

rm /tmp/fileOl.txt

При установленном атрибутом Sticky все вышеперечисленные операции запрещены.

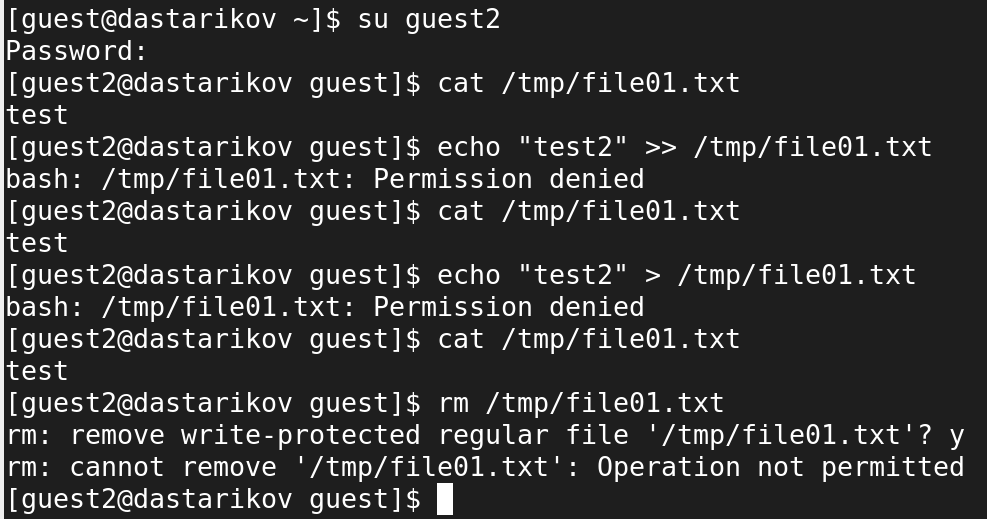


Рис. 11: Проверка прав работы с file01.txt у невладельца файла (guest2).

1. Повысили свои права до суперпользователя следующей командой

su -

и выполнили после этого команду, снимающую атрибут t (Sticky-бит) с директории /tmp (Рис. 12):

chmod -t /tmp

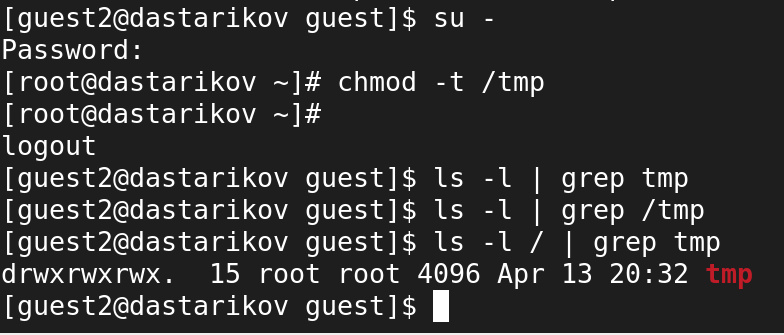


Рис. 12: Снятие Sticky-бита с /tmp.

1. Покинули режим суперпользователя комбинацией Ctrl+D.
2. От пользователя guest2 проверили, что атрибута t у директории /tmp нет (Рис. 12):

ls -l / | grep tmp

1. Повторили предыдущие шаги. После снятия Sticky-бита с файла мы также не могли записывать и перезаписывать данные файла, но смогли его удалить (Рис. 13).

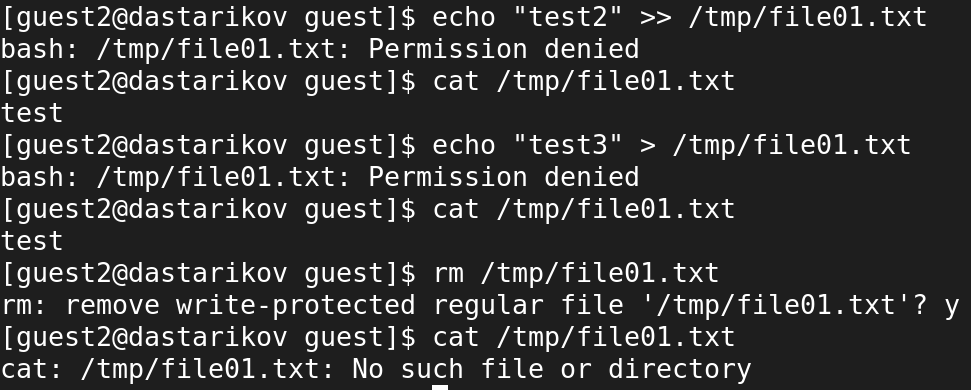


Рис. 13: Проверка прав работы с file01.txt у невладельца файла (guest2) без Sticky-бита.

1. Повысили свои права до суперпользователя и верните атрибут t на директорию /tmp:

su -  
chmod +t /tmp  
exit

# 3 Вывод

В рамках лабораторной работы изучили механизмы изменения идентификаторов, применения SetUID- и Sticky-битов, Получили практические навыкы 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

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.